DISA Review Questions, Answers Manual

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

DISCLAIMER

The views expressed in this material are those of author(s). The Institute of Chartered Accountants of India (ICAI) may not necessarily subscribe to the views expressed by the author(s).

The information in this material has been contributed by various authors based on their expertise and research. While every effort has been made to keep the information cited in this material error free, the Institute or its officers do not take the responsibility for any typographical or clerical error which may have crept in while compiling the information provided in this material. There are no warranties/claims for ready use of this material as this material is for educational purpose. The information provided in this material are subject to changes in technology, business and regulatory environment. Hence, members are advised to apply this using professional judgement. Please visit CIT portal for the latest updates. All copyrights are acknowledged. Use of specific hardware/software in the material is not an endorsement by ICAI.

Revised Edition	:	May 2018
Committee/Department	:	Digital Accounting and Assurance Board
Email	:	cit@icai.in; gdaab@icai.in
Website	:	www.icai.org/ http://pqc.icai.org
Price	:	₹
ISBN No	:	978-81-8441-810-1
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra - 282 003.

Contents

Module 1

Primer on Information Technology, IS Infrastructure & Emerging Technologies

1. The KEY components of IT Infrastructure are _____

A. Users, Applications, DBMS, System Software, Network & Hardware

B. Computing systems, satellite dishes, ISDN lines, Radio towers

C. Concrete building, air conditioning, fire extinguishers, sprinklers

D. Large servers, desktop computers, laptops, tablets

KEY A

Justification

A. All information systems will have these elements as common to them since interactions will take place between them in such systems. This is explained in para 1.2.

B. B, C and D are incorrect since they are not speaking of the common elements of any information systems but are various types of equipment alone (B), physical infrastructure alone (C) or merely various types of computing devices

2. Auditors dealing with organizations deploying IT need to have _____

A. Adequate working knowledge of IT hardware & software

B. Expertise in all areas of IT technology

C. Thorough knowledge on the financial aspects alone

D. Expertise both in financial and IT technology aspects

KEY A

Justification

A. C.A.s knowledge of IT technology need not and cannot be complete and total. They only need adequate knowledge to effectively audit the IT functions of an organization

B. C.A.s cannot be expected to be experts in all areas of IT technology; this is not their role

C. Knowledge of financial aspects alone in a technology oriented function like IT will not facilitate effective auditing of the IT function

D. A C.A. cannot be expected to have thorough knowledge of both financial & IT technology aspects

3. People, the most import element of information systems, comprise _____

A. Users of the system in the head office and branches

B. All users of the system and all information system personnel

C. All employees except information system personnel

D. Employees involved with maintenance of the information system

KEY B

Justification

A. It does not exclude the people managing the IT system

B. As brought out in paragraph 1.2.1, the scope of IT covers both the actual users as well as those involved in managing the IT system

C. It includes the information system management personnel

D. The actual users of the system are also KEY to the IT system

4. Application software is a collection of programs which _____

A. Operates computer hardware & facilitates use of system software

B. Exclusively use for generating applications to govt. bodies

C. Addresses a real life problem for its end users

D. Helps users generate complaints to IT services dept. alone

KEY C

Justification

It is system software which helps run hardware & facilitates use of application software. Options B & D are also wrong & are not generic definitions of application software. As explained in paragraph 1.2.2, application software are programmes that help address business, scientific or other needs of its end users

5. Hardware refers to_____

A. All computer parts except those which are soft, made of glass or plastic

B. Devices performing Input, output, processing & data storage functions of a computer

C. All connecting tubes, hoses, joints, cables and pipelines carrying IT cables

D. All parts of the computer which are complex and hard to understand

KEY B

Justification

A. A, C & D are clearly wrong answers which have no relation to the definition in paragraph 1.2.6

B. As defined clearly in paragraph 1.2.6

6. The basic sequential steps of the machine cycle performed by the CPU are _____

A. Fetch, Decode, Execute and Store

B. Decode, Execute, Store and Fetch

C. Store, Fetch, Decode and Execute

D. Execute, Fetch, Decode and Store

KEY A

Justification

As defined clearly in paragraph 1.3.2

B,C & D are clearly wrong answers which contain the wrong sequence

7. Cache memory _____

A. Is a large, slow memory which is no longer used in computers

B. Helps bridge speed difference between Registers and Primary Memory

C. Is a virtual memory which is an image of another memory

D. Is a memory where only valuable, secret information is stored

KEY B

Justification

Cache memory is a small & fast memory very much in use even today.

As brought out in paragraph 1.3.3

It is not a virtual memory

It maintains copies of most frequently used data from main memories and not only for secret information

8. Secondary Memory _____

A. Is volatile memory with large storage capacities

B. Is non-volatile memory which is fast & responsive

C. Is non-volatile memory with large storage capacities

D. Involves higher cost per unit of information than RAM

KEY C

Justification

Secondary memory is not volatile.

It is not fast.

As brought out in paragraph 1.3.3, secondary memory is non-volatile, with large storage capacities. It is, however, slower than registers or primary storage.

Its cost per unit of information is lower than RAM

9. One Megabyte is equal to _____

A. 1024 x 1024 Bytes

B. 1000 Kilobytes

C. 1000 Bytes

D. 1,000,000 Bytes

KEY A

Justification

1 Megabyte equals 1024 Kilobytes or 1024 x 1024 Bytes.

All the other answers are, therefore, obviously wrong.

10. Unicode _____

A. Uses 16 Bytes for character coding & has replaced other major coding systems

B. Uses 7 bits for character coding

C. Uses 16 bits for character coding & has replaced other major coding systems

D. Uses 8 bits for character coding

KEY C

Justification

A B & D answers are, obviously wrong.

C. Unicode uses 16 bits for character coding & has replaced other major coding systems as brought out in paragraph 1.4

11. Implementing Hardware Monitoring Procedures _____

A. Is expensive and not cost effective

B. Reduces Total Cost of Ownership & improves Return on Investment

C. Is cumbersome & time consuming

D. Leads to increased server downtime

KEY B

Justification

Pra 1.5.3 establishes that the other options are wrong & it makes sense to implement hardware monitoring procedures.

As brought out in paragraph 1.5.3

12. Some factors that affect the requirement & capacity of various hardware are _____

A. Number of employees in the organization

B. Variety of markets in which operations happen

C. Nature of the products dealt with in the organization

D. Transaction volume, Computation complexity

KEY D

Justification

As brought out in paragraph 1.5.4. This para also establishes that the other options are wrong.

13. A KEY issue in retirement of hardware is security & disposal of data. Robust policies need to be in place for hardware retirement cycles, archiving of data, closure of licensing and/or contracts.

A. FALSE

B. TRUE

KEY B

Justification

As brought out in paragraph 1.5.5, this statement is factually correct

14. Hardware Auditing _____

A. Is best carried out by the purchase department of the I.T. department

B. Primarily encompasses hardware acquisition & capacity management

C. Should be restricted to the financial aspects of hardware usage

D. Is not as critical as software auditing which can be a more vulnerable area

KEY B

Hardware is a vulnerable area which needs to be closely reviewed by Audit. Hence, the other three options are not correct

Paragraph1.6 elaborates on the criticality of hardware acquisition & capacity management as **KEY A**reas of Hardware auditing.

15. Software _____

A. Software consists of clearly-defined instruction sets that upon execution, tell a computer what to do

B. Refers to all the soft parts of any computer system

C. Is not as important as hardware; a system can operate even without it

D. Are only those programs which convert machine language to English

KEY A

Justification

Paragraph 2.1 incorporates this definition.

While option B is obviously incorrect, C is wrong since it would be impossible to operate any computer without software. D, too, is wrong since software plays a role much beyond that of converting machine language to English

16. System Software _____

A. Is specific to each application software and cannot be interchanged

B. Co-ordinates instructions between application software and hardware

C. Cannot be used for application development

D. Is not involved in I/O devices connectivity

KEY B

Justification

Definition as per paragraph 2.1.1. It is actually generic and can be used with any application (option A). It can actually be the basis for development of application development (option C). It enables I/O devices connectivity

17. Application Software _____

A. Microsoft Office is not an example of application software

B. Cannot be directly interacted with by end users

C. Is a set of software that performs a function directly for the end user

D. Can be directly used on a computer even without system software

KEY C

Justification

As clearly defined in 2.1.2. Microsoft Office is, indeed, an example of application software. (option A). A KEY Aspect of application software is that it can be directly interacted with by end users (option B). Lastly, a computer cannot be run without system software as brought out in earlier notes

18. An Operating System is _____

A. An intermediary agent that manages computer resources among various processes

B. An application software which is in operation in a computer network

C. A new type of software which has been introduced in the latest computers only

D. A computer system which has been switched on and is in proper operation

KEY A

Justification

The definition is as per paragraph 2.2. As for the other options, an operating system is, obviously a system software and not an application software (option B). It is not a new type of software and has been an intrinsic part of all computer systems for long (option C). Though option D may not appear to be factually incorrect, this is not the sense in which the term Operating System is used in this context.

19. State True or False : **Operating Systems can be single user / multi user, multi processing or real time**.

A. FALSE

B. TRUE

KEY B

Justification

This has been clearly elaborated in paragraph 2.2.1

20. Processor Management refers to _____

A. Management of the various processors by the Systems Executive

B. Training of the end-user for optimal user of computer systems

C. Optimisation of use of application software on a personal computer

D. Process or task scheduling carried out by the Operating System

KEY D

Justification

As brought out in paragraph 2.2.2, Processor Management is one of the KEY roles played by an Operating system. It enables process scheduling. The Operating system is part of the main computer system and one of its KEY roles is process scheduling. It has nothing to do with the management role of Systems Executives or with training of end users (options A & B). It is not relevant to application software optimisation (option C).

21. Which of the following is performed by the Operating System _____

A. Supports virtual memory by carving out an area of hard disk

B. Supports virtual memory on external storage device

C. Supports secondary memory by allocating an area of hard disk

D. Supports end user in carrying out specific functions

KEY A

Justification

The Operating System supports RAM by carving out an area of hard disk to create a virtual memory (option A). It does not do this on any external storage device (option B). The OS can only assist expansion of RAM space by carving out hard disk space, not secondary memory (option C). The OS is only an intermediary agent and does not interact directly with the end user (option D).

22. Which of the following is a role of the Operating System _____

A. Helps manage Data bases of various types

B. Facilitates use of spread sheets by end users

C. Manages device communication with respective drivers

D. Helps programmers to create computer programs

KEY C

Justification:

One of the KEY functions of the Operating system is insulating the end user from the peculiarities of each hardware device (option C). OS are not directly involved in use of Data Bases or spread sheets; nor are they useful for writing programs. One would need program development software for that purpose (options A,B & D)

23. Fifth Generation programming language _____

A. It comprises machine language & code

B. Is mainly used in Artificial intelligence

C. Cannot solve a problem without a programmer

D. It uses long instructions & is machine dependent

KEY B

Justification:

Fifth generation programming language is the most advanced of the languages & is used in artificial intelligence. It is, thus, not based upon primitive machine language and code. It is also pre-programmed with options in such a way that minimum intervention of a programmer is required. It is much simpler and platform independent as compared to first generation programming languages (options A, C & D).

24. What is the function of a Compiler ?

A. It translates Assembly language into Machine language

B. It translates statements of a program into machine code, line by line

C. A compiler translates a high level language program into a machine language program

D. It allows a user to create and edit files

KEY C

Justification

A compiler basically translates a high level program into machine code. It does not operate at the level of converting Assembly language into machine code or, like an Interpreter, translate into machine code line by line (options A and B) It is also not an Editor program to create and edit files (D).

25. Which software controls, among other things, ownership assignment of all data for accountability ?

A. Access Control Software

B. Data Communications Software

C. Utility programs

D. Defragmenters

KEY A

Justification

It is access control software which is vested with the responsibility for assigning ownership of all data for purposes of accountability (para 2.3.2). Data Communications software generally assists the OS for local and remote terminal access (option B). Utility programs and defragmenters basically help improve computer efficiency and performance and have nothing to do with ownership assignment of all data.

26. Access control lists in the OS manage OS Controls. The lowest level of control that can be exercised is, generally, up to :

A. The level of an individual directory

B. The level of a particular page in a file

C. The level of individual words in a file

D. The level of individual files

KEY D

Justification

Most systems are designed to exercise access control only up to the level of a file and not below. Hence the choice of D as the right option above and the rejection of the other options

27. State Yes or No

In a newly formed organization, the System Administrator is faced with requests for access to particular files from multiple users. On closer scrutiny, he finds that though the users are different, he is able to detect a pattern whereby individuals handling particular functions all seek access to the same files. The System Administrator is aware that, while the individuals handling these functions may change, the actual functions, by and large, are permanent. He feels that it would be simpler to provide access control for files to particular functions and would like to know the feasibility of doing so in the Operating system. What is your view ? Is it possible to provide access to 'Roles' which could comprise multiple users, instead of creating individual access controls for each of the users ? :

A. Yes, it would be possible

B. No, it would not be possible

KEY A

Justification

Access control lists are widely used with Roles comprising multiple users. The individual users can keep changing depending upon the roles they take up. Hence, Option A above is correct.

28. What is the first step in Software acquisition ?

A. Establish criteria for selecting and rejecting alternatives

B. Carry out Cost/Benefit analysis, including make or buy decision

C. Establish scope, objectives background & project charter

D. Determine supplier's technical capabilities & support services

KEY C

Justification

Without first establishing the scope and objectives, software acquisition may end up failing on fundamental aspects of meeting end user needs. This would be the starting point, therefore, for any acquisition exercise. The other options get ruled out by default.

29. What is an Endpoint device ?

A. A device used as a pointer during Power point presentations

B. The key-board or a mouse on a computer

C. A device which identifies the end of each software program

D. An internet-capable computer hardware device on a TCP/IP network

KEY D

Justification

Endpoint devices can be computers, smart phones, thin clients, etc. which have connectivity to the internet as brought out in option D. The very fact that they have this connectivity raises concerns of security with respect to possible leakage of information to the outside world or vulnerability to virus or other malicious software which may attempt to enter the system from the internet.

30. What is Digital Rights Management ?

A. Management of binary digit codes in the system software

B. Technology used for preventing users from using the content in any manner other than that permitted by the content provider

C. Conversion of analog records to digital mode

D. Optimization of binary digit codes in application software

KEY B

Justification

Digital Rights Management refers to the control on use of copyrighted / IPR material and, hence, option B is correct. The other options are wrong.

31. Does the Operating system need auditing ?

A. Yes; there is risk of the OS being compromised

B. No; the application software prevents direct access to the OS

C. No; the OS is a robust system which cannot be tampered with

D. No, it is adequate if the application software are audited

KEY A

Justification

Though, in the normal course, end-users to do not have direct access to the OS, they could find ways of by-passing the application software and reaching out to the OS. Unlike the application software which has high security features to prevent end users tampering with data which is not open to them, the OS is relatively more vulnerable since it sees all data as simple bits/bytes & cannot even distinguish between different types of data of different criticality

32. Which of the following is the correct sequence of data hierarchy?

A. File, Database, Record, Field, Characters

B. Database, Record, File, Field, Characters

C. Database, File, Record, Field, Characters

D. Database, File, Field, Character, Records

KEY C

Justification

The sequence of hierarchy from higher to lower levels is clearly as per Option C and the sequence of hierarchy for the other options are, therefore, wrong.

33. What are Characters ?

A. Characters are a group of bytes

B. Characters are a collection of bits

C. Characters are a group of 8 records

D. Characters are a group of 16 records

KEY B

Justification

Characters are at the lowest in the Data hierarchy and comprise a collection of bits (Option B). The other options are wrong.

34. What are some of the major outcomes of the non-existence of an efficient database ?

A. High redundancy and low data integrity

B. Improved data sharing

C. Reduced dependence between data and application software

D. Better linkages between data originating from different sources

KEY A

Justification

An efficient data base can reduce redundancy and improve data integrity (option A). The absence of a database will hinder data sharing & increase dependence between data and application software. An efficiently configured database will provide excellent networking of data from different sources.

35. What is a Database Management System?

A. A set of pre-loaded data relating to specific industries

B. Customer profile data used for managing an organization

C. Software for creation, control & manipulation of a database

D. Hardware specifically designed to handle databases

KEY C

Justification

A database management system is a software which assists in the process of managing a database as brought out in option C. It is not just a set of data or hardware as indicated in the other options.

36. What are the major risks of having a Database management system ?

A. Reduced speed of access to records

B. High redundancy & duplication

C. Reduced data integrity

D. Cost and data security threats

KEY D

Justification

The major risks involved are the cost (including time for implementation of a new system) and increased vulnerability owing to centralisation of information as indicated in Option D. Contrary to what is stated in the other options, a database management system improves speed of access to records, reduces redundancy and improves data integrity.

37. Which of the following is the logic typical of a Relational Database Management System ?

A. Records have a one to many relationship in parent/child format

B. Collection of one or more relations in two dimensional table form

C. Records have many-to-many relationship in network form

D. Data is organized in a tree structure, in hierarchical format

KEY B

Justification

The logic behind RDBMS is in table form with domain & entity constraints which ensure robustness of the system (Option B). The other options relate to the hierarchical and network types of database and are, hence, wrong..

38. Use of integrity constraints and normalisation is strongly typical of which type of software?

A. Relational Database Management System

B. Network Database Management System

C. Hierarchical Database Management System

D. Foxpro, Excel systems of spreadsheet

KEY A

Justification:

The use of integrity constraints and normalization is typical of RDBMS and not of the other three options.

39. Which of the following defines the logical structure of the database, its relations & constraints ?

A. Internal Schema

B. External Schema

C. Conceptual Schema

D. Logic unit in CPU

KEY C

Justification:

It is the Conceptual Schema which defines the logical structure of the database including its relations and constraints and not the other options indicated.

40. Which of the following is a database language used to define & describe data & relationships ?

A. Data Manipulation Language or DML

B. Data Control Language or DCL

C. Data Definition Language or DDL

D. Excel and Lotus 123

KEY C

Justification:

DDL is a collection of instructions and commands used to define and describe data and relationships (Option C). DML, DCL & the spread sheet softwares are not the appropriate answer.

41. Which of the following are typical features of Data Definition Language?

A. Not used by Database administrators or designers

B. SQL commands dealing with data

C. Generally used by a common user

D. Used to define both conceptual & internal schemas

KEY D

Justification:

DDL is a database language used by administrators and designers to define both conceptual & internal schemas. It does not deal with data but only with the structure. It is generally not used by the common user. Hence, only Option D is correct.

42. Which of the following are typical of Data Manipulation Language ?

A. Cannot be used for querying the database

B. Used to retrieve, insert, delete or modify data

C. SQL commands which do not allow changing of data

D. Application software will not be able to access it

KEY B

Justification:

DML is a database language used to query & manipulate data. Application software are able to meet user needs only by interacting with the DML. Hence, only Option B is correct.

43. What is a Data Dictionary ?

A. It provides a definition of terms and data elements

B. A dictionary which facilitates conversion of bytes into numbers

C. A software which helps convert machine language to English

D. A software which helps convert assembly language to English

KEY A

Justification:

It is the documentation of database providing detailed description of every data in the database. It provides a standard definition of terms and data elements (Option A). The other options are factually wrong..

44. What are Meta Data ?

A. Metadata refers to data of large sizes, millions, billions, etc.

B. Metadata is data about one or more aspects of data

C. Metadata is data relating to meteorological parameters

D. Metadata is data that is universal to different types of software

KEY B

Justification:

Metadata is data about data. It covers aspects like meaning, purpose, time & date of creation, etc. of data. Option B, obviously, is the correct choice. The other options are incorrect.

45. Centralised Deployment Strategy involves _____

A. Centralized database & de-centralized decision making

B. De-centralized database and centralized decision making

C. Centralized database & centralized decision making

D. Multiple server usage

KEY C

Justification

Centralized deployment strategy uses a central database with all user communication being directed to it. Decision making, too, therefore, gets centralized as a consequence (Option C). Such a strategy use of a single hardware/software platform & a single server; hence, the other options are not correct.

46. An important drawback of Centralised Deployment Strategy is _____

A. Vulnerability to single point of failure

B. Resource sharing of reduced order

C. Poorer economies of scale

D. Reduced security

KEY A

Justification

Centralized deployment strategy concentrates all its resources at one central point making it vulnerable to total system failure in the event of this central point being compromised in any manner (Option A). Resource sharing, in fact, is a strong plus point for centralised deployment. Similarly, this system has better economies of scale owing to use of large size hardware & larger number of software licences. Since everything is centralized, possibilities of leakages are reduced since the number of exposed points are lesser. Hence, the other options are not correct.

47. An important feature of Decentralized deployment strategy would be _____

A. Information systems would be more compatible

B. Reduced duplication of records, processes

C. Business strategy based localisation of database possible

D. Adequate centralised control through security implementation

KEY C

Justification

The single major advantage of decentralized deployment strategy is its potential for tweaking the database to suit local requirements (Option C). However, compatibility of information systems may take a hit since multiple versions could be involved depending upon the geographic or business segment-wise spread of the organization. Risk of duplication of records is higher since multiple versions at different locations may be involved. Centralized control and security management would also be to a reduced extent. Hence, the other options are not correct.

48. A KEY disadvantage of Decentralised Deployment Strategy is _____

A. Less flexibility to cope with internal/external changes

B. Potentially higher CAPEX requirement

C. Slower system development

D. Information systems could be mutually incompatible

KEY D

Justification

A major disadvantage of decentralized deployment strategy is that, with de-centralized decision making, different tailor-made information systems may be created at different locations leading to potential incompatibility (Option D). On the other hand, given their de-centralized structure, they would have greater flexibility to cope with changes and can be developed/implemented quickly. Capex requirement could also be lesser owing ability to carry out changes in phases. Hence, the other options are not correct.

49. The IT components of a Core Banking Solution Data Centre would <u>mainly</u> depend upon _____

A. Number of employees in the Bank

B. Type of services offered, risk management & control requirements

C. Annual Business volume

D. Nature of software applications used

KEY B

Justification

The complexity of services offered including the response time, risk management objectives and control goals would drive the IT components of a CBS Data Centre (Option B). The elements in the other three options would have limited impact on the configuration of the data centre.

50. A near site facility is _____

A. A data replication facility

B. Disaster recovery facility

C. Facility for storing data of secondary importance

D. Facility for storing employee data alone

KEY A

Justification

A near-site facility is normally used as a data replication facility only (Option A). It would not be a prudent choice for a disaster recovery facility since, as a proximate location, the probability of its getting exposed to the same geographical risks is very high. In the usual course, no separate facility is created for secondary data or for employee data alone. Hence, the other options are not correct.

51. Configuration Identification involves _____

A. Identification of all Information Systems components without reference to version

B. Identification of software components of Information Systems alone

C. Identification of all Information Systems components in a system

D. Identification of hardware components of Information Systems alone

KEY C

Justification

Configuration identification involves identification of all versions & updates of both software and hardware. This facilitates continuous monitoring during the life cycle of the product & becomes useful at the time of any proposed changes in the components (Option C). Option A is wrong since it ignores the version, which is vital. B and D are incorrect since they are addressing either the software or hardware alone.

52. Hardening of Systems is _____

A.Use of robust hardware to strengthen the system

B.Securely configuring systems to minimize security risks

C. Optimising configuration of hardware systems alone

D. Auditing configuration of software systems

KEY B

Justification

Hardening of systems is the process of securely configuring computer systems to eliminate as many security risks as possible (Option B). It does not refer to use of robust hardware (Option A); nor does it limit itself to hardware alone (Option C) or software alone (Option D).

53. In IT, a network refers to _____

A.Two or more devices which are able to exchange data between each other

B. Two or more computers which are able to exchange data between each other

C. Minimum of 8 computers which are able to exchange data between each other

D. Several computers separated over a minimum distance of 100 metres from each other

KEY A

Justification

In IT, a network refers to two or more of any devices which are able to exchange data between each other; it includes devices like printers, computer terminals & other devices of communication (Option A). It is not limited to computers alone (Option B). A network could operate even out of the same building & there is no minimum stipulated distance between the devices (Options C & D)

54. In IT, a node refers to _____

A. Every junction of cables in a computer network

B. Every computer in a computer network

C. Each component in a computer network

D. Every internet device in a computer network

KEY C

Justification

In IT, a node refers to each component in a computer network (Option C). It does not refer to cable junctions (Option A). It is not restricted to computers alone but covers every type of device in the network (Option B). It is not restricted to internet devices in a network (Options D).

55. The main reason for networking computers is _____

A. Reduce hardware cost

B. Reduce software cost

C. Resource sharing and communication

D. Essentially, to increase speed of computing

KEY C

Justification

The main benefit of networking computers is sharing of resources and facilitating communications (Option C). Networking does not have the objective of reducing either hardware or software costs; nor does it have the advantage of improving speed of computing (Options A, B, & D).

56. One major benefit of networking computers is _____

A. Facilitating user communication

B. Compartmentalisation of data

C. Reduced computing power

D. Reduced software costs

KEY A

Justification

A. Facilitation of user communication is a major advantage of computer networking (Option A). Networking helps sharing of data and increases availability of computing power. It may not necessarily reduce software costs; in fact, they may increase on account of multiple licences being required for several terminals. Hence, the other options are not correct.

57. Protocol, in IT, is _____

A. The basis for allotment of new computers

B. Arrangement of employee directories

C. A set of rules for Communication between systems

D. Proper behaviour while using computers

KEY C

Justification

Protocol is a set of rules that makes communication possible (Option C). It does not refer to the basis for allotment of new computers, the arrangement of employee directories or behaviour while using computers (Options A,B, & D).

58. Data transmission _____

A. Can be only through a voltage signal & not through radio or microwave

B. Is always digital in nature; one cannot transfer data in analog form

C. Ìs the physical transfer of data over a communication channel

D. Can happen only through a copper wire or optical fibre

KEY C

Justification

Data transmission is the physical transfer of data. It can be through electrical, radio, microwave or infrared signals. It can be over copper wires, optical fibres, wireless channels or through a storage medium. It can be either digital or analog. Hence, only Option C is correct and the other options are wrong.

59. Simplex communication _____

A. Always involves uni-directional transmission of data

B. Can involve uni-directional or multi-dimensional data transmission

C. Can handle two-way communication

D. facilitates return of error or control signals to the transmitter

KEY A

Justification

A. In simplex communication data always flows from one node to another it is always uni-directional. It does not involve multi-dimensional transmission of data. It also cannot handle two-way communication or allow sending back of error or control signals to the transmitter. Hence, only Option A is correct & the other options are wrong.

60. Half Duplex communication _____

A. has capability to send and receive simultaneously

B. is cheaper than the Simplex system

C. is costlier than the full Duplex system

D. has facilities to send and receive but only one operation can be performed at a time

KEY D

Justification

Half Duplex communication has the capability to both send and receive but with the restriction that only one activity can be done at a time. It is more expensive than the Simplex system but cheaper than the full Duplex system. Hence, only Option D is correct.

61. Full Duplex communication _____

A. Cannot handle two way communication

B. Is the most expensive method in terms of equipment cost

C. Cannot handle simultaneous two way communication

D. is cheaper than Simplex communication

KEY B

Justification

B. Full Duplex communication has the capability to handle simultaneous two way communication. It is like two Simplex systems put together and, hence, is expensive. Hence, only Option B is correct.

62. Asynchronous transmission _____

A. Is a communication technique where signal timing is not used for determining byte boundary

B. Does not require start and stop bits that provide byte timing

C. Is not suited for applications where messages are generated at irregular intervals

D. Is faster since it does not require insertion of start & stop bits into the bit stream

KEY A

Justification

Asynchronous transmission involves the use of start and stop bits that provide byte timing. Hence, signal timing is not important & communication can happen between devices of dissimilar speed. However, speed is slower owing to the intervening start and stop bits. Hence, only Option A is correct.

63. Synchronous transmission _____

A. Does not place the responsibility for grouping the bits on the receiver

B. Is a communication technique where start and stop bits are not used

C. Requires no synchronization between clocks of the sender & receiver

D. Is slow and can handle limited data rate

KEY B

Justification

Synchronous transmission does away with the use of start and stop bits that provide byte timing. It shifts the responsibility for grouping of the bits to the receiver. It, however, requires synchronization of the clocks between sender and receiver. It is faster than asynchronous transmission and can support high data rates. Hence, only Option B is correct.

64. What are the features of a Local Area Network (LAN) ?

A. Connectivity is established only as and when required

B. Its security is low and error rates high

C. It interconnects devices within a limited geographical area

D. Installation and maintenance is cumbersome

KEY C

Justification

LANs interconnect devices within a limited geographical area. Connectivity is ongoing and permanent. Its security is high and error rates low. Installation and maintenance are relatively easy. Hence, only Option C is correct.

65. What are the features of a Wide Area Network (LAN) ?

A. A WAN comprises interconnected switching nodes covering a wide area

B. Connectivity is established on a permanent basis

C. WANs use only private networks

D. All devices in a WAN will have the same network ID

KEY A

Justification

WANs interconnect devices over a large geographical area using both private and public networks. The connected devices, therefore, could have different network Ids. Connectivity can be on demand or permanent. Hence, only Option A is correct.

66. A KEY characteristic of a Metropolitan Area Network (MAN) is _____

A. Can provide only for data transmission

B. Feasibility to service customers in a large city-wide area

C. Can handle only voice & video transmission

D. Higher cost than service from telephone company

KEY B

Justification

MANs play a role in meeting the growing needs of an organization with lower costs and higher capacity. It can provide for both data and voice transmission. Its cost & efficiency are generally more favourable as compared to telephone company services. Hence, only Option B is correct.

67. Client Server architecture is characterized by _____

A. Computational & interface-oriented logic are married together

B. Client process does not avail services of server

C. A dedicated server that provides resources to clients

D. Client executes in the same address space as the server

KEY C

Justification

Client Server architecture is characterized by a dedicated file server that runs the network, granting other nodes or clients access to resources. The computational and interface-oriented logic are separated rather than the computers themselves. The client executes in a different address space from the server. Hence, only Option C is correct.

68. Peer-to-Peer Networking is characterized by _____

A. Sharing of resources without use of a separate server computer

B. Need for a network administrator in lieu of the server

C. Security and integrity of data is better than in client server configuration

D. Horizontal & vertical scalability of architecture feasible

KEY A

Justification

Peer-to-Peer networking involves connection of two or more computers and sharing of resourced without any separate server. All the computers share equal responsibility for processing data. No network administrator is required. Security and integrity of data is more vulnerable as compared to client server architecture. Vertical scalability of architecture is not possible since no server is involved. Hence, only Option A is correct.

69. What are the features of Middleware ?

A. They manage all activities except transporting, queuing and scheduling

B. They can operate with devices/systems on a single platform alone

C. They control communication, leaving authentication/delivery to the server

D. They are software that help clients communicate with server applications

KEY D

Justification

Middleware are programs which help clients communicate with server applications. They control communication, authentication as well as delivery. They manage transporting, queuing as well as scheduling. They have the capability to work with diverse platforms. Hence, only Option D is correct.

70. What are the features of a co-axial cable?

A. The axes of the two conductors in the co-axial cable are different

B. It comprises a core conductor enclosed by a plastic cladding, a wire mesh & plastic cladding

C. It is easy to install but has high attenuation loss

D. It is cheaper than twister pair cables but more expensive than optical fibre cable

KEY B

Justification

Co-axial cables consist of a central core conductor surrounded by a plastic cladding, an outer wire mesh and a protective outer plastic cladding. The axis of both the conductors is the same & hence the name co-axial. It is easy to install and has low attenuation loss. It is moderately expensive but cheaper than optical fibre cable. Hence, only Option B is correct.

71. What are the characteristics of a Twisted pair cable ?

A. Comprises 2 separate insulated wires in a twisted pattern that run parallel to each other

B. Comprises 4 separate insulated wires in a twisted pattern run parallel to each other

C. Comprises 2 separate insulated wires in a twisted but non parallel pattern

D. It is a form of unguided transmission media

KEY A

Justification

Twisted pair cables consist of 2 separate insulated wires in a twisted pattern run parallel to each other. It is a form of guided transmission media with reduced electro magnetic interference. Option A is the only correct option.

72. What are the characteristics of an Optical Fibre cable ?

A. It has high integrity and high attenuation over long distances

B. It has lower carrying capacity as compared to metallic conductors

C. It has an inner core which works through light based signalling

D. It consumes more power since signals degrade faster in the system

KEY C

Justification

C. An Optic fibre cable consists of an inner core made of glass/plastic/polymer/ acrylic which uses light based signalling. It has high integrity as well as low attenuation over long distances. It has higher carrying capacity & consumer lesser power since signals do not degrade as fast as in other systems. Hence, Option C is the only correct option.

73. Which of the following are un-guided transmission media ?

A. Optical Fibre Cables

B. Co-axial cables

C. Twisted pair cables

D. Radio Waves

KEY D

Justification

D. Options A B, C are all instances of guided transmission media wherein data signals are guided through a specific path. Radio waves, on the other hand, are transmitted without any cables & are un-guided. Hence, only Option D is correct.

74. In guided media transmission, signals are propagated through _____

A. Ground wave propagation

B. Various types of cables

C. Ionospheric propagation

D. Line-of-sight propagation

KEY B

Justification

Options A, C and D are all instances of unguided transmission media wherein data signals are not guided through a specific path. Propagation through cables, on the other hand, is a form of guided media transmission wherein the data signals are guided along a specific path through the cable. Hence, only Option B is correct.

75. What is a Hub ?

A. It is a hardware device that provides multiport connectivity

B. It offers intelligence in interpreting data received by it

C. It is a expensive device for transport of data between devices

D. Hubs are exclusively passive & cannot do anything with the signal

KEY A

Justification

A hub is a hardware device that contains multiple independent ports matching the cable type. It does not offer any intelligence in dealing with data received by it. However, an active hub can amplify/regenerate incoming signals before onward transmission. It is relatively inexpensive. The correct answer is in Option A.

76. What is a Switch ?

A. It does not offer intelligence in interpreting data received by it

B. It increases congestion & slows up the network

C. It is a special type of hub with additional layer of intelligence which reads the MAC address

D. It is a type of network interface card operating without a switching table

KEY C

Justification

A switch is a special type of hub with an additional layer of intelligence. It reads the MAC address of each frame received by it and, based upon the switching table, carries out onward transmission to the node to which the frame is addressed. It decreases congestion and speeds up the network. It is not a type of network interface card. The correct answer is in Option C.

77. What are Bridges ?

A. Bridges are used to extend or segment networks

B. Bridges sit within a segment & manage incoming/outgoing data

C. Bridges cannot block or forward the data

D. Bridges can forward the data to the relevant address but not block it

KEY A

Justification

bridge is used to extend or segment networks. It sits between two physical segments & manages the flow of data. It can choose to either block or forward the data. The correct answer, hence, is in Option A.

78. What is a typical feature of a Router ?

A. It is a networking device used to forward data packets along networks

B. It is always a dedicated hardware device & cannot be a computer

C. It copies the packets to all connected destinations without discrimination

D. It does not contain any database of network addresses or pathways

KEY A

Justification

A router is a dedicated networking device or computer system with more than one network interface. It is used to forward data packets along networks utilising its database of network addresses and alternate pathways. It selectively forwards data packets to the next hope in the route to the destination. The correct answer, hence, is in Option A.

79. What is a typical feature of a Gateway ?

A. It is necessary for connecting networks with identical protocols

B. It is a device that translates one data format to another

C. It translates both the data format as well as the data itself

D. It is used to forward data packets along networks

KEY B

Justification

A gateway is a device that translates one data format to another, eg Email gateways. It is useful in connecting networks with different protocols. It does not tinker with the actual data & only translates the data format.. The correct answer is Option B

80. What is typical of Bus topology ?

A. Bus topology contains a single hub connecting all nodes

B. Connects computers on a single circle of cable

C. Computers are connected on a single backbone cable

D. In this system, every node is connected to every other node

KEY C

Justification

In Bus topology, all the computers in the network are connected on a single backbone cable. All the computers in the network receive incoming messages from any other computer; however, only the intended recipient accepts and processes the message. It is not on a single hub or circle of cable and each of the nodes are not connected to each other. The correct answer is Option C.

81. What is typical of Star topology ?

A. Contains a central hub or switch to which each node is connected

B. All the computers are connected to a single backbone hub

C. Connects computers on a single circle of cable

D. In this system, every node is directly connected to every other node

KEY A

Justification

Star topology comprises a system of a central hub or switch to which each node is connected. Separate cables are drawn from each and every node to the central hub. It does not involve a single backbone hub or a single circle of cable. Every node is connected to the central hub or switch and not to each other. The correct answer, therefore, is Option A.

82. What are the features of Ring topology ?

A. All the computers are connected to a single backbone hub

B. Connects computers to a central hub or switch

C. In this system, every node is directly connected to every other node

D. It connects computers on a single ring of cable

KEY D

Justification

D. In star topology, every computer is connected to two other neighbours for communication. Messages travel uni-directionally, either clockwise or anti-clockwise. It does not involve use of a single backbone hub or a central hub/switch. The correct answer, therefore, is Option D.

83. What are the features of Mesh topology ?

A. All the computers are connected to a single backbone hub

B. Involves physical connection of every node with every other node

C. Connects computers to a central hub or switch

D. Ideally suited for systems with need for low degree of fault tolerance

KEY B

Justification

This involves physical connection of every node with every other node. It is rather complex and requires maximum number of cables. However, it is ideally suited for large telecommunication companies or an internet service provider who cannot afford to have a high degree of fault tolerance. It is not connected to a single backbone or hub/switch. The correct answer, therefore, is Option B.

84. What are the features of Circuit switching ?

A. Involves temporary connection between 2 devices for transmission duration

B. Signal transmission can commence even without end-to-end connection establishment

C. Data transfer can be only through binary data & not through analog/digital voice

D. Special training/protocol required to handle data traffic

KEY A

Justification

Circuit switching is a type of communication when temporary physical connection is established between 2 devices for the duration of the transmission session. Signal transmission can commence only after establishment of end-to-end connection. Information transfer can be through binary data as well as analog/digitabl voice. No special training/protocol is required. The correct answer, therefore, is Option A.

85. What are the features of Packet switching ?

A. Requires point-to-point connection establishment for transmission

B. It breaks up a message into smaller packets for transmission

C. Packets in each message need to travel in the same path & sequence

D. Since sequential transmission happens, destination devices need not reassemble them

KEY B

Justification

Packet switching involves the breaking up of a message into smaller packets for transmission session. Since each packet has the destination address, packets need not travel in the same path or sequence; the destination device reassembles them into proper sequence. The correct answer, therefore, is Option B.

86. What are the features of Message switching ?

A. Data is stored at switching point & sent forward whenever pathway is available

B. Data is not stored at switching points & transmitted continuously

C. Data is transmitted in packets transmitted in the same path & sequence

D. Physical path establishment is a pre-requisite to transmission

KEY A

Justification

Message switching or store-and-forward switching involves accumulation of data at switching points and onward transmission as and when pathway is available. No physical path is established in advance between the sender and the receiver. Data is not transmitted in packets. The correct answer, therefore, is Option A.

87. What is multiplexing ?

A. Permits sequential transmission of multiple signals on a single carrier

B. Facilitates transmission of signals in sequence, one at a time

C. It is the simultaneous transmission of multiple signals on a single carrier

D. Refers to simultaneous transmission of multiple signals on multiple carriers

KEY C

Justification

Multiplexing refers to simultaneous transmission of multiple signals on a single carrier (Option C). The other options are factually incorrect.

88. Frequency division multiplexing involves _____

A. Assigning non-overlapping frequency ranges to different signals/users

B. Assigning overlapping frequency ranges to different signals/users

C. Assigning non-overlapping frequency ranges to a single signal/user

D. Use of digital technology when the link bandwidth is greater than sum of signal bandwidths

KEY A

Justification

FDM assigns non-overlapping frequency ranges to different signals/users. It is an analog technique that can be applied when the bandwidth of the link is greater than the combined bandwidth of the signals to be transmitted. Hence, only Option A is correct .

89. Time Division Multiplexing involves _____

A. Primarily analog technology in which several signals/bitstreams are transferred apparently simultaneously

B. Combination of analog & digital technology in which several signal/ bitstreams are transferred simultaneously

C. Solely analog technology in which several signals/bitstreams are transferred simultaneously

D. Division of time domain into several concurrent time slots of fixed length, one for each sub-channel

KEY D

Justification

TDM involves a type of digital technology (rarely analog) in which several signals/bit streams are transferred apparently simultaneously. In actual practice, however, it uses sub channels & each signal takes turns on the channel . Hence, only Option D is correct

90. Wavelength Division Multiplexing is _____

A. Conceptually similar to Time Division Multiplexing but using various wavelengths of light

B. Conceptually similar to Frequency Division Multiplexing but uses a single wavelength of light

C. Conceptually similar to Frequency Division Multiplexing but using various wavelengths of light

D. Conceptually similar to Time Division Multiplexing and uses a single wavelength of light

KEY C

Justification

C. WDM is conceptually like FDM and which multiplexes multiple optical carrier signals on a single optical fibre by using different wavelengths of laser light. Hence, only Option C is correct

91. Connection oriented networking involves _____

A. Transmission of data prior to establishment of connection

B. Establishment of connection prior to data exchange

C. Simultaneous establishment of connection & data exchange

D. Networking arrangements based upon priority of connection nodes

KEY B

Justification

Connection oriented networking involves establishment of connection prior to data exchange. The other options are factually incorrect and, hence, only Option B is correct

92. Connection less networking involves _____

A. Data is exchanged without any prior establishment of connection

B. Transmission of data after establishment of connection

C. Simultaneous establishment of connection & data exchange

D. Exchanged data has no contact information of recipient

KEY A

Justification

Connectionless networking involves data exchange without any prior establishment of connection. The exchanged data has complete contact information of recipient. The other options are factually incorrect and, hence, only Option A is correct

93. Hardware _____

A. Includes the physical computer as well as all the software loaded on to it

B. Includes the physical computer as well as the operating system loaded on it

C. Refers to the tangible portion of a computer

D. Comprises the cables, the pipes, etc. which carry information in and out of the computer

KEY C

Justification

As defined clearly in paragraph 1.2.6. Hardware does not include the software loaded on to a computer. It also excludes the operating system, which itself is a piece of software. It is definitely not the cables, pipes, etc. Hence, A,B & D are clearly wrong answers which have no relation to the definition in paragraph 1.2.6

94. Input devices include _____

A. Printer

B. Cathode ray tube or monitor

C. KEYboard

D. Speaker

KEY C

Justification

As defined clearly in paragraph 1.3.1, a keyboard helps input information into the computer

The other devices falling under Options A B & D are all instances of output devices. . Hence, A B & D are clearly wrong answers.

95. Output devices include _____

A. Liquid Crystal Display

B. Microphone

C. KEYboard

D. Mouse

KEY A

Justification

As defined clearly in paragraph 1.3.1, a liquid crystal display is a monitor for display or output of information from the computer. Hence it is an output device

The other devices falling under Options B to D are all instances of input devices. . Hence, B,C & D are clearly wrong answers.

96. The Arithmetical & Logical unit of the CPU _____

A. Can also be Accumulators

B. Performs mathematical & logical operations

C. Can also be Address Registers

D. Controls flow of data & instructions to and from memory

KEY B

Justification As defined clearly in paragraph 1.3.2, The Arithmetic and Logical Control unit performs mathematical and logical operations.

The arithmetic & logic unit cannot be called accumulators or address registers. It also

does not control flow of data and instructions. Hence, A,C & D are clearly wrong answers.

97. Storage Registers _____

A. Can store memory addresses that tell the CPU where in memory an instruction is located

B. Can keep running totals of arithmetic values

C. Can temporarily store data coming from or being sent to system memory

D. Can help move data from one location in the computer to another

KEY C

Justification

As defined clearly in paragraph 1.3.2, Storage Registers can temporarily store data coming from or being sent to system memory.

Storage Registers do not store memory addresses; this function is carried out by address registers. Arithmetic and logical operations are handled by the Arithmetic & Logical unit of the computer and not the storage register. Lastly, only buses move data from one location of the computer to another. Hence, A, B, & D are clearly wrong answers.

98. Open Systems Interconnection (OSI)_____

A. Deals with interconnection of Open systems software

B. Is effective in dealing with Open-source software

C. Deals with communication process without truncation in managing internetwork

D. Splits communication process to small portions in managing internetwork

KEY D

Justification

Open Systems Interconnection of OSI is a model which enables integration of various technologies & provides solutions for managing the internetwork environment. It does this by splitting communication processes into small portions. It has nothing to do with Open systems or Open-source software.

Hence, only Option D is correct.

99. What is ARPANET ?

A. Network of computers in Arabia & Pakistan

B. New cloud computing network being set up by the U.S.

C. Computer network set up under auspices of U.S. dept. Of Defence in 1969

D. Network of the Association of Resource Planners

KEY C

Justification

ARPANET is a network of computers set up under the auspices of the U.S. dept. Of Defence in 1969 and a precursor to the internet. The answers in options A, B, and D are imaginary & incorrect.

Hence, only Option C is correct.

100. The suite of network protocol TCP/ IP evolved from _____

A. Conventions developed by ARPA

B. Pioneering work & norm developed by Intel

C. International conference of global IT experts

D. Norms developed by Indian IT developers

KEY A

Justification

The suite of TCP/IP protocol evolved from the conventions developed by ARPANET to specify how individual computers could communicate across a network. The answers in options B, C & D are all imaginary and incorrect.

Hence, only Option A is correct.

101. Which international body takes a lead role in developing common protocols for the World Wide Web to promote its evolution and ensure its inter-operability ?

A. The Internet Society (ISOC)

B. The Internet Architecture Board

C. World Wide Web Consortium (W3C)

D. The Internet Engineering Task Force (IETF)

KEY C

Justification

It is the W3C which handles the role indicated in the question above. The organizations mentioned in the other options handle other responsibilities connected to the internet.

Hence, only Option C is correct.

102. Which international body handles governance of generic Top Level Domain (gTLD) & other related responsibilities ?

A. The Internet Corporation for Assigned Names and Numbers (ICANN)

B. World Wide Web Consortium (W3C)

C. The Internet Society (ISOC)

D. The Internet Architecture Board (IAB)

KEY A

Justification

It is the ICANN which handles the role indicated in the question above. The organizations mentioned in the other options handle other responsibilities connected to the internet.

Hence, only Option A is correct.

103. Which international body bears the responsibility for technical activities of the Internet, including writing specifications & protocols ?

A. World Wide Web Consortium (W3C)

B. The Internet Society (ISOC)

C. The Internet Engineering Task Force (IETF)

D. The Internet Architecture Board (IAB)

KEY C

Justification

It is the IETF which handles the role indicated in the question above. The organizations mentioned in the other options handle other responsibilities connected to the internet.

Hence, only Option C is correct.

104. Networking Protocol _____

A. Is a set of rules that governs what, how and when data is communicated over a network

B. Is the set of international norms laid down for country priority in communication over a network

C. Is the set of international norms laid down for voice data communication alone

D. Is the set of international norms laid down for use of hardware in a network

KEY A

Justification

Networking protocol is the set of rules that governs what, how and when data is communicated over a network. The protocol does not prescribe any country priority for network communication. Its coverage is not exclusive to voice data alone. It does not apply to usage of hardware in a network.

Hence, only Option A is correct.

105. Syntax in Protocol represents _____

A. How data is communicated

B. When data is communicated

C. What is communicated

D. What, When & How data is communicated

KEY C

Justification

Syntax represents only What is communicated. There are other terms which represent the How and the When of data communication.

Hence, only Option C is correct.

106. Semantics in Protocol represents _____

A. What is communicated

B. When data is communicated

C. What, When & How data is communicated

D. How data is communicated

KEY D

Justification

Semantics represents only How data is communicated. There are other terms which represent the What and the When of data communication.

Hence, only Option D is correct.

107. Timing in Protocol represents _____

A. When data is transmitted but not how fast

B. The global time zones when data can be transmitted

C. When data is communicated & how fast

D. What, When & How data is communicated

KEY C

Justification

Timing in Protocol represents How data is communicated & how fast. There are other terms which represent the What and the When of data communication. Hence, only Option C is correct.

108. The Open System Interaction (OSI) reference model _____

A. Makes inter-operability across heterogeneous technology environments possible

B. Is a 5 layered model, each specifying particular network functions

C. Is a 9 layered model, each specifying particular network functions

D. Has layers which are not self-contained & hence, dependent upon other layers

KEY A

Justification

The OSI model describes how information from a software application in one computer moves through a network medium to a software application in another computer. When messages are sent across heterogeneous networks with a large variety of hardware technologies, networking devices and protocols, etc, OSI makes inter-operability across these differing environments possible. It is a 7 layered model which are quite independent and self-contained.

Hence, only Option A is correct.

109. In an OSI model, interfaces _____

A. Describe (horizontal) communication between adjacent layers

B. Describe (vertical) communication between any two layers

C. Describe (horizontal) communication between any two layers

D. Describe (vertical) communication between adjacent layers

KEY D

Justification

In an OSI model, interfaces describe (vertical) communication between adjacent layers. The answers falling in options A to C are factually incorrect.

Hence, only Option D is correct.

110. In an OSI model, protocols _____

A. Describe (vertical) communication between adjacent layers

B. Describe (vertical) communication between any two layers

C. Describe (horizontal) communication between layers

D. Describe (horizontal & vertical) communication between adjacent layers

KEY C

Justification

In an OSI model, protocols describe (horizontal) communication between layers. The answers falling in options A, B and D are factually incorrect & only Option C is correct.

111. The sequence of layers in a typical OSI model is _____

A. Application, Presentation, Session, Transport, Network, Data link, Physical

B. Application, Presentation, Session, Transport, Network, Data link, Application

C. Application, Presentation, Session, Transport, Network, Presentation, Application

D. Physical, Application, Presentation, Session, Transport, Network, Application, Physical

KEY A

Justification

In an OSI model, the sequence of layers is as in Option A. The answers falling in options B to D are factually incorrect & only Option A is correct.

112. TCP/IP protocol suite is a bundle of protocols that area segmented into _____

A. Five layers

B. Seven layers

C. Nine layers

D. Six layers

KEY A

Justification

TCP/IP protocol is segmented into Five layers & only Option A is correct.

113. The sequence of layers in a typical TCP/IP protocol suite is _____

A. Application, Presentation, Session, Transport, Network, Data link, Application

B. Application, Presentation, Session, Transport, Network, Data Link, Physical

C. Application, Transport, Internet, Data link, Physical

D. Physical, Application, Presentation, Session, Transport, Network, Physical

KEY C

Justification

TCP/IP protocol is segmented into five layers, sequenced as shown in Option C.

The answers falling in options A B and D are factually incorrect & only Option C is correct.

114. The protocol typically used for web browsing is _____

A. Simple Mail Transfer Protocol

B. Hyper Text Transfer Protocol

C. Simple Network Management Protocol

D. Domain Name System

KEY B

Justification

The protocol used for web browsing is HTTP and not the protocols indicated in Options A, C and D.

Only Option B is correct.

115. The protocol typically used for sending messages to other computer users based on email addresses is _____

A. Hyper Text Transfer Protocol

B. Simple Network Management Protocol

C. Simple Mail Transfer Protocol

D. Domain Name System

KEY C

Justification

The protocol used for sending messages to other computers using email addresses is SMTP and not the protocols indicated in Options A B and D.

Only Option C is correct.

116. The protocol typically used for logging on to a remote server is _____

A. Terminal Network or TELNET protocol

B. Simple Mail Transfer Protocol

C. Hyper Text Transfer Protocol

D. Domain Name System

KEY A

Justification

The protocol used for logging on to a remote server is TELNET and not the protocols indicated in Options B to D.

Only Option A is correct.

117. The protocol typically used for transferring files from one computer to another is _____

A. Terminal Network or TELNET protocol

B. File Transfer Protocol

C. Simple Mail Transfer Protocol

D. Hyper Text Transfer Protocol

KEY B

Justification

The protocol used for transferring files from one computer to another is FTP and not the protocols indicated in Options A C and D..

Only Option B is correct.

118. The protocol that allows images, audio & non-ASCII formats to be included in email messages is _____

A. Post Office Protocol

B. Internet Message Access Protocol

C. Hyper Text Transfer Protocol

D. Multipurpose Internet Mail Extensions

KEY D

Justification

The protocol that allows images, audio & non-ASCII formats to be included in email messages is MIME. The other protocols indicated in Options A B and C are not appropriate.

Only Option D is correct.

119. One type of protocol used for retrieving email is _____

A. Multipurpose Internet Mail Extensions

B. Hyper Text Transfer Protocol

C. Post Office Protocol

D. Internet Message Access Protocol

KEY C

Justification

One type of protocol used for retrieving email is POP. The other protocols indicated in Options A B and D are not appropriate.

Only Option C is correct.

120. One typical characteristic of Transmission Control Protocol is _____

A. It is not responsible for recovery of packets lost during transmission

B. It is not responsible for re-assembling the message at the other end

C. It is responsible for recovery of packets lost during transmission

D. It is not responsible for re-sending anything that is lost in transit

KEY C

Justification

TCP is responsible for recovery of packets lost during transmission as mentioned in Option C. The choices in other options are factually incorrect. Only Option C is correct

121. Positive Acknowledgement with Re-transmission (PAR), the mechanism that sends data to a recipient repeatedly till it receives a Data OK signal, is an inherent part of _____

A. Transmission Control Protocol

B. Internet Message Access Protocol

C. Simple Mail Transfer Protocol

D. Terminal Network Protocol

KEY A

Justification

PAR is an inherent part of TCP and not the other protocols indicated in Options B to D.

Hence, only Option A is correct.

122. The objective of Network Layer is _____

A. To provide security by building in fail-safe protection

B. To decide which physical path the information should follow from source to destination

C. Accelerate the flow of data through encryption

D. To validate the data & ensure delivery is completed without errors

KEY B

Justification

The objective of Network Layer is to decide which physical path the information should follow from source to destination. The answers given in the other options A, C and D are not correct.

Hence, only Option B is correct.

123. What is Internet Control Message Protocol (ICMP) ?

A. A mechanism to ascertain the IP address given a physical address (MAC)

B. A method of ascertaining the physical address (MAC), given the IP address

C. A mechanism to send notification of datagram problems back to sender

D. A system by which new internet IP addresses can be created

KEY C

Justification

ICMP is a mechanism to send notification of datagram problems back to sender. It cannot help locate the IP address or physical address, given the other element. Nor can it help create new IP addresses. Hence, only Option C is correct

124. What is Address Resolution Protocol (ARP) ?

A. A method of ascertaining the physical address (MAC), given the IP address

B. A mechanism to ascertain the IP address given a physical address (MAC)

C. A mechanism to send notification of datagram problems back to sender

D. A system by which new internet IP addresses can be created

KEY A

Justification

ARP is a method of ascertaining the physical address (MAC), given the IP address. It cannot help locate the IP address given a physical address. It is also not a mechanism

to send notification of datagram problems back to sender. Nor can it help create new IP addresses.

Hence, only Option A is correct.

125. What is Reverse Address Resolution Protocol (RARP) ?

A. A mechanism to ascertain the physical address (MAC), given an IP address

B. A mechanism to send notification of datagram problems back to sender

C. A method of ascertaining the IP address, given the physical address (MAC)

D. A system by which new internet IP addresses can be created

KEY C

Justification

RARP is a method of ascertaining the IP address, given the physical address (MAC). It cannot help locate the physical address given an IP address. It is also not a mechanism to send notification of datagram problems back to sender. Nor can it help create new IP addresses.

Hence, only Option C is correct.

126. The protocol data unit for Transport layer of TCP/IP is called _____

A. A Segment

B. A Packet

C. A Frame

D. A Bit

KEY A

Justification

The protocol data unit for Transport Layer of TCP/IP is called a Segment; the others refer to names used for other layers. Hence, only Option A is correct.

127. The protocol data unit for Network Layer of TCP/IP is called _____

A. A Segment

B. A Bit

C. A Packet

D. A Frame

KEY C

Justification

The protocol data unit for Network Layer of TCP/IP is called a Packet; the others refer to names used for other layers.

Hence, only Option C is correct.

128. The protocol data unit for Data Link Layer of TCP/IP is called _____

A. A Segment

B. A Frame

C. A Packet

D. A Bit

KEY B

Justification

The protocol data unit for Data Link Layer of TCP/IP is called a Frame; the others refer to names used for other layers.

Hence, only Option B is correct.

129. The protocol data unit for Physical Layer of TCP/IP is called ?

A. A Packet

B. A Frame

C. A Bit

D. A Segment

KEY C

Justification

The protocol data unit for Physical Layer of TCP/IP is called a Bit; the others refer to names used for other layers.

Hence, only Option C is correct.

130. The Data Link Layer _____

A. Performs the task of delivery over local networks and error detection

B. Enables us to find the best way from origin to destination

C. Runs application to access other layers' services & defines protocols

D. Provides the path through which data moves among network devices

KEY A

Justification

The Data Link Layer performs the task of delivery over local networks and error detection. The other options refer to functions of other layers of TCP/IP protocol.

Hence, only Option A is correct.

131. The Application Layer _____

A. Performs the task of delivery over local networks and error detection

B. Provides the path through which data moves among network devices

C. Runs application to access other layers' services & defines protocols

D. Enables us to find the best way from origin to destination

KEY C

Justification

The Application Layer runs various applications which provide them the ability to access the services of the other layers and define the protocols that applications use to exchange data. The other options refer to functions of other layers of TCP/IP protocol.

Hence, only Option C is correct.

132. The Cyclic Redundancy Check _____

A. Is a check conducted by Application Layer

B. Is a check carried out by the Physical Layer on each stream of bits

C. Is a calculated value of the Data Link Layer for error detection

D. Is a check carried out by the Network Layer to identify the shortest route

KEY C

Justification

The Cyclic Redundancy Check is a calculated value that is place in the Data Link trailer that is added to the message frame. It helps detect errors. The information given in the other options A B and D are incorrect.

Hence, only Option C is correct.

133. One characteristic of the Physical Layer of TCP/IP is _____

A. The sender and receiver need not be synchronized at the bit level

B. It deals in zeroes and ones and voltages

C. The bits need not be encoded into electrical/optical signals for purposes of transmission

D. Its data unit is called a segment

KEY B

Justification

The Physical Layer deals in zeroes and ones and voltages. The sender and receiver need to be synchronized at the bit level. The bits themselves need to be encoded as electrical or optical signals before transmission. Its data unit is called a bit.

Hence, only Option B is correct.

134. Wi-Fi _____

A. Is a wireless networking technology that uses radio waves

B. Has typical access range of about 130 metres

C. Can handle internet connectivity but not to other networks

D. Is a networking technology that requires physical cable connections

KEY A

Justification

Wi-Fi is a wireless networking technology using radio waves that can handle both internet and other network connections. The typical range of Wi-Fi is about 32 metres. Being a wireless facility, it does not require any physical cabling for access.

Hence, only Option A is correct.

135. Bluetooth Technology _____

A. Has typical access range of about 200 metres

B. Can handle data but not voice transmission

C. Aims at unifying different platforms & devices

D. Has a major drawback, that of data security

KEY C

Justification

Bluetooth technology, a wireless technology for exchange of data over short distances, aims at unifying different platforms and devices. It has a typical range of about 50 metres. Both data as well as voice can be transmitted through it. Data security is fairly good.

Hence, only Option C is correct.

136. An IP Network _____

A. Uses Internet Protocol to send/receive messages between computers

B. Can be implemented only in internet networks

C. Can operate even in the absence of an IP address

D. Is designed to function effectively without configuration of the hosts with the TCP/IP suite

KEY A

Justification

An IP Network uses Inter Protocol to send/receive messages between two or more computers. It can be implemented over internet networks, LAN & enterprise networks. Its fundamental pre-requisites are the need for an IP address to identify the host as also configuration of the host with the TCP/IP suite.

Hence, only Option A is correct.

137. IP Addresses _____

A. Are allocated to computer servers alone on the network

B. Are allocated to client devices alone on the network

C. Are given by IP Addressing Scheme for identifying hosts

D. For the destination host alone are contained in every IP packet

KEY C

Justification

IP addresses are, indeed allocated by the IP Addressing Scheme for every host, whether client, server or network device. While transmitting messages, each IP packet contains both the source host IP address as well as the destination host IP address.

Hence, only Option C is correct.

138. IP Version 4 _____

A. Is an address which is 8-bits in length

B. Is an address which is 32-bits in length

C. Is an address which is 16-bits in length

D. Varies in address length depending upon the message

KEY B

Justification

IP Version 4 addresses are invariably of 32-bit length; the choices given in Options A C & D are incorrect.

Hence, only Option B is correct.

139. IP Version 4 is written in the form of _____

A. 32 bytes separated by dots

B. 16 bytes separated by dots

C. 4 Octets or bytes separated by dots

D. 4 bits separated by dots

KEY C

Justification

IP Version 4 is written in the form of 4 Octets or bytes separated by dots. The choices in options A B and D are erroneous.

Hence, only Option C is correct.

140. An IP Version 4 address can have a value from _____

A. to 11111111.11111111.11111111.11111111

B. to 99999999.99999999.99999999.99999999

C. to 88888888.88888888.88888888.88888888

D. to 32000000.32000000.32000000.32000000

KEY A

Justification

An IP Version 4 can have a value from 00000000.00000000.00000000.00000000 to 11111111.11111111.11111111.11111111 since each bit is binary and can take either a 0 or 1 value. All the other choices from B to D above are incorrect. Only option A is correct.

141. Each Octet in an IP Version 4 address _____

A. Could have as many as 32 values

B. Could have as many as 1 billion values

C. Could have only two values 0 or 1

D. Could have as many as 256 values

KEY D

Justification

Each Octet in an IP Version 4 address could have a value ranging from 0000 to 1111 or 0 to 255 in binary language. Thus 256 values in total are possible.

Hence, only Option D is correct.

142. A Network IP has _____

A. All zeros in the host bit

B. All ones in the network bit

C. All zeros in the network bit

D. All ones in the host bit

KEY A

Justification

A Network IP has all zeros in the host bit whereas a Broadcast IP has all ones in the host bit.

Hence, only Option A is correct.

143. A Broadcast IP has _____

A. All zeros in the network bit

B. All ones in the host bit

C. All ones in the network bit

D. All zeros in the host bit

KEY B

Justification

A Broadcast IP has all ones in the host bit whereas a Network IP has all zeros in the host bit.

Hence, only Option B is correct.

144. The objective of the IP Classful Addressing Scheme is _____

A. To Designate separate classes based upon software used

B. Designate separate classes based upon geographical location

C. Designate separate classes based upon year of allocation

D. improve efficiency in address allocation

KEY D

Justification

The purpose of the IP Classful Addressing Scheme is to improve efficiency in address allocation. It has nothing to do with discrimination based upon software, geographical location or timing of allocation.

Hence, only Option D is correct.

145. The Octet decimal range of Class A of the IP Classful Addressing Scheme is _____

A. 1 to 126

B. 0 to 126

C. 155 to 201

D. 224 to 239

KEY A

Justification

The Octet decimal range of Class A of the IP Classful Addressing Scheme is 1 to 126 as indicated in Option A.

The other options are neither of Class A nor of the other major classes of the addressing scheme and are, hence, wrong.

146. The Octet decimal range of Class B of the IP Classful Addressing Scheme is _____

A. 138 to 191

B. 201 to 239

C. 128 to 191

D. 205 to 255

KEY C

Justification

The Octet decimal range of Class B of the IP Classful Addressing Scheme is 128 to 191 as indicated in Option C.

The other options are neither of Class B nor of the other major classes of the addressing scheme and are, hence, wrong.

147. The Octet decimal range of Class C of the IP Classful Addressing Scheme is _____

A. 201 to 223

B. 1 to 126

C. 205 to 255

D. 192 to 223

KEY D

Justification

The Octet decimal range of Class C of the IP Classful Addressing Scheme is 192 to 223 as indicated in Option D.

The other options are neither of Class C nor of the other major classes of the addressing scheme and are, hence, wrong.

148. The Octet decimal range of Class D of the IP Classful Addressing Scheme is _____

A. 224 to 239

B. 201 to 239

C. 1 to 126

D. 205 to 255

KEY A

Justification

The Octet decimal range of Class D of the IP Classful Addressing Scheme is 224 to 239 as indicated in Option A.

The other options are neither of Class D nor of the other major classes of the addressing scheme and are, hence, wrong.

149. The Octet decimal range of Class E of the IP Classful Addressing Scheme is _____

A. 240 to 256

B. 240 to 254

C. 1 to 126

D. 205 to 255

KEY B

Justification

The Octet decimal range of Class E of the IP Classful Addressing Scheme is 240 to 254 as indicated in Option B.

The other options are neither of Class E nor of the other major classes of the addressing scheme and are, hence, wrong.

150. The Higher Order bit in the first Octet of Class A of the IP Classful Addressing Scheme is _____

A. 0000

B. 1

C. 1111

D. 0

KEY D

Justification

The higher order bit in the first Octet of Class A of the IP Classful Addressing Scheme is 0 as shown in Option D.

The other options are not true.

151. The Higher Order bit in the first Octet of Class B of the IP Classful Addressing Scheme is _____

A. 110

B. 11

C. 10

D. 1111

KEY C

Justification

The higher order bit in the first Octet of Class B of the IP Classful Addressing Scheme is 10 as shown in Option C.

The other options are not true.

152. The Higher Order bit in the first Octet of Class C of the IP Classful Addressing Scheme is _____

A. 110

B. 30

C. 111

D. 1111

KEY A

Justification

The higher order bit in the first Octet of Class C of the IP Classful Addressing Scheme is 110 as shown in Option A. The other options are not true.

153. The Higher Order bit in the first Octet of Class D of the IP Classful Addressing Scheme is _____

A. 9999

B. 111

C. 1110

D. 1111

KEY C

Justification

The higher order bit in the first Octet of Class D of the IP Classful Addressing Scheme is 1110 as shown in Option C.

The other options are not true.

154. The Higher Order bit in the first Octet of Class E of the IP Classful Addressing Scheme is _____

A. 9999

B. 1111

C. 1110

D. 1010

KEY B

Justification

The higher order bit in the first Octet of Class E of the IP Classful Addressing Scheme is 1111 as shown in Option B.

The other options are not true.

155. The Network (N)/Host (H) id of Class A of the IP Classful Addressing Scheme is _____

A. N.H.H.H

B. H.N.N.N

C. N.N.H.H.

D. H.H.N.N

KEY A

Justification

The Network (N)/Host (H) id of Class A of the IP Classful Addressing Scheme is N.H.H.H as indicated in Option A.

The other options are not true.

156. The Network (N)/Host (H) id of Class B of the IP Classful Addressing Scheme is _____

A. H.N.N.N

B. N.H.H.H.

C. H.H.N.N

D. N.N.H.H

KEY D

Justification

The Network (N)/Host (H) id of Class B of the IP Classful Addressing Scheme is N.N.H.H as indicated in Option D.

The other options are not true.

157. The Network (N)/Host (H) id of Class C of the IP Classful Addressing Scheme is _____

A. H.H.H.N

B. N.N.N.H

C. N.H.H.H.

D. H.H.N.N

KEY B

Justification

The Network (N)/Host (H) id of Class C of the IP Classful Addressing Scheme is N.N.N.H as indicated in Option B.

The other options are not true.

158. The default sub-net mask of Class A of the IP Classful Addressing Scheme is _____

A. H.H.H.N

B. N.H.H.H.

C. 255.255.0.0

D. 255.0.0.0

KEY D

Justification:

The default sub-net mask of Class A of the IP Classful Addressing Scheme is 255.0.0.0 as indicated in Option D. The other options are not true.

159. The default sub-net mask of Class B of the IP Classful Addressing Scheme is _____

A. 255.255.0.0

B. H.H.H.N

C. N.H.H.H.

D. 255.255.255.0

KEY A

Justification

The default sub-net mask of Class B of the IP Classful Addressing Scheme is 255.255.0.0 as indicated in Option A.

The other options are not true.

160. The default sub-net mask of Class C of the IP Classful Addressing Scheme is _____

A. 255.255.0.0

B. N.H.H.H.

C. 255.255.255.0

D. 256.256.256.0

KEY C

Justification

The default sub-net mask of Class C of the IP Classful Addressing Scheme is 255.255.255.0 as indicated in Option C

The other options are not true.

161. The number of networks that can be accommodated in Class A of the IP Classful Addressing Scheme is _____

A. 255

B. 1 million

C. 365

D. 126

KEY D

Justification

The number of networks that can be accommodated in Class A of the IP Classful Addressing Scheme is 126 as indicated in Option D. The figures given in the other options are not true.

162. The number of networks that can be accommodated in Class B of the IP Classful Addressing Scheme is _____

A. 16,382

B. 126

C. 1 million

D. 255

KEY A

Justification

The number of networks that can be accommodated in Class B of the IP Classful Addressing Scheme is 16,382 as indicated in Option A. The figures given in the other options are not true.

163. The number of networks that can be accommodated in Class C of the IP Classful Addressing Scheme is _____

A. 16382

B. 1 million

C. 20,97,150

D. 255

KEY C

Justification

The number of networks that can be accommodated in Class C of the IP Classful Addressing Scheme is 20,97,150 as indicated in Option C. The figures given in the other options are not true.

164. The number of hosts per network (usable addresses) that can be accommodated in Class A of the IP Classful Addressing Scheme is _____

A. (2^{24} -2) or 1,67,77,214

B. (2^{10}-2) or 1022

C. 126

D. 255

KEY A

Justification

The number of hosts per network that can be accommodated in Class A of the IP Classful Addressing Scheme is (2^{24}-2) or 1,67,77,214 as indicated in Option A. The figures given in the other options are not true.

165. The number of hosts per network (usable addresses) that can be accommodated in Class B of the IP Classful Addressing Scheme is _____

A. 126

B. 256

C. (2^{24} -2) or 1,67,77,214

D. (2^{16}-2) or 65,534

KEY D

Justification

The number of hosts per network that can be accommodated in Class B of the IP Classful Addressing Scheme is (2^{16}-2) or 65,534 as indicated in Option D. The figures given in the other options are not true.

166. The number of hosts per network (usable addresses) that can be accommodated in Class C of the IP Classful Addressing Scheme is _____

A. 126

B. (2^{16}-2) or 65,534

C. (2^{8}-2) or 254

D. (2^{24} -2) or 1,67,77,214

KEY C

Justification

The number of hosts per network that can be accommodated in Class C of the IP Classful Addressing Scheme is (2^{8}-2) or 254 as indicated in Option C. The figures given in the other options are not true.

167. In IP Addressing, Unicast addressing mode involves _____

A. Sending of data only to one destined host

B. Sending of data universally to all hosts on a network

C. Sending of data to all hosts on all networks

D. Configuration disabling sending of data to all except one host

KEY A

Justification

Unicast addressing mode involves sending of data only to one destined host as indicated in Option A. The information in the other options are not correct.

168. In IP Addressing, Broadcast addressing mode involves _____

A. Sending of data to a single host on a network

B. Sending of data to all hosts on all networks

C. addressing of data packet to all hosts in a network segment

D. Configuration disabling sending of data to individual hosts

KEY C

Justification

Broadcast addressing mode involves addressing of data packets to all hosts in a network segment, as indicated in Option C. The information in the other options are not correct.

169. In IP Addressing, Multicast addressing mode involves addressing of data packets _____

A. Sending of data to a single host on a network

B. to hosts at special addresses in a network segment

C. Sending of data to all hosts on all networks

D. Configuration disabling sending of data to individual hosts

KEY B

Justification

Multicast addressing mode involves addressing of data packets to hosts at special addresses in a network segment, as indicated in Option B. The information in the other options are not correct.

170. In IP Addressing scheme, which of the following class / classes are defined for universal Unicast Addressing ?

A. Classes C alone

B. Class D

C. Classes A, B & C

D. Class E

KEY C

Justification

Classes A, B and C are defined for Universal Unicast addressing as indicated in Option C. The information in the other options are not correct.

171. In IP Addressing scheme, which of the following class / classes are reserved for Multicasting ?

A. Class D

B. Classes A & B alone

C. Class C

D. Class E

KEY A

Justification

Class D alone is reserved for Multicast addressing as indicated in Option A. The information in the other options are not correct.

172. In IP Addressing scheme, which of the following class / classes are reserved for Experimental purposes ?

A. Classes D

B. Class A

C. Class E

D. Classes B & C

KEY C

Justification

Class E alone is reserved for Experimental & research purposes as indicated in Option C. The information in the other options are not correct.

173. Which class/classes of networks are reserved for government agencies & huge companies ?

A. Classes D

B. Class E

C. Classes D & E

D. Class A

KEY D

Justification

Class A alone is reserved for Government agencies and huge companies as indicated in Option D. The information in the other options are not correct.

174. A characteristic of a private address in an IP Network is ?

A. Hosts within the same local network can use the same private address

B. Its IP address will be unique in the internet network as a whole

C. A user in Company A cannot have the same address as a user in Company B

D. Its IP address should not be from the three blocks created by IANA

KEY A

Justification

Multiple hosts within a specified network can use the same private address out of the three blocks spelt out by IANA. Their individual addresses need not be unique in the internet network as a whole; a user in one company can have the same IP address as another user in another company. Hence, Option A alone is correct. The information in the other options are not correct.

175. A characteristic of a public address in an IP Network is ?

A. Hosts within the same local network cannot use the same public address

B. A user in Company A can have the same public address as a user in Company B

C. Its IP address will be unique in the internet network as a whole

D. Its IP address should be from the three blocks created by IANA

KEY C

Justification

A public address is exposed to the internet network & is unique. Multiple hosts within a specified network cannot use the same public address. The public address should be one which is not out of the three blocks spelt out by IANA for use as private addresses. Hence, Option C alone is correct. The information in the other options are not correct.

176. The start address for private networks with Class A addressing is ?

A. 10.0.0.0

B. 192.168.0.0

C. 100.100.100.0

D. 172.16.0.0

KEY A

Justification

The start address for private networks with Class A addressing is 10.0.0.0 as indicated in Option A. The other options are not correct.

177. The start address for private networks with Class B addressing is ?

A. 192.168.0.0

B. 100.100.100.0

C. 172.16.0.0

D. 10.10.0.0

KEY C

Justification

The start address for private networks with Class B addressing is 172.16.0.0 as indicated in Option C. The other options are not correct.

178. The start address for private networks with Class C addressing is ?

A. 192.168.0.0

B. 100.100.100.0

C. 172.16.0.0

D. 10.10.0.0

KEY A

Justification

The start address for private networks with Class C addressing is 192.168.0.0 as indicated in Option A. The other options are not correct.

179. The finish address for private networks with Class A addressing is ?

A. 999.999.999.000

B. 10.255.255.255

C. 172.31.255.255

D. 000.000.000.000

KEY B

Justification

The finish address for private networks with Class A addressing is 10.255.255.255 as indicated in Option B. The other options are not correct.

180. The finish address for private networks with Class B addressing is ?

A. 10.255.255.255

B. 000.000.000.000

C. 999.999.999.000

D. 172.31.255.255

KEY D

Justification

The finish address for private networks with Class B addressing is 172.31.255.255 as indicated in Option D. The other options are not correct.

181. The finish address for private networks with Class C addressing is ?

A. 192.168.255.255

B. 172.31.255.255

C. 101.255.255.255

D. 999.999.999.000

KEY A

Justification

The finish address for private networks with Class C addressing is 192.168.255.255 as indicated in Option A. The other options are not correct.

182. Private IP addresses _____

A. are translated into public IP addresses through IANA process

B. cannot be translated into public IP addresses using NAT process

C. are translated into public IP addresses through NAT process

D. are translated into public IP addresses through SMTP

KEY C

Justification

Private IP addresses are translated into public IP addresses through Network Address Translation or NAT. Thus, multiple hosts with a private IP addresses are enabled to access using one or two public IP addresses as indicated by Option C above. The other options are not correct.

183. Dynamic Host Control Protocol is a software _____

A. That can de-link particular hosts from a network during congestion

B. That allows definition of a range of dynamic IP addresses

C. That allows definition of a range of static IP addresses

D. That regulates host access to a network depending upon priority

KEY B

Justification

Dynamic Host Control Protocol is a software that allows definition of a range of dynamic IP addresses for a specified period of time. Hence, Option B above is correct and the other options are incorrect.

184. What is the IP network address of a default gateway ?

A. 1.1.1.1

B. 255.255.255.255

C. 0.0.0.0

D. 255.255.255.000

KEY C

Justification

As indicated in Option C above, the IP network address for a default gateway is 0.0.0.0. The other options are incorrect.

185. Which IP address is called a Loopback address ?

A. 100.001.100.001

B. 121.0.0.121

C. 127.0.0.127

D. 127.0.0.1

KEY D

Justification

The Loopback address is 127.0.0.1 as indicated in Option D above. It is used to simplify programme testing and troubleshooting. The other options are incorrect.

186. A Loopback address _____

A. Is used to simplify programme testing and troubleshooting

B. Helps communicate with local host using local address

C. Facilitates getting acknowledgement for delivery of messages

D. Helps catalogue errors in communication for future use

KEY A

Justification

The Loopback address is used to simplify programme testing and troubleshooting. The other options are incorrect. Hence, Option A above alone is correct.

187. Which one of the following is a non-reserved address in IP networks ?

A. Broadcast address

B. Default gateway address

C. Loopback address

D. Dynamic IP addresses

KEY D

Justification

The Broadcast, Default gateway and Loopback addresses are all reserved addresses. The Dynamic IP address is not a reserved address and allows hosts to be allotted different IP addresses within a specified range. Hence, Option D above is alone correct.

188. A Subnet Mask is ?

A. Comprises 32 bits divided into 2 octets

B. Comprises 8 bits which are not divided further

C. Used for deriving network & host portions from an IP address

D. Comprises 16 bits which are divided into 2 octets

KEY C

Justification

A subnet mask comprises 32 bits divided into 4 octets. It is used for deriving network and host portions from an IP address and helps minimize waste of IP addresses. The information in Options A B and D is erroneous. Hence, Option C above alone is correct.

189. IP version 6 _____

A. Is a 64 bit addressing scheme

B. Is a 96 bit addressing scheme

C. Is a160 bit addressing scheme

D. Is a 128 bit addressing scheme

KEY D

Justification

IP version 6 is a128 bit version as against the 32 bit of the IP 4 version. The information in Options A to C is erroneous. Hence, Option D above alone is correct.

190. IP version 6 _____

A. Can accommodate as many as 2^{128} addresses

B. Can handle as many as 2^{64} addresses

C. Can handle as many as 2^{32} addresses

D. Can handle only 2^{16} addresses

KEY A

Justification

As against IP version 4,IP version 6 is a128 bit version which can thus accommodate as many as 2^{128} addresses. The information in Options B to D is erroneous. Hence, Option A above alone is correct.

191. Migration from IP version 4 to IP version 6 _____

A. Has not commenced in India yet; they are unwilling to do so

B. Is not possible until all devices are migrated globally

C. Has commenced in India under NASSCOM leadership

D. Is underway but many devices continue to be under version 4

KEY D

Justification

Migration from version 4 to version 6 is underway & India is one of the countries undergoing the transition. The process is anchored by the Telecom Regulatory Authority of India. Till complete migration takes place, it is possible to have both systems in operation with appropriate mechanisms in place. Hence, Option D above alone is correct.

192. IP version 6 is in the form of _____

A. Heptadecimals

B. Decimals

C. Hexadecimals

D. Octodecimals

KEY C

Justification

As against IP version 4, IP version 6 is in Hexadecimal form. The information in Options A, B and D are erroneous. Option C above alone is correct.

193. IP version 6 addresses are separated by _____

A. Single Colons

B. Double Colons

C. Single Periods

D. Semi Colons

KEY A

Justification

As against IP version 4 which uses periods for separation, IP version 6 uses single colons. The information in Options B to D is not correct. Option A above alone is correct.

194. A Port forms a socket along with an IP address. It is composed of _____

A. 8 bits

B. 32 bits

C. 16 bits

D. 64 bits

KEY C

Justification

A port comprises 16 bits. The information in Options A, B and D is not correct. Option C above alone is correct.

195. The maximum number of ports possible per IP network address is _____

A. 2^{16}

B. 2^{32}

C. 2^{64}

D. 2^{8}

KEY A

Justification

A port comprises 16 bits & hence the maximum number of ports possible is 2^{16}. The information in Options B to D is not correct. Option A above alone is correct.

196. Destination ports _____

A. Are used to route packets from source to a destination host computer

B. Are used to route packets on a server to the appropriate network application

C. Are used only for HTTP traffic which are processed by a web server

D. Of numbers 0 to 1023 are used by vendors for proprietary applications

KEY B

Justification

Destination ports are used to route packets on a server to the appropriate network application, as indicated in Option B. It is used for various purposes like HTTP, FTP & SMTP traffic. The numbers used by vendors of proprietary applications are from 1024 to 49151. Hence, Option B above alone is correct.

197. Source ports _____

A. Are assigned to clients & used for tracking user sessions

B. Are the ports through which data packets originate from the source

C. Are allocated numbers ranging from 49,152 to 68,568

D. Are allocated numbers ranging from 0 to 49,152

KEY A

Justification

Source ports are assigned to clients and used for tracking user sessions as indicated in Option A. These can be any random number and no specific range is defined. Hence, Option A above alone is correct.

198. Domain Name System _____

A. Has the host name in binary & heptadecimal form

B. When it is in non-generic category, can be used by any person/organization

C. Envisages that both the host name & IP address are a must for communication

D. Is a distributed database with host name & IP address for all domains

KEY D

Justification

The Domain Name system is a distributed database with host name & IP address for all domains, as indicated in Option D. It has the host name in normal English and the IP address as per decimal format (IP Version 4) of hexadecimal format (IP Version 6). Only the generic category of domain names are available for use by any organization of person for any use. It is possible for us, through the Domain Name system, to identify the IP address, given the host name and vice versa. Hence, Option D above alone is correct.

199. On Demand Computing _____

A. Is less economical for users with volatility in quality/volume of computing needs

B. Is not an issue in terms of privacy or security

C. Envisages provision of computing resources on as-needed/when-needed basis

D. Is ideally suited for users who have consistent quality & volume of computing needs

KEY C

Justification

On Demand Computing envisages provision of computing resources on as-needed/when-needed basis & is best suited to users who have uncertain volume of demand for computing services. It helps them minimise capital expenditure & hire computing resources on need basis. The concept's biggest concern is privacy and security of data. Hence, Option C alone is correct.

200. Firewall _____

A. Can be only software programme designed to secure networks

B. Protects systems/networks of systems from network-based security threats

C. Can be only hardware devices designed to secure networks

D. Needs to be installed well within the perimeter of the network

KEY B

Justification

Firewalls can be either software programmes or hardware devices designed to protect systems/networks of systems from network-based security threats. For best results they need to be installed at the entry point or perimeter of the network. Hence, only Option B is correct.

201. Role of Firewall _____

A. Burns malicious programmes entering the network

B. Allows users free access to external network but blocks entry of suspect programmes

C. Filters both in-bound and out-bound traffic from secured network

D. Blocks users from free access to external network but allows free entry from external network

KEY C

Justification

Firewalls play the dual role of filtering in-bound and out-bound traffic from a secured network. Only Option C above is correct.

202. The nature & scope of the Firewall depends upon _____

A. The security policy laid down by the secured network's organization

B. The rules laid down by TELNET protocol

C. Directives of the Internet Architecture Board (IAB)

D. Rules prescribed by the Internet Engineering Task Force (IETF)

KEY A

Justification

The nature & scope of Firewalls is determined by the security policy laid down by the secured network's organization. It will vary from organization to organization depending upon their perception of the underlying risks, the economics of security software, etc. None of the internet bodies prescribe any rules regarding the firewalls to be erected by any organization. Hence, only Option A above is correct.

203. Firewall can filter _____

A. Only incoming application software but not its data contents

B. Outgoing software but not block access to external networks

C. Incoming application software as well as its data contents

D. Only outgoing software but not its data contents

KEY C

Justification

A well designed firewall can filter both incoming software as well as its data contents for maliciousness. In respect of outgoing information, it can prevent access to undesirable or risky sites as also block sending out of sensitive data. Hence, only Option C above is correct.

204. Firewalls can be configured _____

A. Cannot be configured for maintaining logs or issuing alerts on firewall policy

B. Can be configured to maintain logs but not for issuing alerts on firewall policy

C. Can be configured to maintain logs and issue alerts on firewall policy

D. Can be configured to issue alerts but not for maintaining logs

KEY C

Justification

A well designed firewall can be configured both to maintain logs as well as issuing alerts on firewall policy violations. Hence, only Option C above is correct.

205. Firewalls authenticate access _____

A. Post establishment of connection

B. Prior to establishment of connection

C. Prior to establishment of connection &, thereafter, periodically during the session

D. Post establishment of connection &, thereafter, periodically during the session

KEY B

Justification

A robust firewall system will authenticate access prior to establishment of connection. Once authenticated, the user will no longer be prompted for authentication. Authentication post establishment of connection will not serve the purpose since security of the system could have been compromised by then. Hence, only Option B above is correct.

206. The Default Deny Access Control Policy _____

A. Envisages denial of all traffic & selectively allowing certain traffic through the firewall

B. Prescribes allowing all traffic & selectively denying certain traffic through the firewall

C. Is frequently used for granting access from a trusted network to an external systems

D. Is also called Discretionary Access Control Policy

KEY A

Justification

The Default Deny Access Control Policy envisages denial of all traffic by default and selectively allowing certain traffic alone through the firewall. It is frequently used for granting access from an un-trusted source to a protected system. It is also called Mandatory Access Control Policy. Hence, only Option A above is correct.

207. The Allow All Access Control Policy _____

A. Prescribes blocking of all traffic by default & allowing certain traffic alone selectively the firewall

B. Is frequently used for granting access from an un-trusted source to a protected system

C. Envisages allowing of all traffic & selectively denying certain traffic through the firewall

D. Is also called Mandatory Access Control Policy

KEY C

Justification

The Allow All Access Control Policy envisages allowing of all traffic by default and selectively denying certain traffic alone through the firewall. It is frequently used for granting access from a trusted network to external systems like the Internet. It is also called Discretionary Access Control Policy. Hence, only Option C above is correct.

208. Network Address Translation (NAT) _____

A. Permits a single unique IP address to represent a group of computers & is now a function of most firewalls by concealing the internal network

B. Permits multiple unique IP addresses to represent a group of computers & is now a function of most firewalls

C. Provide firewall protection to systems behind the firewall by allowing connections that originate both from systems inside of the firewall as well as outside the firewall

D. Provide firewall protection to systems behind the firewall by transparently showing the internal network

KEY A

Justification

NAT systems allow a network to use one set of network addresses internally and another unique IP address when dealing with external networks. They, thus, conceal the internal network, thus protecting it from external access. They have thus become an important element of Firewall systems. Hence, only Option A above is correct.

209. A Network Based Firewall _____

A. Is a device deployed within networks for restricting movement of selected traffic types within the networks

B. Is a device deployed on a single host within a network, thus restricting incoming/outgoing traffic for that host alone

C. Is a device deployed between networks for restricting movement of selected traffic types from one network to another

D. Is a device deployed between networks for protecting the network linkages but not the hosts on the network

KEY C

Justification

A Network based firewall, as stated in Option C above, is a device deployed between networks for restricting movement of selected traffic types from one network to another. It is not deployed on a single host within a network. Hence, only Option C above is correct.

210. A Host Based Firewall _____

A. Is a device deployed between networks for restricting movement of selected traffic types from one network to another

B. Is a device deployed within networks for restricting movement of selected traffic types within the networks

C. Is a device deployed between networks for protecting the network linkages but not the hosts on the network

D. Is a device deployed on a single host within a network, thus restricting incoming/outgoing traffic for that host alone

KEY D

Justification

A Host based firewall, as stated in Option D above, is a device deployed on a single host within a network, thus restricting incoming/outgoing traffic for that host alone. It is not deployed between networks or within an entire network for restricting movement of selected traffic types. Hence, only Option D above is correct.

211. A Personal Firewall _____

A. Controls traffic between a personal computer/workstation and the Internet/enterprise network

B. Can be used only on home computers but not in the corporate environment

C. Is typically a piece of hardware installed on a personal computer at home

D. Assumes that inbound traffic can be permitted and outbound traffic has to be inspected

KEY A

Justification

A Personal Firewall controls traffic between a personal computer or workstation on the one side and the Internet / enterprise network on the other. It is normally a piece of software and can be installed on a personal computer at home or even in a corporate environment. It assumes that outbound traffic can be freely permitted and inbound traffic has to be inspected & controlled. Hence, only Option A above is correct.

212. A Personal Firewall Appliance _____

A. Envisages protection to a single computer through a hardware device installed on it

B. Envisages protection to multiple computers & is housed on a router connected to them

C. Is typically a hardware installed on a router which provides protection to a single SOHO computer

D. Is typically built into the operating system of individual computers

KEY B

Justification

A Personal Firewall Appliance refers to housing of firewall functionality on the router connected to multiple computers, generally in a SOHO environment. This is unlike the normal personal firewall which tends to be installed in the computer's operating system. Hence, only Option B above is correct.

213. The Firewall term, Dual Homed _____

A. Means two houses. It is a firewall system which serves two computers

B. Means two houses. It is a computer that has at least 2 computers with minimum 2 network interfaces, both of which are connected to insecure sides

C. Means a house with two doors. It is a computer that has at least 2 network interfaces one connected to a secure side and the other to an unsecure side

D. Means a house with two doors. It is a computer that has at least 2 network interfaces, both of which are connected to insecure sides

KEY C

Justification

The Firewall term, Dual Homed, means a house with two doors. It refers to a computer that has at least 2 network interfaces with one connected to a secure side and the other to an unsecure side. Hence, only Option C above is correct.

214. De-Militarized Zone (DMZ) _____

A. Is the zone between computers which has firewalls on either side

B. Refers to the border between North & South Korea wherein no IT firewalls are installed

C. Houses the IT components which do not require public access

D. Houses the IT components which require public access like mail server, etc.

KEY D

Justification

A DMZ houses the IT components which require public access like mail server, etc as pointed out in Option D. The answers in the other options are incorrect.

215. Bastion Hosts _____

A. Are computer systems that have Hardened systems

B. Are Hardened systems that are not exposed to the Internet

C. Are Hardened systems having non-essential services installed on them

D. Allow free access to all hosts since they have Hardened systems anyway

KEY A

Justification

Bastion Hosts are computer systems that have Hardened systems because they are vulnerable to attack & are exposed to the internet and are also a main point of contact for internal network users. They have essential services installed on them & restrict access to specific hosts alone. Hence, answer in Option A is correct. The answers in the other options are incorrect.

216. Bastion Hosts _____

A. Cannot maintain detailed logs of all traffic

B. Are Hardened systems having non-essential services installed on them

C. Have each proxy independent of other proxies loaded on them

D. Allow free access to all hosts since they have Hardened systems anyway

KEY C

Justification

Bastion Hosts are computer systems that have Hardened systems because they are vulnerable to attack & are exposed to the internet and are also a main point of contact for internal network users. A Bastion Host has each proxy independent of other proxies loaded on it. It has essential services installed on it & restricts access to specific hosts alone. Hence, answer in Option C is correct. The answers in the other options are incorrect.

217. Packet Filtering Router Firewall _____

A. Has no default parameter and drops any traffic whose header does not match firewall rules

B. Is deployed on a router within a private network

C. Matches the header content with the firewall rules to allow or block traffic

D. Is deployed on a router within a public network

KEY C

Justification

Packet Filtering Router Firewall is deployed on a screening router between a private and a public network. It operates by matching the header content of each packet with the firewall rules. If the content matches the firewall rule & it permits, it allows it. In case the rule matches but does not permit, it blocks the traffic. If no match is found, the router goes by the default parameter. Hence, answer in Option C is correct. The answers in the other options are incorrect.

218. Packet Filtering Router Firewall _____

A. Works at the Internet layer of the TCP/IP model

B. Works at the Internet Layer of the OSI model

C. Is deployed on a router within a private network

D. Is deployed on a router within a public network

KEY A

Justification

Packet Filtering Router Firewall works at the Internet layer of the TCP/IP model or at Network layer of the OSI model. It is deployed on a screening router between a private and a public network. It operates by matching the header content of each packet with the firewall rules. If the content matches the firewall rule & it permits, it allows it. In case the rule matches but does not permit, it blocks the traffic. If no match is found, the router goes by the default parameter. Hence, answer in Option A is correct. The answers in the other options are incorrect.

219. Packet Filtering Router Firewall _____

A. Works at the Network Layer of the TCP/IP model

B. Works at the Network Layer of the OSI model

C. Has two main weaknesses speed and flexibility

D. Is one of the simplest but most expensive of firewalls

KEY B

Justification

Packet Filtering Router Firewall works at the Internet layer of the TCP/IP model or at Network layer of the OSI model. It is a very simple and relatively inexpensive firewall model. Its strength lies in its speed and flexibility. It is deployed on a screening router between a private and a public network. It operates by matching the header content of each packet with the firewall rules. If the content matches the firewall rule & it permits, it allows it. In case the rule matches but does not permit, it blocks the traffic. If no match is found, the router goes by the default parameter. Hence, answer in Option B is correct. The answers in the other options are incorrect.

220. Packet Filtering Router Firewall _____

A. Mostly does not support advanced user authentication schemes

B. Works at the Network Layer of the TCP/IP model

C. Has two main weaknesses speed and flexibility

D. Have high impact on network performance

KEY A

Justification

Packet Filtering Router Firewall works at the Internet layer of the TCP/IP model or at Network layer of the OSI model. It is a very simple and relatively inexpensive firewall model. Its strengths lies in its speed and flexibility as also low impact on network performance. One major drawback of this type of firewall is that it does not support most advanced user authentication schemes. Hence, answer in Option A is correct. The answers in the other options are incorrect.

221. Packet Filtering Route Firewalls _____

A. Have the advantage of ease of defining access criteria as also configuration

B. Has two main weaknesses speed and flexibility

C. Are ideal for high speed environments where logging & user authentication is not important

D. Have high impact on network performance

KEY C

Justification

Packet Filtering Router Firewall are ideal for high speed environments where logging and user authentication is not important. One major drawback of this type of firewall is that it does not support most advanced user authentication schemes. It works at the Internet layer of the TCP/IP model or at Network layer of the OSI model. It is a very simple and relatively inexpensive firewall model. Its strengths lies in its speed and flexibility as also low impact on network performance. Hence, answer in Option C is correct. The answers in the other options are incorrect.

222. Packet Filtering Route Firewalls _____

A. Are not vulnerable to IP Address spoofing attack

B. Are not vulnerable to Source Routing attack

C. Are not very costly & have low impact on network performance

D. Have the advantage of ease of defining access criteria as also configuration

KEY C

Justification

Packet Filtering Router Firewall works at the Internet layer of the TCP/IP model or at Network layer of the OSI model. It is a very simple and relatively inexpensive firewall model. It is vulnerable to attacks like the IP Address spoofing attack as also Source Routing Attack. Hence, answer in Option C is correct. The answers in the other options are incorrect.

223. What are Stateful Inspection Packet Filtering Firewall _____

A. They ignore current connection while allowing traffic to pass through

B. They are packet filters that incorporate added awareness of OSI model data

C. They possess packet characteristics but ignore session status

D. They are less secure than Packet Filtering Router Firewall

KEY B

Justification

Stateful Inspection Packet Filtering Firewall are packet filters (like Packet Filtering Firewalls) but incorporate added awareness of OSI model data. They keep track of current connection to ensure that only permitted traffic is allowed to pass. They keep track of both packet characteristics as well as session checks to make sure that a specific session is allowed. They are more secure because they track client ports individually rather than opening all 'high numbered ports' for external access. Hence, answer in Option B is correct. The answers in the other options are incorrect.

224. Stateful Inspection Packet Filtering Firewall _____

A. They possess packet characteristics but ignore session status

B. They are less secure than Packet Filtering Router Firewall

C. Uses a 'State Table' to validate inbound traffic

D. They ignore current connection while allowing traffic to pass through

KEY C

Justification

Stateful Inspection Packet Filtering Firewall are packet filters (like Packet Filtering Firewalls) but incorporate added awareness of OSI model data. They keep track of current connection to ensure that only permitted traffic is allowed to pass. They keep track of both packet characteristics as well as session checks to make sure that a specific session is allowed. They use a State Table to validate inbound traffic. They are more secure because they track client ports individually rather than opening all 'high numbered ports' for external access. Hence, answer in Option C is correct. The answers in the other options are incorrect.

225. Circuit Level Gateways _____

A. Used when internal users cannot be trusted to decide what external devices to access

B. Validate connections before data is exchanged

C. Filter individual packets of data which pass through them

D. They do not hide information about the network they protect

KEY B

Justification

Circuit Level Gateways validate connections before data is exchanged. They do not filter individual packets of data which pass through them; instead they merely decide which connections can be allowed. They do have the advantage of hiding information about the private network they protect. Hence, they are used when internal users can be trusted to decide what external devices to access. Hence, answer in Option B is correct. The answers in the other options are incorrect.

226. Circuit Level Gateways _____

A. Function at the Session layer of the OSI

B. Are relatively expensive in usage

C. Filter individual packets of data which pass through them

D. Scrutinize the application-level content of packets relayed through them

KEY A

Justification

Circuit Level Gateways operate at the Sessions layer of the OSI & validate connections before data is exchanged. They do not examine the application-level content / filter individual packets of data which pass through them; instead they merely decide which connections can be allowed. They do have the advantage of hiding information about the private network they protect. Hence, they are used when internal users can be trusted to decide what external devices to access. Hence, answer in Option A is correct. The answers in the other options are incorrect.

227. What is a characteristic of Application Level Gateway Firewall ?

A. It is not operated on hardened operating systems

B. Like Circuit level gateways, it ignores the content of traffic

C. It functions at the Application layer of the OSI

D. It authenticates devices and not individuals

KEY C

Justification

Application Level Gateways operate at the Applications layer of the OSI. They are similar to Circuit gateways with the exception that they are application specific & monitor content of the application. They have the advantage of authenticating individuals rather than devices. They are operated on hardened operating systems. Hence, answer in Option C is correct. The answers in the other options are incorrect.

228. Application Level Gateway Firewalls _____

A. It is not operated on hardened operating systems

B. Are implemented on hardened operating systems

C. Cannot control access based upon content or source address

D. Will result in compromising the entire network in the event of a break-in

KEY B

Justification

Application Level Gateways operate at the Applications layer of the OSI. They are similar to Circuit gateways with the exception that they are application specific & monitor content of the application. Among other things, they can control access based upon content as also source address. They have the advantage of authenticating individuals rather than devices. They are operated on hardened operating systems. Any break-in will only compromise the firewall and not the entire network. Hence, answer in Option B is correct. The answers in the other options are incorrect.

229. Application Level Gateway Firewalls _____

A. Are process intensive & can cause performance issues

B. Are not vulnerable to bugs in the running application / operating system

C. Cannot provide auditing & logging functions for future review

D. Will result in compromising the entire network in the event of a break-in

KEY A

Justification

Application Level Gateways operate at the Applications layer of the OSI. They are similar to Circuit gateways with the exception that they are application specific & monitor content of the application. Among other things, they can control access based upon content as also source address. They have the advantage of authenticating individuals rather than devices. They are operated on hardened operating systems. Any

break-in will only compromise the firewall and not the entire network. Their drawbacks include vulnerability to bugs in the running application / operating system as also performance issues arising out of process intensive nature. Hence, answer in Option A is correct. The answers in the other options are incorrect.

230. Application Level Gateway Firewalls _____

A. Are not vulnerable to bugs in the running application / operating system

B. Cannot provide auditing & logging functions for future review

C. Will not result in compromising the entire network in the event of a break-in

D. Are less secure than Packet Filters and Stateful Inspection Firewalls

KEY C

Justification

Any break-in will only compromise the firewall and not the entire network in the case of Application Level Gateway firewalls. They can provide auditing and logging functions. They are more secure than Packet Filters and Stateful Inspection Firewalls. Their drawbacks include vulnerability to bugs in the running application / operating system as also performance issues arising out of process intensive nature. Hence, answer in Option C is correct. The answers in the other options are incorrect.

231. One of the major drawbacks of Application Level Gateway Firewalls is _____

A. Compromise the entire network in the event of a break-in

B. Cannot provide auditing & logging functions for future review

C. Are less secure than Packet Filters and Stateful Inspection Firewalls

D. They are process intensive & cause performance issues

KEY D

Justification

Application level gateway firewalls are process intensive and cause performance issues. However, any break-in will only compromise the firewall and not the entire network in the case of Application Level Gateway firewalls. They can provide auditing and logging functions. They are more secure than Packet Filters and Stateful Inspection Firewalls. Hence, answer in Option D is correct. The answers in the other options are incorrect.

232. One of the major drawbacks of Application Level Gateway Firewalls is _____

A. Compromise the entire network in the event of a break-in

B. They are vulnerable to bugs in the running application & operating system

C. Cannot provide auditing & logging functions for future review

D. Are less secure than Packet Filters and Stateful Inspection Firewalls

KEY B

Justification

Application level gateway firewalls are process intensive and cause performance issues. However, any break-in will only compromise the firewall and not the entire network in the case of Application Level Gateway firewalls. They can provide auditing and logging functions. They are more secure than Packet Filters and Stateful Inspection Firewalls. Hence, answer in Option B is correct. The answers in the other options are incorrect.

233. Application Level Gateway Firewalls _____

A. Are also called proxies & are similar to circuit-level gateways but application-specific

B. Compromise the entire network in the event of a break-in

C. Cannot provide auditing & logging functions for future review

D. Are less secure than Packet Filters and Stateful Inspection Firewalls

KEY A

Justification

Application level gateway firewalls are also called proxies and are similar to circuit-level gateways. However, they are application-specific & monitor the contents of applications before allowing traffic. However, any break-in will only compromise the firewall and not the entire network in the case of Application Level Gateway firewalls. They can provide auditing and logging functions. They are more secure than Packet Filters and Stateful Inspection Firewalls. Hence, answer in Option A is correct. The answers in the other options are incorrect.

234. Single Homed Firewalls _____

A. Bypass the Packet Filtering router & allow packets directly to the proxy server

B. Have increased traffic and load on the proxy server despite the Packet Filtering router

C. Combines the Packet Filtering router with a separate, dedicated firewall

D. Screen only for applications and not content, making them more vulnerable

KEY C

Justification

Single Homed Firewalls combine the Packet Filtering router with a separate dedicated firewall called a Bastion proxy server. The system envisages traffic passing through the Packet Filtering router first before crossing the proxy server. This reduces the traffic and the load on the proxy server. They screen both for applications as well as content. Hence, answer in Option C is correct. The answers in the other options are incorrect.

235. One Single Homed Firewalls characteristic is that _____

A. They screen only for applications and not content, making them more vulnerable

B. They do not allow traffic to flow directly between the internet and other hosts on the private network

C. Have increased traffic and load on the proxy server despite the Packet Filtering router.

D. They ensure greater security than a packet filtering router or application level gateway firewall alone

KEY D

Justification

Single Homed Firewalls combine the Packet Filtering router with a separate dedicated firewall called a Bastion proxy server. The system envisages traffic passing through the Packet Filtering router first before crossing the proxy server. This reduces the traffic and the load on the proxy server. They screen both for applications as well as content. They are considered to be more secure than a packet filtering router or application level gateway firewall alone. A disadvantage is that traffic can flow directly between the internet and other hosts on the network if the packet filtering firewall is compromised. Hence, answer in Option D is correct. The answers in the other options are incorrect.

236. An advantage of a Single Homed Firewall is _____

A. It screens only for applications and not content

B. It allows traffic to flow directly between the internet and other hosts on the private network if the packet filtering router is compromised

C. An intruder has to penetrate two systems before security of internal network is compromised

D. It has increased traffic and load on the proxy server despite the Packet Filtering router

KEY C

Justification

Single Homed Firewalls combine the Packet Filtering router with a separate dedicated firewall called a Bastion proxy server. The system envisages traffic passing through the Packet Filtering router first before crossing the proxy server. This reduces the traffic and the load on the proxy server. Also, an intruder has to penetrate two systems before security of internal network is compromised. They screen both for applications as well as content. They are considered to be more secure than a packet filtering router or application level gateway firewall alone. A disadvantage is that traffic can flow directly between the internet and other hosts on the network if the packet filtering firewall is compromised. Hence, answer in Option C is correct. The answers in the other options are incorrect.

237. A Dual Homed Host Firewall is different from Single Homed Firewall in that _____

A. It has two NICs one connected to the external & the other connected to the internal network

B. It screens only for applications and not content

C. It does not allow traffic to flow directly between the internet and other hosts on the private network if the packet filtering router is compromised

D. It has increased traffic and load on the proxy server despite the Packet Filtering router

KEY A

Justification

Single Homed Firewalls combine the Packet Filtering router with a separate dedicated firewall called a Bastion proxy server. The system envisages traffic passing through the Packet Filtering router first before crossing the proxy server. This reduces the traffic and the load on the proxy server. It has two NICs; one connected to the external and the other connected to the internal network. Also, an intruder has to penetrate two systems before security of internal network is compromised. They screen both for applications as well as content. They are considered to be more secure than a packet filtering router or application level gateway firewall alone. A disadvantage is that traffic can flow directly between the internet and other hosts on the network if the packet filtering firewall is compromised. Hence, answer in Option A is correct. The answers in the other options are incorrect.

238. Screened Subnet Firewalls with DMZ _____

A. Has four packet filtering routers, two each between bastion host/internet & bastion host/internal network

B. Screens only the applications but not the content, making their networks more vulnerable to attack

C. Are the best configuration for most secure environment

D. The private network is not invisible to the internet / unsecured network

KEY C

Justification

Screened Subnet firewalls are the best configuration for most secure environment. They have two packet filtering routers, one each between the bastion host & internet and between bastion host & internal network. They screen both for application as well as content. Since the outside router advertises the DMZ to the external network or Internet, the internal private network becomes invisible to it. Hence, answer in Option C is correct. The answers in the other options are incorrect.

239. Screened Subnet Firewalls with DMZ _____

A. Have two packet filtering routers, one each between bastion host/internet & bastion host/internal network

B. Are vulnerable in that Internet systems can see through the DMZ into the internal private network & initiate attacks

C. Permit internal users' risky behaviour of bypassing the proxy server on the bastion system to access the Internet directly

D. Are the least robust of firewall systems, providing limited security to internal network systems

KEY A

Justification

Screened Subnet firewalls are the best configuration for most secure environment. They have two packet filtering routers, one each between the bastion host & internet and between bastion host & internal network. They screen both for application as well as content. Since the outside router advertises the DMZ to the external network or Internet, the internal private network becomes invisible to it. Similarly, the internal user is forced to go through the proxy server on the bastion system to access the Internet, minimizing risky behaviour. Hence, answer in Option A is correct. The answers in the other options are incorrect.

240. Screened Subnet Firewalls with DMZ _____

A. Have four packet filtering routers, two each between bastion host/internet & bastion host/internal network

B. Are robust in that Internet systems cannot see through the DMZ into the internal private network & initiate attacks

C. Are the least robust of firewall systems, providing limited security to internal network systems

D. Permit internal users' risky behaviour of bypassing the proxy server on the bastion system to access the Internet directly

KEY B

Justification

Screened Subnet firewalls are the best configuration for most secure environment. They have two packet filtering routers, one each between the bastion host & internet and between bastion host & internal network. They screen both for application as well as content. Since the outside router advertises the DMZ to the external network or Internet, the internal private network becomes invisible to it. Similarly, the internal user is forced to go through the proxy server on the bastion system to access the Internet, minimizing risky behaviour. Hence, answer in Option B is correct. The answers in the other options are incorrect.

241. Screened Subnet Firewalls with DMZ _____

A. Are vulnerable in that Internet systems can see through the DMZ into the internal private network & initiate attacks

B. Ensure that internal users access the Internet via the proxy services residing on the bastion host

C. Have four packet filtering routers, two each between bastion host/internet & bastion host/internal network

D. Are the least robust of firewall systems, providing limited security to internal network systems

KEY B

Justification

Screened Subnet firewalls are the best configuration for most secure environment. They have two packet filtering routers, one each between the bastion host & internet and between bastion host & internal network. They screen both for application as well as content. Since the outside router advertises the DMZ to the external network or Internet, the internal private network becomes invisible to it. Similarly, the internal user is forced to go through the proxy server on the bastion system to access the Internet, minimizing risky behaviour. Hence, answer in Option B is correct. The answers in the other options are incorrect.

242. Screened Subnet Firewalls with DMZ _____

A. Are the least robust of firewall systems, providing limited security to internal network systems

B. Have four packet filtering routers, two each between bastion host/internet & bastion host/internal network

C. Will need a Network Address Translator (NAT) to be installed on the bastion host to eliminate the need to re-number or re-subnet the private network

D. Are vulnerable in that Internet systems can see through the DMZ into the internal private network & initiate attacks

KEY C

Justification

Screened Subnet firewalls are the best configuration for most secure environment. They have two packet filtering routers, one each between the bastion host & internet and between bastion host & internal network. They screen both for application as well as content. Since the outside router advertises the DMZ to the external network or Internet, the internal private network becomes invisible to it. Similarly, the internal user is forced to go through the proxy server on the bastion system to access the Internet, minimizing risky behaviour. Since the DMZ network is different from the private network, a NAT can be installed on the bastion host to eliminate the need to re-number or re-subnet the private network. Hence, answer in Option C is correct. The answers in the other options are incorrect.

243. In general, Firewalls _____

A. Can enforce password policy and prevent misuse of passwords

B. Are very effective against non-technical security risks such as social engineering

C. Can block internal users from accessing websites with malicious codes

D. Cannot prevent users or attackers with modems from dialling into or out of the internal network, bypassing the firewall

KEY D

Justification

Firewalls have quite a few limitations. They cannot prevent users or attackers with modems from dialling into or out of the internal network. They cannot enforce password policy or prevent misuse of passwords. They are not very effective against non-technical security risks like social engineering. They cannot, also, block internal users from accessing websites with malicious codes. Hence, answer in Option D is correct. The answers in the other options are incorrect.

244. In general, Firewalls _____

A. Cannot enforce password policy and prevent misuse of passwords

B. Can prevent users or attackers with modems from dialling into or out of the internal network, bypassing the firewall

C. Can provide complete protection against viruses

D. Can block internal users from accessing websites with malicious codes

KEY A

Justification

Firewalls have quite a few limitations. They cannot enforce password policy and prevent misuse of passwords. They cannot prevent users or attackers with modems from dialling into or out of the internal network. They cannot enforce password policy or prevent misuse of passwords. They are not very effective against non-technical security risks like social engineering. They cannot provide complete protection against viruses. They cannot, also, block internal users from accessing websites with malicious codes. Hence, answer in Option A is correct. The answers in the other options are incorrect.

245. In general, Firewalls _____

A. Can enforce password policy and prevent misuse of passwords

B. Can prevent users or attackers with modems from dialling into or out of the internal network, bypassing the firewall

C. Cannot provide complete protection against viruses

D. Can block internal users from accessing websites with malicious codes

KEY C

Justification

Firewalls have quite a few limitations. They cannot provide complete protection against viruses. They cannot enforce password policy and prevent misuse of passwords. They cannot prevent users or attackers with modems from dialling into or out of the internal network. They cannot enforce password policy or prevent misuse of passwords. They cannot, also, block internal users from accessing websites with malicious codes. Hence, answer in Option C is correct. The answers in the other options are incorrect.

246. Appliance based firewall _____

A. Is a firewall software installed on top of commercial operating systems

B. Is less secure than those deployed on top of commercial operating systems

C. Is scalable depending upon changing requirements of business

D. Refers to appliances with firewall software embedded as firmware

KEY D

Justification

Appliance based Firewalls refer to appliances with firewall software embedded as firmware. They are more secure than those deployed on top of commercial operating systems since the latter are more vulnerable. Their major drawback is the limitation on scalability. Hence, answer in Option D is correct. The answers in the other options are incorrect.

247. Appliance based firewall _____

A. Does not include appliances with firewall software embedded as firmware

B. Is more secure than those deployed on top of commercial operating systems

C. Is a firewall software installed on top of commercial operating systems

D. Are scalable depending upon changing requirements of business

KEY B

Justification

Appliance based Firewalls refer to appliances with firewall software embedded as firmware. They are more secure than those deployed on top of commercial operating systems since the latter are more vulnerable. Their major drawback is the limitation on scalability. Hence, answer in Option B is correct. The answers in the other options are incorrect.

248. Appliance based firewall _____

A. Is less secure than those deployed on top of commercial operating systems

B. Does not include appliances with firewall software embedded as firmware

C. Suffers from scalability issues & inability to meet changed environmental needs

D. Is a firewall software installed on top of commercial operating systems

KEY C

Justification

Appliance based Firewalls refer to appliances with firewall software embedded as firmware. They are more secure than those deployed on top of commercial operating systems since the latter are more vulnerable. Their major drawback is the limitation on scalability. Hence, answer in Option C is correct. The answers in the other options are incorrect.

249. Software Based Firewall _____

A. Suffers from scalability issues & inability to meet changed environmental needs

B. Is deployed on top of commercial operating systems

C. Is more secure than those deployed on top of commercial operating systems

D. Includes appliances with firewall software embedded as firmware

KEY B

Justification

Software based firewalls are deployed on top of commercial operating systems. They are less secure than Appliance based Firewalls in view of the vulnerability of the operating system itself. Their major advantage, however, is scalability in the face of changes in the environment. They exclude appliances with firewall software embedded as firmware. Hence, answer in Option B is correct. The answers in the other options are incorrect.

250. Software Based Firewall _____

A. Enjoys the major advantage of scalability in the face of changed environment

B. Is never deployed on top of commercial operating systems

C. Is more secure than those deployed on top of commercial operating systems

D. Includes appliances with firewall software embedded as firmware

KEY A

Justification

Software based firewalls are deployed on top of commercial operating systems. They are less secure than Appliance based Firewalls in view of the vulnerability of the operating system itself. Their major advantage, however, is scalability in the face of changes in the environment. They exclude appliances with firewall software embedded as firmware. Hence, answer in Option A is correct. The answers in the other options are incorrect.

251. Unified Threat Management _____

A. Cannot operate on a simple plug and play architecture

B. Has increased technical training requirements owing to its complexity

C. Is the Evolution of the traditional firewall into an all-inclusive security product

D. Complicates installation of security products

KEY C

Justification

Unified Threat Management is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single appliance. It can operate on a simple plug and play architecture. It has reduced technical training requirements since only one product has to be learnt and understood. Installation of security products is also easier and maintenance/vendor issues become simpler. Answer in Option C is correct. The answers in the other options are incorrect.

252. Unified Threat Management _____

A. Is the Evolution of the traditional firewall into a compound security system with multiple products

B. Has increased technical training requirements owing to its complexity

C. Complicates installation of security products

D. Can support various functionalities like VPN, gate-way anti-virus/anti-spam, etc. apart from firewall

KEY D

Justification

Unified Threat Management is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single appliance. Apart from the firewall, it can support VPN, gate-way anti-virus/anti-spam, intrusion prevention, content filtering, bandwidth management, etc. It can operate on simple plug and play architecture. It has reduced technical training requirements since only one product has to be learnt and understood. Installation of security products is also easier and maintenance/vendor issues become simpler. Answer in Option D is correct. The answers in the other options are incorrect.

253. Unified Threat Management _____

A. Can support firewall but not various functionalities like VPN, gate-way anti-virus/anti-spam, etc.

B. Can provide centralized support with complete control for globalized operations

C. Is the Evolution of the traditional firewall into a compound security system with multiple products

D. Has increased technical training requirements owing to its complexity

KEY B

Justification

Unified Threat Management is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single appliance. Apart from the firewall, it can support VPN, gate-way anti-virus/anti-spam, intrusion prevention, content filtering, bandwidth management, etc. It has reduced technical training requirements since only one product has to be learnt and understood. Installation of security products is also easier and maintenance/vendor issues become simpler. Overall, it is very well suited to an organization with global operations wherein it can provide centralized support with complete control. Answer in Option B is correct. The answers in the other options are incorrect.

254. Unified Threat Management _____

A. Can support firewall but not various functionalities like VPN, gate-way anti-virus/anti-spam, etc.

B. Is the Evolution of the traditional firewall into a compound security system with multiple products

C. Can also support data-loss prevention by blocking accidental or incidental loss of KEY data

D. Has increased technical training requirements owing to its complexity

KEY C

Justification

Apart from the firewall, Unified Threat Management can support VPN, gate-way anti-virus/anti-spam, intrusion prevention, content filtering, bandwidth management, etc. It can also support data-loss prevention by blocking accidental or incidental loss of confidential, proprietary or regulated data. It has reduced technical training requirements since only one product has to be learnt and understood. Installation of security products is also easier and maintenance/vendor issues become simpler. Overall, it is very well suited to an organization with global operations wherein it can provide centralized support with complete control. Answer in Option C is correct. The answers in the other options are incorrect.

255. A disadvantage of Unified Threat Management is _____

A. That it becomes a Single Point of Failure (SPOF) for network traffic

B. It cannot support various functionalities like VPN, gate-way anti-virus/anti-spam, etc.

C. Has increased technical training requirements owing to its complexity

D. It cannot support GUI interface for manageability

KEY A

Justification

The single biggest disadvantage of Unified Threat Management (UTM) is the obvious risks of centralization it becomes a Single Point of Failure (SPOF). The other major drawback is that its deployment may have an impact on latency and band width when the UTM cannot keep up with the traffic. Apart from the firewall, it can, indeed, support VPN, gate-way anti-virus/anti-spam, intrusion prevention, content filtering, bandwidth management, etc. It has reduced technical training requirements since only one product has to be learnt and understood. It can comfortably support GUI interface for manageability. Hence, answer in Option A is correct. The answers in the other options are incorrect.

256. A disadvantage of Unified Threat Management is _____

A. It cannot support GUI interface for manageability

B. Has increased technical training requirements owing to its complexity

C. That it can have impact on latency and bandwidth when it cannot cope with the traffic

D. It cannot support various functionalities like VPN, gate-way anti-virus/anti-spam, etc.

KEY C

Justification

A major drawback of UTM is that its deployment may have an impact on latency and band width when the UTM cannot keep up with the traffic. Apart from the firewall, it can, indeed, support VPN, gate-way anti-virus/anti-spam, intrusion prevention, content filtering, bandwidth management, etc. It has reduced technical training requirements since only one product has to be learnt and understood. It can comfortably support GUI interface for manageability. Hence, answer in Option C is correct. The answers in the other options are incorrect.

257. Baseline Configuration of Firewall _____

A. Should have a default policy of allowing all traffic/connections unless not specifically permitted

B. Should not allow remote users access through VPN

C. Should be preceded by a general risk assessment & cost-benefit analysis

D. Should not allow deployment of Web & other publicly accessible servers on a DMZ in respect of multi-location organizations

KEY C

Justification

Baseline configuration of a firewall should be preceded by a general risk assessment & cost-benefit analysis. It should have a default policy of not allowing any traffic/connections unless specifically permitted. It should permit remote users access through VPN. In respect of large multi-location organizations, it should ideally have the Web & other publicly accessible servers place on a DMZ for best security. Hence, answer in Option C is correct. The answers in the other options are incorrect.

258. Baseline Configuration of Firewall _____

A. Should have a default policy of not allowing any traffic/connections unless specifically permitted

B. Need not have an additional firewall for internal users since the main firewall would be adequate

C. Should not allow deployment of Web & other publicly accessible servers on a DMZ in respect of multi-location organizations

D. Should not allow remote users access through VPN

KEY A

Justification

Baseline configuration should have a default policy of not allowing any traffic/connections unless specifically permitted. It should permit remote users access through VPN. In respect of large multi-location organizations, it should ideally have the Web & other publicly accessible servers place on a DMZ for best security. It should also ensure that internal users should be protected with an additional firewall. Hence, answer in Option A is correct. The answers in the other options are incorrect.

259. Personal Firewalls

A. Are based upon different methods & techniques as compared to an enterprise firewall

B. Are more complicated compared to an enterprise firewall & require technical expertise to operate

C. Are software installed on a user's computer protecting against unwanted intrusion & attacks from the Internet

D. Control incoming traffic from the Internet alone, based upon defined security policy

KEY C

Justification

Personal Firewalls are software installed on a user's computer for protection against unwanted intrusion and attacks from the Internet. They are based upon the same methods and techniques as firewalls for enterprises. They are simpler and can be handled by less technically savvy persons too. Like the firewalls for enterprises, they, too, control and monitor both incoming as well as outgoing traffic based upon a defined security policy. Answer in Option C above is correct whereas the other answers are obviously wrong.

260. Personal firewalls _____

A. Are hardware devices installed on a user's computer protecting against unwanted intrusion & attacks from the Internet

B. Need not be monitored as constantly as firewalls for enterprises

C. Control incoming traffic from the Internet alone, based upon defined security policy

D. Are based upon different methods & techniques as compared to an enterprise firewall

KEY B

Justification

Personal Firewalls are software installed on a user's computer for protection against unwanted intrusion and attacks from the Internet. They are based upon the same methods and techniques as firewalls for enterprises. They are simpler and can be handled by less technically savvy persons too. Like the firewalls for enterprises, they, too, control and monitor both incoming as well as outgoing traffic based upon a defined security policy. They need not be monitored as constantly as enterprise firewalls. Answer in Option B above is correct whereas the other answers are obviously wrong.

261. Personal Firewall _____

A. Cannot block or alert the user about outgoing connection attempts

B. Cannot provide information about destination server with which an application is trying to communicate

C. Is based upon security policy of the computer whereas enterprise firewall is based on enterprise security policy

D. Are hardware devices installed on a user's computer protecting against unwanted intrusion & attacks from the Internet

KEY C

Justification

A Personal Firewall is based upon the security policy of the individual computer whereas enterprise firewall is based on enterprise security policy. It is a software installed on a user's computer for protection against unwanted intrusion and attacks from the Internet. Like the firewalls for enterprises, it controls and monitors both incoming as well as outgoing traffic based upon a defined security policy. It can block and alert the user about outgoing connection attempts too. It can go to the extent of providing information about a destination server with which an application is trying to communicate.

Answer in Option C above is correct whereas the other answers are obviously wrong.

262. Personal Firewall _____

A. Can protect a computer from unwanted incoming connection attempts

B. Are hardware devices installed on a user's computer protecting against unwanted intrusion & attacks from the Internet

C. Cannot provide information about destination server with which an application is trying to communicate

D. Cannot block or alert the user about outgoing connection attempts

KEY A

Justification

A Personal Firewall is based upon the security policy of the individual computer whereas enterprise firewall is based on enterprise security policy. It is a software installed on a user's computer for protection against unwanted intrusion and attacks from the Internet. Like the firewalls for enterprises, it controls and monitors both incoming as well as outgoing traffic based upon a defined security policy. It can protect a computer from unwanted incoming connection attempts. It can block and alert the user about outgoing connection attempts too. It can go to the extent of providing information about a destination server with which an application is trying to communicate. Answer in Option A above is correct whereas the other answers are obviously wrong.

263. State True or False One of the limitations of Personal Firewall is that many malwares can compromise the system, manipulate the firewall & even shut it down.

A. TRUE

B. FALSE

KEY A

Justification

It is true that some malwares exist which can penetrate & compromise the firewall system , disarming it in the process, leaving the internal network exposed to security risks. Hence, answer in Option A above is correct.

264. State True or False Personal Firewalls could be impacted by vulnerabilities in the Operating System.

A. TRUE

B. FALSE

KEY A

Justification

It is true that vulnerabilities in the Operating system itself could impinge on the security of the firewall system. Hence, answer in Option A above is correct.

265. State True or False These personal firewalls could sometimes generate false alerts which could irritate non tech-savvy users.

A. TRUE

B. FALSE

KEY A

Justification

It is true that some could sometimes generate false alerts which could irritate non tech-savvy users. Hence, answer in Option A above is correct.

266. Windows 7 software _____

A. Has no inbuilt firewall system; we would need to go in for a third party product for security

B. Has a network-based firewall system, not host-based system

C. Has an inbuilt stateful, host-based firewall that filters incoming and outgoing connections

D. Has a Firewall that cannot block or alert the user about outgoing connection attempts

KEY C

Justification

Windows 7 software has an inbuilt, stateful, host-based Firewall system that can filter both incoming as well as outgoing connections. It can block or alert the user against outgoing connection attempts too. Answer in Option C above is correct whereas the other answers are obviously wrong.

267. Windows 7 software _____

A. Has two network location types with advanced security

B. Has a network-based firewall system, not host-based system

C. Is a network location-aware host firewall

D. Has a Firewall that cannot block or alert the user about outgoing connection attempts

KEY C

Justification

Windows 7 software is a network location-aware host firewall. It has three network location types with advanced security Domain, public & private. It has a Firewall system that can filter both incoming as well as outgoing connections. It can block or alert the user against outgoing connection attempts too. Answer in Option C above is correct whereas the other answers are obviously wrong.

268. Windows 7 software _____

A. Has a Firewall that cannot block or alert the user about outgoing connection attempts

B. Stores firewall properties based on location types or profiles

C. Has a network-based firewall system, not host-based system

D. Has two network location types with advanced security

KEY B

Justification

Windows 7 software is a network location-aware host firewall. It stores firewall properties based on location types called profiles. It has three network location types with advanced security Domain, public & private. It has a Firewall system that can filter both incoming as well as outgoing connections. It can block or alert the user against outgoing connection attempts too. Answer in Option B above is correct whereas the other answers are obviously wrong.

269. Intrusion Detection Systems (IDS) _____

A. Like Firewalls, they are a method of preventive control

B. Monitors, alerts & corrects the problem

C. Cannot detect network scans, packet-spoofing & Denial of service

D. Will alert us if there are intruders in the host or the network

KEY D

Justification

Intrusion Detection Systems (IDS) are a detective control system which will alert us post intrusion into the host or the network. They will monitor & alert the user about exceptions but will not correct the problem. They can, indeed, detect network scans, packet-spoofing & denial of service. Answer in Option D above is correct whereas the other answers are obviously wrong.

270. Network Intrusion Detection Systems (NIDS) _____

A. Are placed at choke points on the network & monitor traffic to & from devices on the network

B. Do not check the content of individual packets for malicious traffic

C. Create substantial system overhead

D. Does not inhibit the effectiveness of packet analysis even with encrypted payloads and high-speed networks

KEY A

Justification

NIDS are placed at choke points like routers, switches, etc. within the network and they monitor to and from devices on the network. In operations, they do check the content of individual packets for malicious traffic. They do not create any significant system overhead. The effectiveness of packet analysis, however, is inhibited with encrypted payloads and high-speed networks. Answer in Option A above is correct whereas the other answers are wrong.

271. Host Intrusion Detection Systems (HIDS) _____

A. Monitors all packets but does not alert the administrator when suspicious activity is detected

B. Involve lesser deployment and reduced maintenance cost

C. Monitors all packets to and fro the hosts only.

D. Are not implemented on individual hosts or network devices

KEY C

Justification

HIDS are implemented on individual hosts or devices on the network and they monitor all packets to and from the hosts only. They alert the administrator when suspicious activity is detected. Since they are deployed on each computer, they involved higher deployment and proportionately higher maintenance cost. Answer in Option C above is correct whereas the other answers are wrong.

272. Signature based IDS _____

A. Monitors packets on network but does not validate them since they do not have a database for comparison

B. Will be able to detect attacks pre-emptively, even before the event

C. Can successfully handle even new attacks

D. Monitors packets on network and compares them against large databases of attack signatures

KEY D

Justification

SIDS are signature based IDS that monitor packets on networks and compare them against large databases of attack signatures. They cannot, however, detect attacks pre-emptively and cannot handle new attacks since a comparable signature would not be available with them. Answer in Option D above is correct whereas the other answers are wrong.

273. Statistical Anomaly / Behaviour based IDS _____

A. Monitors packets on network and validates them by comparing the signature in the database

B. Assume that an intrusion can be detected by observing a normal behaviour of the system/users

C. Will not be able to detect attacks pre-emptively, before the event

D. Cannot handle effectively new attacks

KEY B

Justification

SAB IDS monitor packet traffic on networks and compare them against an established baseline of behaviour. They can detect attempts to exploit new and unforeseen vulnerabilities. Their downside is that they generate a large number of false positives. Answer in Option B above is correct whereas the other answers are wrong.

274. Cryptography is _____

A. The process of transforming data into something that can be understood

B. The process of transforming data into something that cannot be understood with some additional information

C. The practice and study of hiding information

D. Cannot provide mechanisms for authenticating users on a network

KEY C

Justification

Cryptography is the practice and study of hiding information. It involves the process of transforming data into something that cannot be understood without additional information. It provides mechanisms for authenticating users on a network. Answer in Option C above is correct whereas the other answers are wrong.

275. Cryptography_____

A. Involves use of encryption for transforming data into something that can be understood

B. Is the process of transforming data into something that cannot be understood even with some additional information

C. Cannot provide mechanisms for authenticating users on a network

D. Is the theory and practice of secure communication

KEY D

Justification

Cryptography is the practice and study of hiding information with the objective of secure communication. It involves the use of encryption for transforming data into unintelligible form. The unintelligible form can be converted back into understandable information with the help of some additional information like a code or a key. It does provide mechanisms for authenticating users on a network. Answer in Option D above is correct whereas the other answers are wrong.

276. Cryptography _____

A. Provides mechanisms for preventing users from repudiating ownership of messages

B. Cannot provide mechanisms for authenticating users on a network

C. Is the process of transforming data into something that cannot be understood even with some additional information

D. Involves use of encryption for transforming data into something that is intelligible

KEY A

Justification

Cryptography is the practice and study of hiding information with the objective of secure communication. It involves the use of encryption for transforming data into unintelligible form. The unintelligible form can be converted back into understandable information with the help of some additional information like a code or a key. It does provide mechanisms for authenticating users on a network. It also enables prevention of users from repudiating ownership of their messages. Answer in Option A above is correct whereas the other answers are wrong.

277. Cryptography _____

A. Helps assure the receiver about the integrity of the message

B. Does not help in preventing users from repudiating ownership of messages

C. Cannot provide mechanisms for authenticating users on a network

D. Is the process of transforming data into something that cannot be understood even with some additional information

E. Involves use of encryption for transforming data into something that is intelligible

KEY A

Justification

Cryptography is the practice and study of hiding information with the objective of secure communication. It involves the use of encryption for transforming data into unintelligible form. The unintelligible form can be converted back into understandable information with the help of some additional information like a code or a key. It does provide mechanisms for authenticating users on a network. It also enables prevention of users from repudiating ownership of their messages. It helps the receiver in ensuring that the message received by him has not been altered in any fashion; ie, protect the integrity of the message. Answer in Option A above is correct whereas the other answers are wrong.

278. Cryptography _____

A. Does not help in preventing users from repudiating ownership of messages

B. Cannot provide mechanisms for authenticating users on a network

C. Ensures the privacy or confidentiality of the contents of the message

D. Involves use of encryption for transforming data into something that is intelligible

KEY C

Justification

Cryptography ensures the privacy or confidentiality of a message i.e. it ensures that no one except the intended receiver of the message can read the message. Cryptography is the practice and study of hiding information with the objective of secure communication. It involves the use of encryption for transforming data into unintelligible form. The unintelligible form can be converted back into understandable information with the help of some additional information like a code or a key. It does provide mechanisms for authenticating users on a network. It also enables prevention of users from repudiating ownership of their messages. It helps the receiver in ensuring that the message received by him has not been altered in any fashion; ie, protect the integrity of the message. Answer in Option C above is correct whereas the other answers are wrong.

279. Cryptography _____

A. Involves use of encryption for transforming data into something that is intelligible

B. Authenticates & convinces the receiver that the message has actually come from the sender

C. Does not help in preventing users from repudiating ownership of messages

D. Cannot provide mechanisms for authenticating users on a network

KEY B

Justification

Cryptography authenticates & convinces the recipient that the message has actually come from the sender. It involves the use of encryption for transforming data into unintelligible form. The unintelligible form can be converted back into understandable information with the help of some additional information like a code or a key. It does provide mechanisms for authenticating users on a network. It also enables prevention of users from repudiating ownership of their messages. Answer in Option B above is correct whereas the other answers are wrong.

280. Any message that is intelligible is considered to be in _____

A. Encrypted form

B. Coded form

C. Plaintext form

D. Ciphertext form

KEY C

Justification

Any message that is intelligible is considered to be in plaintext form. An encrypted form will not be intelligible without the use of additional information. A ciphertext form would be in unintelligible form till it is decrypted into plaintext form. Hence, answer in Option C above is correct whereas the other answers are wrong.

281. Any message that is converted into un-intelligible form is considered to be in _____

A. Ciphertext form

B. Plaintext form

C. Understandable form

D. Coded form

KEY A

Justification

A ciphertext form arises post encryption & would be in unintelligible form till it is decrypted into plaintext form. Any message that is intelligible is considered to be in plaintext form. An encrypted form will not be intelligible without the use of additional information. Hence, answer in Option A **above is correct whereas the other answers are wrong.**

282. The process of converting a given plaintext into ciphertext form is called _____

A. Decryption

B. Translation

C. Transcription

D. Encryption

KEY D

Justification

The conversion of a given plaintext into ciphertext form is called encryption. This form would be in unintelligible form till it is decrypted into plaintext form through decryption. Any message that is intelligible is considered to be in plaintext form. An encrypted form will not be intelligible without the use of additional information. Hence, answer in Option D above is correct whereas the other answers are wrong.

283. The process of converting ciphertext back into plaintext form is called _____

A. Transcription

B. Encryption

C. Decryption

D. Translation

KEY C

Justification

The conversion of a given plaintext into ciphertext form is called encryption. This form would be in unintelligible form till it is decrypted into plaintext form through decryption. Any message that is intelligible is considered to be in plaintext form. An encrypted form will not be intelligible without the use of additional information. Hence, answer in Option C above is correct whereas the other answers are wrong.

284. The mathematical function used for encryption & decryption is _____.

A. Binomial analysis

B. Cryptographic Algorithm

C. Transcription Algorithm

D. Exponential function

KEY B

Justification

The mathematical function used for encryption & decryption is called the cryptographic algorithm or Cipher. Answer in Option B above is correct whereas the other answers are wrong.

285. The mathematical function used for encryption & decryption is _____.

A. Transcription Algorithm

B. Binomial analysis

C. Cipher

D. Exponential function

KEY C

Justification

The mathematical function used for encryption & decryption is called the cryptographic algorithm or Cipher. Answer in Option C above is correct whereas the other answers are wrong.

286. A Cipher is also called _____

A. A Cryptographic Algorithm

B. Transcription Algorithm

C. Binomial analysis

D. Exponential function

KEY A

Justification

The mathematical function used for encryption & decryption is called the cryptographic algorithm or Cipher. Answer in Option A above is correct whereas the other answers are wrong.

287. A Cryptographic algorithm _____

A. Must be difficult to use but easy to crack

B. Must be easy both to use and crack

C. Must be easy to use but difficult to crack

D. Must be difficult to use as well as to crack

KEY C

Justification

An effective cryptographic algorithm must be easy to use but difficult to crack.

Answer in Option C above is correct whereas the other answers are wrong.

288. A Cryptographic algorithm _____

A. Can be used for one function encryption alone

B. Can be used for one function decryption alone

C. Can be used for one function creation of a key

D. Can be used for two functions encryption as well as decryption

KEY D

Justification

A cryptographic algorithm can be used for encryption as well as decryption.

Answer in Option D above is correct whereas the other answers are wrong.

289. KEYs _____

A. Are not required in the encryption or decryption process

B. Should be difficult to use but easy to break

C. Are additional secret data in the cryptographic process

D. Should be easy to use as well as to break

KEY C

Justification

KEYs are additional secret data which are used in the encryption or decryption process of cryptography. They need to be long enough to make breaking difficult but short enough to use and transmit. Answer in Option C above is correct whereas the other answers are wrong.

290. KEYs _____

A. Should be difficult to use but easy to break

B. Should be easy to use as well as to break

C. Are not required in the encryption or decryption process

D. Prevent the message from being decoded even if the algorithm is known

KEY D

Justification

KEYs are additional secret data which are used in the encryption or decryption process of cryptography. They need to be long enough to make breaking difficult but short enough to use and transmit. Without the keys, even if the mathematical algorithm of encryption were known, decryption into plaintext is not possible.

Answer in Option D above is correct whereas the other answers are wrong.

291. The Caesar cipher was used to transmit messages during Roman wars. It was actually a 'shift by 3' rule wherein alphabet A is replaced by the third alphabet D, B by E and so on. In this case, the KEY is _____

A. 3

B. Alphabet A

C. Alphabet D

D. Alphabet B

KEY A

Justification

KEYs are additional secret data which are used in the encryption or decryption process of cryptography. In this case, the recipient of the message needs to know the algorithm of shifting the alphabet by a few positions. However, in this specific instance, the shifting of the alphabet is by three positions. Hence, the KEY is 3. In another situation, the KEY can be changed to 5 or any other number depending upon security requirements without changing the basic algorithm.

Answer in Option A above is correct whereas the other answers are wrong.

292. Symmetric KEY Cryptography _____

A. Envisages the use of different keys for encryption and decryption

B. Envisages the use of a single KEY both for encryption as well as decryption

C. Suffers from no difficulty in terms of distribution of the key

D. Envisages the use of one KEY by the sender & another by the receiver

KEY B

Justification

Symmetric **KEY c**ryptography envisages the use of a single **KEY b**oth for encryption as well as decryption. Thus, the receiver uses the same KEY for decryption as was used by the sender for encryption. The difficulty lies in distribution of the key.

Answer in Option B above is correct whereas the other answers are wrong.

293. The Digital Encryption Standard _____

A. Is a NIST standard using 2^{56} keys

B. Continues to be used by NIST even today

C. Is a NIST standard using 2^{28} keys

D. Is not a Symmetric Encryption Standard

KEY A

Justification

DES is a National Institute for Standards and Technology Symmetric Encryption Standard using 2^{56} keys. It has been replaced by the Advanced Encryption standard which deploys 128, 192 and 256 bits and proportionately more keys for better security.

Answer in Option A above is correct whereas the other answers are wrong.

294. The Advanced Encryption Standard _____

A. Has been discontinued for use by NIST

B. Is a NIST standard using 2^{28} keys

C. Is not a Symmetric Encryption Standard

D. Is a NIST standard using up to 256 bits or 2^{256} keys

KEY D

Justification

AES is a National Institute for Standards and Technology Symmetric Encryption Standard using up to 256 bits or 2^{256} keys. It has replaced the DES in the interest of for better security.

Answer in Option D above is correct whereas the other answers are wrong.

295. Asymmetric or Public KEY Cryptography _____

A. Involves the use of a single KEY **b**oth for encryption as well as decryption

B. Is inferior to Symmetric KEY since safe distribution of the KEY to the recipient is an issue

C. Involves the use of a pair of keys, one for encryption & the other for decryption

D. Involves the use of two pairs of keys, one each for encryption and decryption

KEY C

Justification

Asymmetric or Public **KEY c**ryptography involves the use of a pair of keys, one for encryption and the other for decryption. It overcomes the difficulty of **KEY d**istribution faced in the case of symmetric **KEY c**ryptography.

Answer in Option C above is correct whereas the other answers are wrong.

296. Asymmetric or Public KEY Cryptography _____

A. Involves the use of a public KEY of the individual in a private domain

B. Involves the use of a private KEY of the individual in a public domain

C. Is thousands of times slower than symmetric KEY cryptography

D. Involves the use of two pairs of keys, one each for encryption and decryption

KEY C

Justification

Asymmetric or Public **KEY c**ryptography involves the use of a pair of keys, one for encryption and the other for decryption. The public KEY of the individual would be in the public domain whereas the private KEY would remain secret and not revealed. It overcomes the difficulty of **KEY d**istribution faced in the case of symmetric **KEY c**ryptography. This process, however, is thousands of times slower than the symmetric **KEY c**ryptography process.

Answer in Option C above is correct whereas the other answers are wrong.

297. Asymmetric or Public KEY Cryptography _____

A. Can be initiated by using either of the two keys first

B. Is not used for exchange of symmetric keys

C. Is not used for exchange of Digital signatures

D. Involves the use of two pairs of keys, one each for encryption and decryption

KEY A

Justification

Asymmetric or Public **KEY c**ryptography involves the use of a pair of keys, one for encryption and the other for decryption. Either of the two keys can be used, without any particular sequence. The public KEY of the individual would be in the public domain whereas the private KEY would remain secret and not revealed. It overcomes the difficulty of **KEY d**istribution faced in the case of symmetric **KEY c**ryptography. This process, however, is thousands of times slower than the symmetric **KEY c**ryptography process. Its use, therefore, is mainly in exchange of symmetric keys and digital signatures.

Answer in Option A above is correct whereas the other answers are wrong.

298. Asymmetric or Public KEY Cryptography _____

A. Is not used for exchange of symmetric keys

B. Is not used for exchange of Digital signatures

C. Uses more computer resources compared to Symmetric KEY cryptography

D. Provides lesser security as compared to Symmetric **KEY c**ryptography

KEY C

Justification

Asymmetric or Public **KEY c**ryptography involves the use of a pair of keys, one for encryption and the other for decryption. Either of the two keys can be used, without any particular sequence. The public KEY of the individual would be in the public domain whereas the private KEY would remain secret and not revealed. It overcomes the difficulty of **KEY d**istribution faced in the case of symmetric **KEY c**ryptography. This process, however, is thousands of times slower than the symmetric **KEY c**ryptography process and uses up more computer resources too. Its use, therefore, is mainly in exchange of symmetric keys and digital signatures.

Answer in Option C above is correct whereas the other answers are wrong.

299. Asymmetric or Public KEY Cryptography _____

A. Uses less computer resources compared to Symmetric **KEY c**ryptography

B. Generally has larger KEY size as compared to Symmetric KEY cryptography

C. Provides lesser security as compared to Symmetric **KEY c**ryptography

D. Is not used for exchange of symmetric keys

KEY B

Justification

Asymmetric or Public **KEY c**ryptography involves the use of a pair of keys, one for encryption and the other for decryption. Either of the two keys can be used, without any particular sequence. The public KEY of the individual would be in the public domain whereas the private KEY would remain secret and not revealed. It overcomes the difficulty of **KEY d**istribution faced in the case of symmetric **KEY c**ryptography. This process, however, involves larger KEY sizes, is thousands of times slower than the symmetric **KEY c**ryptography process and uses up more computer resources too. Its use, therefore, is mainly in exchange of symmetric keys and digital signatures. .Answer in Option B above is correct whereas the other answers are wrong.

300. RSA is _____

A. A form of cryptography which uses 2^{4096} keys

B. Not used in common software products

C. The most common form of Asymmetric KEY Cryptography in use

D. An acronym for its developers Robin Sharma, Sundararaman and Anjaneyulu

KEY C

Justification

RSA was developed by Ronald Rivest, Adi Shamir and Leonard Adleman & hence its name. It is the most common form of Asymmetric **KEY C**ryptography in use. It currently uses 2^{2048} keys for high security. It is used extensively in common software products for KEY exchange, digital signatures or encryption for small blocks of data.

Answer in Option C above is correct whereas the other answers are wrong.

301. What are Message Hash Functions ?

A. They are algorithms involved in computing a fixed length hash value

B. They are algorithms from which the contents & length of the plaintext can be recovered

C. They are algorithms whose limitation is that they cannot guarantee message integrity

They are algorithms involved in computing a variable length hash value

KEY A

Justification

Message Hash Functions are algorithms involved in computing a fixed length hash value. In lieu of a key, a fixed length hash value is computed based upon the plaintext that makes it impossible to recover the contents or length of the plaintext. The hash value is recalculated at the receiver's end and matched with that generated by the sender. If they match, the message has not been altered during transmission.

Hence, Option A alone is correct.

302. Message Hash Functions _____

A. Are algorithms involved in computing a fixed length hash value

B. Are algorithms from which the contents & length of the plaintext can be recovered

C. Are algorithms whose limitation is that they cannot guarantee message integrity

D. Are also called Message Digests and One-way hash functions

KEY D

Justification

Message Hash Functions are algorithms involved in computing a fixed length hash value. They are also called Message Digests and One-way hash functions. In lieu of a key, a fixed length hash value is computed based upon the plaintext that makes it impossible to recover the contents or length of the plaintext. The hash value is

recalculated at the receiver's end and matched with that generated by the sender. If they match, the message has not been altered during transmission.

Hence, Option D alone is correct.

303. What are Digital Signatures ?

A. Are data strings dependent only on a secret known only to the sender

B. Are data strings dependent on a secret known only to the sender & the message content

C. Are cryptography tools which depend upon use of Symmetric KEYs

D. They are algorithms whose limitation is that they cannot guarantee message integrity

KEY B

Justification

Digital signatures are data strings dependent on a secret known only to the sender and, additionally, on the content of the message. They use Asymmetric KEYs and Hash. They meet the communication objectives of authentication, integrity and repudiation. .Option B alone is correct.

304. What are Digital Signatures ?

A. They are algorithms whose limitation is that they cannot guarantee message integrity

B. Are data strings dependent on a secret built into the message content alone

C. Are cryptography tools which depend upon use of Asymmetric KEYs & Message Hash content

D. Are data strings dependent only on a secret known only to the sender

KEY C

Justification

Digital signatures are data strings dependent on a secret known only to the sender and, additionally, on the content of the message. They use Asymmetric KEYs and Hash. They meet the communication objectives of authentication, integrity and repudiation.

Option C alone is correct.

305. What are the characteristics of Digital Signatures ?

A. They achieve the communication objectives of confidentiality, authentication & integrity

B. They comply with the goals of authentication, access control and non-repudiation

C. They are algorithms whose limitation is that they cannot guarantee message integrity

D. They achieve the communication objectives of authentication, integrity & non-repudiation

KEY D

Justification

Digital signatures are data strings dependent on a secret known only to the sender and, additionally, on the content of the message. They use Asymmetric KEYs and Hash & involve the use of private and public keys. They meet the communication objectives of authentication, integrity and repudiation.

Option D alone is correct.

306. What are the characteristics of Public KEY Infrastructure (PKI) ?

A. They achieve the communication objectives of confidentiality & authentication alone

B. They achieve all the five basic communication objectives

C. They provide the infrastructure for generation, storage and security of public keys

D. They are algorithms which are not as effective as Digital signatures

KEY B

Justification

PKI are advanced cryptographic tools which help achieve all the five basic communication objectives of confidentiality, authentication, integrity, non-repudiation and access control. It involves the use of a digital envelope, which, in turn, deploys both secret **KEY** and public **KEY c**ryptography methods to send the secret KEY to the recipient. It thus combines public-KEY encryption and digital signature services to create a comprehensive system.

Hence, Option B alone is correct.

307. What are characteristic of Public KEY Infrastructure (PKI) ?

A. Digital certificates are used with support from Certificate authority & LDAP directory

B. They provide the infrastructure for generation, storage and security of public keys

C. They achieve the communication objectives of confidentiality & authentication alone

D. They are algorithms which are not as effective as Digital signatures

KEY A

Justification

PKI are advanced cryptographic tools which help achieve all the five basic communication objectives of confidentiality, authentication, integrity, non-repudiation and access control. It involves the use of a digital envelope, which, in turn, deploys both secret **KEY a**nd public **KEY c**ryptography methods to send the secret KEY to the recipient. It thus combines public-KEY encryption and digital signature services to create a comprehensive system. The system leans heavily on a robust Certification authority and Lightweight Directory Access Protocol (LDAP) directory. Hence, Option A alone is correct.

308. What are the typical characteristics of a Digital Certificate ?

A. It is a digitally signed document used to verify that a private **KEY b**elongs to an individual

B. It is a digitally signed document used to verify that a public KEY belongs to an individual

C. It is a digitally signed document which is permanent, without any validity/expiry date

D. It is a digitally signed document used to verify both public & private keys of an individual

KEY B

Justification A Digital certificate is a digitally signed document that associates a public KEY with a user. It will be signed by a Certification Authority. Its contents would include serial number, subject, signature, issuer, validity dates(valid from, expiry date), public key, thumbprint algorithm and thumbprint. Hence, Option B alone is correct.

309. Who are Certifying Authorities ?

A. In India, Certifying authorities are not regulated/ licensed & hence, certificates have no legal validity

B. They are not responsible for verification of registration, suspension and revocation requests

C. They are Trusted Third Parties to verify and vouch for the identities of entities in an electronic environment

D. In India, Certifying authorities are regulated/licensed by NASSCOM

KEY C

Justification

Certifying Authorities (CAs) are Trusted Third Parties to verify and vouch for the identities of entities in an electronic environment. In India, the IT Act provides for the Controller of Certifying Authorities, a body under the Ministry of Communications & Information Technology, is responsible for the licensing and regulation of Certifying Authorities & to ensure that the IT Act provisions are complied with. The main role of a CA is to digitally sign and publish the public **KEY b**ound to a given user. One of the major roles & responsibilities is verification of registration, suspension and revocation requests.

Hence, answer in Option C is correct.

310. Who are Registering Authorities ?

A. They authenticate the identity of a person before the CA releases the digital certificate

B. They are independent of the CA and are responsible to NASSCOM

C. They are not responsible for verification of identity but only for formal registration

D. They are a Government department who register the Certifying Authority

KEY A

Justification

Registering Authorities are work under the control of Certifying authorities (CAs) and are responsible for authenticating the identity of a person prior to issue of a digital certificate by the CA. They are also the body who interact with subscribers for providing CA services. The CAs themselves, who are independent entities, are licensed and regulated by the Controller of Certifying Authorities, a government body under the Ministry of Communications and Information Technology.

Hence, only the answer in Option A is correct.

311. Certification Revocation Lists (CRLs) _____

A. Are lists of Certifying Authorities who have been de-licensed by the CCA

B. Are issued by a Certifying Authority different from one that issued the original certificate

C. Are lists of serial numbers of certificates which have been revoked

D. Are issued by Registering Authorities and not signed by the Certifying Authority

KEY C

Justification

Certificate Revocations Lists (CRLs) are lists of serial numbers of digital certificates which have been revoked along with reasons for revocation. These certificates are themselves signed by the Certifying Authority (CA) themselves. The CRL is always issued by the CA who issued the corresponding certificate. Entities presenting those certificates can no longer be trusted.

Hence, only the answer in Option C is correct.

312. Certification Practice Statement is a statement of the practices which a Certification Authority employs in issuing and managing certificates.

A. TRUE

B. FALSE

KEY A

Justification

Certification Practice Statement is a statement of the practices which a Certification Authority employs in issuing and managing certificates. It carries various types of information like policies, procedures & processes involved in certificate issue, policies for revocation, policies for renewal, certificate lifetime, etc.

The answer in Option A is correct.

313. Which of the following is true off Cryptanalysis ?

A. Analysis of data for encryption using Symmetric key

B. Analysis of encryption/decryption records for audit purposes

C. Refers to methods of recovering plaintext from ciphertext without using the key

D. It is used to study strengths of a cryptosystem

KEY C

Justification

Cryptanalysis refers to methods of recovering plaintext from ciphertext without using the key. In other words, it is the study of methods for obtaining the meaning of encrypted information, without access to the secret information which is normally required to do so. It also deals with identifying weaknesses in the cryptosystem. The term cryptanalysis is also used to refer to attempts to break the security of other types of cryptographic algorithms and protocols, apart from encryption.

The answer in Option C only is correct.

314. How does a Cryptanalyst manage to identify the KEY for launching a Known plaintext attack ?

A. He ascertains the **KEY b**y compromising the Certifying Authority's servers

B. He programs his computer to continuously check random keys till he finds the right one

C. He breaks into the sender's system and identifies the private KEY for the transmission

D. He deduces the KEY by accessing both ciphertext as well as plaintext of several messages

KEY D

Justification

The Cryptanalyst can deduce the **KEY b**y accessing & comparing both the ciphertext as well as the plaintext of several messages. He can then launch a Known plaintext attack.

The answer in Option D only is correct.

315. Secure Socket Layer (SSL) _____

A. Cannot work with any program using TCP, even with modifications

B. Is a protocol that provides a secure communication channel between two machines

C. Has limited flexibility in choice of encryption used

D. Does not have built-in data compression capability

KEY B

Justification

SSL is a protocol that provides a secure communication channel between two machines operating on the Internet or an internal network. Any program using TCP can be modified to use SSL connection. SSL is also flexible in choice of symmetric encryption, authentication and message digest that can be used. It does have in-built data compression capability.

Hence, the answer in Option B only is correct.

316. Secure Socket Layer (SSL) _____

A. Subsequently became an internet standard known as Transport Layer Security

B. Does not have built-in data compression capability

C. Has limited flexibility in choice of encryption used

D. Is not widely used currently in the international communication network

KEY A

Justification

SSL was originally developed by Netscape and subsequently became the Internet standard known as Transport Layer Security (TLS). It is a protocol that provides a secure communication channel between two machines operating on the Internet or an internal network. Any program using TCP can be modified to use SSL connection. SSL is also flexible in choice of symmetric encryption, authentication and message digest that can be used. It does have in-built data compression capability. It is the most widely used security protocol system in the world currently.

Hence, the answer in Option A only is correct.

317. Secure Socket Layer (SSL) _____

A. Does not have built-in data compression capability

B. Has limited flexibility in choice of encryption used

C. Is the most widely deployed security protocol used today

D. Is not used for handling sensitive information like credit card/social security numbers, etc.

KEY C

Justification

SSL was originally developed by Netscape and subsequently became the Internet standard known as Transport Layer Security (TLS). It is a protocol that provides a secure communication channel between two machines operating on the Internet or an internal network. SSL is also flexible in choice of symmetric encryption, authentication and message digest that can be used. It does have in-built data compression capability. It is the most widely used system in the world currently. In particular, it is capable of handling sensitive information like credit card numbers, social security numbers and login credentials to be transmitted securely.

Hence, the answer in Option C only is correct.

318. Secure Socket Layer (SSL) _____

A. Has limited flexibility in choice of encryption used

B. Cannot work with any program using TCP, even with modifications

C. Does not have built-in data compression capability

D. Has the capability to handle sensitive information like credit card/social security numbers, etc.

KEY D

Justification

SSL was originally developed by Netscape and subsequently became the Internet standard known as Transport Layer Security (TLS). It is a protocol that provides a secure communication channel between two machines operating on the Internet or an internal network. SSL is also flexible in choice of symmetric encryption, authentication and message digest that can be used. Any program using TCP can be modified to use SSL connection. It does have in-built data compression capability. It is the most widely used system in the world currently. In particular, it is capable of handling sensitive information like credit card numbers, social security numbers and login credentials to be transmitted securely.

Hence, the answer in Option D only is correct.

319. Secure Socket Layer (SSL) _____

A. Is a transparent protocol requiring little user interaction for establishing a secure session

B. Cannot secure cloud-based computing platforms

C. Has limited flexibility in choice of encryption used

D. Cannot secure connection between E-mail Client and E-mail Server

KEY A

Justification

SSL was originally developed by Netscape and subsequently became the Internet standard known as Transport Layer Security (TLS). It is a protocol that provides a secure communication channel between two machines operating on the Internet or an internal network. SSL is also flexible in choice of symmetric encryption, authentication and message digest that can be used. It is a transparent protocol requiring little end user interaction for establishing a secure session.

Hence, the answer in Option A only is correct.

320. Secure Socket Layer (SSL) _____

A. Alerts users to its presence by displaying an eagle's head in the browser

B. Alerts users to its presence by displaying a padlock in the browser

C. Cannot secure system logins and any sensitive information exchanged online

D. Cannot secure connection between E-mail Client and E-mail Server

KEY B

Justification

SSL is a protocol that provides a secure communication channel between two machines operating on the Internet or an internal network. It is a transparent protocol requiring little end user interaction for establishing a secure session. It alerts users to its presence by displaying a padlock in the browser. Among other things, it can secure system logins and other sensitive information normally exchanged online. It can also secure connection between E-mail Client and E-mail Server.

Hence, the answer in Option B only is correct.

321. HTTP Secure _____

A. Is used widely except for payment transactions & other sensitive transactions

B. Is an advanced version of HTTP which is superior to SSL/TLS protocol

C. Is basically layering of HTTP protocol over the SSL/TLS protocol

D. Requires both the client as well as the remote server to be authenticated compulsorily

KEY C

Justification

HTTP Secure is basically layering of HTTP protocol over the proven Secure Sockets Layer (SSL) protocol. It is used widely, especially for payment transactions, emails, etc. While the SSL portion can comfortably authenticate both ends of a session, in the normal course only the server end is authenticated by the client.

Hence, the answer in Option C only is correct.

322. HTTP Secure _____

A. Is an advanced version of HTTP which is superior to SSL/TLS protocol

B. Requires both the client as well as the remote server to be authenticated compulsorily

C. Has a basic limitation of slowing down the web service

D. Is used widely except for payment transactions & other sensitive transactions

KEY C

Justification

HTTP Secure is basically layering of HTTP protocol over the proven Secure Sockets Layer (SSL) protocol. It is used widely, especially for payment transactions, emails, etc. While the SSL portion can comfortably authenticate both ends of a session, in the normal course only the server end is authenticated by the client. Its one limitation is that it slows down the web service.

Hence, the answer in Option C only is correct.

323. Virtual Private Network (VPN) _____

A. Can operate between two private networks but not the Internet

B. Does not provide confidentiality & integrity over un-trusted intermediate networks

C. Not compatible for operations with IPSec

D. Can link two networks or individual systems providing privacy & strong authentication

KEY D

Justification

VPNs can link two individual systems or networks providing privacy and strong authentication. The networks can be private networks or the Internet. They provide confidentiality & integrity over un-trusted intermediate networks. IPSec enables VPN and creates a virtual tunnel with encryption to ensure secure communication.

Hence, the answer in Option D only is correct.

324. IPSec _____

A. Protects application data across IP Networks

B. Requires applications to be specifically designed to work with it

C. Cannot be of help for implementation of VPN

D. Cannot be of help for remote user access through dial-up connection

KEY A

Justification

IPSec protects application data across IP Networks. It is encrypted at network layer of IP. Hence, it does not require applications to be specifically designed for use with it. It is useful for implementation of VPN as also for remote user access through dial-up connection. Hence, the answer in Option A only is correct.

325. IPSec _____

A. Is encrypted at IP(Transport layer)

B. Is implemented at end routers/firewalls

C. Cannot be of help for implementation of VPN

D. Cannot be of help for remote user access through dial-up connection

KEY B

Justification

IPSec protects application data across IP Networks. It is encrypted at network layer of IP. Hence, it does not require applications to be specifically designed for use with it. It is useful for implementation of VPN as also for remote user access through dial-up connection.

Hence, the answer in Option B only is correct.

326. IPSec _____

A. Is encrypted at IP(Transport layer)

B. Can operate in transport mode with both data & packet header encrypted

C. Has as its basic goals authenticity and data integrity

D. Can operate in tunnel mode with entire IP packet encrypted & old header added

KEY C

Justification

IPSec protects application data across IP Networks. It is encrypted at network layer of IP. Hence, it does not require applications to be specifically designed for use with it. It is useful for implementation of VPN as also for remote user access through dial-up connection. It has as its basic goals authenticity and data integrity. It can operate in two modes transport & tunnel. In transport mode, it provides secure connection between two end points. In this mode, the data is encrypted and the packet header is not encrypted. In tunnel mode, used for VPN, the entire IP packet is encrypted and a new header added to the packet for transmission.

Hence, the answer in Option C only is correct.

327. Transport Mode of IPSec _____

A. Involves encryption of data but not of the packet header

B. Involves encryption of the entire packet, for use in VPN

C. Can operate with entire IP packet encrypted & old header added

D. Provides secure connection between two points

KEY D

Justification

IPSec protects application data across IP Networks. It is encrypted at network layer of IP. Hence, it does not require applications to be specifically designed for use with it. It is useful for implementation of VPN as also for remote user access through dial-up connection. It has as its basic goals authenticity and data integrity. It can operate in two modes transport & tunnel. In transport mode, it provides secure connection between two end points. In this mode, the data is encrypted and the packet header is not encrypted. In tunnel mode, used for VPN, the entire IP packet is encrypted and a new header added to the packet for transmission.

Hence, the answer in Option D only is correct.

328. Tunnel Mode of IPSec _____

A. Is used to create Virtual Private Networks

B. Involves encryption of data but not of the packet header

C. Involves encryption of the entire packet, for use in non-VPN functions

D. Can operate with entire IP packet encrypted & old header added

KEY A

Justification

IPSec protects application data across IP Networks. It is encrypted at network layer of IP. Hence, it does not require applications to be specifically designed for use with it. It is useful for implementation of VPN as also for remote user access through dial-up connection. It has as its basic goals authenticity and data integrity. It can operate in two modes transport & tunnel. In tunnel mode, used for VPN, the entire IP packet is encrypted and a new header added to the packet for transmission.

Hence, the answer in Option A only is correct.

329. Secure Shell (SSH) is a protocol _____

A. Which is basically VPN layered on SSL protocol

B. Which cannot operation in conjunction with Telnet

C. Used for secure remote login & for command execution over an insecure network

D. Works only for peer-to-peer mode

KEY C

Justification

SSH is a protocol used for remote login and for executing commands over an insecure network. It is basically Telnet +SSL+ some other features. It works well for client-server mode, with both ends authenticated using certificates. It is usually used on UNIX systems.

The correct answer is as in Option C

330. Secure Shell (SSH) is a protocol _____

A. That cannot be used for remote login or command execution

B. Comprising Telnet+SSL+other features

C. Which is basically VPN layered on SSL protocol

D. Which cannot operation in conjunction with Telnet

KEY B

Justification

SSH is a protocol used for remote login and for executing commands over an insecure network. It is basically Telnet +SSL+ some other features. It works well for client-server mode, with both ends authenticated using certificates. It is usually used on UNIX systems.

The correct answer is as in Option B.

331. Secure Shell (SSH) is a protocol _____

A. Which cannot operation in conjunction with Telnet

B. Which is basically VPN layered on SSL protocol

C. That cannot be used for remote login or command execution

D. That is usually used on UNIX systems

KEY D

Justification

SSH is a protocol used for remote login and for executing commands over an insecure network. It is basically Telnet +SSL+ some other features. It works well for client-server mode, with both ends authenticated using certificates. It is usually used on UNIX systems.

The correct answer is as in Option D.

332. Secure Electronic Transaction (SET) _____

A. Was originally developed by Visa & Master card for secured electronic transactions

B. Uses a system involving three signatures

C. Uses a system involving two signatures, one each of the customer and the merchant

D. Uses a system involving three signatures, one each of the customer, the merchant & the bank

KEY A

Justification

SET is a protocol originally developed by Visa & Master card for securing electronic transactions. It uses a system of Dual Signatures. The objective is to link two messages that are intended for two different recipients. In a typical case, the message to the merchant will not allow reading of the credit card details and that to the bank will not give access to the order number details. The customer will have a link between order information & payment information for resolving disputes, if any.

The correct answer is as in Option A.

333. Secure Electronic Transaction (SET) _____

A. Uses a system involving three signatures, one each of the customer, the merchant & the bank

B. Is basically a combination of Telnet+SSL

C. Used exclusively on UNIX based systems

D. Uses a system of Dual signature to link two messages intended for two different recipients

KEY D

Justification

SET uses a system of Dual Signatures. The objective is to link two messages that are intended for two different recipients. In a typical case, the message to the merchant will not allow reading of the credit card details and that to the bank will not give access to the order number details. The customer will have a link between order information & payment information for resolving disputes, if any.

It uses a combination of RSA public **KEY c**ryptography, DES private **KEY c**ryptography & digital certificates to ensure security of transactions. It is not a combination of Telnet + SSL; nor is it used exclusively on UNIX based systems.

The correct answer is as in Option D

334. Secure Electronic Transaction (SET) _____

A. Uses a system involving three signatures, one each of the customer, the merchant & the bank

B. Used exclusively on UNIX based systems

C. Uses a cryptography combination of RSA public key, DES private KEY & digital certificates

D. Is basically a combination of Telnet + SSL

KEY C

Justification

SET uses a system of Dual Signatures. The objective is to link two messages that are intended for two different recipients. In a typical case, the message to the merchant will not allow reading of the credit card details and that to the bank will not give access to the order number details. The customer will have a link between order information & payment information for resolving disputes, if any.

It uses a combination of RSA public **KEY c**ryptography, DES private **KEY c**ryptography & digital certificates to ensure security of transactions. It is not a combination of Telnet + SSL; nor is it used exclusively on UNIX based systems.

The correct answer is as in Option C

335. Secure Multipurpose Internet Mail Extension _____

A. Uses the DES encryption system

B. Is a secure method for VPN access & remote log in

C. Is a secure method for Internet payment transactions

D. Is a secure method of sending emails and extensions

KEY D

Justification

S/MIME is a secure method for sending emails and extensions. It is based on public **KEY c**ryptography, using RSA encryption system. It does not use the DES encryption system. It is also not used for VPN/remote log in or for internet payment transactions.

The correct answer is as in Option D

336. Secure Multipurpose Internet Mail Extension _____

A. Is based on public KEY cryptography & uses RSA encryption system

B. Is a secure method for Internet payment transactions

C. Is a secure method for VPN access & remote log in

D. Cannot handle emails and attachments

KEY A

Justification

S/MIME is a secure method for sending emails and extensions. It is based on public **KEY** cryptography, using RSA encryption system. It does not use the DES encryption system. It is also not used for VPN/remote log in or for internet payment transactions.

The correct answer is as in Option A.

337. The prime drivers of choice of network technology for a typical large bank will be _____

A. Primarily Business Focus followed by Risk Management

B. Business Focus, Risk Management & Govt. / Compliance needs

C. Primarily Risk Management followed by Govt. / Compliance needs

D. Solely Business Needs

KEY B

Justification

The prime drivers for choice of networking technology would be all the three major factors of Business Focus, Risk Management & Govt. / Compliance needs.

The correct answer is, thus, as in Option B

338. The architecture of an enterprise-wide network in a bank _____

A. Would be dual-layered, comprising Security & Internet

B. Would be dual-layered, comprising WAN Network Topology & Security

C. Would vary significantly, depending upon size, structure & goals of each bank

D. Would be multi-layered, comprising WAN Network Topology, Security & Interfaces to Service delivery & Internet

KEY D

Justification

The architecture of an enterprise-wise network in a bank should ideally be multi-layered, comprising WAN Network Topology, Security & Interfaces to Service Delivery & Internet. It would be able to address the core needs of the bank in terms of business focus, security, Government & compliance needs.

The correct answer is, thus, as in Option D

339. The most popular choice of backbone network technology is _____

A. IP core technology

B. IP/ATM technologies

C. Multi-Protocol Label Switching or MPLS technology

D. AT&T technology

KEY C

Justification

MPLS technology supported networks are being used extensively as the backbone in view of the high usage of data, voice & video.

The correct answer is, thus, as in Option C

340. One feature of WAN Network Topology is _____

A. The backbone is usually of optical fibre, with redundant routes

B. The last mile connects the central or head office to nearby Service Provider POP

C. The last mile primary links, in most cases, are VSATs

D. The Data Centre & the Disaster Recovery Centre are in the same safe seismic zone

KEY A

Justification

The backbone in a typical WAN Network Topology is usually of optical fibre with redundant routes. The last mile connects the branch / small office to the POP of the service provider. The last mile links, in most cases, are leased lines backed up by a secondary link ISDN, WiFi or satellite link. The Data Centre and the Disaster Recovery Centre are invariably located in different seismic zones to prevent the possibility of both being impacted simultaneously.

The correct answer is, thus, as in Option A.

341. One feature of WAN Network Topology is _____

A. The backbone is usually of traditional copper wire used for telephony

B. The Data Centre & the Disaster Recovery Centre are in different seismic zones

C. The last mile connects the central or head office to nearby Service Provider POP

D. The last mile primary links, in most cases, are VSATs

KEY B

Justification

The backbone in a typical WAN Network Topology is usually of optical fibre with redundant routes. The last mile connects the branch / small office to the POP of the service provider. The last mile links, in most cases, are leased lines backed up by a secondary link ISDN, WiFi or satellite link. The Data Centre and the Disaster Recovery Centre are invariably located in different seismic zones to prevent the possibility of both being impacted simultaneously.

The correct answer is, thus, as in Option B

342. One feature of WAN Network Topology is _____

A. The Near-site DC is normally located in a different room/floor within the same complex as the DC

B. The DC, Near-site DC and DRC are not connected, to prevent spread of malicious viruses, etc.

C. Banks maintain a Near-site Data Centre (Near DC) in addition to the Data centre (DC) & Disaster Recovery Centre (DRC)

D. The DC and the DRC are invariably located in the same seismically safe area

KEY C

Justification

The Data Centre and the Disaster Recovery Centre are invariably located in different seismic zones to prevent the possibility of both being impacted simultaneously. The Near-site Data Centre is maintained in addition to the DRC within a radius of about 20-30 kms of the DC. The Near DC is connected both to the DC as well as the DRC through redundant links and would serve as the back-up for operational data in case of failure of the DC.

The correct answer is, thus, as in Option C

343. One feature of WAN Network Topology is _____

A. Data to & from the WAN to branches, DC, Near DC & DRC is in plaintext & not encrypted

B. The DC, Near-site DC and DRC are not connected, to prevent spread of malicious viruses, etc.

C. The DC and the DRC are invariably located in the same seismically safe area

D. Domain services are hosted in the Data centre (DC), Near-site Data Centre (Near DC) & Disaster Recovery Centre (DRC) in different De-Militarized Zones (DMZs)

KEY D

Justification

Domain services are hosted in the DC, Near DC & DRC in different DMZs. The Data Centre and the Disaster Recovery Centre are invariably located in different seismic zones to prevent the possibility of both being impacted simultaneously. The Near-site Data Centre is maintained in addition to the DRC within a radius of about 20-30 kms of the DC. The Near DC is connected both to the DC as well as the DRC through redundant links and would serve as the back-up for operational data in case of failure of the DC. Data to and from the WAN to branches, DC, Near DC & DRC is all encrypted.

The correct answer is, thus, as in Option D

344. This is a feature of WAN Network Topology.

A. Redundancy is built in at DC, with links from minimum of two ISPs

B. The DC and the DRC are invariably located in the same seismically safe area

C. Data to & from the WAN to branches, DC, Near DC & DRC is in plaintext & not encrypted

D. The DC, Near-site DC and DRC are not connected, to prevent spread of malicious viruses, etc.

KEY A

Justification

To pre-empt the risk of failure of ISP (Internet Service Provider) link, redundancy is built in at the DC with links from a minimum of two ISPs. The Data Centre and the Disaster Recovery Centre are invariably located in different seismic zones to prevent the possibility of both being impacted simultaneously. The Near-site Data Centre is maintained in addition to the DRC within a radius of about 20-30 kms of the DC. The Near DC is connected both to the DC as well as the DRC through redundant links and would serve as the back-up for operational data in case of failure of the DC. Data to and from the WAN to branches, DC, Near DC & DRC is all encrypted.

The correct answer is, thus, as in Option A.

345. Chartered Accountants are impacted by IT mainly in the following way _____

A. The IT industry is becoming global

B. The IT industry is being dominated by India

C. Automation of their clients' operations & their data going digital

D. The Institute of Chartered Accountants is going digital

KEY C

Justification

CAs are impacted by IT primarily by the automation of their client's operations & their data going digital. Also, CA firms themselves have to use IT in their own offices to provide services.

The correct answer is, thus, as in Option C.

346. Chartered Accountants are impacted by IT mainly in the following way _____

A. The Institute of Chartered Accountants is going digital

B. The IT industry is being dominated by India

C. CA firms themselves will need to use IT for servicing their customers

D. The IT industry is becoming global

KEY C

Justification

CAs are impacted by IT primarily by the automation of their client's operations & their data going digital. Also, CA firms themselves have to use IT in their own offices to provide services.

The correct answer is, thus, as in Option C

347. A Data Warehouse is a collection of decision-support data that is _____

A. Volatile & updated on a daily basis

B. Exclusively relating to sales & marketing

C. Historical, supporting analysis & reporting functions

D. De-centralized with warehouses distributed over the country

KEY C

Justification

A data warehouse is a centralized analytically oriented, integrated, time-oriented & non-volatile collection of data. It relates to all areas of operations which have relevance to business goals. Hence, only Option C is correct.

348. A Data Mart _____

A. Contains detailed data relating to a single aspect of business in large companies

B. Refers to a data storage product marketed by a business intelligence company

C. Stores all marketing related data alone for a company

D. Is a software used by Data Warehouses

KEY A

Justification

A Data Mart is a subset of a Data Warehouse & contains detailed data about a single aspect of business in large companies. Hence, only Option A is correct.

349. Data Mining _____

A. Is the recovery of all hidden data

B. Refers to the automated extraction of hidden predictive information

C. Helps analyse historical data but has little predictive value

D. Helps summarize data for regular MIS reporting systems

KEY B

Justification

Data Mining refers to the automated extraction of hidden predictive information. The **KEY A**spect is detection of hidden information which helps predict the future through identification of patterns, etc.. Hence, only Option B is correct.

350. Which are the business activities which are strong contenders for conversion to e-commerce ?

A. Those relating to software development

B. Those relating to the 'electronic' aspects of commerce

C. Those that are paper-based, time consuming & inconvenient for customers

D. Those that are not paper-based, speedy & convenient for customers

KEY C

Justification

Maximum mileage can be gained from e-commerce by converting those business activities which are paper-based, time consuming & inconvenient for customers as indicated in Option C. This will help us reduce paperwork, accelerate delivery & make it convenient for customers to operate from the comfort of their homes as also at any other place of their convenience. Hence, the other options are wrong.

351. Your daughter orders five salwar-kameez sets on the Myntra website for door delivery. She uses the Government wireless communication facility for carrying out this task. Which model of e-commerce would this fall in ?

A. Business-to-business

B. Consumer-to-consumer

C. Business-to-Government

D. Business-to-consumer

KEY D

Justification

This would obviously be a case of a business-to-consumer model &, hence, only Option D is correct.

352. Cloud computing refers to _____

A. On demand, networked access to a shared pool of computing resources

B. Computing carried out using software loaded on satellites

C. Strategic planning carried out through computerised simulations

D. Computing with light & minimal software

KEY A

Justification

Cloud computing refers to on demand, networked access to a shared pool of computing resources as indicated in Option A. It is generally offered as a utility to users, payable on the basis of consumption. Hence Option A is correct & the other options incorrect.

353. The Front-end in Cloud computing refers to _____

A. The Client's computer alone; the access software is available on the cloud

B. The various computers, servers & data storage systems in the cloud system

C. The software available on the cloud computing systems

D. The Client's computer as well as the software required to access the cloud

KEY D

Justification

The Front-end in Cloud computing comprises the Client's computer as well as the software required to access the cloud. Hence, Option D is correct whereas the other options are incorrect.

354. The Back-end in Cloud computing refers to _____

A. The Client's computer as well as the software required to access the cloud

B. The various computers, servers & data storage systems in the cloud system

C. The Client's computer alone; the access software is available on the cloud

D. Solely, the software available on the cloud computing systems

KEY B

Justification

The Back-end in Cloud computing comprises the various computers, servers & data storage systems in the cloud system. Hence, Option B is correct whereas the other options are incorrect.

355. Which of the following falls outside the typical features of Cloud computing ?

A. Resource Pooling capability

B. Rapid elasticity in meeting changed client demands

C. A large, offsite, remotely accessible computing facility created by a large enterprise for self use

D. Measured services with pay per use facility for clients

KEY C

Justification

Cloud computing basically involves pooling of resources for use by multiple agencies featuring the various attributes listed in Options B to D. Option A alone doesn't fall within the typical features of cloud computing since it speaks simply of a internal computing facility which happens to be located at a remote site. Hence, Option C is correct whereas the other options are incorrect.

356. What is a Hybrid Cloud computing facility ?

A. It provides both hardware as well as software services to its clients

B. It combines analog as well as digital computing capabilities

C. It provides free services to certain clients while charging others

D. It provides both private & public Cloud computing services

KEY D

Justification

Hybrid Cloud computing provides both private & public computing services, as indicated in Option D. Hence, the other options are incorrect.

357. A Platform as a Service (PaaS) Cloud Computing model allows clients access to _____

A. Hardware & operating system on the cloud but not the underlying infrastructure

B. Hardware & operating system on the cloud and also the underlying infrastructure

C. A variety of software provided on the cloud

D. Infrastructure, in terms of processing, storage & other computer networks, alone

KEY A

Justification

Option A above captures the correct services offered by PaaS; the other options are incorrect.

358. A Software as a Service (SaaS) Cloud Computing model allows clients access to _____

A. Hardware & operating system on the cloud but not the underlying infrastructure

B. Hardware & operating system on the cloud and also the underlying infrastructure

C. Infrastructure, in terms of processing, storage & other computer networks, alone

D. A variety of software applications made available by the provider on the cloud

KEY D

Justification

Option D above captures the correct services offered by SaaS; the other options are incorrect.

359. One of the major risks associated with Cloud computing is _____

A. Increased cost of operations

B. Greater dependency on third parties & vulnerability to risk

C. Increase in manpower requirements

D. Loss of competitive advantage

KEY B

Justification

Options at A,C & D are incorrect; cloud computing should actually help reduce costs, improve competitive advantage & not lead to increased manpower requirements. However, to the extent one is forced to use a third party cloud computing service, the client's dependency increases with consequent risk perception. Hence, Option B alone is correct.

360. What are the major perspectives in the role of a Chartered Accountant (CA) in the post implementation stage of Enterprise Resource Planning (ERP) software ?

A. Defining criticality of the business & applying priorities

B. Cost-benefit analysis of customization

C. Optimization & security of the software system

D. Reports required for monitoring and control

KEY C

Justification

Post implementation, the CA would have already helped map the business processes & arrived at the best configuration of the software and its applications. His focus would, hence, be on optimization of the system & ensure adequate security. Hence, Option C alone is correct.

361. What are some of the major challenges of using Enterprise Resource Planning (ERP) software ?

A. Reduced data access

B. Need for redundant legacy systems to be maintained in parallel

C. Expenses & time in implementation

D. Increased operating costs

KEY C

Justification

The large expenditure involved in purchase as also the intricacies of implementation of this software are the major challenges which would be faced by an individual launching ERP software. Implementation of the ERP system would actually help improve data access, reduce operating costs & eliminate the need for legacy systems, contradicting the answers in Options A, B and D. Hence, Option C alone is correct.

362. Your client has a diversified business with manufacturing units & offices at multi-locations. He is now trying to streamline operations by opting for a centralized

ERP system. You have assisted him in screening potential products & arriving at the one best suited to his needs. The next step which would be critical for optimizing the ERP software & aligning it to the business's needs would be

_____

A. Understanding business processes, identifying priorities & incorporating best practices

B. Eliminating legacy systems

C. Implementing the system immediately to save on time & reap the benefits quickly

D. Implementing the system in a part of the organization alone, to start with

KEY A

Justification

Before commencing implementation of the ERP software, it is important to get a thorough understanding of the business processes involved & identifying priority areas (as mentioned in Option A). Based upon this, relevant best practices & benchmark indices can be identified & incorporated in the final model in order to extract maximum benefit from the software. Legacy systems elimination can be undertaken only after successful commissioning of the ERP (at least at the pilot level). While it may seem attractive to accelerate the implementation with the objective of generating savings earlier, it would be far better to ensure that the approved model is robust & flexible enough to accommodate potential changes in the environment. Lastly, an ERP is ideally implemented enterprise-wide in order to harness the power of the software. Implementing it in part of the organization would leave it in a stunted & sub-optimal form. Hence, Option A alone is correct.

363. Which of the following is true of a typical Enterprise Resource Planning (ERP) system ?

A. Capable of operation only on batch processing basis; cannot be real-time based

B. At any point of time, the same data, on real-time basis, can be accessed by people in different parts of the organization

C. Capable of generating a balance sheet and P&L statement even on a daily basis

D. Implementation of a new ERP system can be done very quickly since it is modular

KEY C

Justification

ERP systems allow all users access to real-time data. Of course, access may be limited to individual users on a 'need-to-know' basis. Once configured & implemented, it should technically be possible to generate financial statements even on a daily basis. One of the limitations of any robust ERP system is the time taken for implementation. For best results, the implementation process has to be rigorous & scrupulously adhered to. Short cuts can be counter-productive. Hence, Option C alone is correct.

364. One of the major risks of Enterprise Resource Planning (ERP) systems is ?

A. Increased complexity of simply legacy processes

B. Increased manpower requirement, particularly in the accounting area

C. Risk of depending upon one ERP vendor for all the critical operations of the organization

D. Increased operating costs

KEY C

Justification

A major risk with ERP systems is the fact that they cover the entire operations of an organization & any default or failure on the part of the ERP system vendor can have catastrophic consequences for operations. The situation is further compounded by the fact that there are very few dependable ERP system vendors, leaving little choice. A well implemented ERP would actually simplify legacy business processes. A major positive outcome of ERP implementation is generally a reduction in manpower, particularly in the accounting department. Costs would, obviously be lower than before. Hence, Option C alone is correct.

365. You are a budding entrepreneur running a Small & Medium Enterprise. The SME is on a rapid growth path & you have ambitious expansion plans. You have invested substantial sums in creating a robust IT system for the organization keeping in mind your future plans. You realize that the success of any system lies in checks and balances, including a proper auditing system & decide on appointing an auditor. The qualities you would pragmatically expect an ideal auditor to possess for this role would be _____

A. Expertise in all areas of IT technology

B. Thorough knowledge on the financial aspects alone

C. Adequate working knowledge of IT hardware & software

D. Expertise both in financial and IT technology aspects

KEY C

Justification

C.A.s knowledge of IT technology need not and cannot be complete and total. They only need adequate knowledge to effectively audit the IT functions of an organization

C.A.s cannot be expected to be experts in all areas of IT technology; this is not their role

Knowledge of financial aspects alone in a technology oriented function like IT will not facilitate effective auditing of the IT function

A C.A. cannot be expected to have thorough knowledge of both financial & IT technology aspects

366. You are a Sales Manager in a consumer product company equipped with the latest laptop computer. You use the laptop for analysing territory-wise sales trends, customer preferences, etc. After a recent upgrade of software by your company's IT department, you observe that you are no longer able to analyze historical sales trends. However, when you check the database in the computer, the historical sales data is very much available. The problem you are facing is probably due to _____

A. A bug or inadequacy in the operating system

B. A bug or inadequacy in the application software

C. Insufficient memory space in the computer

D. Defective hardware in the laptop

KEY B

Justification

The problem has arisen after upgrade of the application software by the IT department. The database clearly has the relevant data & it is the access to and/or manipulation of this data which is the issue. Hence, Option B is correct. The other options are not correct since they are not likely to create the problem encountered by the Sales Manager.

367. Following an orientation programme on Information Technology, four members from the group of participants are picked up and named Mr Fetch, Mr Decode, Ms Execute and Ms Store as representative parts of the CPUs machine cycle. In which sequence should these individuals queue up in order to accurately demonstrate the machine cycle performed by the CPU ?

A. Mr Decode, Ms Execute, Ms Store and Mr Fetch

B. Ms Store, Mr Fetch, Mr Decode and Ms Execute

C. Ms Execute, Mr Fetch, Mr Decode and Ms Store

D. Mr Fetch, Mr Decode, Ms Execute and Ms Store

KEY D

Justification

As defined clearly in paragraph 1.3.2

A B, & C are clearly wrong answers which contain the wrong sequence

368. Your client's business volume has been stagnating & he is keen to explore ways and means of growing it. With the objective of drawing up an appropriate strategy, you advise him to conduct a SWOT analysis for which he collects a lot of operational information related to marketing, manufacturing, etc.. He realizes that his information system is now faced with information overload & he needs to supplement his Secondary Memory capacity. Secondary memory _____

A. Is non-volatile memory with large storage capacities

B. Is volatile memory with large storage capacities

C. Is non-volatile memory which is fast & responsive

D. Involves higher cost per unit of information than RAM

KEY A

Justification

As brought out in paragraph 1.3.3, secondary memory is non-volatile, with large storage capacities. It is, however, slower than registers or primary storage.

Secondary memory is not volatile.

It is not fast.

Its cost per unit of information is lower than RAM

369. You are auditing the recent purchase of IT hardware equipment in your client's office. You study the Mean Time before failure (MTBF) as also Mean Time to Repair (MTTR) of the equipment. Ideally, _____

A. MTBF must be low and MTTR must be high

B. MTBF must be high and MTTR must be low

C. Both MTBF and MTTR must be high

D. MTBF and MTTR must be equal to each other.

KEY B

Justification

As brought out in paragraph 1.5.2., Mean Time Between Failures must be high and Mean Time To Repair must be low.

All the other answers are, therefore, obviously wrong.

370. As a Chartered Accountant, you feel that Hardware Auditing _____

A. Is best carried out by the purchase department of the I.T. department

B. Should be restricted to the financial aspects of hardware usage

C. Primarily encompasses hardware acquisition & capacity management

D. Is not as critical as software auditing which can be a more vulnerable area

KEY C

Justification

Paragraph1.6 elaborates on the criticality of hardware acquisition & capacity management as **KEY A**reas of Hardware auditing.

Hardware is a vulnerable area which needs to be closely reviewed by Audit. Hence, the other three options are not correct

371. Your client reports to you concern about security of the data in his organization and would like to install software which effectively manages ownership assignment of all data for accountability. What type of software would you recommend him to install ?

A. Data Communications Software

B. Access Control Software

C. Utility programs

D. Defragmenters

KEY B

Justification

It is access control software which is vested with the responsibility for assigning ownership of all data for purposes of accountability (para 2.3.2). Data Communications software generally assists the OS for local and remote terminal access (option A). Utility programs and defragmenters basically help improve computer efficiency and performance and have nothing to do with ownership assignment of all data.

372. You are auditing a major software purchase transaction by your client. In your opinion, what should your client have done as a first step in acquiring the software ?

A. Establish scope, objectives background & project charter

B. Establish criteria for selecting and rejecting alternatives

C. Carry out Cost/Benefit analysis, including make or buy decision

D. Determine supplier's technical capabilities & support services

KEY A

Justification

Without first establishing the scope and objectives, software acquisition may end up failing on fundamental aspects of meeting end user needs. This would be the starting point, therefore, for any acquisition exercise. The other options get ruled out by default.

373. Your client is in the process of deploying IT in his business operations & seeks advice about the potential drawbacks of following a Centralised Deployment Strategy. Your answer would be that the major drawback of this strategy would be

_____

A. Resource sharing of reduced order

B. Poorer economies of scale

C. Reduced security

D. Vulnerability due to single point of failure

KEY D

Justification

Centralized deployment strategy concentrates all its resources at one central point making it vulnerable to total system failure in the event of this central point being compromised in any manner (Option D). Resource sharing, in fact, is a strong plus point for centralised deployment. Similarly, this system has better economies of scale owing to use of large size hardware & larger number of software licences. Since everything is centralized, possibilities of leakages are reduced since the number of exposed points are lesser. Hence, the other options are not correct.

374. Your client is in the process of deploying IT in his business operations & seeks advice about the potential drawbacks of following a De-centralised Deployment Strategy. Your answer would be that the major drawback of this strategy would be

_____

A. Less flexibility to cope with internal/external changes

B. Potentially higher CAPEX requirement

C. Information systems could be mutually incompatible

D. Slower system development

KEY C

Justification

A major disadvantage of decentralized deployment strategy is that, with de-centralized decision making, different tailor-made information systems may be created at different locations leading to potential incompatibility (Option C). On the other hand, given their de-centralized structure, they would have greater flexibility to cope with changes and can be developed/implemented quickly. Capex requirement could also be lesser owing ability to carry out changes in phases. Hence, the other options are not correct.

375. A large private sector bank offering Core Banking Solutions has sought your assistance in auditing its Data centre operations. While drawing up your auditing approach to this bank, you would primarily focus upon _____

A. Number of employees in the Bank

B. Annual Business volume

C. Nature of software applications used

D. Type of services offered, risk management & control requirements

KEY D

Justification

The complexity of services offered including the response time, risk management objectives and control goals would drive the IT components of a CBS Data Centre (Option D). The elements in the other three options would have limited impact on the configuration of the data centre.

376. A large international airline has entered Indian airspace & is setting up IT and other infrastructure in a metro city in India. Its business is strongly dependent upon the internet & accuracy and prompt availability of data is critical to successful operations. It has already decided on backing up of all information as also storing of all transactional information at a remote site to overcome the contingency of any break-down of the infrastructure at its metro city office. As a Consultant to the business, what other measures of redundancy would you suggest to improve reliability, fault tolerance & accessibility, without, however, compromising on security?

A. A near-site data replication facility

B. A near-site Disaster recovery facility

C. Filing of hard copies of all transaction documents

D. Hiring cloud storage facilities as an additional back up

KEY A

Justification

A near-site facility is normally used as a data replication facility only (Option A). It would not be a prudent choice for a disaster recovery facility since, as a proximate location, the probability of its getting exposed to the same geographical risks is very high. Use of hard copies of documents would be a retrograde step which would only delay processes & add costs. While cloud storage could be a solution, it could raise issues of data security. Hence, the other options are not correct.

377. You have been appointed as a Consultant to a SME which is slowly outgrowing its status & morphing into a large enterprise. The organization has invested in various types of software at different stages of its growth but now seeks to rationalize its IT infrastructure with an eye on future growth. Faced with the complexity of the existing Information System, you decide on first implementing a process of Configuration Identification (CI). This involves _____

A. Identification of all IS components without reference to version

B. Identification of software components of IS alone

C. Identification of all IS components in a system

D. Identification of hardware components of IS alone

KEY C

Justification

Configuration identification involves identification of all versions & updates of both software and hardware. This facilitates continuous monitoring during the life cycle of the product & becomes useful at the time of any proposed changes in the components (Option C). Option A is wrong since it ignores the version, which is vital. B and D are incorrect since they are addressing either the software or hardware alone.

378. A SME which is slowly outgrowing its status & morphing into a large enterprise has appointed you as a Consultant. The organization has invested in various types of software & hardware at different points of time. You have realized that this disorganized and unplanned method of software & hardware acquisition has made it very vulnerable. Your considered view is that the first step towards securing the systems is to carry out Hardening of the Systems. This involves _____

A. Use of robust hardware to strengthen the system

B. Optimising configuration of hardware systems alone

C. Auditing configuration of software systems alone

D. Securely configuring systems to minimize security risks

KEY D

Justification

Hardening of systems is the process of securely configuring computer systems to eliminate as many security risks as possible (Option D). It does not refer to use of robust hardware (Option A); nor does it limit itself to hardware alone (Option B) or software alone (Option C).

379. Your client asks you as to which type of Communication system facilitates simultaneous two way communication. You would then advise them to go in for _____

A. Half Duplex communication system

B. Full Duplex communication system

C. Simplex communication system

D. Combination of Simplex and Half Duplex systems

KEY B

Justification

Full Duplex communication has the capability to handle simultaneous two way communication. It is like two Simplex systems put together. A half duplex system / simplex system or a combination of these cannot meet this objective.

380. You are being briefed by an accountant in your client's office who has limited knowledge of cable technology. He speaks of the type of cable which has been chosen by his IT department for transmission of information. He explains that the cable's positive features include high integrity, low attenuation over long distances, high carrying capacity & lesser power consumption. He also feels that it comprises an inner core made of glass or plastic type of material. What is your educated guess of the nature of this cable ?

A. Optical fibre cable

B. Co-axial cable

C. Twisted pair cable

D. Bi-metallic cable

KEY A

Justification

An Optic fibre cable consists of an inner core made of glass/plastic/polymer/acrylic which uses light based signalling. It has high integrity as well as low attenuation over long distances. It has higher carrying capacity & consumer lesser power since signals do not degrade as fast as in other systems. Hence, Option A is the only correct option.

381. You have recently taken on a Travel agency as your client. You are familiarizing yourself with the agency & its operations. You are told that they use a network of computers which are designed as per Bus topology. You realize then that the agency's computer system involves _____

A. A single hub connecting all nodes

B. Connection of its computers on a single circle of cable

C. Connection of computers on a single backbone cable

D. Connection of every node to every other node

KEY C

Justification

In Bus topology, all the computers in the network are connected on a single backbone cable. All the computers in the network receive incoming messages from any other computer; however, only the intended recipient accepts and processes the message. It is not on a single hub or circle of cable and each of the nodes are not connected to each other. The correct answer is Option C

382. You have signed on for an audit of an Internet service provider. What sort of network topology do you expect this organization to have adopted ?

A. Ring topology, involving connection of all the computers on a single ring of cable

B. Star topology, connecting all the computers to a central hub or switch

C. Mesh topology, involving physical connection of every node with every other node

D. Bus topology with all systems Ideally suited for systems with need for low degree of fault tolerance

KEY C

Justification

This involves physical connection of every node with every other node. It is rather complex and requires maximum number of cables. However, it is ideally suited for large telecommunication companies or an internet service provider who cannot afford to have a high degree of fault tolerance. It is not connected to a single backbone or hub/switch. The correct answer, therefore, is Option C.

383. Your client has noted that a user with a particular IP address has been trying to access its server & wishes to identify the physical address (MAC) of the user. Which is the protocol which would have to be used for doing this ?

A. Internet Control Message Protocol (ICMP)

B. Transmission Control Protocl (TCP)

C. Simple Mail Transfer Protocol (SMTP)

D. Address Resolution Protocol or ARP

KEY D

Justification

ARP is a method of ascertaining the physical address (MAC), given the IP address. The other protocols in Options B to C have other capabilities. Hence, only Option D is correct.

384. You observe that the first Octet of the IP address of one of your clients is 195 in decimal range. In which Class of the IPv4 Classful Addressing Scheme does this fall ?

A. C

B. D

C. A

D. E

KEY A

Justification

The first Octet of Class C of the IPv4 Classful Addressing Scheme is any number ranging between 192 and 223 & the client's number of 195 falls within this range. Hence, the answer in Option A is correct. The other options are incorrect.

385. Technology development by design from a strategic perspective by CA firms could _____

A. Be a promotional tool for CA firms, attracting more clients

B. Be a Growth Catalyst / KEY differentiator for current/new services to existing / new customers

C. Be an expensive proposition with doubtful long term benefits

D. Be a wasteful exercise since IT technology is very volatile & could become obsolete quickly

KEY B

Justification

Technology development by design from a strategic perspective by CA firms could be a growth catalyst and **KEY d**ifferentiator for current as well as new services for existing and new clients.

The correct answer is, thus, as in Option B.

386. You have just taken on as your client, a huge international organization with a large presence on internet networks. To which class of IPv4 Classful Addressing Scheme do you expect its IP address to belong & within what range would the first Octet of its address fall ?

A. Class B, 128-191

B. Class C, 192-223

C. Class A, 1-126

D. Class E, 240-254

KEY C

Justification

Large organizations with extensive presence on the internet are generally included in Class A of the IPv4 Classful Addressing scheme. The first Octet would then fall within a range of 1 – 126. Option C, thus, gives the correct answer & the other options are incorrect.

387. Your client company is involved in research & development on the internet. Which class of IPv4 Classful Addressing Scheme do you expect it to use & within what range would the first Octet of that address fall ?

A. Class A, 1-126

B. Class B, 128-191

C. Class C, 192-223

D. Class E, 240-254

KEY D

Justification

Class E of the IPv4 Classful Addressing scheme is reserved for research & development / study. The first Octet would fall within a range of 240 to 254. Option D, thus, gives the correct answer & the other options are incorrect.

388. You have just taken on as your client, a huge international organization with a large presence on internet networks. Which of the following types of Network (N)/Host (H) id of the IPv4 Classful Addressing Scheme would you expect the client to have ?

A. N.H.H.H

B. H.N.N.N

C. N.N.H.H.

D. H.H.N.N

KEY A

Justification

Large organizations with extensive presence on the internet are generally included in Class A of the IPv4 Classful Addressing scheme. The first Octet would then represent the network id and the other Octets, the host id, as indicated in Option A. The other options are not correct.

389. Your new client advises you that its IP address falls under Class C of the IPv4 Classful Addressing Scheme. Which of the following types of Network (N)/Host (H) id would you expect the client to have ?

A. H.N.N.N

B. N.N.H.H.

C. N.N.N.H

D. H.H.N.N

KEY C

Justification

Large organizations with extensive presence on the internet are generally included in Class A of the IPv4 Classful Addressing scheme. The first Octet would then represent the network id and the other Octets, the host id, as indicated in Option C. The other options are incorrect.

390. If your client's IT manager advises you that his company's default sub-net mask under the IP Classful Addressing Scheme is 255.255.0.0, which of the following IP classes does his company's network belong ?

A. Class A

B. Class C

C. Class B

D. Class E

KEY C

Justification

The default sub-net mask of Class B of the IP Classful Addressing Scheme is 255.255.0.0; hence, Option C is correct. The other options are not correct.

391. You are with the IT Manager of your client, trying to understand their systems. The IT Manager is a person who revels in creating puzzles. When you ask him about his company's IP address, he tells you that it belongs to an IPv4 class that can accommodate the least number of networks but the maximum number of hosts per network (usable addresses). To which IP class is he referring ?

A. Class A

B. Class B

C. Class C

D. Class D

KEY A

Justification

The IP class A of IPv4 can handle the least number of networks (126) and maximum number of usable addresses (1,67,77,214). Hence, Option A is correct & the other options are incorrect.

392. You are with the IT Manager of your client, trying to understand their systems. The IT Manager is a person who revels in playing with puzzles. When you ask him about his company's IP address, he tells you that it belongs to an IPv4 class that can accommodate nearly 21 lakh networks. He adds, however, that the flip side is that the number of useable addresses per network would be a measly figure of about 250. To which IP class is he referring ?

A. Class A

B. Class B

C. Class D

D. Class C

KEY D

Justification

The IP class C of IPv4 can handle as many as 20,97,150 networks but number of usable addresses can be only 254. Hence, Option D is correct & the other options are incorrect.

393. As an experienced Chartered Accountant, you are addressing a group of freshers on the subject of the massive quantities of information available to any organization. In this background, what would you stress as most critical for successful business operations ?

A. Establishing hardware infrastructure to handle voluminous information

B. Recruiting more IT personnel to handle large volume of data

C. Building more storage space for the voluminous data

D. Capability to pick out the KEY Aspects which can help serve the customer better

KEY D

Justification

The most critical factor for business success in the current information age is the capability to sift the grain from the chaff, pick out the exceptions & appreciate customer preferences & nuances of demand. The other options of creating infrastructure, adding people or storage space are, at best, short term measures for coping with dealing with 'big data' rather than means of identifying customer needs & satisfying them.

A retail grocery chain store analyses data of its sales over different time periods over the day. It observes that in many of its markets, substantial sales happen throughout the day but in certain specific markets, sales peaked late in the evening. In these markets, frequent instances were also reported of staff having to send away customers as late as 10 pm in the night since closing time for the store had been crossed. On carrying out a more detailed analysis of the profile of the customers in these markets, it discovered that these were dominated by young employees of IT & BPO companies, many of whom worked in line with U.S. and European markets & returned home late in the night.

394. The store then decided to experiment with extended timings, up till midnight, for the stores in such markets & was delighted to find sales burgeoning. Which of the following best describes this initiative ?

A. Leveraging Business Intelligence to identify latent customer needs

B. Increasing investments in people for higher returns

C. Improved channel management

D. Cost saving experiment

KEY A

Justification

This is a clear case of leveraging business intelligence to identify latent customer needs. But for the capability to collect, analyse data & draw insightful conclusions therefrom, this success could not have been achieved. Option A, therefore, is correct. The other answers may be the incidental outcomes of the action taken in the process of leveraging business intelligence and not the actual initiative per se.

395. You are a Consultant to a budding Small & Medium Enterprise which is aiming at growing into a large enterprise. You carry out a detailed study of the current state of the enterprise in terms of people, systems, procedures, etc. You decide to focus on systems and IT, in particular, as the backbone for the enterprise's future growth plans. You observe that the existing system has limitations in terms of lack of uniformity of software, databases, delay in availability of analysed data, etc. Your recommended solution would be for _____

A. Up-gradation of all the current versions of software

B. Installation of an Enterprise Resource Planning software

C. Up-gradation of the current versions of software & addition of fresh software

D. Installation of a new Database Management system

KEY B

Justification

Answers at Options A, C & D could at best achieve partial solutions. A robust ERP software system, however, will help integrate all aspects of the business and support online recording as well as speedy analysis & decision support. This could help eliminate multiple legacy systems & help improve business processes. Hence, Option B would be the correct recommendation of the Consultant.

396. The Indian fertilizer industry depends heavily on Government subsidies since they are expected to sell their products to customers at prices far below the cost of production. The Government has evolved a complicated mechanism for deciding the subsidy level for each type of fertilizer depending upon various dynamic factors like the international price of the raw material / finished product, the Rupee/dollar exchange rate, conversion & added costs, etc. The industry association decides to set up a common cloud facility for helping the individual units manage the work of raising regular subsidy claims linked to the various cost

factors as also sales elements, etc. Such a cloud facility would be deemed to be a _____

A. Public Cloud facility

B. Private Cloud facility

C. Community Cloud facility

D. Hybrid Cloud facility

KEY C

Justification

When several businesses share a common cloud computing resource, it is called a community cloud facility. Hence, Option C is correct whereas the other options are incorrect.

397. One of your client's managers tells you that they have recently opted for some cloud computing facilities. Being a non-IT official, he says he does not understand what exactly is meant by the term but he has been told that they have opted for a model of Infrastructure as a Service (IaaS). With your own background knowledge of the subject, you explain to him that an IaaS model involves _____

A. Provision of processing, storage networks & other basic computing resources

B. Provision of various types of software on the cloud which can be used by any client

C. Provision of hardware & operating system platform alone

D. Provision of manpower on remote access basis

KEY A

Justification

The Iaas model involves provision of processing, storage networks & other basic computing resources as brought out in Option A. Hence, the other options are incorrect.

398. Your client hires the services of an e-auction platform for launching its reverse auction for purchase of various raw materials. The client accesses the platform through the internet. Several suppliers register themselves with the platform & participate in the reverse auction on the planned date. Which model of e-commerce would this fall in _____

A. Business-to-Government

B. Business-to-consumer

C. Business-to-business

D. Consumer-to-consumer

KEY C

Justification

This would obviously be a case of a business-to-business model &, hence, only Option C is correct.

399. The Tamil Nadu State Government has announced that payment of house taxes, electricity bills, etc. can be made by citizens through the respective portals using internet banking or credit / debit cards. Which model of e-commerce would this fall in _____

A. Business-to-business

B. Business-to-Government

C. Consumer-to-consumer

D. E-Government

KEY D

Justification

This would obviously be a case of E-Government, facilitating payment of taxes & bills through an Internet based facility. Hence, only Option D is correct.

400. You are a Google account holder. Google informs you that they have begun to offer cloud computing facilities to its users & that, as an existing user, you will be allowed up to 15 GB of data storage on the cloud free of cost & thereafter, a nominal $ 0.026 per GB per month. Delighted, you begin using the facility with your laptop. Soon, you receive an alert on the system that you have exhausted the 15 GB free storage space & would need to begin paying for securing more storage space. Which of the characteristics of Cloud computing does this demonstrate ?

A. Resource Pooling

B. Network access from any device

C. Measured services & on-demand self-service

D. Access to software & computing capabilities

KEY C

Justification

In the given instance, the client is being offered measured services & on-demand self service as brought out in Option C. The example does not throw up any specific information about Resource pooling or facility for accessing the cloud through any device other than the laptop being used. It does not also speak of other Cloud computing services like access to software, etc. Hence, only Option C is correct.

401. The Bring Your Own Device (BYOD) concept _____

A. Envisages permitting employees to use their own personal devices for official work

B. Envisages permitting employees to do their personal work on official devices

C. Is a risk free & beneficial system for corporate

D. Envisages storage of both official & personal information on the same device without any demarcation

KEY A

Justification

The BYOD concept envisages permitting employees to use their own personal devices for official work. It has the advantage of saving IT infrastructure expenditure & convenience for employees. It does not envisage usage of company properties by employees for their personal work. While it has many advantages, it is vulnerable to some risks. In general, when the same device is used both for personal as well as official use, virtual demarcation is made of the information storage system & adequate firewalls incorporated. Thus, Option A alone is correct.

402. eXtensible Markup Language or XML _____

A. Describes how data can be presented in the form of web pages

B. Involves use of pre-determined tags

C. Is a platform-independent, standard data exchange format

D. Is less powerful than Hypertext Markup Language or HTML

KEY C

Justification

As indicated in Option A above, XML is a platform-independent, standard data exchange format. It performs presentation, communication & storage of data. It does not involve use of pre-determined tags; instead, users need to define their own tags. XML is more powerful than HTML since it facilitates automatic manipulation & interpretation of data. Thus, Option C alone is correct.

403. eXtensible Markup Language or XML _____

A. Can handle data transfer only when the data is in a compatible format

B. Facilitates exchange of data even in incompatible formats

C. Is supported only by some of the major software products

D. Involves use of pre-determined tags

KEY B

Justification

The main strength of XML is its ability to create data in a format which can be read by different applications. It is portable, supported by major software products & is in easily readable format. It does not involve use of pre-determined tags; instead, users need to define their own tags. Hence, Option B is correct.

404. A limitation of eXtensible Markup Language or XML is that it _____

A. Software developers do not build their new products on it, limiting interoperability

B. Can handle data transfer only when the data is in a compatible format

C. Is less powerful than Hypertext Markup Language or HTML

D. Lacks inherent security; any means of validation, confidentiality or integrity

KEY D

Justification

One weakness of XML is that it lacks inherent security, any means of validation, confidentiality or integrity. However, its main strength is its ability to create data in a format which can be read by different applications & can handle data even when it is not in compatible format. It is supported by major software products & is in easily readable format. XML is, in fact, more powerful than HTML since it facilitates automatic manipulation & interpretation of data. Hence, Option D is correct.

405. An advantage of eXtensible Business Reporting Language or XBRL over eXtensible Markup Language or XML is that the former _____

A. Can help create data that can be read by different applications

B. Is portable and vendor neutral

C. Is a standard that has been accepted & adopted the world over

D. Provides a standard format for data exchange

KEY C

Justification

As indicated in Option A above, XBRL has the advantage of being a standard that has been accepted and adopted the world over. The other answers in Options A B and D are equally applicable both to XML as well as XBRL. Hence, the correct answer is only in Option C.

406. An advantage of eXtensible Business Reporting Language or XBRL over eXtensible Markup Language or XML is that the former _____

A. Is much faster and allows real-time preparation of reports

B. Provides a standard format for data exchange

C. Is portable and vendor neutral

D. Can help create data that can be read by different applications

KEY A

Justification

As indicated in Option A above, XBRL has the advantage of facilitating faster and real-time preparation of business reports. The other answers in Options B to D are equally applicable both to XML as well as XBRL. Hence, the correct answer is only in Option A.

407. An advantage of eXtensible Business Reporting Language or XBRL over eXtensible Markup Language or XML is that the former _____

A. Provides a standard format for data exchange

B. Is portable and vendor neutral

C. Can express more than one relationship amongst elements

D. Can help create data that can be read by different applications

KEY C

Justification

As indicated in Option A above, XBRL has the advantage of being capable of expressing more than one relationship amongst elements, such as multiple hierarchies. This is because it defines relationships separately from elements, unlike XML. The answers in Options A B and D are equally applicable both to XML as well as XBRL. Hence, the correct answer is only in Option C.

408. A feature of eXtensible Business Reporting Language or XBRL which is not found in eXtensible Markup Language or XML is that the former _____

A. Uses Taxonomy & Instance documents

B. Uses XML standard

C. Can define elements & relationships for data used internally

D. Is supported by XML validation tools

KEY A

Justification

As indicated in Option A above, XBRL uses Taxonomy (procedure for creating files with relevant business terminology, etc. along with the rules that they must follow) & Instance documents (documents containing the data in well-formed XML.) The answers in Options B to D are applicable equally both to XML as well as XBRL. Hence, the correct answer is only in Option A.

409. CAs need to be well versed with the benefits & control issues of eXtensible Business Reporting Language or XBRL because _____

A. It uses XML standard

B. More and more countries are mandating the use of XBRL

C. It can define elements & relationships for data used internally

D. It is supported by XML validation tools

KEY B

Justification

As indicated in Option B above, more and more countries are mandating the use of XBRL because it has been validated and declared as a standard. It also has the advantages of being able to ensure compatibility with regulatory standards, improved data quality & is faster in report preparation. The answers in Options A, C and D are applicable equally both to XML as well as XBRL &, hence, cannot account for the significant difference in importance of XBRL. Hence, the correct answer is only in Option B.

410. Which of the following is an example of Social Media _____

A. LinkedIn

B. Times of India newspaper

C. Society monthly magazine

D. National Geographic magazine

KEY A

Justification

Social media is social interaction among people in which they create, share or exchange information & ideas in virtual communities and networks. LinkedIn as an example of social networking is an example of social media. The other instances are examples of magazines and newspapers which do not fall within the ambits of social media. Hence, the correct answer is only in Option A.

411. State True or False. In Social Media, content is supplied and managed by user himself through the use of tools and platforms supplied by social media sites.

A. TRUE

B. FALSE

KEY A

Justification

Social media is social interaction among people in which they create, share or exchange information & ideas in virtual communities and networks. Social media sites like Facebook do allow users to supply & manage content using the tools and platform provided by the sites. Hence, the correct answer is as in Option A.

412. What is the major aspect of Social Media which is relevant to business, in general

_____

A. It helps sell more software related to tools of social media

B. It renders physical markets and direct contact with customers redundant

C. It facilitates a platform for business to interact with customers

D. It is relevant only to members of the higher income group in society

KEY C

Justification

Social media is social interaction among people in which they create, share or exchange information & ideas in virtual communities and networks. It provides businesses a platform to interact with customers to conduct market research, carry out sales promotion, reward campaigns, etc. The prospect of selling relevant software is not a generalized benefit but restricted to a narrow spectrum of business. While it does increase the importance of presence in social media, it does not, necessarily, reduce the importance of physical markets & direct customer contact. It is also not true to say that social media is more relevant only to members of the higher income group in society. Hence, the correct answer is as in Option C.

413. Breach of privacy, fear of legal action, potential for negative reputation, etc. are potential risks for business leveraging social media. What is the other major type of risk which a CA may have to address _____

A. The risk of ignoring customers who are not members of the social media

B. The risk of development of new social media platforms

C. The risk of use of social media by employees on organization networks/devices

D. The risk of the collapse of all social media

KEY C

Justification

The risk of use of social media by employees on organization networks and devices is the other major risk which CAs would have to be alert to. For, this could lead to intentional or accidental leak of organizational data as also provide a route for hackers to access the organization's data base. The other risks outlined in Options A B and D are not significant enough to cause concern. Hence, the correct answer is as in Option C.

414. What is one of the important measures required for mitigating security concerns in using Social Media?

A. The organization avoiding use of Social media

B. Creation of & compliance with a robust, comprehensive Social Media policy

C. Banning employees from being members of social media

D. Creating firewalls blocking out potential hackers

KEY B

Justification

The single major initiative that an organization can take is the creation of a robust & comprehensive Social Media policy. Avoiding use of social media is a sub-optimal & escapist solution which will not benefit the organization. Banning employees is too tyrannical a measure to take in an era when most people, particularly, from the younger generation, are members of some form or social media. This may actually deter potential employees from joining the organization. The use of firewalls is required as a matter of standard policy, whether the organization is using social media or not. Hence, the correct answer is as in Option B.

415. How is Geolocation different from Global Positioning System (GPS) ?

A. It is not different; it is just another term for GPS

B. Geolocation ascertains location of satellites rather than individuals/devices on the earth

C. Geolocation helps identify the ideal location for installation of disaster recovery systems

D. Geolocation focuses more on a meaningful location rather than mere geographical co-ordinates

KEY D

Justification

Geolocation, as brought out in Option D above, focuses more on a meaningful location rather than just determining the bare geographical co-ordinates which GPS. Hence, the correct answer is as in Option D.

416. State True or False. A major risk involved with the use of Geolocation services is the concern of source, ownership & misuse of data owing to involvement of multiple data controllers.

A. TRUE

B. FALSE

KEY A

Justification

One of the major risks involved with the use of Geolocation services is, indeed, the concern regarding source, ownership & misuse of data arising from the involvement of multiple data controllers. Hence, the correct answer is as in Option A.

417. The Business Information System used for handling structured problems as also doing routine transactional jobs is _____

A. Transaction Processing System or TPS

B. Decision Support System or DSS

C. Executive Support System or ESS

D. Structured Query Language or SQL

KEY A

Justification

The Business Information System used for handling structured problems as also transactional jobs is the Transaction Processing System or TPS. DSS & ESS are higher level systems which aim more at problem solving & also address strategic concerns. Hence, the correct answer is as in Option A.

418. The Business Information System which provides answers to semi-structured problems used for handling structured problems & for validation of business decisions is _____

A. Structured Query Language or SQL

B. Transaction Processing System or TPS

C. Decision Support System or DSS

D. Executive Support System or ESS

KEY C

Justification

The Business Information System used for handling semi-structured problems & for validation of business decisions is the Decision Support System or DSS. TPS address lower level needs while ESS deals with higher level systems which aim more at problem solving & also address strategic concerns. Hence, the correct answer is as in Option C.

419. The Business Information System which provides answers to un-structured problems & supports Executive management in planning strategy & vision is _____

A. Structured Query Language or SQL

B. Executive Support System or ESS

C. Transaction Processing System or TPS

D. Decision Support System or DSS

KEY B

Justification

The Business Information System used for handling un-structured problems & for supporting Executive management in planning strategy & vision is validation of business decisions is the ESS. TPS & DSS address lower level needs. Hence, the correct answer is as in Option B.

420. In an inter school competition on Artificial Intelligence, four children develop software which perform the following different functions respectively. Which of them is a correct example of the use of basic Artificial Intelligence ?

A. A calculation software which arrives at the arithmetic total of figures keyed in

B. A password system which allows access based upon keying in of the correct password

C. Predictive & self learning word-processing software

D. A software which rejects invalid dates like 32nd March 2014

KEY C

Justification

The word-processing software pops up suggested words based upon the first few words keyed in by the user. Also, when the user keys in a new word which is not available in its repertoire, it adds it to its collection & reflects it as an option the next time similar letters are initiated. In effect, the software is able to observe & record patterns and improves through 'learning'. The other answers in Options A B and D involve the basic computing functions of a computer which is based on a 'go / no-go' logic which does not involve pattern recognition or further learning. Hence, the correct answer is only as in Option C which displays characteristics of artificial intelligence.

421. Artificial Intelligence works with the help of two concepts; one of them is Artificial neurons. The other is ?

A. 'If-then' statements and logics

B. 'What-if' scenarios

C. The four 'W's What, When, Where & Why

D. 'How-Why' statements

KEY A

Justification

Artificial intelligence works with the help of Artificial neurons as also 'If-then' statements /logics. The answers in the other options are no correct. Hence, the correct answer is only as in Option A.

422. Artificial Intelligence works with the help of two concepts; one of them is Artificial neurons. The other is ?

A. 'What-if' scenarios

B. The four 'W's What, When, Where & Why

C. 'If-then' statements and logics

D. 'How-Why' statements

KEY C

Justification

Artificial intelligence works with the help of Artificial neurons as also 'If-then' statements /logics. The answers in the other options are no correct. Hence, the correct answer is only as in Option C.

423. An Expert System _____

A. Is a software that supersedes the operation of other software

B. Is a panel of software experts who are consulted for solving security threats

C. Is a computer hardware that manages other hardware in a computer system

D. Is a software that comprises specialized human knowledge in a specific, narrow domain

KEY D

Justification

As indicated in Option A above, an Expert system is a software that contains a significant portion of the specialized knowledge of one or more human experts in a specific, narrow domain. The answers given in the other options are not correct . Hence, the correct answer is only as in Option D.

424. A characteristic of Expert Systems is _____

A. They cannot be used in embedded systems

B. They will have either a knowledge base or a set of rules for application, not both

C. They are used for structured logic like if- then-else

D. They are best suited to situations not requiring precision & error-free operations

KEY C

Justification

As indicated in Option A above, Expert systems are used for structured logic like if-then-else. They are best suited to situations requiring precision and error-free operations & hence, are best suited for use in embedded systems, atomic power plants, space stations, etc. They will have both a knowledge base as well as a set of rules for application. Hence, the correct answer is only as in Option C.

425. You have received an alert about the due date for payment of your post paid mobile phone charges. You log on to the service provider's website and attempt to transfer the payment through net banking. However, while you were able to complete the formalities involved at your bank's portal, the system hangs later on and a message is flashed saying that there is a problem with the service provider's system & asking users to try later. This is an issue with the service provider's _____

A. Transaction Processing System

B. Expert systems

C. Decision Support systems

D. Executive Support systems

KEY A

Justification

The service provider's transaction processing system has obviously failed & hence the difficulty the user is facing in completing the payment process for his bill. The answers in the options B to D are incorrect. Hence, the correct answer is only as in Option A.

426. You are an active player on the stock market & place buy / sell orders for shares throughout the working day with your broker. In the middle of a day characterised by particularly volatile movements in share prices & potential risk of losses, you wish to make an assessment of your positions. However, when you speak to your broker and ask him for a report of the transactions carried out on that day till that point of time, the broker responds saying that you would be able to access an online report by the end of the day, for all the transactions of the day at one go. This is an example of _____.

A. Online Transaction Processing system

B. Online Expert System

C. Batch Transaction Processing System

D. Online Executive Support systems

KEY C

Justification

The service provider's transaction processing system obviously operates on a batch process & reports are run at the end of a particular period, in this case, one day. The answers in Options A, B and D are wrong. Hence, the correct answer is only as in Option C.

427. You are an active player on the stock market & place buy / sell orders for shares throughout the working day with your broker. In the middle of a day characterised by particularly volatile movements in share prices & potential risk of losses, you wish to make an assessment of your positions. You speak to your broker and ask him for a report of the transactions carried out on that day till that point of time. The broker responds saying that you could access their website & be able to generate a report at any point of time in the day & get a report for all the transactions of the day at one go. This is an example of _____

A. Online Transaction Processing system

B. Online Executive Support systems

C. Online Expert System

D. Batch Transaction Processing System

KEY A

Justification

The service provider's transaction processing system obviously operates on online transaction processing system since transactions are reflected in their reports at any point of time in the day. Hence, the answers in Options B to D are wrong. The correct answer is only as in Option A.

428. Your client is in the process of growing his business from the level of a Small & Medium Business into a larger organization. His operations have been computerized & customer transactions are being managed reasonably well. However, in order to take the next leap forward, he would like to get more insights into his business, appreciate customer needs better and would like data from his systems help him take business decisions which would propel him towards his goal of an enlarged business. You realise that his existing computer systems are basically Transaction Processing Systems (TPS) and he needs to transform them into Decision Support Systems (DSS) to enable him achieve his objective. One of the major advantages of DSS over TPS is _____

A. It can handle huge amounts of data from various sources

B. It responds rapidly

C. It is reliable

D. It provides information which helps the manager assess alternatives & choose the best

KEY D

Justification

DSS have as their primary role the provision of information which can help a manager take a decision. The answers in Options A ,B and C are applicable to TPS too and are not exclusive to DSS. Hence, the answers in Options A, B to C are wrong. The correct answer is only as in Option D..

429. State TRUE or FALSE. 'Decision Support Systems can support both semi-structured as well as structured problems; they can be useful both to operational as well strategic decision-making'

A. TRUE

B. FALSE

KEY A

Justification

DSS have the capability to support both semi-structured as well as structured problems. Their configuration is such that they can be used by managers as an aid to both operational as well as strategic decision-making. Hence, the above statement is true and Option A is correct.

430. A KEY differentiator for a Decision Support System over a Transaction Processing System is _____.

A. It can handle large amounts of data in batch as well as online mode

B. It is more interactive & model-driven, performing mathematical & qualitative analysis

C. It has a larger database as compared to the transaction processing system

D. It can more reliably handle large volume of information relating to transactions

KEY B

Justification

Decision support systems are far more interactive and model-driven, as brought out in Option A above. The answers in Options A,C and D are not correct and probably relate more to Transaction processing systems. They are surely not **KEY d**ifferentiators. Hence, the correct answer is only as in Option B.

431. The type of software support system which would generally be suited for top-level decision-making, like spinning-off a portion of the company, acquiring another company, entering a new business, etc. is _____

A. Decision Support System

B. Data Base Management System

C. Executive Support System

D. Delphi system

KEY C

Justification

Executive support systems are the appropriate choice for such top-level decision making support, as brought out in Option C above. The answers in Options A, B and D are not correct. The correct answer is only as in Option C.

432. Executive Support Systems address _____

A. External, un-structured and uncertain information through a structured approach

B. Internal & structured information through a un-structured approach

C. Day-to-day information for operational control & monitoring

D. Analysis of routine transactional data

KEY A

Justification

Executive support systems are the appropriate choice for top-level decision making support. They are futuristic and deal with the macro world & potential changes in the environment & changed times. Hence, intrinsically, it deals with uncertain information substantially into the future but through a structured, well thought out approach. Hence, the answer in Option A above is correct. The answers in Options B to D are not correct.

433. Big Data refers to _____

A. Data connected to the top few companies in each industry

B. Trillions of records from various sources with potentially high value

C. Data related to space research, involving great distances in the galaxy

D. Data relating to the largest selling products of each organization

KEY B

Justification

Big Data refers to a large collection of data from various sources with potentially high value. The high value emanates from the insights which it is possible to derive from a careful analysis of the available data. Hence, the answer in Option B above is correct. The answers in Options A C and D are not correct.

434. The main value of Big Data arises from _____

A. Having more data than the competition

B. Having comprehensive information about all aspects of the business

C. Insights that can be gleaned about niche customers from large data

D. Its ability to cover all transactions with customers

KEY C

Justification

Data collection in large quantities, per se, carries limited value. It is the careful analysis of humongous volumes of data to elicit patterns of customer behaviour, market trends, etc. that are the major prize won through Big Data. Such exercises help companies to tap new markets, implicit demand, etc. and thus, be one up on the competition. Hence, the answer in Option C above alone is correct. The answers in Options A B and D are not correct.

435. What is the major control aspect of dealing with Big Data which a Chartered Accountant needs to be aware of ?

A. Privacy, security & legal aspects of dealing with customer & other parties' information

B. Providing adequate storage space for the large volumes of data

C. Instituting adequate steps for collection & collation of the data

D. Ensuring adequate storage security through redundancy

KEY A

Justification

There are potential risks involved in collecting, storing & utilising customer data. There is a need for ensuring the entire process is carried out in a legal manner without causing dis-comfort or loss of faith with the customer. Protecting information passed on by a customer based upon trust, is another **KEY A**spect. Thus, the answer in Option A above is correct & the other answers are wrong.

436. Returning from school one day, your daughter cannot wait to talk about what they taught her on that day regarding environmental degradation & global warming. She tells you that electricity is generated by power plants to meet our energy needs but they are, at the same time, releasing greenhouse gases like Carbon dioxide which contribute to global warming, leading to cascading effects. An impact of this sort, created by an organization, individual or activity is referred to as _____

A. Carbon credits

B. Carbonification

C. Carbon footprint

D. Oxidisation

KEY C

Justification

The level of green house gases generated by activities & actions of an individual or organization is referred to as a 'carbon footprint'. Hence, the girl's description of her learnings at school refer to the carbon footprint of setting up a power plant. Thus, the answer in Option C above is correct & the other answers are wrong.

437. Apart from the conscious choices of minimising the carbon foot print & networking hardware, Green Information Technology involves _____

A. Use or organic products in the organization

B. Minimizing use of water in the organization

C. Avoiding air conditioning, utilising natural cooling and light

D. Minimization of computer devices' energy consumption

KEY D

Justification

The third of the choices to be made in Green Information technology is minimization of computer devices' energy consumption over their life cycle, as indicated in Option D above. The answers in the other options are not correct.

438. One of following actions could be an intrinsic part of Green Information Technology implementation _____

A. Moving back storage & processing capacity from the cloud

B. Replacing a single server system with multiple servers

C. Installation of automatic shutdown/power-up processes

D. Avoiding replacement of old equipment with new ones

KEY C

Justification

The answers in Options A, B and D would act, by and large, counter to the goals of Green information technology. Moving to cloud computing helps improved utilisation of resources; similarly, a single server system is probably more energy efficient than multiple servers. Though it may appear worthwhile continuing to sweat old equipment, new equipment are generally more energy efficient and can more than compensate the benefits of retaining the old equipment. The answer in Option C, however, is relevant & will make a meaningful contribution to the goals of Green IT. Hence, only Option C is the correct answer.

439. One of the initiatives in Green Information Technology implementation could be _____

A. Using single power efficient server combined with virtualization

B. Avoiding replacement of old equipment with new ones

C. Replacing a single server system with multiple servers

D. Moving back storage & processing capacity from the cloud

KEY A

Justification

The answers in Options B to D would act, by and large, counter to the goals of Green information technology. Though it may appear worthwhile continuing to sweat old equipment, new equipment are generally more energy efficient and can more than compensate the benefits of retaining the old equipment. Moving to cloud computing helps improved utilisation of resources; similarly, a single server system is probably more energy efficient than multiple servers. The answer in Option A, however, is relevant & will make a meaningful contribution to the goals of Green IT. Hence, only Option A is the correct answer.

440. Effective Green Information Technology implementation could involve _____

A. Replacing a single server system with multiple servers

B. Avoiding replacement of old equipment with new ones

C. Using power efficient hardware & thin clients

D. Moving back storage & processing capacity from the cloud

KEY C

Justification

The answers in Options A, B and D would act, by and large, counter to the goals of Green information technology. Moving to cloud computing helps improved utilisation of resources; similarly, a single server system is probably more energy efficient than multiple servers. Though it may appear worthwhile continuing to sweat old equipment, new equipment are generally more energy efficient and can more than compensate the benefits of retaining the old equipment. The answer in Option C, however, is relevant & will make a meaningful contribution to the goals of Green IT. Hence, only Option C is the correct answer.

441. An useful step in Green Information Technology implementation could be _____

A. Setting of clear goals for power reduction, decreased carbon footprint, etc.

B. Replacing a single server system with multiple servers

C. Avoiding replacement of old equipment with new ones

D. Moving back storage & processing capacity from the cloud

KEY A

Justification

The answers in Options B to D would act, by and large, counter to the goals of Green information technology. Moving to cloud computing helps improved utilisation of resources; similarly, a single server system is probably more energy efficient than multiple servers. Though it may appear worthwhile continuing to sweat old equipment, new equipment are generally more energy efficient and can more than compensate for the benefits of retaining the old equipment. The answer in Option A, however, is relevant & will make a meaningful contribution to the goals of Green IT. The setting of clear goals helps direct focus to the effort. Hence, only Option A is the correct answer.

442. What is characteristic of Web 2.0 ?

A. Communication from one person/unit to many

B. HTML Web pages & email newsletters

C. Facilitates collaboration & information sharing online

D. Two-way communication not possible

KEY C

Justification

The Web 2.0 version is a two-way communication facility covering blogs, wikis and social networking sites. It facilitates collaboration & information sharing online, as indicated in Option C. It is not a case of communication from only one person to many. It is also an improvement over the Web 1.0 version which comprised HTML web pages & email newsletters. Hence, Option C is the correct answer.

443. What is a distinguishing feature of Web 3.0 ?

A. Communication from one person/unit to many

B. Facilitates convergence of mobile phones, smartphone apps, etc.

C. HTML Web pages & email newsletters

D. Two-way communication not possible

KEY B

Justification

The Web 3.0 version is an evolving system which is an improvement over Web 2.0. It facilitates convergence of mobile phones, smart phone apps, tablets, etc. It is not a case of communication from only one person to many. Like Web 2.9, it is also an improvement over the Web 1.0 version which comprised HTML web pages & email newsletters. Hence, Option B is the correct answer.

444. What is one of the controls that can be practically established for overcoming the risks of Web 2.0 without compromising on operational efficiencies ?

A. Blocking social networking sites like Facebook

B. Restricting access to blog sites

C. Blocking access to forums

D. Using extended validation, SSL certification for websites

KEY D

Justification

Blocking out features like social networking, forums, blogs, etc. would prevent utilization of some of the KEY features of Web 2.0 and, hence, would be a sub-optimal approach. It would be better to build in preventive measures like website validation, as brought out in Option D. Hence, Option D is the correct answer.

445. One practical control that can be established for overcoming the risks of Web 2.0 without compromising on operational efficiencies is ?

A. To develop & implement internal policies for safeguarding against risks

B. Restricting access to blog sites

C. Blocking access to forums

D. Blocking social networking sites like Facebook

KEY A

Justification

Blocking out features like social networking, forums, blogs, etc. would prevent utilization of some of the KEY features of Web 2.0 and, hence, would be a sub-optimal approach. It would be better to draw up a robust policy which addresses all the potential risks of Web 2.0 and the preventive measures required to minimizing them. Hence, only answer in Option A is correct.

446. What is an example of Click jacking ?

A. Malicious take-over of a computer on remote basis

B. Stealing files in a computer from a remote location

C. Stealing of keyed in credentials information

D. Resolution of software issues on a device from remote location

KEY C

Justification

Click jacking is the malicious stealing of keyed in credentials information through a transparent second layer. The answers in Options A,B and D are incorrect; only the answer in Option C is correct.

447. What is the Web of Everything ?

A. Coverage of all theoretical concepts by the Internet

B. Encompasses the Internet as well as all forms of telecommunication

C. Comprises the Internet, all telecommunication as well as satellites

D. Expansion of Internet to objects like cars, refrigerators, etc.

KEY D

Justification

The Web of Everything or the Internet of Everything is the integration of objects like cars, refrigerators, etc. into the internet. It basically merges the physical world with the digital world. The answers in Options A B and C are incorrect; only the answer in Option D is correct.

448. What is 3D printing ?

A. Printing of a 3 dimensional video or movie on to paper

B. Technology for printing images on paper in 3-dimensional form

C. An additive manufacturing process for printing 3-dimensional objects

D. Technology which permits printing of images incorporating movement/change

KEY C

Justification

3D printing in an exciting development in printing technology which permits the use of various types of materials, including metals, to create 3 dimensional objects. This is done through a process of additive manufacturing (AM) and can be used for creating virtually any 3 dimensional object. Answer at Option C is, hence, correct whereas the other answers are wrong.

449. Which is one of the major areas of emerging technology wherein CAs need to play a KEY role ?

A. Management of social media & the risks associated with it

B. Development of new software technology

C. New techniques of marketing of products

D. Developments in the field of integrated circuits

KEY A

Justification

One major area of importance to CAs in the changing global environment is that of management of social media & the risk associated with it. For, organizations are increasingly shifting their marketing focus from the physical to the virtual market, exploiting the strengths of the Internet. As more and more products get linked to the Internet, the value of social media will increase tremendously as will the risks associated with it. Hence, Option A is the correct answer. The other answers from Options B to D are not correct.

450. Which one of the following is a KEY Area to be focussed upon by CAs in the current era of emerging technologies ?

A. New techniques of marketing of products

B. Developments in the field of integrated circuits

C. Security of Systems and Data

D. Development of new software technology

KEY C

Justification

Apart from social media, the other major area of importance to CAs in the changing global environment is security of systems and data. With the explosion of the Internet & connected devices and expanded use of the Internet, the number of interfaces between an organization & its customers / stake holders has grown exponentially. As a consequence, security risks have mushroomed & the CA would have to focus on this as a KEY element driving not just the success of an organization but also in preventing failures in the organization. Thus, the answer in Option C is the correct answer. The other answers from Options A, B and D are not correct.

451. Information System Audit encompasses independent review & evaluation of _____

A. Automated information systems, related manual systems & their interfaces

B. All computerised information systems alone

C. All financial information stored in computers

D. All financial & regulatory information stored in computers

KEY A

Justification

IS Audit encompasses all automated information systems (containing both financial as well as non-financial information), related manual systems and the interfaces between them. Hence, Answer at Option A is correct & the other answers are incorrect.

Module 2
Information Systems Assurance Services

452. In COBIT 5 enablers are factors that influence that something will work in governance & management of enterprise IT. How many such categories of enablers does the COBIT 5 system identify ?

A. 7 categories of enablers

B. 5 categories of enablers

C. 8 categories of enablers

D. 10 categories of enablers

KEY A

Justification

COBIT5 is a framework for governance & management of enterprise IT. It helps organizations manage risk & ensure compliance, continuity, security & privacy. One of its 5 KEY principles is meeting stakeholders' needs. This principle creates value by balancing the benefits against the optimization of risk & the use of resources. The system identifies 7 categories of enablers that facilitate governance & management of enterprise IT. Hence, the answer in Option A is correct and the other options are wrong.

453. Guidance on evaluating and assessing the internal controls implemented in an enterprise is available in _____

A. MEA 02 of COBIT 5

B. ITAF 1200 series

C. IS/IEF 27001

D. ITAF 1400 series

KEY A

Justification

COBIT5 is a framework for governance & management of enterprise IT. MEA 02 of COBIT5 is a process which provides guidance on evaluating and assessing the internal controls implemented in an enterprise. Hence, the answer in Option A is correct and the other options are wrong.

454. You have been engaged as a Consultant to carry out IS Audit of a large organization. What is the first step you would take while commencing your work ?

A. Commence auditing of the financials

B. List all the software and hardware used in the organization

C. Peruse financials for the previous three years

D. Identify all risks present in the IT environment of the organization

KEY D

Justification

The first step in audit engagement is risk assessment based upon which the auditing programme can be developed, giving more importance to high risk areas. Thus, the auditor needs to identify all the risks present in the IT environment of the organization. Hence, the answer in Option D is correct and the other options are wrong.

455. What is the minimum frequency of risk assessment to be carried out as per ISACA guidelines ?

A. Once in 6 months

B. Once in 3 years

C. Once a year

D. Once in 2 years or whenever any major change in systems takes place

KEY C

Justification

The minimum frequency of risk assessment to be carried out as per ISACA guidance is one year. Hence, the answer in Option C is correct and the other options are wrong.

456. State TRUE or FALSE. As per ISACA guidance, the IS auditor can complete the risk assessment process and present the final findings to the stake holders. The auditor needs to maintain his independence and does not need to seek the specific approval of the stake holders for the findings.

A. FALSE

B. TRUE

KEY A

Justification

As per ISACA guidance, the IS auditor needs to seek approval of the risk assessment from the audit stake holders and other appropriate parties Hence, the statement in the question stem is false & the answer in Option A is correct.

457. State True or False. Standards on Risk assessment pertaining to IS Audit are different from those prescribed by ICAI under SA315. IS Audit follow a different set of standards laid down by ISACA.

A. TRUE

B. FALSE

KEY B

Justification

The standards on risk assessment pertaining to IS audit as prescribed by ICAI under SA315 are also applicable to risk assessment under IS Audit. Hence, the statement in the question stem is false & the answer in Option B is correct.

458. For effective risk assessment, auditors should ideally supplement the regular risk assessment procedures with _____

A. Observation, inspection & analytical procedures

B. Interviews with client's competitors

C. Intensive analysis of historical data

D. Interviews with client's suppliers

KEY A

Justification

While the risk assessment procedures outlined by ISACA, ICAI, etc. provide a ready-made template that helps ensure typically vulnerable areas to be captured, observation, inspection & analytical procedures help zero in on risk areas which are peculiar to the particular business or specific period of time. The approaches in the other options may also add value but may not be as significant as that achievable through the answer at Option A. Hence, the statement in the question stem is false & the answer in Option A is correct.

459. The ideal risk assessment technique _____

A. Is a computerized scoring system based upon evaluation of risk factors

B. Is judgemental, based upon the auditor's personal assessment

C. Depends upon the complexity level & detail appropriate for the organization

D. Is a combination of computerized scoring & judgemental system

KEY C

Justification

The ideal risk assessment technique depends upon the complexity level & detail appropriate for the particular organization. It could be one or a combination of more than one technique. Hence, the statement in the question stem is false & the answer in Option C is correct.

460. An IS Auditor carries out a preliminary visit to his client's site to get a feel of the operations and identify risks, if any, missed out during his initial study of the records of the organization. In the server room, he feels uncomfortable and realizes that the humidity level as well as the ambient temperature are quite high. On further probing, he discovers that the air conditioning equipment had failed & the original supplier had ceased operations. The administration manager was struggling to find an alternate agency to set the problem right. Also, no fall back system was in place. The IS Auditor is wondering whether this would fall within the purview of his IT General Controls Review. What is your view ?

A. Yes, it would fall within the purview of IT General Control Review

B. No, it would not fall within the purview of IT General Control review

KEY A

Justification

A general control review would include infrastructure and environment controls too. Hence, the answer in Option A is correct.

461. As part of his exploratory trips to his client's office, an IS Auditor meets up with the Server Manager. The manager is despondent and the auditor learns it is because of his network cable supervisor's resignation and impending relief. The manager is unable to find a substitute immediately and dreads the thought of managing any network cabling issues in the interim. The auditor discusses the matter with the manager who feels that the incumbent supervisor is virtually indispensable and he has no subordinate who could step into his shoes.

The auditor probes further and also visits some of the locations wherein cable inspection slots were located. He discovers that the cabling junctions had been done in a very haphazard fashion and were not even labelled. Nor was there any manual or chart identifying the network of cables, their junctions/ports, etc. He realizes that the incumbent supervisor had become indispensable on account of this disorganized cabling system as also the absence of any manual. Ideally, the cabling should have been carried out more scientifically, there should have been a ready-reckoner or manual showing the details of the network and a second-in-

line should have been in place to stand in for the supervisor in the event of his short term absence or resignation.

Would the auditor be well within his rights to include this aspect as a lacuna in the general controls review ?

A. No, he would not be right to include this as a lacuna in his general controls review

B. Yes, he would be right in including this aspect as a lacuna in his general controls review

KEY B

Justification

A general control review would include infrastructure and environment controls too. Hence, the answer in Option B is correct.

462. Is segregation of duties useful as an Organizational control ? Why ?

A. Yes, it reduces employee cost

B. Yes, it reduces fraud risk & facilitates accuracy check of one person's work by another

C. No, it is not an advantage; it increases employee cost

D. No, it complicates the role of the manager who has to manage more employees

KEY B

Justification

Segregation of duties is an important control tool whereby, conflicting roles in particular, are segregated and handled by different individuals. It reduces the risk of fraud since one person cannot independently commit any fraud but would need to collude with the second. Also, since the output of one individual may become the input of another, an independent accuracy check of one person's work by another person becomes a built-in reality. This may increase head-count and, hence, manpower cost but, employed judiciously, the higher manpower cost can be more than compensated by the reduced risks to the organization. Hence, the answer in Option B is correct.

463. A newly appointed Senior executive in an organization, who happened to be a close relative of the promoter, is miffed when the IT Manager refuses access to him to the Server room citing policy guidelines. The executive shares with you, the Auditor of the organization, what he perceives to be insulting behaviour by the IT Manager. You question him about the purpose of the visit and learn that the executive just wanted to have a tour of the facility, as part of his induction. Do you agree or disagree with the executive ? Why ?

A. Yes, I would agree. As a close relative of the promoter, he would surely have the organization's best interests at heart.

B. No, I would not agree. As a new employee, he should not be given access to the server room

C. Yes, I would agree. The server, in any case, would be password protected & no harm can be done

D. No, I would not agree. Physical access control to the server is an important control mechanism

KEY D

Justification

Physical access control to the server room is an important part of IT General controls in any organization. The server is a sensitive equipment with certain commands & settings being exclusive to it. Un-authorized access to it could compromise the security of the IT system & the organization, obviously, has a clearly defined access policy which has to be respected. Relationship to the promoter cannot be an excuse for breaking the policy; if, indeed, he had genuine need to visit the server room, he could have got the necessary clearances. Denial of access cannot be owing to the newness of the employee. Lastly, any robust system operates at different levels of redundancy & the mere existence of password protected access to the server does not prevent a second level of defence, in the form of access control, being done away with. Hence, the answer in Option D is correct.

464. As a measure of IT General control, an organization decides to separate those who can input data from those that can reconcile or approve data. Is this a good move ? Why ?

A. No, it is not a good move; the person who inputs the data is the best person to approve the data too

B. Yes, it is a good move; it can help prevent unauthorised data entry

C. Yes, it is a good move; inputting data & reconciling data requires different skills

D. No, it is not a good move; data entry errors would be compounded

KEY B

Justification

Segregation of duties is an important control tool whereby, conflicting roles in particular, are segregated and handled by different individuals. It reduces the risk of fraud since one person cannot independently commit any fraud but would need to collude with the second. Also, since the output of one individual may become the input of another, an independent accuracy check of one person's work by another person becomes a built-in reality

Hence, the answer in Option B is correct.

465. As a measure of IT General control, an organization decides to separate those who can test programs (e.g. Users) from those who can develop programs (e.g. Application programmers). Is this a good move ? Why ?

A. No, it is not a good move; the person who develops the program is the best person to test it too

B. Yes, it is a good move; program testing and program development require different skills

C. Yes, it is a good move; it can help prevent unauthorised programs from being run

D. No, it is not a good move; significant time would be lost in the process

KEY C

Justification

Segregation of duties is an important control tool whereby, conflicting roles in particular, are segregated and handled by different individuals. It reduces the risk of fraud since one person cannot independently commit any fraud but would need to collude with the second. Also, since the output of one individual may become the input of another, an independent accuracy check of one person's work by another person becomes a built-in reality. In this case, conflict in roles is clearly existing. Time savings could, perhaps, be gained by using the same person but this would mean paying the expensive price of potentially unauthorised programs being run. Hence, the answer in Option C is correct.

466. As a measure of IT General control, an organization decides to separate those who can run live programs (e.g. Operations department) from those who can change programs (e.g. programmers). Is this a good move ? Why ?

A. Yes, it is a good move; it can help prevent unauthorised programs from being run

B. No, it is not a good move; the user dept. knows best & should be allowed to change programs

C. Yes, it is a good move; since the programmers would have no work to do otherwise

D. No, it is not a good move; significant time would be lost in the process & potential savings lost

KEY A

Justification

Segregation of duties is an important control tool whereby, conflicting roles in particular, are segregated and handled by different individuals. It reduces the risk of fraud since one person cannot independently commit any fraud but would need to collude with the second. Also, since the output of one individual may become the input of another, an

independent accuracy check of one person's work by another person becomes a built-in reality. In this case, conflict in roles is clearly existing. Also, while the user dept. may have the need for a change, it is up to the programmer to devise an appropriate method of programming logic to satisfy the user's requirement. Time savings could, perhaps, be gained by using the same person but this would mean paying the expensive price of potentially unauthorised & defective programs being run. Hence, the answer in Option A is correct.

467. Thanks to its growing popularity, a family-run fast food restaurant is transforming itself into a chain of branded restaurants & has created a formal organization structure to manage the growing organization. Having identified young and upcoming IT industry employees as their core base of customers, the family decides to build a strong backbone of IT to facilitate online ordering of food, creation of customer database, etc. Since the immediate primary purpose is to enable online payments for the purchases by customers, the trustworthy family retainer & Junior Accountant is given the responsibility of installing and maintaining the IT system.

As an IS Auditor, do you think the family was right in giving the Junior Accountant the responsibility ? Why ?

A. No. A senior management representative should take responsibility in the interest of IT General Control

B. Yes, since the accountant is the main beneficiary of the IT system

C. No. The Senior Accountant in the chain should have been given the responsibility

D. Yes, this role requires a trustworthy person & the family retainer is the best fit

KEY A

Justification

Responsibility for IT systems should lie with the top management with appropriate delegation to lower levels. This would not only ensure that the highly vulnerable IT systems are properly controlled at the highest levels in the company but also ensure that appropriate IT policies are framed, keeping in mind organizational objectives and goals. The perspective of an accountant, whether junior or senior, would be rather limited to his area of operations and responsibility; it may lack the breadth of vision which would be essential at the top management level as also the interfaces between various functions in the business. In any professional organization, no positive bias can be allowed for the dominance of so-called 'family retainers' however trustworthy they may be. The operations have to be system driven & not personality driven. Hence, the answer in Option A is correct.

468. An important element of Management Control for the Information System in an organization is the Information Technology Steering Committee. The Committee _____

A. Will be exclusively representatives from the IT division

B. Will cover core IT alone, excluding telecommunication, automation systems, etc.

C. Will handle operational issues only; overall goals & strategies would be outside its purview

D. Will include members from all areas of business, apart from IT personnel

KEY D

Justification

The IT Committee in an organization would drive IT in line with organizational goals, vision & mission. It will be manned by senior officials from all areas of the business, apart from IT professionals. Its scope will include all types of IT related operations including telecommunication, automation systems, manufacturing processing systems, etc. Hence, the answer in Option D is correct.

469. A leading exporter of cut & polished diamonds has a specially designed vault for storing its raw as well as processed diamonds. At any point of time, the material stored in the vault is worth several crores of rupees.

The exporter has laid down a clear procedure for operation of the vault. It can be opened or closed using two different keys which are held by the Operations Head and the Finance Head respectively. These officials cannot pass on their individual KEY to the other official or any other official. They have to be necessarily present and operate their KEY themselves. Both at the time of every opening the vault as also every closing of the vault, a vault register is signed by both these officials after filling in relevant information. The vault is also sealed with individual unique seals of these officials & checked every time before the vault is opened afresh. Thus, the vault can be opened only when both these officials are present & a record is also maintained of every transaction. These officials carry their individual keys home but never travel together while coming to the office or while leaving it.

What type of control is being exercised by this Diamond exporter through this process ?

A. Dual Finance Control

B. Physical Access Control

C. Operating System Control

D. Management Control

KEY A

Justification

This is a dual control system which falls under Finance control mechanism since it entails two people simultaneously accessing an asset. Hence, the answer in Option A is correct.

470. What is the first step for an Auditor in an Application software review ?

A. Ascertain the creator of the application software

B. Ascertain the validity of the user licence for the software

C. Ascertain the business function or activity that the software performs

D. Identify the users who have been granted access to the software

KEY C

Justification

The first step for an Auditor is to ascertain the business function or activity that the software performs. The auditor needs to understand the intricacies of the business and the way in which the software facilitates the business. Hence, the answer in Option C is correct.

471. As an IS Auditor reviewing Application software in your new client's organization, you have started by thoroughly understanding the nature of the business and the manner in which the Application software meets the business requirements. What is the next step which you would take in the process of the Application software review ?

A. Identify the users who have been granted access to the software

B. Ascertain the creator of the application software

C. Ascertain the validity of the user licence for the software

D. Check how the software handles the risks associated with the particular area of business dealt with by it

KEY D

Justification

The next important step for an Auditor is to identify the potential risks associated with the business activity/function served by the software & see how the risks are handled by the software. Hence, the answer in Option D is correct.

472. State True or False. IT Application controls are controls which are in-built in the software application itself.

A. FALSE

B. TRUE

KEY B

Justification

IT application controls are, indeed, controls which are in-built in the software application itself. Hence, the answer in Option B is correct.

473. Which of the following are one of the KEY Areas that should be covered during an IS Audit of Application software ?

A. List of authorised users of the software

B. Adherence to business rules in the flow & processing accuracy

C. Validity of software licence

D. Cost of the software & availability of cheaper alternatives

KEY B

Justification

One of the **KEY A**reas to be covered is the software's adherence to business rules in the flow and processing accuracy. The other answers in Options A, C and D are not of immediate relevance or urgency. The answer in Option B is correct.

474. Which of the following are one of the KEY Areas that should be covered during an IS Audit of Application software ?

A. Cost of the software & availability of cheaper alternatives

B. List of authorised users of the software

C. Validations of various data inputs

D. Validity of software licence

KEY C

Justification

One of the **KEY A**reas to be covered is the validation of various data inputs. The other answers in Options A, B and D are not of immediate relevance or urgency. The answer in Option C is correct.

475. Which of the following are one of the KEY Areas that should be covered during an IS Audit of Application software ?

A. Logical access control and authorization

B. Validity of software licence

C. Cost of the software & availability of cheaper alternatives

D. List of authorised users of the software

KEY A

Justification

One of the **KEY A**reas to be covered is logical access control and authorization. The other answers in Options B to D are not of immediate relevance or urgency. The answer in Option A is correct.

476. Which of the following are one of the KEY Areas that should be covered during an IS Audit of Application software ?

A. Validity of software licence

B. Cost of the software & availability of cheaper alternatives

C. Exception handling and logging

D. List of authorised users of the software

KEY C

Justification

One of the **KEY A**reas to be covered is exception handling and logging. The other answers in Options A, B and D are not of immediate relevance or urgency. The answer in Option C is correct.

477. Audit Sampling _____

A. Involves application of audit procedures to less than 100 % of the population

B. Can be carried out only through rigorous statistical sampling

C. Can be applied only for compliance and not for substantive testing

D. Involves use of Auditing standard SA 350 in the auditing process

KEY A

Justification

When it is not practically feasible to check every one of the elements in a population & the population is reasonably random, sampling is resorted to as an indication of the nature of the population as a whole. It can be carried out both through statistical sampling as well as non-statistical sampling. It can be applied both for compliance as well as substantive testing. Auditing standard SA 530 is the relevant one applicable to use of sampling in the auditing process. Hence, the answer in Option A is the correct one.

478. Audit Sampling _____

A. Involves use of Auditing standard SA 350 in the auditing process

B. Can be carried out only through rigorous statistical random sampling

C. For IS Audit can be done using ISACA's guidelines

D. Can be applied only for compliance and not for substantive testing

KEY C

Justification

When it is not practically feasible to check every one of the elements in a population & the population is reasonably random, sampling is resorted to as an indication of the nature of the population as a whole. It can be carried out both through statistical sampling as well as non-statistical sampling. The statistical sampling could be either random or systematic. It can be applied both for compliance as well as substantive testing. Auditing standard SA 530 is the relevant one applicable to use of sampling in the auditing process. ISACA guidelines in this regard can also be followed. Hence, the answer in Option C is the correct one.

479. In IS Audit, sample design would be driven by _____

A. Resource availability & auditor's convenience

B. Type of sampling whether statistical or haphazard/judgemental

C. The advice of the auditee, based upon his past experience

D. Objectives of test & attributes of the population

KEY D

Justification

Sample design would be driven by test objectives and attributes of the population. The sample size & complexity cannot be compromised owing to resource constraint on the part of the auditor; the outcome could be sub-standard. The sampling type chosen would not have that significant impact on the sample size. The auditee's advice will not be the basis for sample design for obvious reasons. Hence, the answer in Option D is the only correct answer.

480. What are CAATs ?

A. Computer Assisted Audit Tools

B. Council for Association of Auditors & Trainers

C. Chartered Accountants' Audit Tools

D. Corporate Audit & Accounting Tools

KEY A

Justification

CAATs are basically computer assisted audit tools which help auditors sift through large volumes of information to identify control issues, defaults, etc. They can greatly enhance the efficiency and effectiveness of IS auditors. The answer in Option A is the correct one.

481. What are some of the KEY reasons for establishing controls and auditing in a computerized environment ?

A. Computers are more prone to make errors in handling subjective big data

B. There is more scope for fraud & error in a computerized environment

C. Data may be entered into the system without supporting documents

D. There is no choice since most operations are computerized

KEY C

Justification

A KEY vulnerability of computerized systems is the fact that, at times, data may be entered into the system without supporting documents. This is a fundamental principle of accounting which we cannot afford to ignore. Hence, the answer in Option C is the correct one. The others are incorrect Computer are not more prone than humans in making errors & one cannot say that there is increased scope for fraud & error in a computerized environment.

482. What are some of the KEY reasons for establishing controls and auditing in a computerized environment ?

A. Transaction trail may be partly in machine language & retained only for a limited period

B. There is more scope for fraud & error in a computerized environment

C. Computers are more prone to make errors in handling subjective big data

D. There is no choice since most operations are computerized

KEY A

Justification

A KEY vulnerability of computerized systems is the fact that, at times, data may be entered into the system without supporting documents. This is a fundamental principle of accounting which we cannot afford to ignore. Another aspect is the fact that transaction trails may not be visible they may be partly in machine language & retained

only for a limited period. Hence, the answer in Option A is the correct one. The others are incorrect Computer are not more prone than humans in making errors & one cannot say that there is increased scope for fraud & error in a computerized environment.

483. What is one of the KEY tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs) ?

A. Projections on future trends for specific parameters

B. Carrying out employees' reference checks

C. Identification of exceptional transactions based upon set criteria

D. Carry out employee appraisals

KEY C

Justification

One of the many Key tests that can be carried out by CAATs is identification of exceptional transactions based upon set criteria. The IS auditor can set the criteria based upon the sort of transactions which are not expected to occur basis the controls which are to have been incorporated in the organization's systems. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options A, B and D above. Hence, answer at Option C alone is correct.

484. What is one of the Key tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs) ?

A. Carry out employee appraisals

B. Identify potential areas of fraud

C. Projections on future trends for specific parameters

D. Carrying out employees' reference checks

KEY B

Justification

One of the many Key tests that can be carried out by CAATs is identification of potential areas of fraud. The IS auditor can set the criteria based upon the sort of transactions which are not expected to occur basis the controls which are to have been incorporated in the organization's systems. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in other options above. Hence, answer at Option B alone is correct.

485. What is one of the Key tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs) ?

A. Carry out employee appraisals

B. Projections on future trends for specific parameters

C. Identify data which is inconsistent or erroneous

D. Carrying out employees' reference checks

KEY C

Justification

One of the many KEY tests that can be carried out by CAATs is identification of data which is inconsistent or erroneous. The IS auditor can set the criteria based upon the sort of data which are not expected to occur basis the controls which are to have been incorporated in the organization's systems. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options A,B and D above. Hence, answer at Option C alone is correct.

486. What is one of the key tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs) ?

A. Carry out employee appraisals

B. Projections on future trends for specific parameters

C. Carrying out employees' reference checks

D. Perform various types of statistical analysis

KEY D

Justification

One of the many key tests that can be carried out by CAATs is the carrying out of various types of statistical analysis which could throw up areas of in-consistencies, defaults, etc. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options A to C above. Hence, answer at Option D alone is correct.

487. What is one of the KEY tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs) ?

A. Establishing whether the set controls are working as prescribed

B. Carry out employee appraisals

C. Projections on future trends for specific parameters

D. Estimation of competitor activity

KEY A

Justification

One of the many KEY tests that can be carried out by CAATs is establishing whether the set controls are working as intended. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options B to D above. Hence, answer at Option A alone is correct.

488. What is one of the KEY tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs) ?

A. Carry out market surveys for a new product launch

B. Projections on future trends for specific parameters

C. Establishing relationship between two or more areas & identify duplicate transactions

D. Estimation of competitor activity

KEY C

Justification

One of the many KEY tests that can be carried out by CAATs is establishing whether the set controls are working as intended. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options A, B and D above. Hence, answer at Option C alone is correct.

489. What is Compliance testing ?

A. Testing any activity in compliance with Government rules and regulations

B. Checking whether the organization has remitted employee provident fund into the relevant account

C. Checking whether the office employees are checking into and leaving the office as per approved working hours

D. Checking whether controls are operated in compliance with management policies/procedures

KEY D

Justification

Compliance testing deals with checking the controls which have been established in the organization rather than checking compliance of any specific activity per se. Hence, answer at Option D alone is correct. The answers in other options deal with the actual activity rather than the controls and, hence, are not correct.

490. What are Substantive tests ?

A. Tests which validate the internal controls exercised over financial transactions

B. Tests which are done only by choice, if required, rather than by default

C. Tests to evaluate the integrity of individual transactions, data, etc.

D. Tests which are not used for checking for monetary errors affecting financial parameters

KEY C

Justification

Compliance testing deals with checking the controls which have been established in the organization. In contrast, Substantive testing tests to evaluate the completeness, accuracy, etc. or the integrity, in general, of individual transactions, data, information, etc. They are carried out in most audits & are often called default procedures. They are often used for checking for monetary errors affecting financial statement balances. Hence, answer at Option C alone is correct. The answers in other options are obviously not correct.

491. How can design effectiveness for compliance for a process be evaluated ?

A. By a walkthrough of the business process and the risk controls

B. By carrying out substantive testing

C. By carrying out compliance testing

D. By checking the financials for errors & inconsistencies

KEY A

Justification

Design effectiveness for compliance for a process can be evaluated by a walkthrough of the business process This will help identifying the existence of controls, the design of the risk controls as well as the accuracy of process documentation. Compliance testing deals with checking the controls which have been established in the organization. In contrast, Substantive testing tests to evaluate the completeness, accuracy, etc. or the integrity, in general, of individual transactions, data, information, etc. In isolation, neither of them will comprehensively address design effectiveness. Merely checking the financials will also not achieve the desired objective. Hence, answer at Option A alone is correct.

492. In IS Audit, Operational Effectiveness _____

A. Refers to effectiveness of the organization's operations

B. Refers to effectiveness of the IS Audit

C. Refers to actual performance of the Control in IT environment

D. Refers to achievements in line with overall organizational strategy

KEY C

Justification

In IS Audit, Operational Effectiveness refers to the actual performance of the Control in IT environment. This is in contrast with the intended design or goal. Answer at Option C alone is correct.

493. In IS audit, for manual controls, documented evidence substantiating control performance as per design is _____

A. Through physical records created when the controls have been operated

B. Through appropriate reports and screen shots from the system

C. Through records of interviews with operational staff

D. Through software trail of the various components of the control process

KEY A

Justification

For manual controls, documented evidence substantiating control performance as per design is through physical records created when the controls have been operated. This can be supplemented by samples of samples to ensure that purported reviews conducted by an individual have actually taken place. Answer at Option A alone is correct.

494. Audit evidence in IS Audit _____

A. Excludes IS Auditor observations, notes from interviews etc.

B. Is not subject to the usual audit rules of sufficiency & competency

C. Is information substantiating alignment with objectives & supporting audit conclusions

D. That which would stand scrutiny in a court of law

KEY C

Justification

Audit evidence in IS Audit is any information that substantiates alignment of that particular aspect with the intended objectives and that also support audit conclusions. Thus, the answer at Option C alone is correct.

495. In IS Audit, when is evidence said to be competent ?

A. When it is given by an individual who is competent

B. When it is both valid and relevant

C. When the evidence is backed by senior management of the organization

D. When the evidence has been historically demonstrated

KEY B

Justification

In IS Audit, evidence is said to be competent when it is both valid and relevant. Thus, the answer at Option B alone is correct.

496. In IS Audit, how is sufficiency of evidence assessed ?

A. Through Audit judgement

B. When the evidence is valid at the two standard deviation level

C. When the evidence is valid at the three standard deviation level

D. When more than 90 % of the relevant transactions can be explained

KEY A

Justification

In IS Audit, sufficiency of evidence is assessed through Audit judgement. Thus, the answer at Option A alone is correct.

497. Which is the ICAI standard on auditing which deals with the Auditor's responsibility to prepare audit documentation for financial statements ?

A. SA 500

B. SA 580

C. SA 230

D. SA 1205

KEY C

Justification

The ICAI standard on auditing which deals with the Auditor's responsibility to prepare audit documentation for financial statements is SA 230. Hence, the answer at Option C alone is correct.

498. Which is the ICAI standard on auditing which deals with what constitutes audit evidence in an audit of financial statements as also with the Auditor's responsibility to design and perform audit procedures ?

A. SA 230

B. SA 500

C. SA 1205

D. SA 580

KEY B

Justification

SA 500 is the ICAI standard on auditing which deals with what constitutes audit evidence in an audit of financial statements as also with the Auditor's responsibility to design and perform audit procedures. Hence, the answer at Option B alone is correct.

499. Which is the ICAI standard on auditing which deals with the Auditor's responsibility to obtain written representations from the management as also those charged with governance ?

A. SA 580

B. SA 230

C. SA 1205

D. SA 500

KEY A

Justification

SA 580 is the ICAI standard on auditing which deals with the Auditor's responsibility to obtain written representations from the management as also those charged with governance. Hence, the answer at Option A alone is correct.

500. Which is the ISACA standard on evidence which IS auditors are required to comply with?

A. 230

B. 1206

C. 500

D. 1205

KEY D

Justification

The ISACA standard on evidence which IS auditors are required to comply with is 1205. Hence, the answer at Option D alone is correct.

501. What are Test working papers in IS Audit Documentation ?

A. Draft of the final IS audit report prepared for the Board of Directors

B. Those prepared or obtained as a result of compliance/testing procedures

C. Draft of the preliminary IS audit report submitted to senior management for comments

D. IS audit team's answers to test questions on the auditee's business & environment

KEY B

Justification

Test working papers in IS Audit documentation are those prepared or obtained as a result of compliance/testing procedures. Hence, the answer at Option B alone is correct.

502. Which is the ISACA standard relating to use of services of external experts ?

A. 1206

B. 230

C. 1205

D. 500

KEY A

Justification

The ISACA standard relating to use of services of external experts is 1206. Hence, the answer at Option A alone is correct.

503. Which is the tool used in IS audit for assessing the proper level of controls ?

A. ISACA method 230

B. Random sampling of transactions

C. A control matrix, comparing known types of errors with known type of controls

D. ICAI guidelines on the appropriate level of controls

KEY C

Justification

The tool used in IS audit for assessing the proper level of controls is the control matrix. This basically involves comparison of known types of errors with known types of controls. Hence, the answer at Option C alone is correct.

504. Prior to reporting a control weakness, an IS auditor _____

A. Should carry out random sampling of transactions

B. Should check whether there are 2 or more weak controls

C. Should check for a minimum of 3 strong controls

D. Should look for compensating controls

KEY D

Justification

Prior to reporting a control weakness, an IS auditor should look for compensating controls. . Hence, the answer at Option D alone is correct.

505. State True or False. Materiality of an IS auditor's findings will not be different for different levels of management. The auditor will have to report his findings impartially & consistently whether it be to the lower echelons of management or senior management.

A. FALSE

B. TRUE

KEY A

Justification

Materiality of an IS auditor's findings to different levels of management would depend upon its significance to each level. Thus, what may be material to a lower level of the management may not be so for the higher level and vice versa. Hence, the cited statement is false & the answer at Option A alone is correct.

506. What is Forensic Audit ?

A. Audit specializing in discovering, disclosing and following up on frauds and crimes

B. Audit relating to the Chemical and Pesticide industry

C. Audit relating to environmental matters, including pollution

D. Audit relating to hospitals and healthcare facilities

KEY A

Justification

Forensic audit specializes in discovering, disclosing and following up on frauds and crimes. It is assuming increasing significance owing to the enhanced risks involved with increased use of IT and globalization. Answer at Option A alone is correct.

507. What are Control Self-Assessments ?

A. These are self- assessments of the auditing process adopted by auditors

B. These are self- assessments by business process owners independent of auditors

C. These are conducted by business process owners but facilitated by auditors

D. These are compliance audits carried out by auditors

KEY C

Justification

Control Self-Assessments are those that are conducted by business process owners on their own but facilitated by auditors. Answer at Option C alone is correct.

508. Protective / Preventative controls and Detective controls are two of the three fundamental types of controls. Which is the third type of control ?

A. Forensic Controls

B. Security Controls

C. Reactive / Corrective Controls

D. Legislative Controls

KEY C

Justification

The third type of Controls is Reactive/Corrective Control. Answer at Option C alone is correct.

509. Reactive / Corrective Controls and Detective controls are two of the three fundamental types of controls. Which is the third type of control ?

A. Protective / Preventative controls

B. Security Controls

C. Forensic Controls

D. Legislative Controls

KEY A

Justification

The third type of Controls is Protective / Preventative Control. Answer at Option A alone is correct.

510. Reactive / Corrective Controls and Protective / Preventative controls are two of the three fundamental types of controls. Which is the third type of control ?

A. Legislative Controls

B. Detective controls

C. Security Controls

D. Forensic Controls

KEY B

Justification

The third type of Controls is Detective Control. Answer at Option B alone is correct.

511. What is Cyber fraud ?

A. A fraud that involves use of computers and computer networks

B. A fraud committed exclusively through the internet

C. A fraud exceeding U.S. $ 1 million in value

D. A fraud involving software alone

KEY A

Justification

Cyber fraud is a fraud that involves use of computers and computer networks. Answer at Option A alone is correct.

512. Which standard of auditing defines fraud & the management's responsibility ?

A. SIA 2

B. SIA 17

C. SIA 11

D. SIA 21

KEY C

Justification

SIA 11 defines fraud & lays the responsibility on the management for prevention & detection of frauds. Answer at Option C alone is correct.

513. A holistic approach to deterrence & prevention of fraud would be ?

A. Focussing on integrity of new recruits

B. Establishing severe punishment for fraud

C. Compensating employees adequately to minimize temptation

D. Strengthening of Governance and management framework

KEY D

Justification

A holistic approach to deterrence and prevention of fraud would require strengthening of governance and management framework. The answers in options A to C address the issue in bits and pieces and, hence, are not the right answers . Answer at Option D alone is correct.

514. State True or False. Computer Forensics deals only with digital evidence acceptable to a court of law; non-digital evidence would not fall under this category.

A. TRUE

B. FALSE

KEY A

Justification

Computer Forensics is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally admissible in legal proceedings. Hence, answer at Option A is correct.

515. Evidence loses its value in legal proceedings in the absence of _____

A. Recency of information

B. Validation by the I.T. dept. of the police

C. Professional maintenance of the chain of custody

D. Authenticated hard copies

KEY C

Justification

Evidence loses its value in legal proceedings in the absence of professional maintenance of the chain of custody. Hence, answer at Option C is correct.

516. Demonstrating integrity & reliability of evidence are KEY for it to be acceptable to law enforcement enforcers. This can be done through identification of evidence,

preservation of evidence including documentation of chain of custody, analysis & interpretation of data and _____.

A. Recency of information

B. Validation by the I.T. dept. of the police

C. Use of authenticated hard copies

D. Presentation to relevant parties for acceptance of evidence

KEY D

Justification

Evidence loses its value in legal proceedings in the absence of professional maintenance of the chain of custody. Hence, answer at Option D is correct.

517. Which is one of the most effective tools and techniques to combat fraud ?

A. Computer Assisted Audit Techniques (CAAT)

B. Threats of severe punishment

C. Validation by the I.T. dept. of the police

D. Use of authenticated hard copies

KEY A

Justification

CAAT is one of the time-tested tools required for carrying out the above exercise. . Hence, answer at Option A is correct.

Module 3

Governance and Management of Enterprise Information Technology, Risk Management & Compliance

518. Distinguish between Enterprise Governance and Corporate Governance.

A. Corporate governance is applying the principles of enterprise governance to the corporate structure of enterprises

B. Corporate governance relates to principles applying to the top management of a company whereas enterprise governance relates to all the employees of the company or enterprise

C. Corporate governance relates to compliance related to regulatory mechanisms whereas enterprise governance relates to protection of shareholders' interests

D. Corporate governance pertains to conformance whereas enterprise governance relates to performance

KEY A

Justification

As indicated in Option A, corporate governance is applying the principles of enterprise governance to the corporate structure of enterprises. The answers in the other Options are not factually correct.

519. Which of the following provides for mandatory Internal Audit and reporting on Internal financial controls for companies in India?

A. Companies Act, 2013

B. IT Act, 2008

C. Sarbanes Oxley Act, 2002

D. Shops and Establishments Act

KEY A

Justification

As indicated in Option A, the Companies Act, 2013, under section 138, provides for mandatory Internal Audit and reporting on internal financial controls. Hence, the answers in the other Options are not factually correct.

520. Which of the following provides for compliance requirements & maintenance of privacy of information for companies in India?

A. IT Act, amended 2008

B. Companies Act, 2013

C. Sarbanes Oxley Act, 2002

D. Shops and Establishments Act

KEY A

Justification

As indicated in Option A, the IT Act amended during 2013 provides for maintaining privacy of information & compliance requirements on management, including penalties for non-compliance. Hence, the answers in the other Options are not factually correct.

521. Which of the following prescribes mandatory audit covering corporate governance as per clause 49 ?

A. IT Act, amended 2008

B. Companies Act, 2013

C. SEBI, for listed companies

D. Sarbanes Oxley Act, 2002

KEY C

Justification

As indicated in Option C, SEBI has provided for mandatory audit as per clause 49 of the equity listing agreement. The audit primarily covers governance. Hence, the answers in the other Options are not factually correct.

522. As per Clause 49 V (C) and (D) of the SEBI Equity listing agreement, which of the following are held responsible for establishment and maintenance of internal controls for financial reporting ?

A. Managing Director of listed companies

B. The Board of Directors of listed companies

C. Audit Committee of the Board of Directors of listed companies

D. CEO/CFO of listed companies

KEY D

Justification

As per Clause 49 V (C) and (D) of the SEBI Equity listing agreement, the CEO/CFO are held responsible for establishment and maintenance of internal controls for financial reporting. Hence, the answer in Option D is correct and those in the other Options are not factually correct.

523. Good governance alone cannot make an organization successful. Governance should ideally be implemented with the right balance in two dimensions of conformance and a second element. What is the second element ?

A. Risk protection

B. Internal Audit

C. Performance

D. Trust

KEY C

Justification

Good governance alone cannot make an organization successful. Governance should ideally be implemented with the right balance in two dimensions of conformance and a second element, performance. Hence, the answer in Option C is correct and those in the other Options are not factually correct.

524. Which is one of the major oversight mechanisms available to the Board of Directors to ensure that corporate governance processes are effective ?

A. Incentive schemes for Directors

B. The company's annual report

C. Committees like audit committee comprising independent non-executive Directors

D. Quarterly Board meetings

KEY C

Justification

One of the major oversight mechanisms available to the Board of Directors to ensure that corporate governance is effective are mandatory committees like the Audit committee.

525. State TRUE or FALSE. 'Unlike the conformance dimension of Corporate Governance, which is backed by an audit committee manned by independent directors, the performance dimension has no dedicated oversee mechanism.'

A. TRUE

B. FALSE

KEY A

Justification

It is true that the performance dimension of Corporate governance has no dedicated oversee mechanism, unlike the conformance dimension. Hence, answer at Option A is correct.

526. There are oversight mechanisms for the Performance and Conformance dimensions of business governance. One other KEY Aspect of business conformance that is often left out is _____

A. Profitability

B. Information Technology

C. Strategy

D. Capital investments

KEY C

Justification

The neglected aspect of oversight is generally that of strategy. Hence, answer at Option C is correct.

527. What is the key benefit of Governance of Enterprise IT (GEIT) ?

A. It ensures the efficiency of the IT system

B. It facilitates the Balance Score card system

C. It facilitates capital investment decision making

D. It provides a consistent approach integrated & aligned with enterprise governance

KEY D

Justification

The **key b**enefit of GEIT is that it provides a consistent approach, integrated & aligned with enterprise governance. Hence, answer at Option D is correct.

528. State True or False. With reference to Governance of Enterprise IT, the Reserve Bank of India issues guidelines covering various aspects of secure technology deployment. These guidelines are prepared based on various global practices such as COBIT & ISO 27001.

A. TRUE

B. FALSE

KEY A

Justification

Yes, the RBI does issue guidelines covering various aspects of secure technology deployment which are based upon various global practices such as COBIT & ISO 27001. Hence, answer at Option A is correct.

529. Benefit realization & Risk optimization are two of the three areas of focus of Governance of Enterprise IT as specified under COBIT 5. What is the third area of focus ?

A. The third area of focus is Personnel Policies

B. The third area of focus is Information Technology

C. The third area of focus is Resource optimization

D. COBIT 5 specifies only two areas of focus

KEY C

Justification

The third area of focus prescribed by COBIT 5 is Resource optimization. Hence, answer at Option C is correct.

530. Resource optimization & Risk optimization are two of the three areas of focus of Governance of Enterprise IT as specified under COBIT 5. What is the third area of focus ?

A. The third area of focus is Information Technology

B. The third area of focus is Personnel Policies

C. The third area of focus is Benefit realization

D. COBIT 5 specifies only two areas of focus

KEY C

Justification

The third area of focus prescribed by COBIT 5 is Benefit realization. Hence, answer at Option C is correct.

531. Which of the following could be a recommended framework for internal controls & risk management ?

A. COSO 2013 (Council of Sponsoring Organizations of the Tread way Commission)

B. ISO 17001

C. ITAF 1200 series

D. COBIT 5

KEY A

Justification

COSO 2013 framework would be ideal for internal controls and risk management. Hence, answer at Option A is correct.

532. GEIT involves both Conformance as well as Performance perspectives. What would be the KEY Areas of focus of GEIT from the Conformance perspective ?

A. Strategic decision making and value creation

B. Best practices, tools and techniques

C. Board Structure, Roles and Remuneration

D. Balanced Score Card

KEY C

Justification

The Board Structure, Roles and Remuneration would be the KEY focus areas of GEIT from the Conformance perspective. Hence, answer at Option C is correct. The other options are incorrect.

533. GEIT involves both Conformance as well as Performance perspectives. What would be the KEY Areas of focus of GEIT from the Performance perspective ?

A. Board Structure, Roles and Remuneration

B. Standards and Codes

C. Strategic decision making and value creation

D. Audit Committee

KEY C

Justification

From the Business performance angle, quite obviously, strategic decision making and value creation would be the KEY focus areas for GEIT. The other options from A,B to D are incorrect. Hence, answer at Option C is correct.

534. Operations and reporting are two of the three categories of objectives of the COSO 2013 framework. What is the third category of objectives ?

A. Information Technology

B. Security

C. Compliance

D. Risk Management

KEY C

Justification

Compliance is the third category of objectives of the COSO 2013 framework as indicated in Option C. The answers in the other options are incorrect.

535. Reporting and Compliance are two of the three categories of objectives of the COSO 2013 framework. What is the third category of objectives ?

A. Information Technology

B. Security

C. Operations

D. Risk Management

KEY C

Justification

Compliance is the third category of objective of the COSO 2013 framework as indicated in Option C. The answers in the other options are incorrect.

536. Control environment, risk assessment, control activities and information & communication are four of the five integrated components of internal control in COSO. What is the fifth component ?

A. Risk Management

B. Information Technology

C. Security

D. Monitoring activities

KEY D

Justification

Monitoring activities is the fifth component of internal controls in COSO as indicated in Option D. The answers in the other options are incorrect.

537. Control environment, control activities, information & communication and monitoring activities are four of the five integrated components of internal control in COSO. What is the fifth component ?

A. Risk Management

B. Information Technology

C. Risk assessment

D. Security

KEY C

Justification

Risk assessment is the fifth component of internal controls in COSO as indicated in Option C. The answers in the other options are incorrect.

538. Risk assessment, control environment, control activities and monitoring activities are four of the five integrated components of internal control in COSO. What is the fifth component ?

A. Information & communication

B. Risk Management

C. Information Technology

D. Security

KEY A

Justification

Information and communication is the fifth component of internal controls in COSO as indicated in Option A. The answers in the other options are incorrect.

539. State True or False. The COSO 2013 framework prescribes the controls to be selected, developed and deployed for effective internal control. The management is not left with any choice in the matter and has to rigorously comply with the COSO 2013 framework.

A. FALSE

B. TRUE

KEY A

Justification

The COSO 2013 framework does not prescribe the controls to be selected, developed and deployed. It is a function of management judgement based upon factors unique to the entity. Hence, the statement in the stem is false and Option A is correct.

540. State True or False. What COSO 2013 is to internal controls, COBIT 5 is to governance in Governance of Enterprise Information Technology.

A. FALSE

B. TRUE

KEY B

Justification

In GEIT, COBIT 5 is the business framework of governance and management of IT. COSO 2013 is a framework for managing internal controls. Hence, the statement in the stem above is correct and the answer is true as per Option B above.

541. COBIT 5 _____

A. Is best suited for large corporates

B. Is best suited for small and medium enterprises

C. Is a set of globally accepted principles, practices, analytical tools and models

D. Is not ideally suited for non-profit and government enterprises

KEY C

Justification

As indicated in Option C above, COBIT 5 is a set of globally accepted principles, practices, analytical tools and models for governance. It can be used by all types and sizes of organizations, whether profit-oriented or otherwise. Hence, answers at Options A,B and D are wrong.

542. Meeting stakeholder needs, Covering the enterprise end-to-end, Applying a single integrated framework and Enabling a holistic approach are 4 of the 5 KEY principles of COBIT 5. Which is the fifth principle ?

A. Separating Governance from Management

B. Risk management

C. Human resources management

D. Strategic and long term planning

KEY A

Justification

The fifth principle of governance of COBIT 5 is Separating Government from Management. The answers in Options B to D are, hence, wrong and Option A is correct.

543. Covering the enterprise end-to-end, Applying a single integrated framework, Enabling a holistic approach and Separating Governance from Management are 4 of the 5 KEY principles of COBIT 5. Which is the fifth principle ?

A. Risk management

B. Human resources management

C. Meeting Stakeholder needs

D. Strategic and long term planning

KEY C

Justification

The fifth principle of governance of COBIT 5 is Meeting Stakeholder needs. The answers in Options A,B and D are, hence, wrong and Option C is correct.

544. Meeting Stakeholder needs, Covering the enterprise end-to-end, Applying a single integrated framework, and Separating Governance from Management are 4 of the 5 KEY principles of COBIT 5. Which is the fifth principle ?

A. Enabling a holistic approach

B. Human resources management

C. Risk management

D. Strategic and long term planning

KEY A

Justification

The fifth principle of governance of COBIT 5 is Enabling a holistic approach. The answers in Options B to D are, hence, wrong and Option A is correct.

545. Which is the ISO standard for corporate governance ?

A. ISO 31000

B. ISO 27001

C. ISO 20100

D. ISO 38500

KEY D

Justification

The ISO standard for corporate governance is ISO 38500. The other Options are, hence, wrong and Option D is correct.

546. Which is the ISO standard for IT risk management ?

A. ISO 31000

B. ISO 38500

C. ISO 27001

D. ISO 20100

KEY A

Justification

The ISO standard for IT risk management is ISO 31000. The answers in Options B to D are, hence, wrong and Option A is correct.

547. Which is the ISO standard for Risk management ?

A. ISO 38500

B. ISO 27001

C. ISO 31000

D. ISO 20100

KEY C

Justification

The ISO standard for IT risk management is ISO 31000. The answers in other Options are, hence, wrong and Option C is correct.

548. A company has developed a mobile phone which is unique for its simplicity and ease of use. During laboratory tests, it finds that the product is really robust and rarely fails. The industry norm is that mobile phone manufacturers invariably offer customers the comfort of prompt and efficient after sales service, including repair. After a lot of introspection, the company decides that the probability of failure of their product was so low and it would not be worth their while to invest in a network of servicing facilities. They decided, instead to offer a free replacement in the event of failure of their product. In fact, they decided to leverage this itself as a marketing strategy for their product and it turned out to be a roaring success. What type of risk management strategy has the company adopted in this case ?

A. Terminate/eliminate the risk

B. Transfer/share the risk

C. Tolerate/accept the risk

D. Treat/mitigate the risk

KEY C

Justification

The company has obviously chose to tolerate/accept the risk in view of the low probability of its occurrence and likely lower cost of incurring the risk. The answers in other Options are, hence, wrong and Option C is correct.

549. A company markets agro chemicals on a pan India basis. Farmers use agro chemicals, typically, only when they perceive a pest attack and would like to act immediately then to save their crop. Hence, prompt and speedy availability is the main driver for sales of this product. The company, which had its manufacturing facility located in South India, found that it invariably lost out in meeting the demand from the Northern States owing to their inability to reach their product in time to meet such unpredictable demand. Since the market size being lost out was substantial as compared to the cost of setting up a new plant, they ultimately decide to set up a new manufacturing facility in Punjab which could ensure availability of product in a timely fashion. What type of risk management strategy has the company adopted in this case ?

A. Terminate/eliminate the risk

B. Tolerate/accept the risk

C. Transfer/share the risk

D. Treat/mitigate the risk

KEY A

Justification

The company has obviously chosen to terminate/eliminate the risk after weighing the pros and cons of loss of business/profit versus cost of setting up a new manufacturing facility. The answers in Options B to D are, hence, wrong and Option A is correct.

550. Section 49 C of the Listing Agreement of SEBI addresses the need for _____

A. Minimum public shareholding percentage

B. Creation of a board sub-committee for auditing

C. Board disclosures related to risk management & states

D. Compliance with government regulations

KEY C

Justification

This section relates to need for Board disclosures related to risk management & states. Hence, answer at Option C is correct and the other options are incorrect.

551. Section 49 V of the Listing Agreement of SEBI deals with _____

A. Board disclosures related to risk management & states

B. Minimum public shareholding percentage

C. Creation of a board sub-committee for auditing

D. CEO/CFO certification, among other things, of internal controls

KEY D

Justification

This section of SEBI's Listing agreement relates to need for CEO/CFO certification accepting, among other things, responsibility for establishing and maintaining internal controls. Hence, answer at Option D is correct and the other options are incorrect.

552. Section 49 (VII) of the Listing Agreement of SEBI deals with _____

A. Creation of a board sub-committee for auditing

B. Compliance aspects & certificate of compliance

C. Minimum public shareholding percentage

D. Compliance with government regulations

KEY B

Justification

This section of the Listing Agreement of SEBI deals with compliance aspects and the need for certificate either from the auditors or the company secretary regarding compliance of conditions of corporate governance. Hence, answer at Option B is correct and the other options are incorrect.

553. How can a Governance-Risk-Compliance (GRC) program be enhanced from merely ensuring compliance to ensuring performance too ?

A. Reward compliance at all levels

B. Ensure Risk-Reward ratio is commensurate with the cost/investment

C. Implement GRC program using GEIT (Governance of Enterprise IT) framework

D. Implement GRC utilising external resource like auditor

KEY C

Justification

A GRC program will basically ensure compliance. However, the GEIT framework focuses on benefit realization, risk optimization and resource optimization. Hence, implementing a GRC program using the GEIT framework will help achieve both the objectives of compliance as well as performance. Hence, Option C is the correct answer.

554. Apart from Clause 49 of the SEBI Listing agreement, which is based upon SOX provisions, which other mandatory provision exists on internal controls for corporate in India ?

A. The Indian Companies Act, The Companies (Auditor's Report) Order 2003

B. Information Technology Act 2008

C. Sarbanes Oxley Act, 2003

D. COBIT 5

KEY A

Justification

Mandatory provisions on internal controls do exist, as per CARO, as brought out in Option A above. The IT Act has no such provision, the SOX Act applies in the USA and COBIT 5 is not an Act but a framework. Hence, answer at Option A above is correct.

555. State True or False. Under GRC (Governance, Risk and Compliance) norms, compliance refers exclusively to compliance with statutory Laws and Regulations; compliances with internal policies of an organization are not a part of it.

A. TRUE

B. FALSE

KEY B

Justification

Compliance under GRC refers both to external compliances, in terms of statutory laws and regulations, as also internal compliances with regard to policies of an organization. Hence, the above statement is false and answer at Option B is correct.

556. Principles, policies & framework, (b) Processes, (c) Organization structure, (d) Roles, responsibilities & risks of IT department, (e) Information and (f) Services, infrastructure & applications are six of the seven enablers of COBIT 5. Which is the 7th enabler ?

A. Planning & communication

B. Delegation of authority

C. Compliance with statutory regulations

D. Culture, ethics & behaviour

KEY D

Justification

Culture, Ethics & Behaviour is the 7th enabler under COBIT 5. Hence, answer at Option D is the correct one.

557. Principles, policies & framework, (b) Processes, (c) Organization structure, (d) Roles, responsibilities & risks of IT department, (e) Culture, ethics & behaviour and (f) Services, infrastructure & applications are six of the seven enablers of COBIT 5. Which is the 7th enabler?

A. Information

B. Planning & communication

C. Delegation of authority

D. Compliance with statutory regulations

KEY A

Justification

Information is the 7th enabler under COBIT 5. Hence, answer at Option A is the correct one.

558. What is the purpose of Principles, policies and framework in an organization ?

A. To control the employees

B. To arrive at the business strategy of the organization

C. To convey the management's direction & instruction

D. To comply with statutory regulations

KEY C

Justification

The purpose of Principles, policies and framework in an organization is to communicate downward the direction the management would like the organization to take and the means through which this can be done. They reflect the culture, ethics and values of the organization. The objective is not to control the employees; not are they in compliance with statutory regulations. Principles, policies and framework are not drawn up for the purpose of business strategy; however, the strategy will evolve based upon these elements and other strategic inputs like the market, competition, etc. Hence, answer at Option C is the correct one.

559. Apart from being effective and efficient, what other characteristic should a good policy possess ?

A. To control the employees

B. Making sense & appearing logical to those who have to comply with them

C. To arrive at the business strategy of the organization

D. To comply with statutory regulations

KEY B

Justification

The third important attribute of any good policy is that it makes sense and appears logical to those who are required to comply with them. But for this, policies would fail in actual practice during implementation for want of buy in. Hence, answer at Option B is the correct one.

560. Processes are one of the 7 enablers of Governance of Enterprise IT under COBIT 5. What are the types of processes distinguished under COBIT 5 ?

A. Strategy processes and action processes

B. Group processes versus individual processes

C. Governance processes and management processes

D. Macro versus micro processes

KEY C

Justification

COBIT 5 distinguishes between governance and management processes with the latter concerned more with performance matters. Answer at Option C is the correct one.

561. How does the RACI (Responsible, Accountable, Consulted, Informed) model help in an organization ?

A. Helps clarify roles and responsibilities

B. Facilitates documentation of processes

C. Basis for development of organization chart

D. Accelerates decision-making process

KEY A

Justification

The RACI model helps clarify roles and responsibilities and is particularly of value in cross departmental projects and processes. Answer at Option A is the correct one.

562. In Governance of Enterprise IT, the IT Strategy Committee should include _____

A. Board members alone, considering the strategic content

B. Non-Board members alone, considering the need for implementation support

C. Both Board as well as non-Board members

D. Board members and IT managers alone

KEY C

Justification

The IT Strategy Committee should have representation from Board as well as non-Board members, with representation from all divisions. Answer at Option C is the correct one.

563. Which of the following has primary responsibility for implementation of Governance of Enterprise IT ?

A. The Managing Director or CEO of the Organization

B. The CIO of the organization

C. The IT Strategy Committee

D. The IT Steering Committee

KEY C

Justification

It is the IT Strategy Committee whose primary responsibility it is to implement GEIT, while the accountability is of the Board of Directors itself. Answer at Option C is the correct one.

564. Which of the 7 enablers of COBIT 5 is considered the most important ?

A. Organization structure

B. Principles, policies & framework

C. Processes

D. Information

KEY D

Justification

Information is considered the most important of the enablers of COBIT 5. Answer at Option D is the correct one.

565. What is most important in developing a performance management system ?

A. Deciding on incentive schemes

B. Identifying enterprise goals & their linkage to operating environment

C. Developing clear organization structure

D. Benchmarking with industry

KEY B

Justification

The most important aspect of performance management development is ensuring that organizational goals, vision, mission are cascaded downwards to all, establishing a clear linkage. But for this, the entire exercise would be fruitless since the performance could be directed at goals other than those established through the vision / mission of the organization. Answer at Option B is the correct one.

566. A good performance management system assesses performance against goals through Key Goal Indicators. Simultaneously, it monitors performance of process through _____

A. Work flow indicators

B. Moving average indicators

C. KEY Process Indicators

D. Industry benchmarks

KEY C

Justification

Monitoring of performance of process is through the KEY Process Indicator. Hence, the answer at Option C is the correct one.

567. The approach of using lead indicators for performance measurement is called _____

A. Reactive approach

B. Retroactive approach

C. Proactive approach

D. Retrospective approach

KEY C

Justification

The approach of using lead indicators for performance measurement is called Proactive approach. Hence, the answer at Option C is the correct one.

568. The approach of using lag indicators for performance measurement is called ?

A. Proactive approach

B. Reactive approach

C. Retroactive approach

D. Retrospective approach

KEY B

Justification

The approach of using lag indicators for performance measurement is called Reactive approach. Hence, the answer at Option B is the correct one.

569. Where is the Capability Maturity framework of Performance Management Systems generally used?

A. Hardware Development Company

B. Research & Development institution

C. Software Development Company

D. Educational institutions

KEY C

Justification

The Capability Maturity framework of Performance Management Systems is generally used in the software development companies. . Hence, the answer at Option C is the correct one.

570. Mr Johnson has just taken charge as Head of a fledgling educational institution which has not had a good track record. He feels that he has his task cut out for him he needs to focus more on the lead parameters rather than lag indicators so that he can create sustainable results. Which of the following would be an example of lead indicators ?

A. Number of passes by students in the Matriculation examination

B. Number of all-India rank holders from the school in the Matriculation examination

C. Number of failures in the Matriculation examination

D. Number of hours of refresher courses attended by teachers

KEY D

Justification

The correct answer would obviously be the number of hours of refresher courses. Hence, the answer at Option D is the correct one.

571. In Governance, value creation happens through Benefits Realisation, Risk optimization & Resource Optimization decisions taking into account _____

A. All Stakeholders' needs

B. All Shareholders' needs

C. Organizational goals

D. Organizational vision, mission

KEY A

Justification

In Governance, all stakeholders' needs should be taken into account while taking decisions related to benefits realization, risk optimization & resource Optimization. Hence, the answer at Option A is the correct one.

572. Which framework specifically enables users to relate their enterprise's current business & IT environment to specific objectives & relevant processes ?

A. Quality management system

B. Six Sigma approach

C. COBIT 5 framework

D. Blue Ocean framework

KEY C

Justification

While many frameworks may address such linkages generically, the advantage of COBIT 5 is that it specifically enables users to relate their enterprise's current business and IT environment to specific objectives and relevant processes. Hence, the answer at Option C is the correct one.

573. The Balanced Score Card is an invaluable management tool that helps translate strategy into action and also for _____

A. Balancing share holders needs with employee needs

B. Bringing non-financial indicators into better focus

C. Balancing needs of multiple functions within an organization

D. Balancing lead and lag indicators

KEY B

Justification

As brought out in Option B above, one of the major advantages of the Balanced score card mechanism is its ability to focus on non-financial indicators too, thus bringing in a balance between financial & non-financial parameters. The answers in other Options are incorrect.

574. The Balanced Score Card is designed to ensure that performance metrics and strategic themes are balanced with financial & non-financial, operational & financial, lead & lag indicators. Financial, Customer & Internal Business process perspectives are three of the four perspectives of BSC. The fourth perspective is _____.

A. Learning & Growth

B. Shareholders versus Employees

C. Short term versus Long term

D. Lead and lag indicators

KEY A

Justification

As brought out in Option A above, the fourth perspective of BSC is Learning & Growth. The answers in Options B to D are incorrect.

575. The Balanced Score Card _____

A. Is meant for the use of only the senior level executives

B. Cannot be linked to the IT goals & objectives

C. Cannot be the basis for performance incentives

D. Can be cascaded down to all levels of the organization

KEY D

Justification

As brought out in Option D above, the BSC can, indeed, be cascaded down to all the levels of organization. The answers in other options are incorrect.

576. What is the most important aspect of the CIMA Strategic Score Card approach ?

A. Focuses exclusively on strategy matters

B. Focuses exclusively on IT governance & strategy aspects

C. Addresses conformance as well as performance, focussing on strategic issues

D. Unlike the Balanced Score card, it focuses on lead indicators alone

KEY C

Justification

The CIMA Strategic Score Card approach addresses both conformance as well as performance, focussing on strategic issues. The answers in other options are incorrect.

577. Strategic position, Strategic options and Strategic implementation are three of the four basic elements of the CIMA Strategic Score card. What is the fourth element ?

A. Strategic Risks

B. Strategic Conformance

C. Strategic Performance

D. Strategic IT

KEY A

Justification

The fourth element of the CIMA Strategic Score Card approach is Strategic Risks. The answers in Options B to D are incorrect.

578. What is fundamental to the Capability Maturity Model Integration (CMMI) ?

A. Used universally, except in the I.T. industry

B. Is superior to COBIT 5 which does not have process capability

C. It is a process improvement approach

D. Focuses on internal process alone

KEY C

Justification

The CMMI model is a process improvement approach & is a preferred model for the IT industry. COBIT 5, too, has process capability built in. CMMI addresses all processes. Hence, answer at Option C above alone is correct.

579. What is the essence of Total Quality Management strategy ?

A. Focus exclusively on products & services rather than processes

B. Producing best quality products

C. Focus on exclusively on processes as a means to an end

D. Achieving long term success through customer satisfaction

KEY D

Justification

TQM strategy aims at achieving long term success through customer satisfaction. It aims to do this through quality management at all levels, improving products, services, processes as also culture. Hence, answer at Option D above alone is correct.

580. State True or False. The guidelines for specific processes and procedures in COBIT 5 have been designed robustly with the latest best practices incorporated. While implementing the framework, these processes / procedures need to be kept intact and not tweaked or tinkered with.

A. FALSE

B. TRUE

KEY A

Justification

The design of processes and procedures suggested in COBIT 5 need to be tailored appropriately to suit the needs of the enterprise's culture, management style & IT environment. The recommended best practices, too, should be adapted to suit the particular enterprise where it is being implemented. Hence, the statement in the Stem is incorrect and the answer at Option A is correct.

581. One of the primary reasons for implementing Governance of Enterprise IT (GEIT) is to alleviate pain points in the organization. Another major reason is _____

A. Ensure up-to-date technology

B. Trigger events like merger/acquisition, new regulations, etc.

C. Achieve stake holder satisfaction

D. Higher vulnerability of IT compared to other functions

KEY B

Justification

The other major reasons for implementing GEIT are trigger events which create changes in the environment. Answers in Options A and C may also be factually true but are not necessarily major reasons for implementing GEIT. Answer in Option D is not correct.

Hence, the answer at Option B is correct.

582. Which one of the following could be a Critical Success factor in GEIT implementation ?

A. The project is handled exclusively & in isolation to day-to-day business

B. Execution authority & responsibility is retained at the highest levels

C. Top management provides direction and mandate

D. Trigger events like merger/acquisition, new regulations, etc.

KEY C

Justification

One of the critical success factors above is the need for top management to provide direction and mandate for the project, as indicated in Option C. Integration of the project with day-to-business is essential for the success of the project contrary to what is stated in Option B. Similarly, authority & responsibility have to be cascaded down to the level at which project implementation happens, ideally at the level of an anchor person. Trigger events may precipitate the implementation of GEIT but cannot be critical success factors. Hence, the answer at Option C is correct

583. Which one of the following could be a Critical Success factor in GEIT implementation ?

A. Trigger events like merger/acquisition, new regulations, etc.

B. The project is handled exclusively & in isolation to day-to-day business

C. Focus on quick wins to demonstrate benefit & build confidence

D. Execution authority & responsibility is retained at the highest levels

KEY C

Justification

Early successes help instil confidence in the initiative & stimulate co-operation, as indicated in Option C. Trigger events may precipitate the implementation of GEIT but cannot be critical success factors. Integration of the project with day-to-business is

essential for the success of the project contrary to what is stated in Option A. Similarly, authority & responsibility have to be cascaded down to the level at which project implementation happens, ideally at the level of an anchor person.

Hence, the answer at Option C is correct.

584. What should be the first phase of GEIT implementation ?

A. Forming an implementation team

B. Communication desired vision

C. Enable operation & use

D. Establish desire to change, stressing pain points, trigger events

KEY D

Justification

The first phase of GEIT implementation is preparing the ground for the project to take off and targeting the mind sets of the people concerned. This can be done by identifying the pain points / trigger events as also the consequences of inaction for the organization as well as the individual. The answers in other options can be successive steps in the project implementation and not the initial one.

Hence, the answer at Option D is correct.

585. What should be the final phase of GEIT implementation ?

A. Establish desire to change, stressing pain points, trigger events

B. Communication desired vision

C. Sustain changes through conscious reinforcement

D. Enable operation & use

KEY C

Justification

Any initiative, however good it may be, will not yield the desired results unless mechanisms are built in for sustaining the momentum which has been gained in the initial launch. This can be done, as pointed out in Option C above, through conscious reinforcement & continuous top management commitment. The answers in the other options are intermediate phases in the GEIT implementation process and, hence, are not correct.

586. In line with ISO/IEC 38500, Governance processes under COBIT 5 are based upon the principles of _____

A. Evaluate, Direct, Monitor

B. Align, Plan & Organize

C. Monitor, Evaluate & Assess

D. Build, Acquire and Implement

KEY A

Justification

Governance process under COBIT 5 are based upon the principles of Evaluation of strategic options, Direction to IT & Monitoring of the outcome. Hence, answer in Option A above is correct and the other answers are wrong.

587. The most critical factor in implementing GEIT is _____

A. Taking a bottom-up perspective

B. Identifying implementation scope & objectives, prioritization of processes

C. Availability of trained individuals to spearhead the project

D. Organization chart combined with Delegation of Authority

KEY B

Justification

The most critical factor in implementing GEIT is identifying implementation scope and objectives as also prioritization of processes, as shown in Option B. Answers in other options are not correct. Hence, answer in Option B above is correct.

588. How is alignment of strategic IT Plans with business done?

A. Holding regular meetings with IT department participation

B. Having an IT department nominee in non-IT meetings

C. Clearly communicating the objectives & accountabilities

D. Taking a bottom-up perspective

KEY C

Justification

Alignment of strategic IT Plans with business is done by clearly communicating the objectives & accountabilities so that they are understood by all & IT strategic options are integrated with the business plans as required. Hence, Option C is the correct answer.

589. Which one of the following is a KEY management practice for aligning IT strategy with enterprise strategy ?

A. Identify gaps between current & target environments

B. Taking a bottom-up perspective

C. Holding regular meetings with IT department participation

D. Having an IT department nominee in non-IT meetings

KEY A

Justification

Identifying gaps between the current & target environments is one of the KEY management practices for aligning IT strategy with enterprise strategy. Hence, Option A is the correct answer.

590. How is Value Optimization of IT achieved ?

A. Going in for low cost IT equipment

B. Replacing full time IT employees with outsourced personnel

C. Taking a bottom-up perspective

D. Value Optimization of business processes, IT services & assets

KEY D

Justification

Value Optimization of IT is achieved through value optimization of business processes, IT services & IT assets. Hence, Option D is the correct answer.

591. Which of the following metrics could be used for evaluation of value optimization ?

A. Number of low cost IT equipment procured during a financial year

B. Replacing full time IT employees with outsourced personnel

C. Percentage of IT enabled investments where claimed benefits were met or exceeded

D. Wage cost reduction through non-filling of some vacant IT positions

KEY C

Justification

One metric which could be used for evaluation of value optimization could be the percentage of IT enabled investments where claimed benefits were met or exceeded. Answers in other options, however, will not meet the requirement. Hence, Option C is the correct answer.

592. COBIT 5 has a resource governance process to ensure that resources needs of the enterprise are met in an optimal manner. Which one of the following is KEY governance process to be followed ?

A. Evaluate, Direct and Monitor resource management

B. Build, Acquire and Implement

C. Align, Plan & Organize

D. Monitor, Evaluate & Assess

KEY A

Justification

The KEY governance process to be followed in this case is Evaluate, Direct and Monitor resource management as brought out in Option A. The answers in the other options B to D are incorrect and not applicable to the instant case.

593. Which one of the following is an important tool used for managing & monitoring service providers ?

A. Regular meetings

B. Third party inspection arrangements

C. Service Level Agreements (SLAs)

D. Cost comparison through industry benchmarking

KEY C

Justification

While all the answers in the options above may be true to some extent or the other, the most important tool used for managing & monitoring service providers are Service Level Agreements which play the role not only of enforceability of commitments but, simultaneously, of capturing clearly the responsibilities of both parties as also other aspects like delivery expectations, escalation clauses, penalties, etc. Hence, the answer in Option C above is correct and the rest can be deemed to be wrong.

594. The success of capacity management would depend most upon which one of the following factors ?

A. Historical trend of capacity expansions

B. Availability of precise and timely business forecasts

C. Cost comparison through industry benchmarking

D. Availability of adequate funds for procurement

KEY B

Justification

Capacity Management success would depend to a great extent upon the availability of precise and timely business forecast, as indicated in the answer in Option B. The answers in other options are incorrect.

595. With reference to Capex & Opex, how can valuation of any business be improved ?

A. Increasing Capex & proportionately reducing Opex

B. Reduction in Opex irrespective of impact on day-to-day operations

C. With Capex constant, reduction in Opex without hurting day-to-day operations

D. Increasing both Capex & Opex with the objective of increased profits

KEY C

Justification

In general, industry prefers to restrict Capex & also optimize Opex to get best results for stakeholders. Capex is considered undesirable owing to restrictions on dividend cost being allowed as a business cost for tax purposes unlike Opex. However reduction in Opex can hurt operations too, leading to reduced profits. Hence, the ideal situation would be, while Capex is kept constant, Opex is reduced without hurting day-to-operations, as indicated in Option C above. The answers in other 0ptions are incorrect.

596. What is Information ?

A. It is a collection of data which need not necessarily have meaning for its user

B. It is restricted to data in the form of numbers

C. It is data which is not necessarily specific & organized

D. It is all data processed in a meaningful context

KEY D

Justification

Information is data processed in a meaningful context. It is specific & organized and has value to the user. It includes all forms of information like numbers, text, images, sound, codes, etc. Hence, the answer at Option D is correct & the other options incorrect.

597. State TRUE or FALSE. When the Information System Auditor delegates work to others, he will continue to be responsible for forming and expressing his opinion on auditee environment as per the scope and objectives of the audit.

A. TRUE

B. FALSE

KEY A

Justification

The responsibility for forming and expressing opinion on auditee environment rests with the IS Auditor even in respect of work he delegates to others. Hence, answer at Option A above is correct.

598. Are Audit professionals considered to be the most appropriate professionals to audit Information Systems (rather than IT professionals) ?

A. No; since they do not have adequate expertise in Information Technology

B. Yes; since it involves the evaluation of internal controls in computerized business processes

C. No; since Information systems have built-in safeguards and an audit would be superfluous

D. Yes; but only to the extent of regulatory matters about which they are proficient

KEY B

Justification

Audit professionals are, indeed, considered to be the most appropriate professionals to audit Information systems since knowledge of business processes is extremely critical for such audit, more than that of technical knowledge of Information technology. What is required is an audit professional who has supplemented his audit/financial/regulatory background with knowledge of the basics of Information technology. Hence, answer at Option B above is correct. IS can build safeguards to meet all contingencies. The other answers are, therefore, incorrect.

599. Risk in Information Technology _____

A. Can be depicted as hierarchically dependent upon other risk categories

B. Does not impact on long term strategy

C. Can also be defined as Threat exploiting Vulnerabilities

D. Is not considered operational in financial industry as per Basel II framework

KEY C

Justification

Since Information systems impinge on each and every part of an organization's business today, any risks in IT would automatically extend to all aspects of the business. It is, in fact, considered even an operational risk in the financial industry as per Basel II framework. However, since it is relevant to different aspects of an organization, it is not to be depicted as hierarchically dependent upon other risk categories. Hence, answers in Options A, B and D are incorrect. However, the definition given in Option C is correct it is, in a way, threat exploiting vulnerabilities. Hence, answer at Option C above is correct.

600. What is the Risk Universe ?

A. Is restricted to selected components of the business

B. Is restricted to the enterprise & excludes suppliers, service providers, clients

C. It needs to be defined & frozen for a reasonable period of time of about 5 years

D. It defines the overall environment & provides a structure for managing the IT risk

KEY D

Justification

The Risk Universe extends to the overall environment, covering all stake holders including suppliers, service providers & clients. It aims at providing a structure for managing IT risk. It crosses functional silos and is intended to cover end-to-end business perspective. It needs to be dynamic & updated regularly to be aligned with changes in the environment. Hence, answer at Option D alone is correct.

601. During 2009, the Satyam Computers scandal broke out. The Company's Chairman admitted to falsification of accounts to the tune of U.S. $ 1.47 billion. The auditors for this company were mainly exposed to what type of risk ?

A. Audit Risk

B. Financial Risk

C. Procedural Risk

D. IT Risk

KEY A

Justification

Audit risk refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. The cited example clearly refers to such a situation and, hence, answer at Option A above is the correct answer.

602. Audit risk is _____

A. A product of control risk & detection risk

B. A product of inherent risk, control risk & detection risk

C. Sum of inherent risk, control risk & detection risk

D. A product of inherent risk and detection risk

KEY B

Justification

Audit risk refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. It is a product of inherent risk, control risk & detection risk. Hence, answer at Option B alone is correct.

603. In the case of IS Audit, materiality is _____

A. Based upon value and volume of transactions

B. Based on impact of non compliance

C. Consequence of risk in terms of potential loss

D. A product of inherent risk and detection risk

KEY C

Justification

Materiality in IS Audit is a consequence of risk in terms of potential loss. Hence, answer at Option C is correct while the other answers are incorrect.

604. In the case of Financial audit, materiality is _____

A. Based upon value and volume of transactions

B. Based on impact of non compliance

C. Consequence of risk in terms of potential loss

D. A product of inherent risk and detection risk

KEY A

Justification

Materiality in Financial Audit is based upon value and volume of transactions and the relevant error or discrepancy or control weakness detected. Hence, answer at Option A is correct while the other answers are incorrect.

605. In the case of Regulatory audit, materiality is _____

A. Based upon value and volume of transactions

B. Consequence of risk in terms of potential loss

C. Based on impact of non- compliance

D. A product of inherent risk and detection risk

KEY C

Justification

Materiality in Regulatory Audit is based upon the impact of non-compliance with regulations. Hence, answer at Option C is correct while the other answers are incorrect.

606. Internal Controls _____

A. Are restricted to tools for prevention of risks alone

B. Focus exclusively on financial rather than non-financial risks

C. Are driven exclusively by automated computerised systems

D. Facilitate achievement of business objectives & management of risks

KEY D

Justification

Internal controls are designed to assure the management that the organization's business objectives will be achieved and risk events prevented or detected and corrected. They target prevention as well as detection & correction and are aimed at both financial as well as non-financial risks. They can be driven either by automated computerised systems or even manual systems. Hence, answer at Option D alone is correct.

607. Internal Controls _____

A. Target risk management rather than achievement of business objectives

B. Comprise Preventive, Detective & Corrective controls

C. Are driven exclusively by automated computerised systems

D. Focus exclusively on financial rather than non-financial risks

KEY B

Justification

Internal controls are designed to assure the management that the organization's business objectives will be achieved and risk events prevented or detected and corrected. They target prevention as well as detection & correction and are aimed at both financial as well as non-financial risks. They can be driven either by automated computerised systems or even manual systems. Hence, answer at Option B alone is correct.

608. Internal Controls _____

A. Are the sum total of IT General controls and IT Application Controls

B. Focus exclusively on prevention of errors or irregularities

C. Are driven exclusively by automated computerised systems

D. Focus exclusively on financial rather than non-financial risks

KEY A

Justification

Internal controls are designed to assure the management that the organization's business objectives will be achieved and risk events prevented or detected and corrected. They target prevention as well as detection & correction and are aimed at both financial as well as non-financial risks. They can be driven either by automated computerised systems or even manual systems. They include General controls which encompass all administrative areas and Application controls which are related to specific application software. Hence, answer at Option A alone is correct.

609. The authority, scope and responsibility of the Information System Audit function is _____

A. Defined by the I.T. Head of the organization, as the expert in the matter

B. Defined by the various functional divisions, depending upon criticality

C. Defined by the audit charter approved by the senior management/Board

D. Generated by the Audit division of the organization

KEY C

Justification

The authority, scope and responsibility of the Information system audit is invariably defined by the audit charter which is approved by the senior management and, most often, by the Board of Directors. It is not left to the Audit division, the IT Head or the functional heads to decide on this. Hence, answer at Option C alone is correct..

610. Audit objectives, in general _____

A. Are not concerned with substantiation of internal controls

B. Refer to the specific goals that must be met by audit

C. Are not concerned with how internal controls function

D. Are derived & stated at the end of the audit process

KEY B

Justification

Audit objectives refer to the specific goals that must be met by audit. This is in contrast to a control objective which refers to how an internal control functions. They often focus on substantiating the existence of internal controls & the appropriateness of functioning. They are invariably set down at the beginning of the audit process. Hence answer at Option B alone is correct.

611. The major purpose of Information Systems Audit is whether _____

A. Internal control system design is robust & operated effectively

B. Financials are properly reflected in the books of the organization

C. All the hardware in the organization have appropriate warranties

D. All the software in the organization have valid licences

KEY A

Justification

A major purpose of Information Systems audit is whether the internal control system design is robust and is operated effectively. It is not directly related to ensuring financial correctness or to validate warranties/licences for hardware/software. Hence, answer at Option A alone is correct.

612. A Request for Proposal (RFP) _____

A. Is sent by prospective supplier to buyer, seeking information

B. Will help identify the lowest-priced bidder as the successful bidder

C. Is used for acquiring services &, sometimes, goods

D. Is used exclusively for buying goods and not services

KEY C

Justification

A RFP is used primarily for acquiring services and, on occasion, goods. It comprises a complete description of the buyer's requirements of the service/product. The successful bidder in this process need not necessarily be the lowest-priced; non-financial aspects like credibility, technical superiority, etc. will also be taken into account to arrive at the optimal supplier. Hence, answer at Option C alone is correct.

613. You are advising your client on the selection & appointment of an IT service provider. You suggest that the client should go through a Request for Proposal (RFP) process for best results. Your client is happy with your suggestion but requests that not all aspects of the selection process be publicised up-front. For, the client had faced situations in the past wherein, openness in such matters had lead to issues of disputes with suppliers who were rejected in the selection process. The client's argument is that, in any case, the selection will be on a fair and equitable basis & the idea is just to avoid giving too much information to the bidders and create the potential for nuisance attacks by mischievous, unsuccessful bidders. As a Chartered Accountant, would your suggestion be to clearly spell out the selection criteria or leave it ambiguous ?

A. Clearly spell out the selection criteria

B. Leave the selection criteria ambiguous

KEY A

Justification

It would be best to clearly spell out all the selection criteria. For, it would give confidence to the potential bidders about the credibility of the buyer and also avoid build up of un-necessary cushions to take care of any unknown contingencies. Also, ambiguities cut both ways & may provide loopholes for unscrupulous bidders to wriggle out of commitments or raise disputes. Contractually & legally speaking, too, such a RFP will strengthen the organization's hands in the event of any default or failure on the part of the chosen supplier. Hence, answer at Option A alone is correct.

614. What are the elements common to both the Audit Charter and Audit Engagement Letter ?

A. Responsibility, Authority & Professional Fees payable

B. Responsibility, Authority & Travel expenses budget for auditors

C. Responsibility, Authority & Accountability

KEY C

Justification

The elements common to both the Audit Charter & Audit Engagement Letter are Responsibility, Authority & Accountability. Aspects like the Professional fees payable, travel expenses budget for auditors, etc. are generally dealt with in the Engagement Letter and not in the Charter. Hence, answer at Option C alone is correct.

615. Based upon scope, objectives, etc. drawn up in consultation with the senior management of an organization, an experienced audit team which has sound knowledge of I.T. has completed & filed its preliminary audit report of the I.T. department of the organization. On receiving the draft report, the officials in the I.T. department react negatively to the report. They argue that the bulk of the conclusions drawn in the report, the information reported, etc. are erroneous. They question the validity of the findings. In your view, which one of the following could be the likely major cause for this situation ?

A. Lack of adequate technical IT knowledge of the auditing team

B. Poor quality of audit by the team

C. Malafide intentions of the auditee team

D. In-effective communication with Auditee & buy-in

KEY D

Justification

It is clear that the auditing team is a competent one with sound knowledge of I.T. It is unlikely that the auditee team deliberately sought to scuttle the auditing team's report. For, given the fact that they have the top management's approval, the I.T. department cannot hope to gain anything by throwing mud on the auditing team. If the auditee still questions the validity of the team's report, the single major cause which can be inferred from the question stem is that the communication to the auditee has not been carried out in an effective manner & adequate steps have not been taken to secure auditee buy-in for the process . Hence, answer at Option D appears to be more appropriate.

616. You have just taken on the Audit of a large, established multinational company with operations spread geographically across continents. You need to draw up detailed scope of the proposed audit of the organization in consultation with its top management. Your approach would be to focus upon _____

A. Areas identified to be high risk &/or high significance to the organization

B. Sample audit of each and every geographical unit of the organization

C. Sample audit of each and every function in the organization

D. Areas related to I.T. software and hardware alone

KEY A

Justification

Given the fact that any audit team would have limitations in terms of auditing resources as well as budget, it would have to get maximum mileage for the auditee with the limited resources at its disposal. Hence, rather than spreading itself too thin by trying to audit as many areas as possible, the ideal strategy would be to arrive at a consensus regarding a few areas of high risk as also high significance for the organization. Auditing these areas alone initially would help maximise the value of the auditing exercise. Hence, answer at Option A is the most appropriate one.

617. You have just taken on the Audit of a large, established company with diverse businesses involving manufacturing as well as trading. You are now at the planning stage & need to draw up your draft audit plan for clearance by the top management. What is the most important planning activity involved at this stage of the exercise ?

A. Historical financial for the organization

B. Cost of carrying out the audit

C. Thorough understanding of the nature of each of the businesses & nuances

D. Number of people required for carrying out the auditing exercise

KEY C

Justification

Considering the diverse nature of the organization's businesses as also its existence both in trading as well as manufacturing, the fundamental drivers of these areas of business are likely to be totally different. The most important part of the planning exercise would hence be the thorough understanding of each of the organization's businesses & its nuances. This alone will help the auditor to appreciate the areas of significance & high risk so that focus can be shifted to these areas for maximum results. Hence, answer at Option C above is the most appropriate.

618. Which are the three major categories of IS Controls ?

A. Fiduciary, Quality & Security

B. Financial, Quality & Security

C. Audit, Quality & Security

D. Economic, Financial & Quality

KEY A

Justification

The major categories of IS Controls are Fiduciary, Quality & Security. Hence, answer at Option A above is the correct one.

619. The basic principles of Fiduciary Controls in Information Systems are _____

A. Efficiency & Effectiveness of process, service or activity

B. Reliability of information & Compliance with laws, regulations, etc.

C. Confidentiality & Integrity of information

D. Confidentiality, Integrity & Availability of information

KEY B

Justification

The basic principle of Fiduciary Controls in IS are reliability of information & compliance with laws, regulations, etc.. Hence, the correct answer is as per Option B. The other answers are incorrect.

620. The basic principles of Quality Controls in Information Systems are _____

A. Reliability of information & Compliance with laws, regulations, etc.

B. Confidentiality & Integrity of information

C. Efficiency & Effectiveness of process, service or activity

D. Confidentiality, Integrity & Availability of information

KEY C

Justification

The basic principle of Quality Controls in IS are efficiency & effectiveness of processes, services or activities. Hence, the correct answer is as per Option C. The other answers are incorrect.

621. The basic principles of Security Controls in Information Systems are _____

A. Confidentiality, Integrity & Availability of information

B. Reliability of information & Compliance with laws, regulations, etc.

C. Efficiency & Effectiveness of process, service or activity

D. Confidentiality & Integrity of information

KEY A

Justification

The basic principle of Security Controls in IS are Confidentiality, Integrity & Availability of information. Hence, the correct answer is as per Option A. The other answers are incorrect.

622. Which of the following is one of the four KEY Areas which have to be understood by Information System Auditors prior to commencement of audit ?

A. Thorough understanding of the business of the entity

B. Efficiency & Effectiveness of process, service or activity

C. Sales turnover & employee strength of the entity

D. Status of entity whether government or private

KEY A

Justification

One of the **KEY A**reas which have to be understood by Information System Auditors is thorough understanding of the business of the entity. Hence, the correct answer is as per Option A. The other answers are incorrect.

623. Which of the following is one of the four KEY Areas which have to be understood by Information System Auditors prior to commencement of audit ?

A. Status of entity whether government or private

B. Efficiency & Effectiveness of process, service or activity

C. Organization structure, roles, responsibilities, policy framework, etc.

D. Sales turnover & employee strength of the entity

KEY C

Justification

One of the **KEY A**reas which have to be understood by Information System Auditors is the organization structure, roles, responsibilities, policy framework. Hence, the correct answer is as per Option C The other answers are incorrect.

624. Which of the following is one of the four KEY Areas which have to be understood by Information System Auditors prior to commencement of audit ?

A. Status of entity whether government or private

B. Efficiency & Effectiveness of process, service or activity

C. Sales turnover & employee strength of the entity

D. IT infrastructure including capacities, age of software/hardware, etc.

KEY D

Justification

One of the **KEY A**reas which have to be understood by Information System Auditors is the IT infrastructure in terms of capacities, age of software/hardware, etc. Hence, the correct answer is as per Option D. The other answers are incorrect.

625. Which of the following is one of the four KEY Areas which have to be understood by Information System Auditors prior to commencement of audit ?

A. Statutory regulations, standards, frameworks

B. Status of entity whether government or private

C. Efficiency & Effectiveness of process, service or activity

D. Sales turnover & employee strength of the entity

KEY A

Justification

One of the **KEY A**reas which have to be understood by Information System Auditors includes statutory regulations, standards & frameworks. Hence, the correct answer is as per Option A. The other answers are incorrect.

626. Section 7A of the Information Technology Act 2000 (as amended in 2008) addresses which of the following issues ?

A. Damage liability to a corporate negligent handling of personal data

B. Identity theft by corporate or individual

C. Extension of audit coverage to documents, etc. in electronic form

D. Publishing or transmission of obscene material

KEY C

Justification

Section 7A relates to extension of audit coverage to documents, records or information stored in electronic form. Hence, the correct answer is as per Option C. The other answers are incorrect.

627. Recently, there were reports of some criminal hacking of Facebook accounts and theft of passwords and other personal information. You, as a Facebook account holder, apprehend personal loss/damage and would like to proceed legally against the Facebook organization. You would like to issue a notice to them, to start with. Which Indian Act and which section of the Indian Act would you cite in your notice alleging violations ?

A. Information Technology Act, 2000, Section 7A

B. Right to Information Act, 2006, Section 43A

C. Information Technology Act, 2000, Section 43 A

D. Right to Information Act, 2006, Section 7A

KEY C

Justification

A Corporate's liability to damages on negligent handling of personal information is covered by Section 43A of the IT Act, 2000. Hence answer in Option C is correct and the other options are wrong.

628. A famous cinema actor has learnt that his password and personal information on a social networking website have been compromised owing to suspected breach of the security of the relevant networking website. The actor is furious and feels that the potential for damage to his image and reputation is great. The actor is convinced that there has been negligence involved & is particular that the website needs to be taught a lesson and made to understand that such breaches in security leading to violation of privacy are not acceptable. He proceeds, therefore, to sue the website and seeks damages of the seemingly steep amount of Rs. 1000 crores. Is there any Indian Act which would cover this situation ? If so, which Act and which clause of the Act, do you think, the actor would be able to cite for claiming such a large quantum of damages ?

A. Information Technology Act, 2000, Section 7A, damages limited to proven loss suffered

B. Information Technology Act, 2000, Section 43 A

C. Right to Information Security Act, 2006, Section 43A

D. No Indian Act covers this situation &, hence, the actor's claim may not be enforceable

KEY B

Justification

A Corporate's liability to damages on negligent handling of personal information is covered by Section 43A of the IT Act, 2000. There is no upper limit specified for compensation under the Act &, hence, even a Rs. 1000 crore claim for damages would be tenable. Hence answer in Option B is correct and the other options are wrong.

629. An employee of an organization is caught using his official computer for sending offensive messages to one of his colleagues in the organization. Which Indian Act and which clause of the Act would cover this violation of the law ?

A. Sarbanes Oxley Act, 2002, Sections 401 to 403

B. Information Technology Act 2000, Sections 7A, B and C

C. Information Technology Act 2000, Sections 66 to 66F and 67

D. Right to Information Security Act, 2006, Section 7A

KEY C

Justification

The illegal act of sending offensive messages through electronic media is covered under Sections 66 to 66F and 67 of the Information Technology Act 2000. Hence answer in Option C is correct and the other options are wrong.

630. A small scale industry has developed an effective, organic mosquito repellent which shows great promise. Since they had limitations in terms of resources, capability to scale up operations & marketing, they decided to join hands with a large marketing company. They signed off on a contract for marketing of their product, working capital funding and long term product development in the larger company's R& D laboratories. They also built in protective clauses on non-disclosure of manufacturing formula, secret ingredients, etc. which were provided to them as encrypted soft copies. After a few months, the small scale industry learns that the larger company has begun marketing a me-too product abroad, manufactured by another unit, utilising the knowledge obtained while manufacturing the small scale industry's unique product. Since informal discussions on the subject failed to make progress, the small scale industry has decided to proceed legally against the larger company.

Which Indian Act and which clause of the Act would support the small scale industry in their legal battle ?

A. Sarbanes Oxley Act, 2002, Sections 401 to 403

B. Information Technology Act 2000, Sections 43A

C. Right to Information Security Act, 2006, Section 7A

D. Information Technology Act 2000, Section 72A

KEY D

Justification

Intentional disclosure of information, without the consent of the person concerned and in breach of lawful contract, is covered under Section 72A of the Information Technology Act 2000. Hence answer in Option D is correct and the other options are wrong.

631. A small scale industry has developed an effective, organic mosquito repellent which shows great promise. Since they had limitations in terms of resources, capability to scale up operations & marketing, they decided to join hands with a large marketing company. They signed off on a contract for marketing of their product, working capital funding and long term product development in the larger company's R& D laboratories. They also built in protective clauses on non-disclosure of manufacturing formula, secret ingredients, etc which were provided to them as encrypted soft copies. After a few months, the small scale industry learns that the larger company has begun marketing a me-too product abroad, manufactured by another unit, utilising the knowledge obtained while manufacturing the small scale industry's unique product.

Under the Information Technology Act 2000, what is the potential punishment & penalty for such intentional disclosure of information, without the consent of the person concerned and in breach of lawful contract ?

A. Fine of Rs. 3 lacs alone, no imprisonment

B. Imprisonment up to 3 years and fine up to Rs. 5 lacs

C. Imprisonment up to 5 years and fine up to Rs. 10 lacs

D. Fine of Rs. 5 lacs alone, no imprisonment

KEY B

Justification

Under Section 72A of the Information Technology Act 2000, such intentional disclosure of information, without the consent of the person concerned & in breach of lawful contract is punishable with imprisonment up to 3 years and fine up to Rs. 5 lacs. Hence answer in Option B is correct and the other options are wrong.

632. In addition to giving opinion on the fair presentation of the organization's accounts, an independent auditor of an organization is expected to opine on the effectiveness of internal control over financial reporting as per a particular Act. This is mandatory as per which Act and which section of the Act ?

A. Information Technology Act 2000, Section 43A

B. Information Technology Act 2000, Section 7A

C. Sarbanes Oxley Act 2002, Section 404

D. Gramm Leach Bliley Act or the Financial Services Modernisation Act 1999, Section 14A

KEY C

Justification

This is mandatory in the U.S. as per Section 404 of the Sarbanes Oxley Act 2002. Hence answer in Option C is correct and the other options are wrong.

633. What does Auditing Standard 5 of the Public Company Accounting Oversight Board (PCAOB) relate to ?

A. Independence & performance of statutory auditors

B. Appointment, removal & terms of the Chief Internal Auditor

C. Audit of Internal control over financial reporting integrated with audit of financial statements

D. Implementation of enterprise risk management system in the organization

KEY C

Justification

The PCAOB was set up as a non-profit body as per the provisions of the Sarbanes Oxley Act with the objective of setting up standards of auditing. Auditing Standard 5 of the PCAOB relates to audit of internal control over financial reporting integrated with audit of financial statements. Hence answer in Option C is correct and the other options are wrong.

634. Corporate governance, including internal controls, enterprise risk management, etc. are covered under the provisions of _____

A. Clause 49 of the Listing agreement of SEBI

B. Section 43A of the Information Technology Act 2000

C. Section 126A of the Sarbanes Oxley Act 2002

D. Section 14A of the Gramm Leach Bliley Act or the Financial Services Modernisation Act 1999

KEY A

Justification

Corporate governance, including internal controls, enterprise risk management, etc. are covered under the provisions of Clause 49 of the Listing agreement of SEBI. Hence answer in Option A is correct and the other options are wrong.

635. ISO/IEC 27000 is basically a/an _____

A. Information security standard

B. Auditing related standard

C. Standard for quality in auditing

D. Generic standard for quality in accounting

KEY A

Justification

ISO/IEC 27000 is basically an Information security standard established by the International Standards Organization in association with the International Electro-technical Commission. It lays down the specification for information security management. Hence answer in Option A is correct and the other options are wrong.

636. Which is the International system which has laid down standards for information security & information security management system ?

A. IS 21000

B. GAAP 2014

C. IS / IEC 27001

D. IS /IEC 24007

KEY C

Justification

ISO/IEC 27001 is basically an Information security management system established by the International Standards Organization in association with the International Electro technical Commission. It lays down the specification for information security management. Hence answer in Option C is correct and the other options are wrong.

637. Information Technology Assurance Framework (ITAF) _____

A. Is a good-practice-setting reference standard for audit & assurance

B. Standards are divided into two categories

C. Standards are divided into four categories

D. Is not recognized by ISACA

KEY A

Justification

ITAF has been designed and created by ISACA. It is a good-practice-setting reference standard for audit and assurance. It is divided into three categories. Hence answer in Option A is correct and the other options are wrong.

638. Information Technology Assurance Framework (ITAF) standards comprise three categories, viz. _____

A. General, IT and non IT standards

B. General, industry specific and non-financial standards

C. General, performance and reporting standards

D. Macro, micro and non-financial standards

KEY C

Justification

The three categories of ITAF are General, Performance and Reporting standards. Hence answer in Option C is correct and the other options are wrong.

639. General standards under Information Technology Assurance Framework (ITAF) _____

A. Fall under the 1100 series of ITAF standards

B. Are the guiding principles under which IS assurance profession operates

C. Relate to the non-financial aspects of audit & assurance

D. Are yet to be validated & approved by ISACA

KEY B

Justification

ITAF has been designed and created by ISACA. The General standards, falling under the 1000 series, are the guiding principles under which the IS assurance profession operates. Hence, the answer in Option B is correct and the other options are wrong.

640. Performance standards under Information Technology Assurance Framework (ITAF) _____

A. Deal with the minimum performance standards expected of installed software

B. Deal with conduct of the assignment & exercising of professional judgement & due care

C. Relate to the minimum level of quality of audit to be carried out by IS auditors

D. Fall under the 1400 series of ITAF

KEY B

Justification

ITAF has been designed and created by ISACA. The Performance standards, falling under the 1200 series, deal with conduct of the assignment & the exercising of professional judgement & due care. Hence, the answer in Option B is correct and the other options are wrong.

641. Reporting standards under Information Technology Assurance Framework (ITAF) _____

A. Deal with report types, communication means & communicated information

B. Deal with the minimum performance standards expected of installed software

C. Relate to the minimum level of quality of audit to be carried out by IS auditors

D. Fall under the 1200 series of ITAF

KEY A

Justification

ITAF has been designed and created by ISACA. The Reporting standards, falling under the 1400 series, deal with report types, communication means & communicated information. Hence, the answer in Option A is correct and the other options are wrong.

642. COBIT 5 _____

A. Is a framework for governance & management of enterprise IT, excluding risk aspects

B. Operates through 7 principles

C. Is a framework for governance & management of enterprise IT

D. Can be useful only for large organizations with ERP systems

KEY C

Justification

COBIT is a framework for governance & management of enterprise IT. It helps organizations manage risk & ensure compliance, continuity, security & privacy. It has 5 KEY principles and can be used in any type of organization, irrespective of size or nature of business. Hence, the answer in Option C is correct and the other options are wrong.

643. COBIT 5's KEY principles _____

A. Are 3 in number & focus on shareholders' needs

B. Are 7 in number and applies multiple frameworks to cover the whole organization

C. Are 5 in number & Include meeting stakeholders' needs

D. Marries the management & governance, creating shared goals & objectives

KEY C

Justification

COBIT5 is a framework for governance & management of enterprise IT. It helps organizations manage risk & ensure compliance, continuity, security & privacy. It has 5 KEY principles and can be used in any type of organization, irrespective of size or nature of business. It applies a single integrated framework to address the entire organization. It deliberately separates governance & management. Hence, the answer in Option C is correct and the other options are wrong.

644. COBIT 5's KEY principle of meeting stakeholders' needs creates value by _____

A. Maximizing dividend payout to shareholders

B. Balancing benefits and the optimization of risk & use of resources

C. Reducing costs to the minimum

D. Eliminating risks & avoiding wasteful expenditure

KEY B

Justification

COBIT5 is a framework for governance & management of enterprise IT. It helps organizations manage risk & ensure compliance, continuity, security & privacy. One of its 5 KEY principles is meeting stakeholders' needs. This principle creates value by balancing the benefits against the optimization of risk & the use of resources. Hence, the answer in Option B is correct and the other options are wrong.

Module 4
Protection of Information Assets

645. In order to protect its critical data from virus attacks an organisation decides to limit internet access to its employees. What type of risk response has the organisation exercised?

A. Mitigate

B. Avoid

C. Accept

D. Transfer

KEY A

A. "Mitigate" is the correct answer. Risk Mitigation primarily focuses on designing and implementing controls to prevent incidents due to risk materialisation.

B "Avoid" is not correct as the organisation is not avoiding the use of technology to avoid risks

C "Accept" is not correct as the organisation has not chosen to accept the risk

D "transfer" is not correct as the organisation is not passing on the risk to another entity

646. A production company decides to insure against production loss due to natural calamities. What type of response is this classified as?

A. Mitigate

B. Accept

C. Transfer

D. Avoid

KEY A

C "Transfer" is correct as the organisation passes on the risk to the insurance company.

A: "Mitigate" is not correct as the organisation is not implementing any controls within

B: "Accept" is not correct as organisation has not accepted the risk

D "Avoid" is not correct as the organisation has not decided to avoid technology to minimise risk

647. Implementation of Information system control in an organisation ensures that:

A. Risk is transferred to another entity

B. Desired Outcome from business process is not affected

C. Losses are avoided

D. Incidents due to risk materialisation are avoided

KEY B

B is correct – Information Control includes implementation of policies, procedures and practices which ensure that the desired outcome from business is not affected

A is not correct – this is a type of risk response

C & D are not correct – They are not a direct result of implementation of controls

648. Which of the following leads to destruction of information Assets such as hardware, software and critical data?

A. Data error during data entry

B. Non maintenance of privacy with respect to sensitive data

C. Unauthorised access to computer systems

D. Using systems that do not meet user requirements

KEY C

C is correct - Unauthorised access to computer systems, computer viruses, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets

A is not correct – data error causes damage to the business process only

B is not correct – non maintenance of privacy does not cause damage to Information Assets, it infringes on the privacy of the customer

D is not correct – this is a system efficiency objective

649. Maintenance of privacy in relation to data collected by an organisation is very important because:

A. Errors committed during entry would cause great damage

B. It has an impact on the infrastructure and business competitiveness

C. It can be easily accessed by third parties

D. It contains critical and sensitive information pertaining to a customer

KEY D

D is correct - Today data collected in a business process contains details about an individual on medical, educational, employment, residence etc.

A B and C are incorrect as these are not related to privacy of data

650. The role of an internal auditor in Information Systems auditing includes:

A. Safeguarding data integrity

B. Attesting management objectives

C. Attesting System effectiveness and system efficiency objectives

D. Implementing control procedures

KEY C

C is correct - management objectives of the internal auditor includes not only attest objectives but also effectiveness and efficiency objectives.

A & B are incorrect – these are the responsibilities of an external auditor

D is incorrect – this is the responsibility of the organisation

651. What does an external Information Systems auditor focus on?

A. Attesting objectives that focus on asset safeguarding and data integrity

B. Attesting system effectiveness

C. Attesting system efficiency

D. Implementing control procedures

KEY A

A is correct - Information systems auditing is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding and data integrity

B & C are incorrect – these are the responsibilities of an external auditor

D is incorrect. This is the responsibility of the organisatio006E

652. By auditing the characteristics of the system to meet substantial user requirements, which control objective does an IS Auditor attest?

A. Data integrity objectives

B. System Effectiveness Objectives

C. Asset safeguarding objectives

D. System efficiency objectives

KEY B

B is correct - Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet substantial user requirements.

A is incorrect – the auditor checks the extent of access to information and the value of data to business

C is incorrect – the auditor assesses the internal controls to protect software and hardware

D is incorrect – the auditor assesses the optimal usage of system resources

653. A statement of purpose achieved by implementing control procedures in a particular IT process is defined as:

A. IS Control framework

B. Internal Controls

C. Control Objective

D. Preventive Controls

KEY C

C is correct - Control objective is defined as "A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT process or activity"

B is incorrect – it is the basic outline of the policies of the organisation towards IS control

A & D are incorrect – these are the steps taken by the organisation to protect information and system assets

654. Which of the following is an example of technical implementation of Internal Control?

A. Outlining policies that safeguard information assets

B. Installing a security guard in the premises to restrict entry of unauthorised persons

C. Locking the room containing sensitive documents

D. Investing in tools and software to restrict unauthorised access to information

KEY D

D is correct - this is an example of technical implementation

B is incorrect – this is an example of administrative implementation

A & C are incorrect – these are examples of physical implications

655. What are preventive controls?

A. those mechanisms which refer unlawful activities to the appropriate person/group

B. those controls which attempt to predict potential problems before they occur

C. those mechanisms which modify the processing system to minimise error occurrences

D. those controls which corrects the error arising from a problem

KEY B

B is correct - Preventive controls attempts to predict problems before they occur and make necessary adjustments. They are designed to protect the organisation from unauthorised activities

A is incorrect – this is a characteristic of detective control

C & D are incorrect – these are characteristics of corrective control

656. What are detective controls?

A. Provision for control of probable threats from materializing

B. Those controls that are designed to detect errors and omissions of malicious acts

C. Those controls which assess probable threats

D. Those controls which minimise the impact of threat

KEY B

B is correct - These controls are designed to detect errors, omissions of malicious acts that occur and reporting the occurrence.

A & C are incorrect – this is a characteristic of preventive control

D is incorrect – this is a characteristic of corrective control

657. What are corrective controls?

A. Those controls that correct an error once it has been detected

B. Those mechanisms which provide a clear understanding of the vulnerabilities of an asset

C. Surprise checks by an administrator

D. Those mechanisms by which the management gets regular reports of spend to date against a profiled spend

KEY A

A is correct - These controls are designed to reduce the impact or correct an error once it has been detected.

B is incorrect – this is a characteristic of preventive control

C is incorrect – this is a characteristic of detective control

D is incorrect – this is an example of detective control

658. An organisation decides to control the access to a software application by segregating entry level and updation level duties. What type of internal control does this amount to?

A. Preventive Control

B. Detective Control

C. Corrective Control

D. physical implementation of a control

KEY A

A is correct - Examples of preventive controls include – employing qualified personnel, segregation of duties, access control, documentation etc.

B and C are incorrect – detective and corrective controls are not designed to predict potential problems

D is incorrect – physical implementation of a control includes only physical aspects like security guards and locked rooms

659. Under which type of control mechanism does taking a back up of everyday activity classify as?

A. Detective Control

B. Preventive control

C. Corrective control

D. Administrative Implementation of Control

KEY C

C is correct – Examples of Corrective Controls are - contingency planning, backup and restoration procedure, rerun procedure, procedure for treating error, etc.

A & B are incorrect – Detective and Preventive controls are not designed to reduce the impact or correct an error once it has been detected.

D is incorrect – Administrative implications of controls are items such as policies and processes

660. As an IS auditor, how would you rate a computerised detective control which is moderately efficient and with corresponding corrective action?

A. High

B. Low

C. Moderate

D. Blank

KEY A

A is correct - Computerised control which is most effective, generally controls that are computerized and applied before processing can take place; moderately efficient, with corresponding corrective action are rated as "High"

B, C and D are incorrect –

***M**oderate*- Controls implemented over a cause of exposure/error type and is moderately effective.

***L**ow*-Controls implemented over a cause of exposure/error type but have low effectiveness.

***B**lank*- Controls not implemented or does not exist to that cause or exposure or error type.

661. As an IS auditor, how would you rate a least effective and inefficient manual detective control without corrective action?

A. High

B. Low

C. Blank

D. Moderate

KEY C

C is correct - Manual control which is least effective, generally manual controls applied at front-end of processing; moderately efficient are rated as "Blank"

A, B & D are incorrect –

***H**igh*- Controls implemented over a cause of exposure/error type and should be highly effective.

***M**oderate*- Controls implemented over a cause of exposure/error type and is moderately effective.

***L**ow*-Controls implemented over a cause of exposure/error type but have low effectiveness.

662. Which of the following describes the role of a risk owner?

A. Ensuring that all control objectives that focus on asset safeguarding and data integrity are attested

B. Ensuring that the risk response is effective enough and is translated into actions that will prevent and/or detect the risk.

C. Ensuring that all system effectiveness and system efficiency objectives are attested

D. Ensuring that risk associated with a certain activity is mitigated either by reducing likelihood or reducing impact

KEY B

B is correct - Generally owner is a person or position within the organization that has close interest about the processes affected due to risk. The person responsible needs to ensure that the risk response is translated into actual day-to-day actions that will prevent and/or detect the risk.

A, C and D are incorrect – These are the roles of IS auditors

663. The process of Information Security does not end with implementation of risk responses. The next step is to:

A. Facilitate to conduct risk assessment workshops

B. Ensure that KEY business risks are being managed appropriately

C. Plan the audit cycle according to the perceived risk

D. Ensure that the identified risk stays within an acceptable threshold

KEY D

D is correct - After implementation of the risk responses and management techniques, the managers need to monitor the actual activities to ensure that the identified risk stays within an acceptable threshold.

A, B and C are incorrect – these are the roles that an auditor has to perform in view of control assessment

664. What process must an organisation follow to ensure that the identified risk stays within the acceptable limits?

A. Evaluate the efficiency of the objectives of controls

B. Designing an effective internal control framework

C. Periodic review of the risk assessment exercise and proactive review of possible risks

D. Optimise the use of various information resources

KEY C

C is correct - To ensure that risks are reviewed and updated organizations must have a process that will ensure the review of risks. Periodic review: the risk assessment exercise may be conducted after predefined period say annual. Change management processes proactively review the possible risks and ensure they are part of organization's risk register.

A B and D are incorrect – these are steps to be taken towards identifying, assessing risks and implementing internal controls

665. How does an IS auditor prioritise the controls that needs to be tested?

A. By reviewing the control catalogue (which is a collective record of all controls implemented)

B. By reviewing control procedure documents

C. By facilitating risk assessment workshops

D. Planning the audit cycle according to the risks perceived

KEY A

A is correct - The first step in control's assessment is to review the control catalogue (which is a collective record of all controls implemented) and ensure that associated risk is mitigated either by reducing likelihood or reducing impact or both.

B is incorrect – This should be done after reviewing the control procedure documents

C and D are incorrect – These are the roles of an auditor with respect to Information risk management

666. In case of control self assessment, who does the actual testing of controls?

A. The owner of the identified risk for which the control has been implemented

B. Internal auditor, during the audit cycle as planned

C. Staff whose day-to-day role is within the area of the organisation

D. External auditor, while reviewing the management of KEY risks

KEY C

C is correct - In case organization has implemented control self-assessment, the actual testing of the controls is performed by staff whose day-to-day role is within the area of the organisation that is being examined as they have the greatest knowledge of how the processes operate.

A is incorrect – though he/she is the risk owner, it is appropriate that the person who is actually involved in the activity does the self- assessment

B and D are incorrect – they are external to the specified activity and are not eligible to do the self- assessment.

667. Of the below mentioned roles, which one should an auditor refrain from performing?

A. Giving assurance that the risks are being evaluated correctly

B. Implementing risk response on management's behalf.

C. Evaluating the risk management process

D. Reviewing the management of KEY risks

KEY B

B is correct - This is the job of the management, an auditor only needs to review the risk response

A, C and D are incorrect – these are the roles of an IS auditor

668. Of the below mentioned roles, which one of the following should be performed by an IS auditor?

A. Set the risk appetite

B. Impose risk management process

C. Evaluate Risk Management process

D. Take decision on risk responses

KEY C

C is correct - Evaluating the risk management process is the KEY role of an IS auditor

A, B and D are incorrect – these are the roles of the management and the risk owner.

669. A data centre housing about 200 employees is involved in handling businesses processes of multinational companies. For security reasons, it decides to shift its network server and mail server to a secluded room with restricted entry. What kind of internal control is this?

A. Manual Preventive Control

B. Manual Detective Control

C. Computerised Preventive Control

D. Computerised Corrective Control

KEY A

A is correct - This is a preventive control which is designed to protect the data and mail server from unauthorised access. Moreover, it is a manual control as the servers are physically moved to a secluded room.

B, C and D are incorrect – The action does not categorise under any of these categories for the reasons mentioned above.

670. Company depends on an MIS given to it by an outsourced vendor to identify payment defaulters and fine them. On further investigation about the correctness of data supplied, he finds that though at the entry level, a lot of mistakes are prone to happen, there are computerised controls at the vendors end and also the company's end at processing level to minimise these. As an IS auditor, how would you rate efficiency of these controls?

A. Blank

B. Low

C. Moderate

D. High

KEY D

D is correct – Computerised corrective controls are applied before processing and hence efficiency of controls is high

A, B and C are incorrect – The Company is not relying on unchecked information. The information is checked not by manual corrective control but computerised corrective control. Hence the efficiency cannot be rated as blank, low or moderate.

671. The HR department of a company pays its employees medical claims subject to a maximum limit per employee per year. For this, it relies on data partaining to a full year downloaded through the appropriate software. However, it does not have a proper back up or restoration procedure in place. How will an IS auditor rate this?

A. High control

B. Low Control

C. Blank Control

D. Moderate Control

KEY B

B is correct - Here there is no corrective control in case of loss of data and there is no way the department can ascertain how much it has paid an employee in a year.

A, C and D are incorrect – Reason is as mentioned above

672. A data centre handling outsourced operations decides to set up a parallel facility for its critical activities at some place other than its present place of operations. This is done with an intention to facilitate return of business to normal levels in case of impact of natural disasters or unforeseen events. Under what security policy is this categorised?

A. Business Continuity Management Policy

B. Acceptable use of Information Assets policy

C. Physical Access and Security Policy

D. Asset Management Policy

KEY A

A is correct - This policy defines the requirements to ensure continuity of business critical operations. It is designed to minimize the impact of an unforeseen event (or disaster) and to facilitate return of business to normal levels.

B is incorrect - An acceptable use policy (AUP), also known as an Acceptable Usage policy or Fair Use policy, is a set of rules applied by the owner or manager of a network, website or large computer system that restrict the ways in which the network, website or system may be used.

C is incorrect - Physical security describes security measures that are designed to restrict unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).

D is incorrect – This policy defines the requirements for Information Asset's protection. It includes assets like servers, desktops, handhelds, software, network devices etc. Besides, it covers all assets used by an organization- owned or leased.

673. What are the three KEY objectives of Information Security Management (CIA Triad)?

A. Compliance, Integrity and Availability

B. Confidentiality, Information Security and Availability

C. Confidentiality, Integrity and Availability

D. Confidentiality, Integrity and Asset Management

KEY C

C is correct - Protection of information assets includes the KEY components that ensure confidentiality, integrity and availability (CIA) of information assets. There are three KEY objectives of Information Security Management viz.: ***Confidentiality, Integrity and Availability*** also called ***CIA Triad***.

A, B and D are incorrect – Though important for Information Security, these are not the KEY components.

674. What does "Integrity" mean with respect to Information Security Management?

A. No data/information or programs shall be allowed to be modified by anyone without proper authority.

B. No data or information is made available to any person within or outside the organization, other than the persons who are authorized to use that data.

C. All Information Systems including hardware, communication networks, software applications and the data they hold, is available to authorized users to carry out business activities.

D. Executive management endorsement of intrinsic security requirements to ensure that security expectations are met at all levels of the enterprise

KEY A

A is correct – This is the correct definition as per paragraph 2.1 of the chapter

B and C are incorrect – these are definitions of "Confidentiality" and "Availability"

D is incorrect – this clause pertains to Senior Management Commitment and support

675. What provides the basis for ensuring that information security expectations are met at all levels of an enterprise?

A. Adopting an internationally recognized reference framework to establish an Information Security framework

B. Successful establishment and endorsement of intrinsic security measures by the senior management

C. Prioritising expenditures to mitigate risks and avoid spending more resources in assessing risks

D. Ensuring that the framework followed to implement, maintain, monitor and improve Information Security is consistent with the organisational culture.

KEY B

B is correct - Commitment and support from senior management are important for successful establishment and continuance of an information security management program.

A C and D are incorrect – These are some of the critical success factors to Information Security Management.

676. How does an enterprise ensure that the information present in any of its business processes is protected and secure?

A. By ensuring that the framework followed to implement, maintain, monitor and improve Information Security is consistent with the organisational culture.

B. By adopting an internationally recognized reference framework to establish an Information Security framework

C. By spending resources widely and transparently

D. By establishing and enforcing an Information Security Program

KEY D

D is correct - Information Security program focuses on protecting information present in business processes. Establish a program to improve Information Security management enterprise-wide and enforce it.

A B, and C are incorrect – These are other critical success factors to Information Security Management.

677. How does an enterprise demonstrate to staff, customers and trading partners that their data is safe?

A. By establishing and enforcing an Information Security Program

B. By ensuring that the framework followed to implement, maintain, monitor and improve Information Security is consistent with the organisational culture.

C. Adopting an information security standard

D. By spending resources widely and transparently

KEY C

C is correct - Adopting an information security standard seems to demonstrate to staff, customers and trading partners that their data is safe, and that there is an independent verification of this fact.

A B and D are incorrect – These are other critical success factors to Information Security Management.

678. The IS policy of an enterprise that talks about protecting non-public personal information from unauthorised use, corruption, disclosure and distribution is:

A. Acceptable usage policy or Fair Use policy

B. Data classification and Privacy Policy

C. Physical Access and Security policy

D. Asset Management Policy

KEY B

B is correct - the policy of the Organization to protect against the unauthorized access, use, corruption, disclosure, and distribution of non-public personal information in its possession, and to comply with all applicable laws and regulations regarding such information is termed as the Data Classification and privacy policy

A is incorrect – is a set of rules applied by the owner or manager of a network, website or large computer system

C is incorrect – Physical security describes security measures that are designed to restrict unauthorized access to facilities, equipment and resources

D is incorrect - This policy defines the requirements for Information Asset's protection

679. The policy which restricts the ways in which the network, website or system may be used by a user of an enterprise is termed as:

A. Acceptable usage policy or Fair Use policy

B. Physical Access and Security policy

C. Asset Management Policy

D. Business Continuity Management Policy

KEY A

A is correct - An acceptable use policy (AUP), also known as an Acceptable Usage policy or Fair Use policy, is a set of rules applied by the owner or manager of a network, website or large computer system that restrict the ways in which the network, website or system may be used.

B is incorrect – Physical security describes security measures that are designed to restrict unauthorized access to facilities, equipment and resources

C is incorrect - This policy defines the requirements for Information Asset's protection

D is incorrect - This policy defines the requirements to ensure continuity of business critical operations.

680. The IS policy which talks about protecting personnel and physical property from damage or harm is termed as:

A. Asset Management policy

B. Business Continuity Management policy

C. Physical access and security policy

D. Password policy

KEY C

C is correct - Physical security describes security measures that are designed to restrict unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).

A is incorrect - This policy defines the requirements for Information Asset's protection

B is incorrect - This policy defines the requirements to ensure continuity of business critical operations.

D is incorrect - This policy defines high-level configuration of password to be used within organization to access the information assets.

681. What is the IS policy that defines the requirements for Information Assets protection?

A. Business Continuity Management Policy

B. Asset Management Policy

C. Network Security Policy

D. Password policy

KEY B

B is correct - This policy defines the requirements for Information Asset's protection. It includes assets like servers, desktops, handhelds, software, network devices etc. Besides, it covers all assets used by an organization- owned or leased.

A is incorrect - This policy defines the requirements to ensure continuity of business critical operations.

C is incorrect - A network security policy defines the overall rules for organisation's network access

D is incorrect - This policy defines high-level configuration of password to be used within organization to access the information assets.

682. The characteristics of a strong password that protects information assets should be:

A. Maximum 8 characters, case specific

B. Minimum 8 characters, only alpha numeric

C. Minimum 8 characters, only alphabets and easy to remember

D. Minimum 8 characters, case specific and containing special characters

KEY D

D is correct - The password policy defines high-level configuration of password to be used within organization to access the information assets. For example:

- Password length must be more than 8 characters
- Password must be complex containing upper case, lower case, numeric and special characters
- Password must be changed regularly
- Password should not be used again for minimum period
- Password should not be changed in consecutive sequence

A B and C are incorrect – These are not the characteristics of a strong password

683. What should be done to ensure that security policies are in tune with the management's intent?

A. Change passwords regularly

B. Restrict unauthorised access to facilities

C. Review the security policies periodically

D. Hold non public personal information in strict confidence

KEY C

C is correct - Information security policies need to be maintained and updated regularly. This might need to revisit the security requirements and hence policies. Hence, it is necessary to review the security policies periodically to ensure that they are in line with the management's intent.

A, B and D are incorrect – These are the parts of an information security policy

684. Policies are generic and sometimes cannot be enforced in specific situations. Can there be a relaxation of adherence to policy in such cases?

A. Yes. But, it is necessary to ensure that there are suitable compensating controls

B. Yes. Policies can be relaxed in case of such situations unconditionally

C. No. Under no circumstances can an Information Security policy be relaxed

D. Yes. Adherence to the policy can be relaxed for an indefinite period for the specific activity only.

KEY A

A is correct - In such situations it is necessary to ensure there are suitable compensating controls so that the risks mitigated by enforcement of policy are within acceptable limits.

B, C and D are incorrect – Policies can be relaxed for a specific period provided the exceptions are appropriately approved and these exceptions must be reviewed periodically.

685. Standards, Guidelines and Procedures are the three elements of policy implementation. In what order should they be followed for proper implementation?

A. Guidelines, Procedures and Standards

B. Procedures, Standards and Guidelines

C. Standards, Guidelines and Procedures

D. Guidelines, Standards and Procedures

KEY C

C is correct - The next level down from policies is three elements of policy implementation as given here: **Standards:** Specify the uniform way for the use of specific technologies in an organization. **Guidelines:** Guidelines are similar to standards; they refer to the methodologies of securing systems, but they are only recommended actions and are not compulsory. **Procedures:** Procedure contains the detailed steps that are followed to perform a specific task. Procedures are the detailed actions that must be followed.

A, B and D are incorrect – These do not specify the correct levels of implementation. Unless Standards are set, guidelines cannot be recommended. Unless guidelines are recommended, procedures cannot be outlined for implementing policies.

686. With respect to Information Security, what does 'Segregation of Duties' mean?

A. No individual, of whatever seniority in the organization, should have the ability to carry out every step of a sensitive business transaction.

B. The responsibility of powerful and KEY access to the system should not be carried out by one person alone.

C. No person should be kept in one particular post for too long

D. Organisations should avoid situations where an individual becomes indispensable to the business

KEY A

A is correct - No individual, of whatever seniority in the organization, should have the ability to carry out every step of a sensitive business transaction. Access to too many functions enables staff to carry out a fraudulent transaction and hide their tracks.

B is incorrect – This pertains to the 'Four Eyes' or 'Two Person' principle

C is incorrect – This pertains to rotation of duties

D is incorrect – This pertains to 'KEY Man' policies

687. In a bank, the chest in which cash is kept has to be opened with two keys, one which is in the control of the manager and the other which is in the control of the accountant/sub manager. Under what security rule does this aspect classify?

A. Segregation of Duties

B. The 'Four Eyes' or 'Two Person' principle

C. Rotation of Duties

D. 'KEY Man' policies

KEY B

B is correct - To reduce the opportunities for any person to breach security, those responsibilities and duties which would afford particularly powerful access to the system, or which act at KEY control points, should not be carried out by one person alone.

A, C and D are incorrect – These are other security rules designed for implementation of IS policies

688. An organisation which is IS compliant requires its employees to take two weeks consecutive mandatory leave. Under which security rule does this feature classify as?

A. Rotation of duties

B. 'KEY Man' policies

C. Two person principle

D. Segregation of duties

KEY A

A is correct - No one person should be kept in one particular post for too long, especially if that appointment involves any particular security responsibilities opportunities for dishonesty. A similar rule should insist that staff take at least two consecutive weeks; holiday in any year, as experience has shown that many frauds need continual masking by the perpetrator and may surface when the individual is away.

B, C and D are incorrect – These are other security rules designed for implementation of IS policies

689. Every corporate asset, building, item of equipment, bank account and item of information should have a clearly defined 'owner'. What are the responsibilities of the owner of such assets?

A. Adding and deleting user identifiers from the system

B. Defining security responsibilities for every person in the organization

C. Ensuring that the asset is well maintained, accurate and up to date

D. Establishing and Implementing an effective IS program

KEY C

C is correct - The owner should have a defined set of responsibilities.

- Ensuring that computer rooms are kept clean and tidy
- Ensuring that equipment is well maintained and kept operational
- Ensuring that an item of data used by the organization is accurate and up to date.

A,B and D are incorrect – These are steps to ensure that Information Security is implemented in an organisation.

690. When an owner is not able to manage a particular asset on a day to day basis, the responsibility is passed on to a custodian. Which of the following is an example of a custodian?

A. a vendor responsible for an outsourced activity

B. data center controlling access to production data

C. a subordinate doing the function of an owner during his absence

D. an auditor auditing the effectiveness of an asset

KEY B

B is correct - The owner should clearly state the requirements, the responsibilities and associated levels of authority of the custodian and final management responsibility will always reside with the owner. Examples of custodian include a data center operations function controlling access to production data, and a computer bureau running an application for a client.

A,C and D are incorrect – these are not examples of a custodian. They pertain to roles of other players in Information Security Management.

691. The actual security mechanism has its application in certain KEY tasks of security systems. What are these called as?

A. Organisational control

B. Backup data

C. Control points

D. Operating System

KEY C

C is correct - In all security systems there are KEY tasks which can be called control points. It is at these control points that the actual security mechanism has its application.

A is incorrect – this is the control that an organisation places to secure its information assets

B is incorrect – this is a procedure that is adopted for safeguarding critical data

D is incorrect – Operating system is a software that manages computer hardware and software resources

692. Name the participant which ensures that all stakeholders impacted by security considerations are involved in the Information Security Management process.

A. Steering committee

B. Information Owner

C. Information Custodian

D. System Owner

KEY A

A is correct - It serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives. It can also be instrumental in achieving modification of behavior toward a culture more conducive to good security.

B is incorrect - Information Owner (also called ***Data Owners***) is responsible for a company information asset.

C is incorrect – Information custodian is assigned the task of implementing the prescribed protection defined by the security procedure

D is incorrect – The system owner is responsible for one or more systems, each of which may process and store data owned by different information owners.

693. Name the participant who ensures that security controls have been implemented in accordance with the information classification.

A. information Custodian

B. Information Owner

C. System Owner

D. Process Owner

KEY B

B is correct - Information Owner (also called ***Data Owners***) is responsible for a company information asset. The responsibilities are generally assigned to person/position that owns business process.

A is incorrect - Information custodian is assigned the task of implementing the prescribed protection defined by the security procedure

C is incorrect – The system owner is responsible for one or more systems, each of which may process and store data owned by different information owners.

D is incorrect – This person is responsible for the implementation, management and continuous improvement of a process that has been defined to meet a business requirement.

694. Name the participant who ensures safe keeping of information on behalf of the information owner.

A. System Owner

B. Process Owner

C. Information Custodian

D. System Administrator

KEY C

C is correct - Information custodian is assigned the task of implementing the prescribed protection defined by the security procedure and top level/Senior management decisions. Among other activities, information custodian also performs following activities:

- Ensuring safe keeping of information on behalf of information owner
- Providing access to users that are approved by owners
- Running regular backups and routinely testing from backup data
- Performing data restoration activity from the backups when necessary

A is incorrect – The system owner is responsible for one or more systems, each of which may process and store data owned by different information owners.

B is incorrect – This person is responsible for the implementation, management and continuous improvement of a process that has been defined to meet a business requirement.

D is incorrect - System Administrator is the one with administrative / root level privileges of the Operating systems like Windows, Unix etc.

695. Whose responsibility is it to ensure that adequate security is built once the applications and systems have been acquired and are ready for use in the production department?

A. System Owner

B. Process Owner

C. System Administrator

D. User Manager

KEY A

A is correct - A system owner is responsible for:

- Integrating security considerations into application and system purchasing process and decisions.
- Ensuring that adequate security is built or defined once the applications and systems have been acquired and are ready for use in production environment.
- Ensuring that the systems are properly assessed for vulnerabilities and report any to the incident response team and information owner.

B is incorrect – This person is responsible for the implementation, management and continuous improvement of a process that has been defined to meet a business requirement.

C is incorrect - System Administrator is the one with administrative / root level privileges of the Operating systems like Windows, Unix etc

D is incorrect - User manager is the immediate manager or reporting manager of an employee.

696. Who is the person responsible for creating new system user accounts and changing permissions of existing user accounts?

A. User Manager

B. System Administrator

C. Super User

D. Security Manager

KEY B

B is correct - A system administrator is responsible for:

- Creating new system user accounts,
- Changing permissions of existing user accounts,
- Implementing new security software,
- Testing security patches and updates, and
- Resetting user passwords.

A is incorrect - User manager is the immediate manager or reporting manager of an employee.

C is incorrect – Super User is the person with the highest level of authorization access, who can make any transaction and master setup activity immediately and sets the conditions for transaction approvals, financial daily limits of each transaction type, and classifies and authorizes other Users.

D is incorrect - Security manager is responsible for defining security strategy and policies for the organization.

697. Who holds the ultimate responsibility for all user id's and information assets owned by the company's employees?

A. Super User

B. Security Manager

C. Steering Committee

D. User Manager

KEY D

D is correct - User manager is the immediate manager or reporting manager of an employee. They have ultimate responsibility for all user IDs and information assets owned by company employees.

A is incorrect – Super User is the person with the highest level of authorization access, who can make any transaction and master setup activity immediately and sets the conditions for transaction approvals, financial daily limits of each transaction type, and classifies and authorizes other Users.

B is incorrect - Security manager is responsible for defining security strategy and policies for the organization.

C is incorrect - a steering committee is comprised of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives.

698. Who is responsible for defining security strategy and policies for an organisation?

A. Steering Committee

B. Information Owner

C. Security Manager

D. Information Custodian

KEY C

C is correct - Security manager is responsible for defining security strategy and policies for the organization. The manager also ensures defining roles and responsibilities.

A is incorrect - a steering committee is comprised of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives.

B is incorrect - Information Owner (also called ***Data Owners***) is responsible for a company information asset. The responsibilities are generally assigned to person/position that owns business process.

D is incorrect - Information custodian is assigned the task of implementing the prescribed protection defined by the security procedure

699. What is the role of Human Resources Security when the employment of a person is terminated?

A. Ensure that access to sensitive data is revoked immediately

B. Define appropriate access to sensitive information for another person

C. Send regular updates in an effort to safeguard the data which was in their possession

D. Educate the terminated employee to prevent data disclosure to 3rd parties

KEY A

A is correct - To prevent unauthorized access to sensitive information, access must be revoked immediate upon termination/separation of an employee and 3rd parties with access to such information. This also includes the return of any assets of the organization that was held by the employee.

B is incorrect – Before granting access to a replacement, access of the leaving employee should be revoked

C and D are incorrect – these are wrong steps – terminated employee should not have access to sensitive data

700. What is 'Acknowledge Policy' with regard to Security Awareness training program?

A. All employees are required to undergo security awareness training

B. All employees and third parties having access to sensitive information have to complete training at least once a year

C. All employees are required to acknowledge that they have read and understood the organization's information security / acceptable use policy.

D. All employees have to go through a formal induction process designed to introduce the organisations security policies

KEY C

C is correct - **Acknowledge Policy e**nsures that all employees are required to acknowledge that they have read and understood the organization's information security / acceptable use policy.

A, B, and D are incorrect – These are other important considerations for a security awareness training program

701. What is the primary goal of configuration management?

A. Ensuring that changes to the system do not unintentionally diminish security

B. Mitigate the impact that a change might have on the security of other systems

C. Configuring systems to meet the security requirement of the organisation

D. Updating the software with the latest versions of all applications

KEY A

A is correct - The primary security goal of configuration management is to ensure that changes to the system do not unintentionally diminish security.

B is incorrect – This is also a goal of configuration management, though not primary

C and D are incorrect – These are not goals, they form part of configuration management

702. What is the objective of a non- disclosure agreement?

A. Identify functional and physical characteristics of each configuration setting

B. Impose limitations on like organisations that operate in the same competitive space

C. Creates a confidential relationship between parties to protect any type of confidential information

D. Follow a checklist to address whether any of the security holes remain unplugged

KEY C

C is correct - A non-disclosure agreement (NDA), also known as a confidentiality agreement (CA), is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties.

A, B and D are incorrect – these are some of the issues and challenges of IS Management

703. What is the primary cause for lack of integration in system and security design?

A. inadequacy of checklists as a means to address security concerns

B. limitations imposed on like organizations that operate in its competitive space

C. the challenge of finding the right balance between protecting the organization's core assets and processes and enabling them to do their job

D. systems and security design are undertaken in parallel rather than in an integrated manner

KEY D

D is correct - Development duality is a phenomenon where systems and security design are undertaken in parallel rather than in an integrated manner.

A.B and C are incorrect – These are other issues and challenges of IS management

704. What is a Denial-of-Service attack?

A. An attempt to make a machine or network unavailable to its intended users.

B. Unauthorized access to an organisation's internal network.

C. Illegal copying of software.

D. Creation of Internet Protocol (IP) packets with a forged source IP address

KEY A

A is correct - A Denial-of-Service attack (DoS) is an attempt to make a machine or network unavailable to its intended users. This causes legitimate users to not be able to get on the network and may even cause the network to crash.

B is incorrect - unauthorized access to an organisation's internal network is referred to as Network Intrusion

C is incorrect – Illegal copying of software is referred to as Software Piracy

D is incorrect – creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system is termed as 'spoofing IP addresses'.

705. What is 'Phishing'?

A. Unauthorized real-time interception of a private communication

B. Attempting to obtain otherwise secure data by conning an individual into revealing secure information

C. Trying to obtain information like user ID and password for bank accounts, credit card pin etc. using electronic communication means

D. Exploiting vulnerabilities of a system to gain unauthorized access to system or resources

KEY C

C is correct - Phishing is the act of trying to obtain information like user ID and password for bank accounts, credit card pin etc. using electronic communication means like emails, fake websites etc.

A is incorrect - unauthorized real-time interception of a private communication is called eavesdropping

B is incorrect - attempting to obtain otherwise secure data by conning an individual into revealing secure information is called Social Engineering

D is incorrect – exploiting vulnerabilities of a system to gain unauthorized access to system or resources like a website, bank accounts etc. is called hacking

706. What are 'botnets'?

A. underground network established by hackers by sending malware

B. targeted attack that continues for a sustained period for about a year or more

C. attacks that are specifically targeted to selected organization

D. changing of data before or during entry into the computer system

KEY A

A is correct - **Botnets:** Acronym for robotic network. An underground network established by hackers by sending malware. This malware goes undetected since it is part of targeted attack.

B is incorrect - A type of targeted attack that continues for a sustained period for about a year or more is called Advanced Persistent Threat (APT)

C is incorrect - attacks that are specifically targeted to selected organization are called 'targeted attacks'.

D is incorrect - changing of data before or during entry into the computer system is called 'dat diddling'.

707. What should be done to minimise damage from security incidents and and to recover from them?

A. Report an incident to an appropriate authority to know what action should be taken

B. Handle the incident independently and follow it up if required

C. Establish a formal incident response capability and centralise it with the KEY roles and responsibilities

D. Plan and prepare a response system proactively in case of the occurrence of an incident

KEY C

C is correct - Establishing a formal incidence response capability and coordinating it within the organisation to include all KEY roles and responsibilities is the proper way to minimise damage from security incidents

A and B are incorrect – These are some of the actions to be taken while addressing a security incident

D is incorrect – This is the first phase of an incident response capability

708. Generating a higher level of compliance by creating realistic workable policies is one way of increasing compliance to security policies. Which guideline of implementation does this fall under?

A. Simplify enforcement

B. Increase Awareness

C. Communicate Effectively

D. Integrate Security with corporate culture

KEY A

A is correct – Simplifying enforcement means convincing employees to comply with every policy. Generating a higher level of compliance by creating realistic, workable policies shall help.

B, C and D are incorrect – these are other guidelines to improve employee compliance of security policies

709. As part of auditing Information Security of a multinational bank, an auditor wants to assess the security of information in ATM facilities. Under which privacy policy should he look for details pertaining to security guards and CCTV surveillance of ATM's?

A. Acceptable use of Information Assets Policy

B. Physical Access and Security Policy

C. Asset Management Policy

D. Business Continuity Management Policy

KEY B

B is correct - Physical security describes security measures that are designed to restrict unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, Biometric access, RFID cards, access cards protective barriers, locks, access control protocols, and many other techniques.

A is incorrect - An acceptable use policy (AUP), also known as an Acceptable Usage policy or Fair Use policy, is a set of rules applied by the owner or manager of a network, website or large computer system that restrict the ways in which the network, website or system may be used.

C is incorrect – This policy defines the requirements for Information Asset's protection. It includes assets like servers, desktops, handhelds, software, network devices etc. Besides, it covers all assets used by an organization- owned or leased.

D is incorrect – This policy defines the requirements to ensure continuity of business critical operations. It is designed to minimize the impact of an unforeseen event (or disaster) and to facilitate return of business to normal levels.

710. You work in a company which has strict Information Security Procedures. One of the requirements which you have to adhere to is setting a strong login password. Which of the following is an example of a strong password?

A. Abcde

B. Rosy98

C. 31567

D. qqbRqs$W

KEY D

D is correct - According to the password policy, Password length must be more than 8 characters, Password must be complex containing upper case, lower case, numeric and special characters.

A, B, and C are incorrect – For the same reasons as mentioned above

711. The customer data for the loyalty card issued by a retail store is picked from a form filled by the customer. The data from the form is entered into software by data entry operators who report to a manager. In order to protect customer data, segregation of duties are built in the software in such a way that the operators have permission only to enter data. Any editing or modification can be done only by the manager. It so happens that the manager quits his employment and the store elevates the position of one of the operators to that of a manager. Who do you think is responsible for removing the permission of the exiting manager and changing that of the new manager?

A. Information Owner

B. New Manager

C. System Administrator

D. Information Owner

KEY A

A is correct - System Administrator is the one with administrative / root level privileges of the Operating systems like Windows, Unix etc. This means that they can add and remove permissions and set security configurations. A system administrator is responsible for:

- Creating new system user accounts,
- Changing permissions of existing user accounts,
- Implementing new security software,
- Testing security patches and updates, and
- Resetting user passwords.

B, C and D are incorrect – for reasons mentioned above

712. The retail store (mentioned in question 3) has branches in locations across India and the same process for collecting customer data for loyalty programs is followed in all the branches. This data is then consolidated into one database and is accessible across all branches. The persons who are assigned responsibilities with respect to this database are as follows:

- **Management as Information Owners**
- **General Manager – Marketing: As custodian for the data**
- **General Manager – Operations: as owner of the process**
- **System Administrator**
- **Branch Manager**

- **Data Entry Operator**

Who, do you think, is responsible for processing the information that is received from the branches, checking it and circulating it?

A. Management

B. General Manager, Marketing

C. General Manager, Operations

D. Branch Manager

KEY C

C is correct - The system owner is responsible for one or more systems, each of which may process and store data owned by different information owners. Here a system refers to group of assets required for hosting one or more applications that support a business function.

A is incorrect –The management as information custodian is assigned the task of implementing the prescribed protection defined by the security procedure and top level/Senior management decisions.

B is incorrect –The General Manager, Marketing as Information Owner (also called ***Data Owners***) is responsible for a company information asset.

D is incorrect – Branch manager as the user manager is the immediate manager or reporting manager of an employee.

713. In the same case as mentioned in Questions 3 and 4, who, do you think is responsible for ensuring that the customer data is secure and running regular back ups?

A. General Manager, Marketing

B. General Manager, Operations

C. Data Entry Operator

D. System Administrator

KEY A

A is correct –General Manager, Marketing, as Information custodian is assigned the task of implementing the prescribed protection defined by the security procedure and top level/Senior management decisions. He is usually an information technology or operations person, and is the system administrator for the Information Owner.

Among other activities, information custodian also performs following activities:

- Ensuring safe keeping of information on behalf of information owner

- Providing access to users that are approved by owners
- Running regular backups and routinely testing from backup data
- Performing data restoration activity from the backups when necessary

B, C and D are incorrect – for reasons stated above

714. You are an Information Systems Security Awareness Training Manager employed in a Multinational Bank. You have been part of a team that has created a security training program including classroom, online and web based trainings which is mandatory for all employees and third parties who have access to the bank's sensitive information. How would you ensure that employees and third parties are continually updated on latest issues?

A. By introducing them to the bank's expectations with respect to Information Security

B. By making Security Awareness training mandatory for the management

C. By getting a written acknowledgement from employees that they have read and understood the policy

D. By giving security awareness training to employees and third parties at least once a year

KEY D

D is correct - **Training at Least Annually**: Ensure that all employees and third parties (having access to company information and information systems) are given security awareness training at least once per year. This keeps all updated about the latest developments and issues in this area.

A, B, and C are incorrect – These are the important considerations for a Security training program to ensure that all employees and third parties have attended the training and understood the policies.

715. A bank has outsourced certain processes related to its personal loans unit to a third party vendor. As an IS auditor of the bank, what would you look for to assure yourself that non- public business information accessed by **the third party vendor is protected and not misused?**

A. A non -disclosure agreement signed by the vendor

B. Check if all employees of the vendor are given enough training

C. Verify if there are instances of data being misused earlier

D. Check for a written acknowledgement from the vendor that they have read and understood the company's policy

KEY A

A is correct - A non-disclosure agreement (NDA), also known as a confidentiality agreement (CA), is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties. It's a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or trade secrets. As such, an NDA protects non-public business information.

B, C and D are incorrect – for reasons as mentioned above

716. Organisations have to identify the information that needs various levels of protection and put them in the appropriate 'bucket'. Why can't the entire information within an organisation be protected uniformly?

A. There is a great dependence on information by organizations

B. It provides a systematic approach to protecting information consistently

C. Maintaining security in a network environment is complex

D. It will be a massive task to protect all information uniformly

KEY B

B is correct - Information classification can provide organizations with a systematic approach to protecting information consistently across all parts of organization and for all versions of information (original, copies, discarded, outdated etc.)

A, C and D are incorrect – though these are also reasons for classification, the primary reason is that the appropriate bucket can be protected as per the nature of information it contains

717. How must an organisation ensure that its information is adequately protected, i.e., neither over protected nor under protected.

A. By training its employees who are using the information

B. By ensuring that its information is not shared in any network

C. By classifying its information and placing it in the appropriate bucket

D. By not sharing information with third parties

KEY C

C is correct - Information classification can help in determining the risk associated in case of loss and thus prevent 'over-protecting' and/or 'under-protecting', ensuring that information is adequately protected (e.g. against unauthorized disclosure, theft and information leakage)

A B and D are incorrect – An organization may want to: 1. Publish 2. Share with select entities and business partners 3. Made available to internal users and stakeholders 4.Should not be known for more than select few. A uniform protection may introduce unnecessary delay and sometimes create challenges for operations. The solution organization adopt is known identify the information that needs various levels of protection and put them in appropriate "bucket". Now the bucket can be protected as per nature of information it contains.

718. Information classification ensures that security controls are only applied to information that requires such protection. What is the benefit of such an exercise?

A. Reduces operational costs of protecting information

B. Helps the management access sensitive information

C. Ensures that such information is not shared with third parties

D. Ensures that such information is not accessible to employees

KEY A

A is correct - Information classification helps to ensure that security controls are only applied to information that requires such protection. This can help reduce the demand on resources and staff and ultimately reduce the cost of protecting information. B, C and D are incorrect – Classification of information labels information in such a way that it is shared only with the appropriate person

719. How does an organisation ensure that appropriate users gain access to appropriate files?

A. By classifying users to groups

B. By classifying and labeling information

C. By not sharing information in the general network

D. By having a supervisor for groups who controls access

KEY B

B is correct - Information classification can help enforce access control policies by using the classification label to determine if an individual can gain access to a piece of information (e.g. information labeled as Secret can only be accessed by individuals that have been granted a security clearance of Secret)

A, C and D are incorrect – these options cannot effectively ensure that the appropriate information is used by the appropriate user.

720. What are the factors to be considered for determining the level of confidentiality of information?

A. Relevancy to a business transaction

B. Meeting particular compliance requirements

C. Changes to the content and external conditions of information

D. Appropriate User groups

KEY C

C is correct - Factors that should be considered when determining the level of confidentiality of information are:

- Changes to the content of information
- Changes to external conditions over time
- Aggregation of individual pieces of information.

A, Band D are incorrect – these are the advantages of classifying information

721. An Information classification policy determines the accountability of Information Owners, custodians and users. Who is responsible for assigning classifications to information assets?

A. System Owner

B. Information Owner

C. System administrator

D. Process Owner

KEY B

B is correct - Information Owner (also called ***Data Owners***) is responsible for a company information asset. The responsibilities are generally assigned to person/position that owns business process. Primary responsibilities are:

- Assign appropriate information classification and periodically review the classification to ensure it still meets the business requirements.
- Ensure security controls have been implemented in accordance with the information classification.
- Review and ensure currency of the access rights associated with the information assets they own.

A, C and D are incorrect – These are some of the KEY roles in Information Security Management – system owner is responsible for the systems – which hold the information, a system administrator can set security configurations and a process owner for the implementation and management of a process.

722. Under what information category does widely distributed product brochures fall?

A. Sensitive Information

B. Client Confidential Information

C. Unclassified/Public Information

D. Company Confidential Information

KEY C

C is correct - Information is not confidential and can be made public without any implications for Company.

A is incorrect –Does not require special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion. It does not require higher than normal assurance of accuracy and completeness.

B is incorrect – Is not Information received from clients in any form for processing in production by Company.

D is incorrect – Is not information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance.

723. Under what category does Company developed software codes fall?

A. Sensitive Information

B. Client Confidential Information

C. Company Confidential Information

D. Unclassified/Public Information

KEY A

A is correct - It requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion. It also requires higher than normal assurance of accuracy and completeness.

B is incorrect – Is not Information received from clients in any form for processing in production by Company.

C is incorrect – Is not information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance.

D is incorrect – Information is confidential and cannot be made public without any implications for Company.

724. Under what category does information received from clients fall?

A. Client Confidential Information

B. Company Confidential information

C. Unclassified/Public Information

D. Sensitive Information

KEY A

A is correct - Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.

B is incorrect – Is not information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance.

C is incorrect – Information is confidential and cannot be made public without any implications for Company.

D is incorrect – It does not requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion. Does not require higher than normal assurance of accuracy and completeness.

725. What is Personally Identifiable Information (PII)?

A. Personal Information of any person who needs to provide this to the organisation

B. Information held by an organisation which can identify a stakeholder

C. Personal Information pertaining to the employees of an organisation

D. Personal Information pertaining to the third parties associated with the organisation

KEY A

A is correct - PI generally refers to personal information. This personal information can be related to any person or stake holders who need to provide this information to organization. For example Banks may have to collect identification proofs, PAN card details, address, telephone numbers from the customers, and generates information like credit cards details, bank account numbers for customers.

B, C and D are incorrect – These do not classify under personally identifiable information.

726. What is the standard that must be complied with by all those deals with credit/debit cards?

A. PCIDSS

B. Electronic Communications Privacy Act

C. Information Technology Acct 2000

D. Regulations mandated by Reserve Bank

KEY A

A is correct -

Pay-card industry data security standard: De-facto standard for card related information. Must be complied by all those deals with credit or debit cards which include banks, merchants, intermediately. Although there may not be regulatory or legal requirements as of now for compliance with PCIDSS, it has been accepted by industry.

B is incorrect – Electronics Communications Privacy Act extends government restrictions on wire taps to include transmissions of electronic data.

C is incorrect - Information technology Act 2000, (Amendment 2008): Provides that any organization is collecting PII shall be liable in case absence of reasonable security of such information results in identify theft.

D is incorrect – These regulations have mandated processes for collecting, storing, securing data and information including PII.

727. What is the Act which mandates how financial institutions must deal with the private information of individuals?

A. Information technology Act 2000

B. Video Privacy Protection Act

C. Gramm-Leach-Bliley Act

D. Electronic Communications Privacy Act

KEY C

C is correct - Gramm-Leach-Bliley Act: Mandates how financial institutions must deal with the private information of individuals.

B is incorrect - Video Privacy Protection Act: Prevents wrongful disclosure of an individual's personally identifiable information stemming from their rental or purchase of audio-visual material.

A is incorrect - Information technology Act 2000, (Amendment 2008): Provides that any organization is collecting PII shall be liable in case absence of reasonable security of such information results in identify theft.

D is incorrect –Electronic Communications Privacy Act (ECPA): Extends government restrictions on wire taps to include transmissions of electronic data.

728. Which of the following does not classify under Personally identifiable Information?

A. Company advertisement information

B. Medical information of patients

C. Location information of clients

D. Information collected by websites

KEY A

A is correct - This is public/unclassified information which is not sensitive and does not require any security

B, C and D are incorrect – these are PII's

729. How is information classification applied for information contained in a critical database?

A. at the file or data level

B. to the entire database

C. to each individual document

D. at column level at the discretion of the information owner

KEY D

D is correct - For critical databases, classification may apply to column level, at the discretion of the information owner

A is incorrect - For server-based systems, classification will be done at the file or data level;

B is incorrect - For information in a database, the classification will normally apply to the entire database;

C is incorrect – For paper documents, including output from systems, classification will apply to each individual document

730. How can critical data be protected during transmission, processing and storing?

A. By keeping the information physically secured

B. By encrypting

C. By controlling access

D. By taking a backup

KEY B

B is correct - By encrypting critical information, we ensure that such information is accessible only to the appropriate person

A, C and D are incorrect – these do not apply to information that is being transmitted, stored and processed.

731. What are the solutions referred to under DLP (Data Leak Prevention)?

A. Protecting data based on the rule set and classification

B. Expecting creator of data file to choose who shall access data

C. Authenticating users out of the organisation

D. Working at data base level and managing the access rights

KEY A

A is correct - The solutions generally referred under popular acronym DLP (Data leak prevention/ Data loss prevention/ Data leak protection) provide few capabilities to be implemented independently e.g. there are solutions that focuses on protecting data passing through networks based on the rule-set and classification.

B and C are incorrect – solutions referred by acronym DRM (Digital rights Management) that can be applied to data files. The solutions expects creator of data file to decide who shall access the data and need to add in central user list. Sometimes this becomes impractical when such files are meant for users out of organization and they need to be authenticated by DRM server.

D is incorrect - DAM (Digital access management) that works at data base level and manages the access rights while providing data to applications, based on rules and classification.

732. What is the pre requisite for successful implementation of data protection tools like DLP, DRM and DAM?

A. Identifying information resources

B. Creating an information risk profile

C. Creating appropriate rule set and classification based on impact of risks

D. Establishing a process for data classification

KEY C

C is correct - A prerequisite for successful implementation of these tools is appropriate rule set and data classification based on impact of risks associated with data leak.

A, B and D are incorrect – These are steps that have to be followed to create appropriate rule set and classification

733. Which of the following is a risk associated with Portable Devices?

A. Users can access Company's internal information from anywhere

B. It is prone to physical security problems because of availability within the workplace

C. Unauthorised users may access hard copy of electronic data

D. Its overall security is dependent on the physical security of the work stations

KEY A

A is correct - **Portable devices**: Can be an organization's security nightmare. Although issuing laptops and PDAs to employees facilitates flexibility and productivity in an organization, it poses several serious risks with regard to physical security. Besides, more and more organizations are adopting Bring Your Own Device (BYOD) policy which further makes the portable device and the corporate network vulnerable. With users accessing the company's internal information systems from anywhere, a breach in physical security on one of these devices could undermine an organization's information security. Extreme care must be taken with this class.

B is incorrect - **Workstations**: Usually located in more open or accessible areas of a facility. Because of their availability within the workplace, workstations can be prone to physical security problems if used carelessly.

C is incorrect - **Printers:** Although the data is stored on electronic for the purpose. The reports, letters, communications etc. have to be printed. Organizations deploy printers. In order to optimize use of printer most organization deploy network based printers shared among group of users.

D is incorrect – **Servers**: Servers are the most physically secure class of systems. This is due to the common practice of placing them in a location that has better access and environmental control. Although this class may be the most physically secure, their overall security is dependent on the physical security of the workstations and portable devices that access them.

734. What are network devices?

A. Device in which all data in a network is placed

B. Devices deployed for establishing communication

C. Devices installed by telecom companies to facilitate mobile communication

D. Devices that facilitate accessing data from anywhere

KEY B

B is correct - **Network devices**: devices deployed for establishing communication which includes routers, switches, firewalls, cables, wireless devices and other network monitoring tools.

A is incorrect – Devices in which all the data in a network is placed is a server

C is incorrect – Devices installed by telecom companies to facilitate mobile communication are towers

D is incorrect – Devices that facilitate accessing data from anywhere are portable devices

735. In order to ensure the privacy of personal information of an individual, a company has to:

A. Write policies and procedures

B. Define roles and responsibilities

C. Implement an effective privacy program

D. Define incident response plans

KEY C

C is correct - It is important that the organization implements an effective privacy program in order to ensure the privacy of the personal information of an individual

A, Band D are incorrect – These are the steps to be taken to implement a successful privacy program

736. An auditor need not involve in one of the following while evaluating an organisation's privacy framework. Which is it?

A. Liaise with in-house legal counsel to understand legal implications

B. Design Incident response plans

C. Liaise with information technology specialists to understand security implications

D. Understand internal policies and guidelines

KEY B

B is correct - This is done by the organisations governing body

A, C and D are incorrect – These are the roles of an internal auditor

737. An insurance company is in the process of classifying its information according to its sensitivity. If you formed a part of the team responsible for this

classification, how would you classify personal information pertaining to insurance holders as?

A. Unclassified/Public Information

B. Sensitive Information

C. Client Confidential data

D. Company Confidential data

KEY C

C is correct - Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.

A, B and D are incorrect – Sensitive Information recd from clients cannot be placed under these categories.

738. You head a data processing center which handles an outsourced activity of employee medical reimbursements of a multinational. You have employed professionals who have developed the required software for the activity and who maintain the same. Under which of the following would you classify the software codes?

A. Client Confidential Data

B. Company Confidential Data

C. Sensitive Information

D. Unclassified data

KEY C

C is correct - All company developed software codes whether used internally or sold to clients and know how used to process client information should be classified as Sensitive Information

A, B and D are incorrect – for reason mentioned above

739. The personal loans department of a bank maintains a database of personal information of its customers who have availed loans. This database is used for various purposes by the bank. As an IS auditor you find that there are security breaches related to this information. Under what Act would the company be liable?

A. PCIDSS

B. Information Technology Act 2000

C. Gramm Leach Bliley Act

D. Video Privacy Protection Act

KEY B

B is correct - **Information technology Act 2000, (Amendment 2008)**: Provides that any organization is collecting PII shall be liable in case absence of reasonable security of such information results in identify theft.

A is incorrect – **PCIDSS: Pay-card industry data security standard:** De-facto standard for card related information. Must be complied by all those deals with credit or debit cards which include banks, merchants, intermediately. Although there may not be regulatory or legal requirements as of now for compliance with PCIDSS, it has been accepted by industry.

C is incorrect – **Gramm-Leach-Bliley Act**: Mandates how financial institutions must deal with the private information of individuals.

D is incorrect - **Video Privacy Protection Act:** Prevents wrongful disclosure of an individual's personally identifiable information stemming from their rental or purchase of audio-visual material.

740. As an employee of the HR department of a multinational company, you are required to send through email, sensitive data pertaining to the employees of your organisation to a data centre for processing. Though there is approval from the management that the data centre can have access to this data, there is a precautionary measure that you should take while transmitting this data. Which of the following is it?

A. Encrypting the data before sending

B. Taking a back up before sending

C. Sending information only on a need to know basis

D. Setting strong access controls at the vendors site

KEY A

A is correct - Encryption of information during transmission ensures that it is not misused by any third party

B, C and D are incorrect – though these are important security considerations, they are not mandatory for this case

741. Which of the following is not a part of Physical Access Control?

A. Preventing unauthorised physical access to resources

B. Protection of information in stored, transit and processing stages

C. Control entry during and after normal business hours

D. Identification checks

KEY B

B is correct - This is a part of Logical Access Control

A, C and D are incorrect – Physical access controls encompass securing physical access to computing equipment as well as facilities housing the IS computing equipment and supplies. The choice of safeguard should be such that they prevent unauthorized physical access but at the same time cause the least inconvenience to authorized users. All the three options form a part of Physical Access Control.

742. Which of the following is an information asset that need not be included in physical access control?

A. Information in transit through mail

B. Primary computer facilities

C. Micro computers

D. Printers

KEY A

A is correct - Information in transit through mail cannot be restricted physically.

B, C and D are incorrect – These are assets that should be included under Physical Access Control

743. Which of the following is not a physical access control?

A. Manual doors or cipher KEY locks

B. Protecting data with passwords

C. Controlling the reception area

D. Logging in visitors

KEY B

B is correct - Protecting data with passwords is part of logical access control

A, C and D are incorrect – Physical access controls may include – manual door or cipher KEY locks, photo Ids and security guards, entry logs, perimeter intrusion locks etc. Physical controls should also include: Pre-planned appointments, Identification checks, controlling the reception area, Logging in visitors, Escorting visitors while in sensitive areas etc.

744. Threats to Information Assets like computing equipment, media and people are known as:

A. Cyber threats

B. Environmental Threats

C. Physical Threats

D. Logical Access Threats

KEY C

C is correct - Physical threats to information system assets comprises of threats to computing equipment, facilities which house the equipment, media and people.

A is incorrect - Cyber threats are threats due to exposure of information in the world wide web

B is incorrect – Environment threats are undesired or unintentional or intentional alteration in the environment in which computing resources function can result in threats to availability of information systems and integrity of information.

D is incorrect – Logical access threat arising where unauthorized persons tried to get information useful for breaking into organization system.

745. "Preventing modification of data by unauthorised personnel" falls under which core principle of Information Safety?

A. Integrity

B. Confidentiality

C. Availability

D. Security

KEY A

A is correct - Confidentiality, Integrity and Availability (CIA Triad) are the core principles of information safety. **Integrity:** Prevent modification of data by unauthorized personnel.

B and C are incorrect – **Confidentiality:** Preventing disclosure of information to unauthorized individuals or systems, **Availability:** Information must be available when it is needed.

D is incorrect – This Is not a part of the CIA Triad

746. Under what category of Physical Security threat does poor handling and cabling of electronic equipments fall?

A. Electrical

B. Environmental

C. Maintenance

D. Hardware

KEY C

C is correct - **Maintenance**: These threats are due to poor handling of electronic components, which cause ESD (electrostatic discharge), the lack of spare parts, poor cabling, poor device labelling, etc.

A is incorrect - Electrical vulnerabilities are seen in things such as spikes in voltage to different devices and hardware systems, or brownouts due to an insufficient voltage supply. Electrical threats also come from the noise of unconditioned power and, in some extreme circumstances like total power loss.

B is incorrect – interference of natural disasters such as fires, hurricanes, tornados, and flooding, fall under the realm of environmental threat.

D is incorrect - It has the threat of physical damage to corporate hardware or its theft.

747. Which of the following is not a source of Physical Security threat?

A. Uncontrolled/Unconditioned Power, Low voltage

B. Physical Access to IS resources by unauthorised personnel

C. Discontented or disgruntled employees

D. Interested or Informed outsiders

KEY A

A is correct - This is not a source of physical security threat, it is a source of environmental threat

B, C and D are incorrect – These are sources of physical security threats

748. In an organisation there are instances of employees using the internet for personal purposes. Under what threat is this classified?

A. Logical access threat

B. Environment threat

C. Improper physical access threat

D. Electrical threat

KEY C

C is correct - Threats from improper physical access usually are human-induced. Some examples are:

- Unauthorized persons gaining access to restricted areas. Examples are prospective suppliers gaining access to computer terminal of purchases department, thereby viewing list of authorized suppliers and rates being displayed on the screen during data entry.
- Employees gaining access to areas not authorized, e.g. sales executives gaining access to server room.
- Damage, vandalism or theft of equipment or other IS resources.
- Abuse of data processing resources, e.g. employees using internet for personal purposes.
- Damage due to civil disturbances and war.
- Embezzlement of computer supplies, e.g. floppies, cartridges, printer consumables.
- Public disclosure of sensitive information, e.g. Information regarding location of servers, confidential or embarrassing information.

A, B and D are incorrect – This is neither a logical access, environmental or electrical threat

749. Viewing or copying of sensitive information by visitors who have gained unauthorised access to the same is:

A. An Improper Physical Access Exposure

B. An Unintentional or Accidental Exposure

C. A Deliberate Exposure

D. An Environmental Exposure

KEY A

A is correct - Improper physical access to IS resources may result in losses to organization which can result in compromising one or any of the following:

- **Confidentiality** of organizational information or knowledge of protected organizational resources. Example: unauthorized access to systems containing sensitive information may be viewed or copied by visitors accidentally gaining access to such systems.
- **Integrity** of information by improper manipulation of information or data contained on systems or media. Example: Unauthorized access to record rooms or databases may result in modification or deletion of file content.
- **Availability** of information. Improper access to IS resources may be used to adversely impact availability of IS resources' ultimately preventing or delaying

access to organizational information and business applications. Example: A disgruntled bank employee may switch of power to information servers thus sabotaging operations.

B is incorrect - Authorized personnel or unauthorized personnel unintentionally gaining physical access to IS resources result in accidentally or inadvertently causing loss or damage to the organization.

C is incorrect - Unauthorized personnel may deliberately gain access or authorized personnel may deliberately gain access to IS resources, for which they are not permitted or possess rights of access. This may result in the perpetrator achieving his objective of causing loss or damage to the organization or gain personal monetary benefits or otherwise.

D is incorrect – Environmental exposure are not human induced and caused by nature

750. If windows exist in a data centre, they must be translucent and shatterproof. Why?

A. To avoid data leakage through electromagnetic radiation

B. To prevent anyone from peeping and viewing data

C. To avoid environmental threats to physical systems

D. To avoid theft of physical assets

KEY A

A is correct - Windows are normally not acceptable in a data centre to avoid data leakage through electromagnetic radiation emitted by monitors. If they do exist, however, they must be translucent (semi-transparent, i.e. allowing light without being able to view things clearly) and shatterproof or monitors should not be facing them.

B, C and D are incorrect – There is a negligible chance of these threats due to the presence of windows

751. Why audit trials and control are logs important for Security Management?

A. To know where access attempts occurred and who attempted them

B. To reduce unauthorised access to sensitive information

C. To prevent modification or deletion of file content

D. To prevent unintentional physical access

KEY A

A is correct - With respect to physical security, audit trails and access control logs are vital because management needs to know where access attempts occurred and who

attempted them. The audit trails or access logs must record the following:

- The date-and time of the access attempt
- Whether the attempt was successful or not
- Where the access was granted (which door, for example)
- Who attempted the access
- Who modified the access privileges at the supervisor level

B, C and D are incorrect – These have no relevance to maintenance of audit logs

752. What is the first step once an unauthorised event is detected?

A. Process owner should investigate and take action

B. The incident should be reported to the appropriate authority

C. Security administrator should effect modifications to the security policy

D. Should be effectively handled to mitigate losses

KEY B

B is correct - Once an unauthorised incident is detected, the first step is to report the same.

Appropriate procedures should be in place to enable reporting of such incidents

A, C and D are incorrect – These are subsequent steps

753. Which of the following is not a Human Resource Control?

A. Providing identity cards

B. Providing training in Physical Security

C. Locking system screens when not in seat

D. Monitoring behavior

KEY C

C is correct - Locking screens forms part of logical access control

A, B and D are incorrect – These are examples of human resources control

754. The most important human resource control is:

A. Providing access cards to employees

B. Assigning responsibilities to employees

C. Provide training to employees

D. Escort terminated or resigned/retired employees

KEY A

A is correct - One of most important control is process of providing access cards to employees, vendor personnel working onsite and visitors. The process should aim in preventing generation of false cards, modifying contents of cards, accounting for lost cards and reconciliation of cards to detect missing/lost cards. In addition a process to grant, change and revoke access must be in place.

B, C and D are incorrect – These controls are other human resource controls

755. Which of the following is a perimeter security?

A. Screen savers

B. Passwords

C. Access cards

D. Guards

KEY D

D is correct - Guards are commonly deployed in perimeter control, depending on cost and sensitivity of resource to be secured. While guards are capable of applying subjective intelligence, they are also subject to the risks of social engineering. They are useful whenever immediate, discriminating judgment is required.

A is incorrect – Screen savers are used to lock screens when not in use

B is incorrect – Passwords are used to prevent unauthorised access to sensitive data

C is incorrect – Access cards are used as a physical security measure

756. Which of the following is not a perimeter security?

A. Compound walls and Fencing

B. Lighting exteriors

C. Encrypting data in transit

D. Bolting door locks

KEY C

C is correct - Encrypting data in transit is a logical access security

A,B and D are incorrect – thee are examples of perimeter security

757. What perimeter security is used to reduce the risk of piggy backing?

A. Dead man doors

B. Bolting door locks

C. Combination or Cipher locks

D. Compound walls

KEY A

A is correct - Also called as Mantrap systems. These are typically used to secure entrance to sensitive computing facilities or storage areas. This technique involves a pair of doors and the space between the doors is enough to accommodate just one person. Such doors reduce the risk of piggybacking, in which an unauthorized person could enter the secured facility by closely following an authorized person which may or may not be monitored by a guard.

B is incorrect - This is the most commonly used means to secure against unauthorized access to rooms, cabins, closets. These use metal locks and keys and access can be gained by any person having physical possession of the key. This is cheap yet a reasonably effective technique, however control over physical custody and inventory of keys is required.

C is incorrect - To gain entry, a person presses a four digit number in a particular pre-determined sequence which disengages the levers for a pre-set interval of time.

D is incorrect – A common method of securing against unauthorized boundary access to the facility. It helps in deterring casual intruders but is ineffective against a determined intruder.

758. The advantages of Electronic door locks do not include:

A. Distinguishing between various categories of users

B. Most secure locks since they enable access based on individual features such as finger prints

C. Restricting individual access through the special internal code

D. Deactivation of card entry from a central electronic control mechanism

KEY B

B is correct - The feature pertains to Biometric door locks

A, C and D are incorrect – These are the advantages of Electronic Door locks

759. Which of the following is a disadvantage of a Biometric Door lock?

A. Easy duplication

B. Is not as sophisticated as electronic door locks

C. High cost of acquisition, implementation and maintenance

D. They are not very secure

KEY C

C is correct - While these devices are considered highly secure, they suffer from the following disadvantages:

- Relatively high cost of acquisition, implementation and maintenance, hence they are used mainly to secure sensitive installations.
- Time consuming process of user registration.
- Privacy issues relating to use of devices like retina and fingerprint scanners.
- High error rates compared to other devices since they may result in a false rejection or more critically a false acceptance.

A, B and D are incorrect – Biometric locks are sophisticated and highly secure. Duplication of biometrics is not possible.

760. A device which creates a grid of visible white light or invisible infra red light, which when broken activates an alarm is:

A. Photo electric sensors

B. Dry contact switches

C. Video cameras

D. Identification badges

KEY A

A is correct - Photoelectric sensors receive a beam of light from a light-emitting device, creating a grid of either visible white light, or invisible infrared light, which when broken activates an alarm.

B is incorrect - Dry contact switches and tape are probably the most common types of perimeter detection. This can consist of metallic foil tape on windows or metal contact switches on doorframes to detect when a door or window has been opened.

C is incorrect – **Cameras** provide preventive and detective control. Closed-Circuit Television (CCTV) cameras have to be supplemented by security monitoring and guards for taking corrective action.

D is incorrect - Special identification badges such as employee cards, privileged access pass, visitor passes etc. enable tracking movement of personnel. These can also be cards with signature and/or photo identity.

761. The process requiring all visitors to sign a visitors log at the time of entry/exit is known as

A. Electronic logging

B. Manual logging

C. Controlled visitor access

D. Controlled single point access

KEY B

B is correct - Manual **Logging:** All visitors to the premises are prompted to sign a visitor's log recording the date and time of entry/exit, name of entrant, organization, purpose etc. The visitor may also be required to authenticate his identity by means of a business card, photo identification card, driver's license etc.

A is incorrect - **Electronic Logging:** Electronic card users may be used to record the date and time of entry/exit of the card holder by requiring the person to swipe the card both time of entry and exit. This is a faster and more reliable method for restricting access to employees and pre-authorized personnel only. These devices may use electronic/biometric security mechanisms.

C is incorrect - **Controlled single point access:** Physical access to the facility is granted though a single guarded entry point. Multiple entry points may dilute administration of effective security.

D is incorrect – **Controlled Visitor access:** A pre-designated responsible employee or security staff escorts all visitors such as maintenance personnel, contract workers, vendors, consultants for a specified time period

762. A card reader that senses the card in possession of a user in the general area and enables faster access is:

A. Wireless proximity readers

B. Motion detectors

C. Cable locks

D. Identification Badges

KEY A

A is correct - A proximity reader does not require physical contact between the access card and the reader. The card reader senses the card in possession of a user in the general area (proximity) and enables faster access.

B is incorrect - **Alarm Systems/Motion detectors.** Alarm systems provide detective controls and highlight security breaches to prohibited areas, access to areas beyond restricted hours, violation of direction of movement e.g. where entry only/exit only doors are used. Motion detectors are used to sense unusual movement within a predefined interior security area and thus detect physical breaches of perimeter security, and may sound an alarm.

C is incorrect - A cable lock consists of a plastic-covered steel cable that chains a PC, laptop or peripherals to the desk or other immovable objects.

D is incorrect – Special identification badges such as employee cards, privileged access pass, visitor passes etc. enable tracking movement of personnel.

763. Lockable switches that prevent a KEY board from being used is:

A. Switch controls

B. Biometric Mouse

C. Laptop security

D. Peripheral switch controls

KEY D

D is correct - **Peripheral switch controls:** These types of controls are lockable switches that prevent a keyboard from being used.

A is incorrect - A switch control is a cover for the on/off switch, which prevents a user from switching of the file server's power.

B is incorrect - **Biometric Mouse:** The input to the system uses a specially designed mouse, which is usable only by pre-determined/pre-registered person based on the fingerprint of the user.

C is incorrect – Cable locks, biometric mice/fingerprint/iris recognition and encryption of the file system are some of the means available to protect laptops and their data.

764. A smart card used for access control is also called a security access card. Which of the following is not a type of smart card?

A. Identification cards

B. Photo Image Cards

C. Digital coded cards

D. Wireless proximity readers

KEY A

A is correct - Special identification badges such as employee cards, privileged access pass, visitor passes etc. enable tracking movement of personnel.

B is incorrect - Photo-image cards are simple identification cards with the photo of the bearer for identification.

C is incorrect - Digitally encoded cards contain chips or magnetically encoded strips (possibly in addition to a photo of the bearer).

D is incorrect – A proximity reader does not require the user to physically insert the access card.

765. Which of the following is not a biometric characteristic?

A. Finger prints

B. Retina scans

C. Passport photo

D. Palm scans

KEY C

C is correct - Passport photo does not have a biometric characteristic

A, B and D are incorrect – All these are typical biometric characteristics used to uniquely identify or authenticate an individual

766. Name the performance measure in biometrics which is the percentage of invalid subjects that are falsely accepted.

A. False Rejection Rate (FRR)

B. False Acceptance Rate (FAR)

C. Crossover Error Rate (CER)

D. Throughput rate

KEY B

B is correct - **False acceptance rate (FAR), or Type II error**: The percentage of invalid subjects that are falsely accepted. FAR is more critical than FRR.

A is incorrect - **False rejection rate (FRR), or Type I error**: The percentage of valid subjects that are falsely rejected

C is incorrect - **Crossover error rate (CER)**: The percent at which the FRR equals the FAR. In most cases, the sensitivity of the biometric detection system can be increased or decreased. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher FRR. Conversely, if the sensitivity is decreased, the FAR will increase.

D is incorrect – There is no such measure as throughput rate in biometrics

767. With respect to biometrics evaluation, how is the time taken to register with a system referred as?

A. Enrolment time

B. Throughput rate

C. Acceptability

D. Registration time

KEY A

A is correct - *Enrolment time* is the time it takes to initially register with a system by providing samples of the biometric characteristic to be evaluated.

B is incorrect - The *throughput rate* is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a system.

C is incorrect - *Acceptability* refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.

D is incorrect – there is no such evaluation as registration time with respect to biometrics

768. With respect to audit of physical access controls, what does controls assessment mean?

A. Ensuring that the risk assessment procedure adequately covers periodic and timely assessment of all assets

B. Evaluating whether physical access controls are in place

C. Examining relevant documentation such as the security policy and procedures, premises plans, building plans, etc

D. Reviewing physical access controls for their effectiveness.

KEY B

B is correct - **Controls Assessment:** The auditor based on the risk profile evaluates whether physical access controls are in place and adequate to protect the IS assets against the risks.

A is incorrect – This procedure is risk assessment

C is incorrect – This procedure is review of documentation

D is incorrect – This procedure is testing of controls

769. The review of physical access controls by an auditor need not include:

A. Observing safeguards and Physical access procedures

B. Interviewing personnel to get information of procedures

C. Authorising special access

D. Touring organisational facilities

KEY C

C is correct - This is the role of the manager/management, not of an auditor

A,B and D are incorrect – These are the roles of an auditor

770. What should an auditor check for in case of employee termination?

A. The employees tenure and his conduct during the same

B. Withdrawal and deactivation of access rights

C. Whether appropriate rights have been granted to the replacement

D. Whether there is any due from the employee to the organisation

KEY B

B is correct - Employee termination procedures should provide withdrawal of rights such as retrieval of physical devices such as smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organization.

A, C and D are incorrect – these are not the concerns of an auditor

771. What is the review procedure that should be adopted by an auditor to ensure that there is adequate security at entrance and exits?

A. Review physical layout diagrams , risk analysis, procedure for removal and return of storage media, knowledge and awareness of emergency procedures by employees

B. Inspect guard procedures and practices, and facility surveillance system apart from assessing vehicle and pedestrian traffic around high risk facility

C. Review security policies and procedures at enterprise level and system level are aligned with business stated objectives

D. Review employee and visitor entry logs, entry/exit procedures used by management, documentation of logs

KEY D

D is correct

A is incorrect – these procedures are to review that physical safeguards are commensurate with the risks of physical damage or access

B is incorrect – These procedures are to review the perimeter security

C is incorrect – These procedures are to review whether security control policies and procedures are properly documented

772. From the perspective of environmental exposures and controls, how are computer rooms, server rooms and printer rooms categorised?

A. Information System supporting infrastructure or facilities

B. Hardware and Media

C. Documentation

D. Supplies

KEY A

A is correct - **Information Systems Supporting Infrastructure or Facilities:** This typically includes the following:

- Physical Premises, like Computer Rooms, Cabins, Server Rooms/Farms, Data Centre premises, Printer Rooms, Remote facilities and Storage Areas
- Communication Closets
- Cabling ducts
- Power Source
- Heating, Ventilation and Air Conditioning (HVAC)

B is incorrect - **Hardware and Media**: Includes Computing Equipment, Communication equipment, and Storage Media

C is incorrect - **Documentation**: Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.

D is incorrect – **Supplies**: The third party maintenance procedures for say air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.

773. Which of the following is a natural environmental threat?

A. War action and Bomb threats

B. Air conditioning failure

C. Earthquakes

D. Undesired activities in computer facilities such as smoking

KEY C

C is correct - Earthquake is a natural environmental threat

A, B and D are incorrect – These are man made environmental threats

774. Which of the following is a man-made environmental threat?

A. Extreme variations in temperature

B. Static Electricity

C. Humidity, vapors, smoke and suspended particles

D. Fire due to negligence and human action

KEY D

D is correct - This is a man- made threat

A,B and C are incorrect – These are natural threats

775. Given below are some examples of exposures. Which of these do not pertain to violation of environmental controls?

A. The possibility of a fire destroying valuable computer equipment due to use of inflammable material for construction of server cabin

B. The possibility of Unauthorised access to sensitive data through hacking

C. The possibility of a fire due to poor cabling

D. The possibility of damage of keyboards and other devices due to accidental dropping of beverages

KEY B

B is correct - This is an example of exposure due to violation of physical access

A, C and D are incorrect – these are examples of exposure due to violation of environmental controls

776. What is a sudden rise in in voltage in the power supply known as?

A. Surge

B. Blackout

C. Sag/dip

D. Transient

KEY A

A is correct - Surge is a sudden rise in voltage in the power supply. A strong power surge can easily harm unprotected computers and other microprocessor circuits. It also puts a stress on anything else powered by the electric supply, from air conditioning motors to light bulbs.

B is incorrect – Blackout is a complete loss of commercial power

C is incorrect – Sag or dip is a short period of low voltage

D is incorrect – Transient is line noise or disturbance superimposed on the supply circuit and can cause fluctuations in electrical power.

777. Which of the following need not be considered while choosing a safe site?

A. Probability of natural disasters

B. Transportation

C. Proximity to other like companies

D. External services like police, fire, hospital etc

KEY C

C is correct - This is not a factor to be considered while choosing a safe site

A, B, and D are incorrect – These are some of the factors to be considered while choosing a safe site

778. While designing a site, it is important that the location of media libraries is:

A. Fungi Resistant and heat resistant

B. Easily accessible

C. Not easily accessible

D. Outside the work area

KEY A

A is correct - **Media Protection:** Location of media libraries, fire proof cabinets, kind of media used (fungi resistant, heat resistant).

B, C and D are incorrect – These are not important considerations for storing media

779. The organisation should consider newer environmental threats like generator installation by a neighbor or sudden changes in climate as part of:

A. Facilities planning

B. Choosing a site

C. Designing a site

D. Documentation

KEY A

A is correct - The risk profile of the organization should take into consideration newer environmental threats. A few examples of threats to be considered are given below:

- Installation of a generator by a neighbor.

- Sudden changes in climate leading to extreme changes in humidity levels.
- Building construction in the vicinity of IPF leading to increase in suspended dust particles in the environment.
- Raising of foundation and flooring by a neighbor causing change in the flow of rainwater.
- Installation of high power consumption equipment adversely affecting the quality of power.

B, C and D are incorrect – The aspect need not be considered at these levels

780. New employee induction programs should be conducted as part of:

A. Documentation

B. Facilities planning

C. People Responsibility and training

D. Emergency plan

KEY C

C is correct - Responsibility and accountability for environmental controls planning and management should be fixed and should be expressly communicated as part of job description. New employee induction programs should include informing and educating employees on environmental control procedures, prohibited activities (eating, smoking, drinking inside IPF), and maintaining secrecy and confidentiality.

A, B and D are incorrect – Induction programs are not part f any of these.

781. An effective emergency plan of an organisation should include:

A. Detailed analysis of third party and outsourced vendors/suppliers

B. Evaluation of effectiveness and efficiency of environmental facilities

C. Preventive maintenance plans

D. Control Action, Evacuation plan and paths

KEY D

D is correct - Disasters result in increased environmental threats e.g. smoke from a fire in the neighborhood or in some other facility of the organization would require appropriate control action, evacuation plan should be in place and evacuation paths should be prominently displayed at strategic places in the organization.

A, B and C are incorrect. These are parts of Vendors/Suppliers security and Maintenance plans

782. How can an organisation reduce Mean Time to Repair/recover/respond/restore (MTTR)?

A. By stocking spare parts on site

B. By planning for environmental controls

C. By identifying, parameterizing and documenting risks of utility failure

D. By evaluating alternatives with low MTBF

KEY A

A is correct - Stocking spare parts on site and training maintenance personnel can reduce MTTR.

B, C and D are incorrect – Failure modes of each utility, risks of utility failure, should be identified, parameterized and documented. This includes estimating the MTBF (Mean Time between Failures) and MTTR (Mean-Time to Repair/recover/respond/ restore). Planning for Environmental controls would need to evaluate alternatives with low MTBF or installing redundant units.

783. Listed below are some of the controls to ensure uninterrupted supply of clean power. Out of these which is the equipment which cleanses the incoming power supply of problems such as spikes, sags, etc.?

A. Generators

B. Electrical surge protectors/line conditioners

C. Uninterruptible power supply (UPS)

D. Power leads from two substations

KEY B

B is correct - Power supply from external sources such a grid and generators are subject to many quality problems such as spikes, surges, sag and brown outs, noise, etc. Surge protectors, spike busters and line conditioners are equipment which cleanses the incoming power supply of such quality problems and delivery clean power for the equipment.

A, C and D are incorrect – UPS generally is a good solution in case of applications enabling their proper closure of processing and systems. In respect of continuous process equipment, UPS may fail to meet the purpose if regular power supply is not available for a prolonged period of time. Diesel or kerosene generators could also be used, but they

require some time to be switched on and the power from generators has to be cleansed before delivery to computer systems.

D is incorrect - To protect against such exposures, redundant power lines from a different grid supply should be provided for. Interruption of one power supply should result in the system immediately switching over to the stand-by line.

784. How does a smoke/fire detector function?

A. Activate audible alarms on sensing a particular degree of smoke or fire

B. Activate audible alarms and are linked to monitoring stations within and outside the organisation

C. Activate an audible alarm on detecting water

D. Switches off power in case of emergency situations like fire etc.

KEY A

A is correct - Smoke and fire detectors activate audible alarms or fire suppression systems on sensing a particular degree of smoke or fire. Such detectors should be placed at appropriate places, above and below the false ceiling, in ventilation and cabling ducts.

B is incorrect - By manual operation of switch or levers, these devices activate an audible alarm and may be linked to monitoring stations both within and/or outside the organization.

C is incorrect - When necessity of immediate power shutdown arises during situations such as computer facility fire or emergency evacuation, emergency power-off switches should be provided.

D is incorrect – Risks to IPF equipment from flooding and water logging can be controlled by use of water detectors placed under false flooring or near drain hole. Water detectors should be placed on all unattended or unmanned facilities. Water detectors on detecting water activate an audible alarm.

785. How are fires caused by flammable liquids and gases suppressed?

A. Water or soda acid

B. Dry powder

C. Carbon dioxide, soda acid or FM200

D. Gas based systems

KEY C

C is correct - Fires caused by flammable liquids and gases are classed as Class B and are suppressed by Carbon Dioxide (CO), soda acid, or FM200.

A is incorrect - Fires caused by common combustibles (like wood, cloth, paper, rubber, most plastics) are classed as Class A and are suppressed by water or soda acid (or sodium bicarbonate).

B is incorrect - Electrical fires are classified as Class C fires and are suppressed by Carbon Dioxide (CO), or FM200. Fire caused by flammable chemicals and metals (such as magnesium and sodium) are classed as Class D and are suppressed by Dry Powder (a special smothering and coating agent).

D is incorrect – This is a classification of suppression systems

786. Which of the following is a gas based fire suppression system?

A. Wet pipe sprinklers

B. FM 200

C. Dry pipe sprinklers

D. Pre action

KEY B

B is correct - FM200 is an inert gas, does not damage equipment as water systems do and does not leave any liquid or solid residues, however it is not safe for humans as it reduces the levels of oxygen.

A, C & DF are incorrect – These are water based fire suppression systems

787. How does an auditor ensure that there are safeguards against the risks of heating, ventilation and air-conditioning systems?

A. Review heating, ventilation and air-conditioning design

B. Review any shielding strategies

C. Verify critical systems and emergency power supplies

D. Interview officials and review planning documents

KEY A

A is correct - The auditor has to review a heating, ventilation and air-conditioning design to verify proper functioning within an organization in order to ensure safeguards against risks of heating, ventilation and air-conditioning

B is incorrect – This is done to check control of radio emissions effect on computer systems

C is incorrect – This is done to establish adequate interior security based on risk

D is incorrect – This is done to adequately protect against emerging threats

788. How does an auditor ensure that adequate environmental controls have been implemented?

A. Interview security personnel to ensure their awareness and responsibilities

B. Verify critical systems and emergency power supplies

C. Interview staff, determine humidity, temperature and voltage are within acceptable levels

D. Interview officials and review planning documents and review training records and documentation

KEY C

C is correct - To ensure adequate environmental controls have been implemented, an auditor has to: Interview managers and scrutinize that operations staff are aware of the locations of fire alarms, extinguishers, shut-off power switches, air -ventilation apparatus and other emergency devices.

Determine that humidity, temperature and voltage are controlled within the accepted levels.

Check cabling, plumbing, room ceiling smoke detectors, water detectors on the floor are installed and in proper working order.

A is incorrect –This is done to ensure that Staff has been trained to react to emergencies

B is incorrect – This is done to establish adequate interior security based on risk

D is incorrect – This is done to adequately protect against emerging threats

789. Which of the following is not a component in the information systems infrastructure between the user and the Data Base?

A. Network operating systems

B. Application software

C. Physical documents

D. Data Base Management System

KEY C

C is correct - Physical documents do not form a component in the information systems infrastructure between the user and the database

A, B and D are incorrect – These are components in the information systems infrastructure which have to be subjected to appropriate means of security

790. What is the task of an auditor when evaluating the risks associated with hardware components?

A. Consider vulnerabilities of different communication channels and devices like workstations, peripherals etc.

B. Ensure that logical access to system software are controlled to detect changes in system configuration

C. Evaluate the access security enforced by the DBMS

D. Focus on the effectiveness of boundary controls and I/O controls

KEY A

A is correct - Hardware includes computer workstations, terminal devices, communication devices, peripherals etc., constituting the physical interface with the users. Here the auditor should consider vulnerabilities of different communication channels and devices specifically (e.g. modems, network interface cards) connected to computers. Software

B, C and D are incorrect – These are the auditors tasks when auditing systems software, Database Management System and Application software respectively.

791. What are the tasks of an auditor while evaluating the vulnerabilities of a Data Base Management System (DBMS)?

A. Evaluate access permissions configured in software

B. Evaluating the access security enforced by the DBMS

C. Ensure that logical access to system software are controlled to detect changes in system configuration

D. Focus on the effectiveness of boundary controls and I/O controls

KEY B

B is correct - In environments involving voluminous data handling, a Database Management System (DBMS) manages the organisation of data in the databases. The auditor is required to evaluate the access security enforced by the DBMS, which could include schema definitions, access to data dictionary, directory services and scripts to restrict access implemented by the DBMS.

A, C and D are incorrect – These are the auditors tasks when auditing application software, systems software and access control software respectively

792. What is Masquerading?

A. Disguising or Impersonation

B. Using an unattended terminal

C. Tapping a communication cable

D. Flooding Memory buffers and communication ports

KEY A

A is correct - **Masquerading** means disguising or impersonation. The attacker pretends to be an authorized user of a system in order to gain access to or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism.

B is incorrect - Unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification) and left unattended is called Piggy backing

C is incorrect - Tapping a communication cable to collect information being transmitted is called Wire trapping

D is incorrect – In **Denial of Service t**he perpetrator attempts to flood memory buffers and communication ports to prevent delivery of normal services.

793. What is Phishing?

A. Requesting personal details over phone posing as an originator

B. Sending a mail posing as an originator (ex. bank) requesting to provide information by clicking a link

C. Installing software that captures user information like login id and password

D. Specially design programs that captures and transmits information

KEY B

B is correct - **Phishing:** User receives a mail requesting to provide authentication information by clicking on link provided. The mail and link appears to be actual originator e.g. Bank. Unaware users click on link and provide confidential information. The most popular attacks on banking systems in the recent times, they target gullible victims, using a combination of social engineering, e-mail and fake websites to con the victim to click on a link embedded in an apparent authentic mail from a reputed bank. The link takes the victim (generally a customer of the bank) to a look-alike Bank website that gets the personal details of the victim including details such as PIN and internet banking password, which is then exploited by the hacker.

A is incorrect – The above technique used over phone is called Impersonating

C is incorrect – This technique is **KEY logging:** Perpetrator installs software that captures the KEY sequence used by user including login information. KEY logger can be sent thru mail or infected pen drive like virus or other malware. There are hardware KEY loggers available that are connected to system where KEY board is attached.

D is incorrect – These programs are called Malware.

794. What are malicious codes that attaches to a host program and propogates when an infected program is executed?

A. Worms

B. Trojan Horses

C. Viruses

D. Logic Bombs

KEY C

C is correct - Viruses are malicious code that attaches to a host program and propagates when an infected program is executed? The perpetrator's objective is to multiply and spread the code. However they are dependent on another program or human action to replicate or to activate their payload. They are not capable of self-actuating.

A is incorrect – Worms are malicious programs that attack a network by moving from device to device and create undesirable traffic.

B is incorrect – These are malicious code which hides inside a host program that does something useful. Once these programs are executed, the hidden malicious code is released to attack the workstation, server, or network or to allow unauthorized access to those devices.

D is incorrect – These are legitimate programs, to which malicious code has been added. Their destructive action is programmed to "blow up" on occurrence of a logical event such as time or a logical event as number of users, memory/disk space usage, etc.

795. What is a macro virus?

A. A virus that infects Microsoft Word or similar applications

B. A virus that hides itself from anti virus software

C. A virus which encrypts itself and is very hard to detect

D. Software that tracks the internet activities of the user

KEY A

A is correct - A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or an event trigger. If a user accesses a document containing a viral macro and unwittingly executes this macro virus, it can then copy itself into that application's start-up files.

B is incorrect - Polymorphic viruses are difficult to detect because they hide themselves from antivirus software by altering their appearance after each infection. Some polymorphic viruses can assume over two billion different identities.

C is incorrect - Stealth viruses attempt to hide their presence from both the operating system and the antivirus software by encrypting themselves. They are similar to polymorphic viruses and are very hard to detect.

D is incorrect – These are Adware and Spyware that often come with some commercial software, both packaged as well as shareware software. There is often a reference to the Adware and Spyware software in the license agreement.

796. Which of the following is not a characteristic of Logic Bombs?

A. This blows up on the occurrence of a logical event

B. These are programmed to open specific ports to allow access for exploitation

C. This checks whether a particular condition has been met to execute the logic code

D. These are very difficult to detect as its destructive information set is known only after it is executed

KEY B

B is correct - This is the characteristic of a Trojan Horse

A, C and D are incorrect – These are the characteristics of Logic Bombs.

797. Which of the following is not a characteristic of a Macro Virus?

A. When executed unwittingly by a user, it copies itself to the applications start up files

B. Its infection spreads to other machines on a network

C. These are relatively harmless

D. This can assume over two billion two billion different identities

KEY D

D is correct - This is the characteristic of a polymorphic virus

A, B and D are incorrect – These are the characteristics of macro Viruses

798. User Registration is generally approved by:

A. User himself

B. IS Auditor

C. User Manager

D. System Administrator

KEY C

C is correct - User Registration is generally done based on the job responsibilities and confirmed by User manager. This must be approved by information owner. User registration process must answer:

- Why the user is granted the access?
- Has the data owner approved the access?
- Has the user accepted the responsibility?

A, B, and D are incorrect – These people are not authorised to approve User Registration.

799. On what basis are access privileges assigned to a user?

A. Seniority level

B. Expertise and qualification

C. Job requirements and responsibilities

D. There is no basis. It is randomly assigned

KEY C

C is correct - Access privileges are to be aligned with job requirements and responsibilities. These are defined and approved by the information asset owner.

A, B and D are incorrect – Access privileges cannot be assigned based on these criteria

800. In password management, how can misuse of passwords by system administrators be prevented?

A. Force change on first login by the user

B. Secure communication of password to user

C. By generating hash while storing

D. By taking an undertaking from the system administrator

KEY A

A is correct - Force change on first login by the user so as to prevent possible misuse by system administrators

B and C are incorrect – These are a few of the other password management functions

D is incorrect – Taking an undertaking is not an appropriate method

801. Which of the following is not mandatory for good password management?

A. All passwords should be authenticated

B. Password expiry must be managed as per policy

C. Every user's password should be known to the user manager

D. Users have to be educated and made responsible for their password

KEY C

C is correct - It is not necessary for the user manager to know the passwords of all the users

A, B and D are incorrect – these are some of the functions of password management

802. How is it possible to detect excess rights due to changes in responsibilities, emergencies etc.?

A. By assigning access privileges

B. By getting the password of the user

C. By a person who has administrative privileges

D. By Periodic review of user's access rights

KEY D

D is correct - Periodic review of user's access rights is essential process to detect possible excess rights due to changes in responsibilities, emergencies, and other changes. These reviews must be conducted by information owner and administrators facilitates by providing available accesses recorded in system.

A, B and C are incorrect – excess rights due to changes in responsibilities cannot be detected by these methods

803. What must an IS auditor ensure while reviewing access controls related to user id and passwords of default users with administrative privileges?

A. They can remain but it should be known to the organisation

B. These user ids should be disabled and passwords changed

C. Default users cannot have a user id or password

D. Default users should be educated about their responsibility

KEY B

B is correct - Applications, operating systems and databases purchased from vendor have provision for default users with administrative privileges required for implementation and/or maintenance of application, OS or database. The user ID and Passwords for these users are published by the vendor required for implementing. It is expected that these password must be changed immediately as soon as system is implemented. While reviewing these access controls IS auditor must ensure that these user ID are either disabled, or passwords have been changed and suitably controlled by the organization.

A, C and D are incorrect – None of these options will ensure protection to information

804. What is segregation of networks with respect to network access control?

A. Isolation of network from internet usage service availability

B. Aligning internet service requirements with the business need policy

C. Restriction of traffic between networks

D. Specifying the exact path or route connecting the network

KEY A

A is correct - Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office this network is to be isolated from the internet usage service availability for employees.

B is incorrect - An enterprise wide applicable internet service requirements aligned with the business need policy based on business needs for using the Internet services is the first step for network access control. Selection of appropriate services and approval to access them will be part of this policy. The policy also specify the use on internet and internet based services while access internet using organization's devices.

C is incorrect – This is another feature of network access control – network connection and routing control - The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility. The techniques of authentication and authorization as per access policy have been implemented across the organization's network.

D is incorrect – Enforced path - Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; say for example internet access by employees will be routed through a firewall. And to maintain a hierarchical access levels for both internal and external user logging. An Internet connection exposes an organization to the entire world. This brings up the issue of benefits the organization should derive along with the precaution against harmful elements.

805. Name the control which helps in auditing and tracking of transactions along with date and time?

A. Segregation of Networks

B. Network connection and routing control

C. Clock synchronisation

D. Enforced path

KEY C

C is correct - Clock synchronization is useful control to ensure that event and audit logs maintained across an enterprise are in synch and can be correlated. This helps in auditing and tracking of transactions along with date and time that is uniform across organization. In modern networks this function is centralized and automated.

A is incorrect – Segregation of Networks - Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office this network is to be isolated from the internet usage service availability for employees.

B is incorrect - This is another feature of network access control – network connection and routing control - The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility. The techniques of authentication and authorization as per access policy have been implemented across the organization's network.

D is incorrect – Enforced path - Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; say for example internet access by employees will be routed through a firewall. And to maintain a hierarchical access levels for both internal and external user logging. An Internet connection exposes an organization to the entire world. This brings up the issue of benefits the organization should derive along with the precaution against harmful elements.

806. A user is allowed to access only those items he is authorised to access. How is access to information prevented in an application?

A. By application specific menu interfaces

B. System Access is monitored

C. By Event logging

D. By monitoring system use

KEY A

A is correct - The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items he is authorized to access. Controls are implemented on the access rights of users, For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations.

B is incorrect – This is a part of Sensitive system isolation - Based on the critical constitution of a system in an enterprise it may even be necessary to run the system in an isolated environment. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.

C is incorrect - In Computer systems it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. This is called event logging.

D is incorrect – Monitor system use - Based on the risk assessment a constant monitoring of some critical systems is essential. the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.

807. In operation system control, what is the use of system utilities?

A. Ensures that a particular session can be initiated from a particular location

B. Help manage critical functions of the operating system

C. Provides means to alert authorities if users are forced to execute instructions

D. Prevents unauthorised access by limiting time slot

KEY B

B is correct - System utilities are the programs that help to manage critical functions of the operating system—for example, addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.

A is incorrect - **Automated terminal identification** helps to ensure that a particular session could only be initiated from a particular location or computer terminal.

C is incorrect - **Duress alarm to safeguard users**: If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities. An example could be forcing a person to withdraw money from the ATM. Many banks provide a secret code to alert the bank about such transactions.

D is incorrect – **Limitation of connection time**: Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m.—or on a Saturday or Sunday. This is useful in preventing unauthorized accesses by authorized users.

808. Methods like Biometric Authentication or digital certificates are employed for which aspect of operating system control?

A. Password Management

B. Terminal log on procedures

C. User identification and authentication

D. Automated terminal identification

KEY C

C is correct - **User identification and authentication:** The users must be identified and authenticated in a fool proof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

A is incorrect - An operating system could enforce selection of good passwords. Internal storage of password should use one-way encryption algorithms and the password file should not be accessible to users.

B is incorrect - **Terminal log-on procedures:** The log-on procedure does not provide unnecessary help or information, which could be misused by an intruder.

D is incorrect – **Automated terminal identification**: This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.

809. What are 'Audit Trails'?

A. History of transactions

B. Record of system activities enabling examination of a transaction

C. Attempts to gain unauthorised access to system

D. Unauthorised privileges granted to users

KEY B

B is correct - Logs are also called 'audit trail'. It is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Violation reports should be frequently and regularly reviewed by information owner to identify any unauthorized change or access.

A, C and D are incorrect – An audit associated with information system security searches for these activities that are obtained from Audit trails.

810. What is authentication with regard to Access Control Mechanism?

A. Process by which user provides a claimed identity

B. Process by which a user is allowed to perform a pre determined set of actions

C. Prevention of unauthorised access by a user

D. Mechanism through which user's claim is verified

KEY D

D is correct - Authentication is a mechanism through which the user's claim is verified.

A is incorrect - process by which a user provides a claimed identity to the system such as an account number is called identification

B is incorrect - The authenticated user is allowed to perform a pre-determined set of actions on eligible resources. This is called authorisation

C is incorrect – The primary function of access control is to allow authorized access and prevent unauthorized access to information resources in an organization.

811. A physical/biometric comparison falls under which category of authentication factor?

A. Something the user is

B. Something the user knows

C. Something the user has

D. Two factor authentication

KEY A

A is correct - Finger print, Biometric templates etc. come under this category

B is incorrect – Password, PIN entry etc. come under this category

C is incorrect – Identification Badge, Smart card, Bank card etc. come under this category

D is incorrect – Two-factor or dual factor authentication uses two factors and the three-factor authentication uses all the three factors.

812. Which is the authentication technique which allows the password to be based on changing input rather than just time?

A. Passwords

B. Challenge response

C. PIN's

D. One time passwords

KEY B

B is correct - An alternative to one-time passwords is challenge response schemes. Instead of having the device just blindly generate a password, a user identifies himself to the server, usually by presenting his user ID. The server then responds with a challenge, which is usually a short phrase of letters and numbers. The user types the challenge into the device and, based on the challenge, the device responds with an output. The user then types that output in as his password to the server. This scheme is slightly more complicated, but it allows the password to be based on changing input rather than just time.

A is incorrect - This is the most common authentication technique that depends on remembered information. The user, initially, identifies him using his login-id to the system and then provides the password information. Once the system is able to locate the match and is successful for both fields, the system authenticates the user and enables access to resources based on the authorization matrix. However if a match is not successful, the system returns a message (such as “Invalid User or password”) thus preventing access to resources.

C is incorrect - **PIN** is a type of password, usually a 4-digit numeric value that is used in certain systems to gain access, and authenticate. The PIN should be such that a person or a computer cannot guess it in sufficient time by using a guess and check method, i.e. where it guesses the PIN, and checks for correctness by testing it on the system that the person is attempting to gain access to and the process is repeated with a different guess till access is obtained. PINs are commonly used for gaining access to Automatic Teller Machines (ATMs).

D is incorrect – One-time passwords solve the problems of user-derived passwords. With one-time passwords, each time the user tries to log on he is given a new password. Even if an attacker intercepts the password, he will not be able to use it to gain access because it is good for only one session and predetermined limited time period. For example one time password for online card transaction is provided by bank to user on registered mobile is valid for 10 minutes only. One-time passwords typically use a small hardware device or software that generates a new password every time. The server also has the same software running, so when a user types in his password, the server can confirm whether it is the correct password. Each time the user logs on he has a new password, so it is much more secure.

813. What is the attacking technique in which the attacker uses a malicious software to steal passwords and other information?

A. Trojan attack

B. Brute force

C. Dictionary attack

D. Spoofing attack

KEY A

A is correct - **Trojan**: A malicious software, which the attacker can use to steal access control lists, passwords or other information.

B is incorrect - In this crude form of attack, the attacker tries out every possible combination to hit on the successful match. The attacker may also use various password cracking software that assist in this effort.

C is incorrect - **Dictionary attack:** On the similar lines as brute force, this type of attack is based on the assumption that users tend to use common words as passwords, which can be found in a dictionary, hence the name. The "dictionary" simply consists of a list of words, including proper names (Raju, Ramesh, Ibrahim, etc.) and also that of mythological or religious names (Krishna, Jesus, Osiris, Buddha, etc.).

D is incorrect – **Spoofing attacks:** In this technique, the attacker plants a Trojan program, which masquerades as the system's logon screen, gets the logon and password information and returns control to the genuine access control mechanism. Once the information is obtained, the attacker uses the information to gain access to the system resources.

814. Automatic log out after a predetermined period of inactivity is a technique used against which type of attack?

A. Spoofing attacks

B. Dictionary attacks

C. Piggy backing

D. Trojan attack

KEY C

C is correct - **Piggybacking:** As stated earlier, an unauthorized user may wait for an authorised user to log in and leave a terminal unattended. The logical techniques that are used to secure against this attack are to automatically log out the session after a pre-determined period of inactivity or by using password-protected screen savers.

A Band D are incorrect – For these attacks other techniques are used

815. Which of the following is the feature of a Smart token only?

A. Contains information such as name, identification no, photograph etc

B. Contains a magnetic strip which stores information

C. The user is required to KEY in remembered information

D. Contains a processor chip which enables storing dynamic information

KEY D

D is correct - **Smart Tokens:** In this case, the card or device contains a small processor chip which enables storing dynamic information on the card. Besides static information about the user, the smart tokens can store dynamic information such as bank balance, credit limits etc., however the loss of such smart cards can have more serious implications.

A B and C are incorrect – These are the features of a memory token also

816. In which of the following tokens does the card contain a bar code which is read when brought in proximity to the reader device?

A. Processor based proximity reader

B. Smart tokens

C. Static proximity reader

D. Memory tokens

KEY C

C is correct - In static tokens, the card contains a bar code, which has to be brought in proximity of the reader device.

A is incorrect – In case of processor based tokens, the token device, once in the range of the reader, senses the reader and transmits a series of codes to the reader.

B is incorrect - In this case, the card or device contains a small processor chip which enables storing dynamic information on the card.

D is incorrect – In its most common form, the cards contain visible information such as name, identification number, photograph and such other information about the user and also a magnetic strip.

817. In Biometrics, what is the Crossover Error rate (CER)?

A. A very low FRR

B. The point at which FRR equals FAR

C. A very high FAR

D. The point at which FAR and FRR are zero

KEY B

B is correct - An overall metric used is the Crossover Error Rate (CER) which is the point at which FRR equals FAR.

A, C and D are incorrect – False Rejection Rate (FRR) which is wrongfully rejecting a rightful user and False Acceptance Rate (FAR) which involves an unauthorized user being wrongfully authenticated as a right user. Ideally a system should have a low false rejection and low false acceptance rate. Most biometric systems have sensitivity levels which can be tuned. The more sensitive a system becomes, FAR drops while FRR increases. Thus, FRR and FAR tends to inversely related.

818. Which of the following is not a function of the operating system?

A. Provides independent user and access privilege management mechanism

B. Supports execution of applications and enforces and security constraints defined at that level

C. Isolates processes from each other and protects permanent data stored in its files

D. Provides controlled access to shared resources

KEY A

A is correct - This is not the function of an operating system, this is the function of an application

B, C and D are incorrect – These are the functions of an operating system

819. The flexibility of a Pluggable authentication module allows to:

A. Execute applications and support any security constraints

B. Use multiple authentications for a given service

C. Provide controlled access to shared resources

D. Use physiological and behavioral characteristics to identify user

KEY B

B is correct - Applications enabled to make use of PAM can be plugged-in to new technologies without modifying the existing applications. This flexibility allows administrators to do the following:

Select any authentication service on the system for an application

- Use multiple authentication mechanisms for a given service
- Add new authentication service modules without modifying existing applications

- Use a previously entered password for authentication with multiple modules
- A general Authentication scheme independent of the authentication mechanism may be used

A and C are incorrect – These are the functions of an operating system

D are incorrect – This is the identification technique of biometrics

820. Most operating systems have at least three types of file permissions: read, write and execute. The least access that have to be given to users is:

A. Write

B. Execute

C. Read

D. Read and Write

KEY C

C is correct - The users have to be given at least read access to many of the system files.

A, B and D are incorrect – These accesses are given only to authorised users.

821. When a system receives a request, how does it determine access rights for the particular request?

A. By authenticating the password entered by the user

B. By using the access matrix

C. By consulting a hierarchy of rules in the Access Control List

D. By a challenge response

KEY C

C is correct - Access control enables one to protect a system or part of the system (directories, files, file types, etc.). When the system receives a request, it determines access by consulting a hierarchy of rules in the ACL.

A This is one of the authentication techniques

B is incorrect – This is used by the operating system

D is incorrect – This is one of the authentication techniques

822. What does an Access Control Entry in an ACL consist of?

A. Name of the database and its path

B. Name of the user and his reporting structure

C. Name of the user and his group or role

D. Name of users and their access privileges

KEY D

D is correct - ACL has one or more access control entries (ACEs), each consisting of the name of a user or a group of users. The user can also be a role name, such as programmer or tester. For each of these users, groups, or roles, the access privileges are stated in a string of bits called an access mask. Generally, the system, administrator or the object owner creates the access control list for an object.

A, B and C are incorrect – These are not the constituents of an Access Control Entry

823. The core objective of an IdM system in a corporate setting is:

A. One identity per individual

B. One user per database

C. One role per individual

D. One user one group

KEY A

A is correct - The core objective of an IdM system in a corporate setting is: *one identity per individual*. And once that digital ID has been established, it has to be maintained, modified and monitored throughout what is called the "User access lifecycle."

B, C and D are incorrect – these are not the objectives of an IdM system.

824. Which of the following does not form a part of Identity Management?

A. Controls User Access Provisioning Lifecycle

B. Maintains the identity of a user and actions they are authorised to perform

C. Determines which user can access which resource

D. Manages descriptive information about the user

KEY C

C is correct - This is the attribute of Access Control Policies

A B and D are incorrect – These are the tasks of Identity Management

825. System administrators/Network Administrators who have the powers to create or amend user profiles are:

A. Privileged users

B. Administrative users

C. Special users

D. Maintenance users

KEY A

A is correct - Privileged user is a user who has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

B, C and D are incorrect – There are no such user categories

826. A privileged user can use the user account that has privileged access for only:

A. Normal business use

B. Non privileged activities

C. Privileged activities

D. Logging in to a system

KEY C

C is correct - Privileged Users should be required to create strong passwords comprising of letters, numbers, and special characters. The user account that has privileged access should have a unique password that is different from all other accounts accessed by the User.

A, B and D are incorrect – All Users that have access to privileged accounts should be assigned their own user ID for normal business use. Privileged Users must use their personal user IDs for conducting non-privileged activities. Wherever possible the User must login to a system using their personal user ID prior to invoking a privileged account.

827. What is a 'back door' or 'trap door'?

A. Flaw that allows data to circumvent the encryption process

B. Bypass which is a means of access for authorised access

C. Flaw that allows an attacker to circumvent security mechanisms

D. Mechanism put in place by an attacker

KEY B

B is correct - A bypass that is purposefully put in place as a means of access for authorized users is called a ***back door*** or a ***trap door***.

A is incorrect - A flaw that allows data to circumvent the encryption process and escape, unencrypted, as plaintext isa crypto by pass

C and D are incorrect – These are definitions for bypass

828. What are the rows of an access control matrix called?

A. Access Control lists

B. Subjects

C. Objects

D. Capability lists

KEY D

D is correct - the rows are called ***capability lists***.

A, B and C are incorrect – A *subject* is an active entity that is seeking rights to a resource or object. A subject can be a person, a program, or a process. An *object* is a passive entity, such as a file or a storage resource. The columns of the access matrix are called ***Access Control Lists (ACLs)***

829. What is the major concern of using group/generic ids?

A. Fixing accountability of actions to individual

B. It needs special approval

C. It is not allowed in ERP packages

D. It is not wise to share user id with others

KEY A

A is correct - The main concern in using group id is the fixing accountability of actions to individual.

B, C and D are incorrect – These are all the conditions that have to be met in case group/generic ids are used

830. What is the specialty of a Single Sign On session?

A. User ids and passwords are shared among select users

B. A single user id and password to log on to all required applications

C. Verifies that the users are whoever they claim to be

D. Verifies that the network components used by the users are within their permission profile

KEY B

B is correct - In SSO, a user provides one ID and password per work session and is automatically logged on to all the required applications.

A is incorrect - users Ids are created and password is shared among select users when generic/group id's are used

C and D are incorrect – These are the features of Kerberos

831. What is the function of Active Directory (AD) domain controller?

A. Accesses and maintains distributed directory information services over an Internet Protocol network

B. Plays an important role in developing intranet and internet applications by allowing the sharing of information by users

C. Authenticates and authorises all users and computers in a Windows domain type network

D. Verifies that users are who they claim to be and the network components they use are within their profile

KEY C

C is correct - AD is a directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems. An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

A and B are incorrect - The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.[1] Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.

D is incorrect – This is the primary use of Kerberos - to verify that users are who they claim to be and the network components they use are contained within their permission profile.

832. Which authentication mechanism issues 'tickets' which have a limited life span and are stored in the users credential cache?

A. AD

B. LDAP

C. Kerberos

D. DNS

KEY C

C is correct - The primary use of Kerberos is to verify that users are who they claim to be and the network components they use are contained within their permission profile. To accomplish this, a trusted Kerberos server issues “tickets” to users. These tickets have a limited life span and are stored in the user’s credential cache.

A, B and D are incorrect – when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Active Directory makes use of Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

833. Which of following is an advantage of Single Sign On?

A. Easier administration of changing or deleting passwords

B. It can avoid a potential single point of failure issue

C. Maintaining SSO is easy as it is not prone to human errors

D. It protects network traffic

KEY A

A is correct - The advantages of SSO include having the ability to use stronger passwords, easier administration of changing or deleting the passwords, and requiring less time to access resources.

B is incorrect – This is the advantage of Kerberos

C and D are incorrect – These are not advantages of SSO. Maintaining SSO is atedious process and it is prone to human errors. It does not protect network traffic.

834. In a SSO system, once a user’s identity and authentication is established, on what basis are access criteria determined?

A. All identified users are granted access

B. Based on Roles, groups or network location

C. All authenticated users are granted access

D. It is not necessary to establish identity or authenticity

KEY B

B is correct - Once a user’s identity and authentication are established, authorization levels determine the extent of system rights that a user can hold.

Access criteria types can be broken up into:

- Roles
- Groups
- Physical or logical (network) location
- Time of day
- Transaction type

A, C and D are incorrect – Only after identity and authenticity is established, authorisation comes into play

835. In a Single Sign On system, all access criteria should default to:

A. No access

B. Full access

C. Granting access to all identified users

D. Granting access to all authenticated users

KEY A

A is correct - All access criteria should default to "no access" and authorizations should be granted on need to know basis.

B, C and D are incorrect – Just because a subject has been identified and authenticated does not automatically mean they have been authorized. It is possible for a subject to be logged onto a network (i.e., identified and authenticated) but be blocked from accessing a file or printing to a printer (i.e., by not being authorized to perform that activity). Most users are authorized to perform only a limited number of activities on a specific collection of resources. Identification and authentication are all-or-nothing aspects of access control. Authorization has a wide range of variations between all or nothing for each individual object within the environment. A user may be able to read a file but not delete it, print a document but not alter the print queue, or log onto a system but not access any resources.

836. What should an access control mechanism ensure?

A. Subjects should be identified before they are granted access

B. All subjects that are authenticated should be authorised to access objects

C. All Objects can be accessed by authorised subjects

D. Subjects gain access to objects only if they are authorised to

KEY D

D is correct - The access control mechanism should ensure that subjects gain access to objects only if they are authorized to.

A B and C are incorrect – ***Subject*** of operating systems are (active) entities that communicate with the system and use its resources. The best example for a subject is the user or a process. ***Objects*** on the other hand are entities of the operating system that are accessed (requested) by the subject. The access control mechanism should ensure that subjects gain access to objects only if they are authorized to.

837. This is a multi- level secure access control which defines a hierarchy of levels of security.

A. Discretionary Access Control

B. Mandatory Access Control

C. Role Based Access Control

D. Database Access Control

KEY B

B is correct - **Mandatory Access Control**- It is a multi-level secure access control mechanism. It defines a hierarchy of levels of security. A security policy defines rules by which the access is controlled.

A is incorrect - In this type of access control, every object has an owner. The owner (subject) grants access to his resources (objects) for other users and/or groups.

C is incorrect - In role based systems, users get assigned roles based on their functions in that system.

D is incorrect – This is not a type of access control mechanism

838. Which of the following is a feature of Role Based Access Control?

A. Multilevel secure access control mechanism

B. The Matrix defines the whole state of the system

C. Systems are centrally administered and are nondiscretionary

D. Access control lists are used to store the rights with object

KEY C

C is correct - **Role Based Access Control**- In some environments, it is problematical to determine who the owner of resources is. In role based systems, users get assigned roles based on their functions in that system. These systems are centrally administered, they are nondiscretionary. An example is a hospital.

A is incorrect – This is the feature of Mandatory Access Control

B and D are incorrect – These are the features of discretionary access control

839. Access to database can be controlled through permission settings. On what basis is this permission system designed?

A. Principle of least privileges

B. Permissible values or limits

C. Approval by data owner

D. Access levels

KEY D

D is correct - Each database has its own customizable permissions system. The permission system is based on *access levels*.

A and B are incorrect – Relational Database works on the principles of tables and relations and allows rules of integrity and access to be specified. The principle of least privileges to data items can be enforced using views as against reads. Such rules can be restricted by a range of parameters such as permissible values or limits.

C is incorrect - The access to data base can be **Discretionary** based on the approved by data owner (usually business process owner who is accountable for data stored in database)

840. What permissions does a user with 'Manage' access level have with regard to a database?

A. View, Edit, Add and delete

B. View, add, edit and delete (only information added by them)

C. View, Edit, Add, Delete and change database design

D. Only view

KEY C

C is correct - Users can view, edit, add, and delete any information in the database and any aspect of the database design. They can also export any information to a file, and import information from a file. A member who has Manage access is called a *Database Manager*. This is a powerful permission level, so use it carefully.

A, B and D are incorrect – Access levels are 'Edit', 'Read and Add (own records only)' and 'Read' respectively

841. When access to database is controlled through application software, how is maintenance of database done?

A. Users are granted access for maintenance

B. Direct access is granted to DBA

C. Direct access is granted to system administrator

D. User managers are granted access

KEY B

B is correct - Direct access to database level (also sometimes referred as backend access) are then restricted only to data base administrators (DBA) to perform maintenance work. It is possible to restrict DBA to access data.

A, C and D are incorrect – When access to database is controlled, only DBA's have direct access.

842. What is user access to applications with respect to their job responsibilities or logical access control called?

A. User Password Management

B. Equipment Management

C. Privilege Management

D. Network Management

KEY C

C is correct - Privileged user is a user who has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

A, B and D are incorrect – These are other aspects of access control

843. Which of the following operating system access control ensures a particular session is initiated from a particular location or computer terminal?

A. Automated Terminal Identification

B. Terminal Log On Procedures

C. Password Management Stem

D. User identification and Authentication

KEY A

A is correct - **Automated terminal identification**: This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.

B is incorrect – **Terminal log-on procedures:** The log-on procedure does not provide unnecessary help or information, which could be misused by an intruder.

C is incorrect – **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way encryption algorithms and the password file should not be accessible to users.

D is incorrect – **User identification and authentication:** The users must be identified and authenticated in a fool proof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

844. Which of the following is a process by which a user provides a claimed identity to access a system?

A. User Authorisation

B. User Registration

C. User Identification

D. User logging

KEY C

C is correct - **Identification:** Identification is a process by which a user provides a claimed identity to the system such as an account number.

A is incorrect – **Authorization**: The authenticated user is allowed to perform a pre-determined set of actions on eligible resources.

B and D are incorrect -These are not par the three step process of Access Control Mechanism

845. What are the three steps in the process of access control mechanism?

A. Authorisation, information and identification

B. Synchronisation, verification and authentication

C. Identification, authentication and authorisation

D. Synchronisation, identification and authentication

KEY C

C is correct - Access control mechanism is actually a three step process – identification, authentication and authorisation

A, B and D are incorrect – these are not the steps involved in access control mechanism

846. In _____ authentication techniques, the system authenticates the user and enables access to resources based on the authorisation matrix.

A. Token or smart card

B. Password

C. Biometric comparison

D. Personal Identification Number (PIN)

KEY B

B is correct – In password authentication technique, once the system is able to locate the match and is successful for both fields, the system authenticates the user and enables access to resources based on the authorization matrix

A, C and D are incorrect – These are other types of authentication techniques

847. Which of the following is the weakness of the password logon mechanism?

A. Periodic changing of password

B. Encrypted password

C. Repeated use of the same password

D. One user one password

KEY C

C is correct - Repeated use of the same password makes it vulnerable to attacks

A B and D are incorrect – these are techniques to protect passwords

848. _____ is defined as automated mechanism, which uses physiological and behavioral characteristics to determine or verify identities.

A. Biometrics

B. Plastic cards

C. Logon/password systems

D. Smart Cards

KEY A

A is correct - Biometrics as the name suggests is based on certain physical characteristics or behavioral patterns identified with the individual, which are measurable. The International Biometric Group defines biometrics as automated mechanism which uses physiological and behavioral characteristics to determine or verify identity and further explains that the physiological biometrics are based on measurements and data derived from direct measurement of a part of the human body.

B, C and D are incorrect – These are other types of authentication techniques

849. What is/are the error(s) caused by biometrics due to the complexity of data?

A. False Rejection Rate (FRR)

B. False Acceptance Rate (FAR)

C. Crossover Error Rate (CER)

D. FRR and FAR

KEY D

D is correct - However due to the complexity of data, biometrics suffer from two types of error viz. False Rejection Rate (FRR) which is wrongfully rejecting a rightful user and False Acceptance Rate (FAR) which involves an unauthorized user being wrongfully authenticated as a right user.

A and B incorrect – False Rejection Rate (FRR) which is wrongfully rejecting a rightful user and False Acceptance Rate (FAR) which involves an unauthorized user being wrongfully authenticated as a right user.

C is incorrect - An overall metric used is the Crossover Error Rate (CER) which is the point at which FRR equals FAR.

850. Facial scan, iris and retina scanning are used in _____.

A. Biometric security

B. Smart tokens

C. Bio direct security

D. Backup security

KEY A

A is correct - Some of the biometric characteristics which are used are:

- Fingerprint
- Facial Scan

- Hand Geometry
- Signature
- Voice
- Keystroke Dynamics
- Iris Scanners
- Retina Scanners

B, C and D are incorrect – these are not security measures

851. Which of the following provides system administrators the ability to incorporate multiple authentication mechanisms into an existing system using pluggable modules?

A. Personal Authentication Module

B. Password Processing Module

C. Pluggable Authentication Module

D. Login identification Module

KEY C

C is correct - The pluggable authentication module (PAM) framework provides system administrators with the ability to incorporate multiple authentication mechanisms into an existing system through the use of pluggable modules. Applications enabled to make use of PAM can be plugged-in to new technologies without modifying the existing applications.

A, B and D are incorrect – Thee are not authentication modules

852. Access privileges of a user for two entities, A and B for read and write are maintained in the _____ within an application.

A. Actual access control list

B. Access control list

C. Acquired control entry

D. Secret policy entry

KEY B

B is correct - ACL has one or more access control entries (ACEs), each consisting of the name of a user or a group of users. The user can also be a role name, such as programmer or tester. For each of these users, groups, or roles, the access privileges are stated in a string of bits called an access mask.

A, C and D are incorrect

853. The characteristic of network that improves reliability and performance due to dynamic routings between two end points is better known as:

A. Anonymity

B. Automation

C. Routing diversity

D. Opaqueness

KEY C

C is correct - **Routing diversity:** To maintain or improve reliability and performance, routings between two endpoints are usually dynamic. That is, the same interaction may follow one path through the network the first time and a very different path the second time. In fact, a query may take a different path from the response that follows a few seconds later.

A is incorrect - **Anonymity:** A network removes personal interaction i.e. most of the clues, such as appearance, voice, or context, by which we recognize acquaintances.

B is incorrect – **Automation:** In some networks, one or both endpoints, as well as all intermediate points, involved in a given communication may be machines with only minimal human supervision.

D is incorrect - **Opaqueness:** Because the dimension of distance is hidden, users cannot tell whether a remote host is in the room next door or in a different country. In the same way, users cannot distinguish whether they are connected to a node in an office, school, home, or warehouse, or whether the node's computing system is large or small, modest or powerful. In fact, users cannot tell if the current communication involves the same machine with which they communicated the last time.

854. Network establishes communication among disperse users/machines. Which of the following is a disadvantage of this characteristic of networks?

A. Risks like impersonation, intrusion, tapping

B. Very fast communication speed

C. Physically far end points

D. Humans cannot tell the location of the remote site

KEY A

A is correct - Though networks makes it easier to establish communication among geographically dispersed users/machines, it also introduces risks like impersonation, intrusion, tapping.

B, C and D are incorrect – Many networks connect endpoints that are physically far apart. Although not all network connections involve distance, the speed of communication is fast enough that humans usually cannot tell whether a remote site is near or far. These are not disadvantages but advantages of a network

855. What is the program that an attacker uses which reports to him which ports responds to messages and the vulnerabilities present in each port?

A. Social Engineering

B. Dumpster diving

C. Port Scan

D. Malware

KEY C

C is correct - **Port Scan:** An easy way to gather network information is to use a port scanner, a program that, for a particular IP address, reports which ports respond to messages and which of several known vulnerabilities seem to be present.

A, B and D are incorrect – These are other methods used by an attacker

856. What does Social Engineering involve?

A. Gathering bits of on formation from various sources

B. Using social skills to persuade a victim

C. Looking through items that have been discarded

D. Eavesdropping

KEY B

B is correct - Social engineering involves using social skills and personal interaction to get someone to reveal security-relevant information and perhaps even to do something that permits an attack.

A, C and D are incorrect – These methods of gathering information are classified under Reconnaissance

857. 'Dumpster Diving' is a commonly used _____ technique.

A. Reconnaissance

B. Social Engineering

C. Documentation

D. Application fingerprint

KEY A

A is correct - One commonly used reconnaissance technique is "dumpster diving." It involves looking through items that have been discarded in garbage bins or waste paper baskets.

B, C and D are incorrect – Dumpster diving does not fall under any of these attacking techniques

858. The process by which an attacker comes to know about the commercial server on which an application is running, the version and operating system for the same is known as:

A. Biometrics

B. Protocol flaws

C. Wiretapping

D. OS and Application Fingerprinting

KEY D

D is correct - **Operating System and Application Fingerprinting:** Here the attacker wants to know which commercial server application is running, what version, and what the underlying operating system and version are.

A is incorrect – This is a method of identification of system user

B is incorrect – There are flaws in many of the commonly used protocols called protocol flaws. These flaws can be exploited by an attacker.

C is incorrect – Wiretapping is the technique intercepting communications through some effort.

859. How does an attacker use Malware to gather information?

A. Investigate a product that can be the target of an attack

B. Search for additional information on systems, applications or sites

C. Scavenge the system and receive information over network

D. Post latest exploits and techniques

KEY C

C is correct - **Malware:** Attacker may use malware like virus or worms to scavenge the system and keep sending information to attacker over network without the knowledge of system user.

A is incorrect – Resource kits distributed by application vendors to other developers can also give attackers tools to use in investigating a product that can subsequently be the

target of an attack. Here, the vendors themselves distribute information that is useful to an attacker.

B and D are incorrect – **Bulletin Boards and Chats:** Underground bulletin boards and chat rooms support exchange of information among the hackers. Attackers can post their latest exploits and techniques, read what others have done, and search for additional information on systems, applications, or sites.

860. The process by which an attacker picks off the content of a communication passing in an unencrypted form is known as:

A. Eavesdropping

B. Wiretapping

C. Microwave signal tapping

D. Satellite signal interception

KEY A

A is correct - An attacker can pick off the content of a communication passing in unencrypted form. The term eavesdrop implies overhearing without expending any extra effort. For example, an attacker (or a system administrator) is eavesdropping by monitoring all traffic passing through a node.

B is incorrect – wiretapping means intercepting communications through some effort.

C is incorrect – Microwave signal tapping is a process by which an attacker can intercept a microwave transmission by interfering with the line of sight between sender and receiver.

D is incorrect – The process of intercepting satellite communication

861. What is active wiretapping?

A. Listening to communications intentionally

B. Overhearing without extra effort

C. Injecting something into the communication stream

D. Placing an illegitimate antenna to intercept communication

KEY C

C is correct - Active wiretapping means injecting something into the communication stream.

A and B are incorrect – These methods are classified under passive wiretapping or eavesdropping

D is incorrect – This method is microwave signal tapping

862. The costs of intercepting satellite communications are very high because:

A. All traffics passing through a node have to be monitored

B. Neither the sender nor receiver should know that contents have been intercepted

C. Satellite communications are heavily multiplexed

D. Cost of placing an illegitimate antenna is more

KEY C

C is correct - In satellite communication, the potential for interception is even greater than with microwave signals. However, because satellite communications are heavily multiplexed, the cost of extracting a single communication is rather high.

A B and D are incorrect – These are not reasons for the high cost of satellite communication interception

863. A wireless signal can be picked up easily within 60 meters. Why?

A. The signal is strong up to 60 meters

B. The signal is weak up to 60 meters

C. There is no signal up to 60 meters

D. The signal is strong after 60 meters

KEY A

A is correct - A wireless signal is strong for approximately 30 to 60 meters. A strong signal can be picked up easily.

B, C and D are incorrect – for the same reason as mentioned above

864. It is not possible to tap an optical system without detection. Why?

A. Optical fiber carries electricity but does not emanate a magnetic field

B. Optical fiber carries light energy which does not emanate a magnetic field

C. An optical signal is not very strong and hence cannot be picked up

D. An antenna needs to be placed to intercept which is detectible

KEY B

B is correct - It is not possible to tap an optical system without detection. Further optical fiber carries light energy, not electricity, which does not emanate a magnetic field as electricity docs.

A ,C and D are incorrect – for the same reasons as mentioned above.

865. A term used for a virtual network of zombies used to launch attack on a system is:

A. BOTnets

B. Spam

C. Malware

D. Spoofing

KEY A

A is correct - BOTnets is a term (robotic network) used for virtual network of zombies. BOTnet operator launches malware/virus on system that once activated remains on system and can be activated remotely. This malware helps the BOTnet operator use the compromised system (Zombie) remotely with to launch attack or collect information. For example Zombies have been used extensively to send e-mail spam. This allows spammers to avoid detection and presumably reduces their bandwidth costs, since the owners of zombies pay for their own bandwidth.

B, C and D are incorrect – These are other methods of attack

866. An employee who is on leave reveals his authentication details to another in order to allow access to carry out urgent activities in his absence. It so happens that these details are passed on without encryption. How is the employee making his authentication information vulnerable to an impersonator?

A. The impersonator can guess the identity by using common passwords

B. The impersonator can exploit flaws and weaknesses of the operating system

C. The attacker can circumvent or disable the authentication mechanism

D. These details can be rescued by an impersonator by eavesdropping or wiretapping

KEY D

D is correct - **Authentication foiled by eavesdropping or wiretapping:** When the account and authentication details are passed on the network without encryption, they are exposed to anyone observing the communication on the network. These authentication details can be reused by an impersonator until they are changed.

A is incorrect - **Authentication foiled by guessing:** Guess the identity and authentication details of the target, by using common passwords, the words in a dictionary, variations of the user name, default passwords, etc.

B is incorrect - **Authentication Foiled by Avoidance:** A flawed operating system may be such that the buffer for typed characters in a password is of fixed size, counting all characters typed, including backspaces for correction. If a user types more characters than the buffer would hold, the overflow causes the operating system to by-pass

password comparison and act as if a correct authentication has been supplied. Such flaws or weaknesses can be exploited by anyone seeking unauthorized access.

C is incorrect – **Non-existent Authentication:** Here the attacker circumvents or disables the authentication mechanism at the target computer. If two computers trusts each other's authentication an attacker may obtain access to one system through an authentication weakness (such as a guest password) and then transfer to another system that accepts the authenticity of a user who comes from a system on its trusted list. The attacker may also use a system that has some identities requiring no authentication. For example, some systems have "guest" or "anonymous" accounts to allow outsiders to access things the systems want to release to the public. These accounts allow access to unauthenticated users.

867. An organisation purchases 10 new systems which are installed by the seller using a test account without any password. However, authentications are put in place and users access information after proper authentication. But the test account has not been deleted. How can an impersonator foil authentication in this case?

A. Information can be accessed through session hijacking

B. Information can be hijacked by intruding between two authenticated users

C. Information becomes vulnerable through well- known test password

D. Information can be accessed through spoofing or masquerading

KEY C

C is correct - **Well-Known Authentication:** Most vendors often sell computers with one system administration account installed, having a default password. Or the systems come with a demonstration or test account, with no required password. Some administrators fail to change the passwords or delete these accounts, creating vulnerability.

A is incorrect - **Session Hijacking:** Session hijacking is intercepting and carrying on a session begun by another entity. In this case the attacker intercepts the session of one of the two entities that have entered into a session and carry it over in the name of that entity. For example, in an e-commerce transaction, just before a user places his order and gives his address, credit number etc. the session could be hijacked by an attacker.

B is incorrect – **Man-in-the-Middle Attack:** A man-in-the-middle attack is a similar to session hijacking, in which one entity intrudes between two others. The difference between man-in-the-middle and hijacking is that a man-in-the-middle usually participates from the start of the session, whereas a session hijacking occurs after a session has been established. The difference is largely semantic and not particularly significant.

D is incorrect - **Spoofing attacks:** In this technique, the attacker plants a Trojan program, which masquerades as the system's logon screen, gets the logon and

password information and returns control to the genuine access control mechanism. Once the information is obtained, the attacker uses the information to gain access to the system resources.

868. Not only is the message itself sensitive but the fact that a message exists is also sensitive. How can an attacker infer that sensitive messages exist between two confidential parties?

A. Traffic flow analysis

B. Using exposures as part of attack

C. By modifying a destination address

D. Taking advantage of mis-delivery due to congestion at network elements

KEY A

A is correct - **Traffic Analysis (or Traffic Flow Analysis):** Sometimes not only is the message itself sensitive but the fact that a message exists is also sensitive. For example, if a wartime enemy sees a large amount of network traffic between headquarters and a particular unit, the enemy may be able to infer that significant action is being planned involving that unit. In a commercial setting, messages sent from the president of one company to the president of a competitor could lead to speculation about a takeover or conspiracy to fix prices.

B is incorrect - **Exposure:** The content of a message may be exposed in temporary buffers, at switches, routers, gateways, and intermediate hosts throughout the network; and in the workspaces of processes that build, format, and present the message. A malicious attacker can use any of these exposures as part of a general or focused attack on message confidentiality.

C and D are incorrect – **Mis-delivery:** Message mis-delivery happens mainly due to congestion at network elements which causes buffers to overflow and packets dropped. Sometimes messages are mis-delivered because of some flaw in the network hardware or software. Most frequently, messages are lost entirely, which is an integrity or availability issue. Occasionally, however, a destination address will be modified or some router or protocol will malfunction, causing a message to be delivered to someone other than the intended recipient. All of these "random" events are quite uncommon. More frequent than network flaws are human errors, caused by mistyping an address.

869. Which of the following amounts to compromising the integrity of messages?

A. Mistyping an address so that it reaches the wrong recipient

B. Mis-delivery of messages due to some flaw in the network hardware or software

C. Exposure of messages in temporary buffers

D. Combining pieces of different messages into one false message

KEY D

A, B and C are incorrect - These amount to message confidentiality threats

D is correct – This amounts to compromising on the integrity of messages

870. It is easy for an attacker to obtain information necessary to attack the website. How?

A. Website codes are downloaded and executed in the browser from which the information can be obtained

B. The attacker exploits vulnerabilities in multiple machines and uses them to attack the target simultaneously.

C. An attacker can monitor the communication between a browser and a server to see how changing a web page entry affects what the browser sends and reacts.

D. attackers execute scripts in the victim's browser which can hijack user sessions

KEY A

A is correct - Web site defacement is common not only because of its visibility but also because of the ease with which one can be done. Web sites are designed so that their code is downloaded and executed in the client (browser). This enables an attacker to obtain the full hypertext document and all programs and references programs embedded in the browser. This essentially gives the attacker the information necessary to attack the web site. Most websites have quite a few common and well known vulnerabilities that an attacker can exploit.

B is incorrect – This is a Distributed Denial of Service Attack

C is incorrect – This pertains to threats from scripts

D is incorrect – This is a form of Cross site scripting

871. What is 'Ping of Death'?

A. Sending more data that what a communication system can handle, thereby preventing receipt of legitimate data

B. Crashing a large number of systems by sending a ping of certain size from a remote machine

C. Corrupting the routing so that traffic can disappear

D. corrupting a name server or causing it to cache spurious entries, thereby redirect the routing of any traffic

KEY B

B is correct - **Ping of death:** It is possible to crash, reboot or otherwise kill a large number of systems by sending a ping of a certain size from a remote machine. This is a serious problem, mainly because this can be reproduced very easily, and from a remote machine. Ping is an ICMP protocol which requests a destination to return a reply, intended to show that the destination system is reachable and functioning. Since ping requires the recipient to respond to the ping request, all the attacker needs to do is send a flood of pings to the intended victim.

A is incorrect – **Connection Flooding:** This is the oldest type of attack where an attacker sends more data than what a communication system can handle, thereby preventing the system from receiving any other legitimate data. Even if an occasional legitimate packet reaches the system, communication will be seriously degraded.

C is incorrect - **Traffic Redirection:** A router is a device that forwards traffic on its way through intermediate networks between a source host's network and a destination's. So if an attacker can corrupt the routing, traffic can disappear.

D is incorrect - **DNS Attacks:** DNS attacks are actually a class of attacks based on the concept of domain name server. A domain name server (DNS) is a table that converts domain names like www.icai.org into network addresses like 202.54.74.130, a process called resolving the domain name or name resolution. By corrupting a name server or causing it to cache spurious entries, an attacker can redirect the routing of any traffic, or ensure that packets intended for a particular host never reach their destination.

872. What are the multiple machines that are used by an attacker for DdS attacks called?

A. Cookies

B. Routers

C. Zombies

D. FTP

KEY C

C is correct - In distributed denial of service (DDoS) attack more than one machine are used by the attacker to attack the target. These multiple machines are called zombies that act on the direction of the attacker and they don't belong to the attacker.

A is incorrect - Cookies are data files created by the server that can be stored on the client machine and fetched by a remote server usually containing information about the user on the client machine. Anyone intercepting or retrieving a cookie can impersonate the cookie's legitimate owner.

B is incorrect – A router is a networking device, commonly specialized hardware, that forwards data packets between computer networks.

D is incorrect - FTP is an application known to transmit communication including user id and password in plain text.

873. A code which can cause serious damage to a system because it is not screened for safety when it is downloaded and runs with the privileges of its invoking user is called:

A. Hostile applet code

B. Cookies

C. Scripts

D. Active X

KEY A

A is correct - A hostile applet is downloadable code that can cause harm on the client's system. Because an applet is not screened for safety when it is downloaded and because it typically runs with the privileges of its invoking user, a hostile applet can cause serious damage.

B is incorrect - Cookies are data files created by the server that can be stored on the client machine and fetched by a remote server usually containing information about the user on the client machine. Anyone intercepting or retrieving a cookie can impersonate the cookie's legitimate owner.

C is incorrect - Clients can invoke services by executing scripts on servers. A malicious user can monitor the communication between a browser and a server to see how changing a web page entry affects what the browser sends and then how the server reacts.

D is incorrect – The popular types of active code languages are Java, JavaScript, VBScript and ActiveX controls.

874. A virus that is difficult to detect because it modifies itself and changes its identity thus hiding itself from antivirus software:

A. MBR Virus

B. Stealth Virus

C. Polymorhic virus

D. Macro Virus

KEY C

A is incorrect - **Master Boot Record (MBR) Viruses:** Affects the boot sector of storage device and further infects when the storage is accessed.

B is incorrect – Stealth viruses hide themselves by tampering the operating system to fool antivirus software into thinking that everything is functioning normally.

C is correct - **Polymorphic Viruses**: Polymorphic viruses are difficult to detect because they can modify themselves and change their identity thus able to hide themselves from antivirus software

D is incorrect – **Macro Viruses:** Macro viruses are the most prevalent computer viruses and can easily infect many types of applications, such as Microsoft Excel and Word.

875. What is a Trojan Horse?

A. Virus that affects the boot sector of storage device

B. Virus that affects applications like Microsoft Word and Excel

C. Stand- alone viruses that are transmitted independently

D. Malicious codes hidden under a legitimate program

KEY D

A is incorrect - MBR virus

B is incorrect – Macro viruses

C is incorrect – Worms

D is correct.

876. Malicious codes added to an existing application to be executed at a later date is known as:

A. Logic bomb

B. Trojan Horse

C. Polymorphic virus

D. Stealth virus

KEY A

A is correct - Logic bombs are malicious code added to an existing application to be executed at a later date. These can be intentional or unintentional. For example Year2000 problem was an unintentional logic bomb. Every time the infected application is run, the logic bomb checks the date to see whether it is time to run the bomb. If not, control is passed back to the main application and the logic bomb waits. If the date

condition is correct, the rest of the logic bomb's code is executed and the result can be anything from a harmless message to a system crash.

B, C and D are incorrect – These are different types of viruses.

877. What is the method used by most of the antivirus software to identify virus infections in a system?

A. Monitoring traffic

B. Signature detection

C. Repair or quarantine

D. Scan processes

KEY B

A, C and D are incorrect - these are the types of controls of antivirus tools

B is correct - Most of the antivirus software utilizes a method known as signature detection to identify potential virus infections on a system. Essentially, they maintain an extremely large database that contains the known characteristics (signatures) of all viruses. Depending upon the antivirus package and configuration settings, it can scan storage media periodically, check for any files that contain data matching those criteria.

878. When do injection flaws occur?

A. When untrusted data is sent to an interpreter as part of a command or query

B. When application functions related to authentication and session management are not implemented correctly

C. When an application takes untrusted data and sends it to a web browser without proper validation

D. When a developer exposes a reference to an internal implementation object

KEY A

A is correct - **Injection (SQL Injection):** Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

B is incorrect - **Broken Authentication and Session Management**: Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

C is incorrect - **Cross-Site Scripting (XSS):** XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

D is incorrect - **Insecure Direct Object References:** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

879. What is a Cross Site Request Forgery Attack?

A. It forces a logged on victim's browser to send a forged HTTP request

B. It forges request in order to access functionality without proper authorisation

C. It helps steal or modify weakly protected data

D. It facilitates serious loss or data takeover

KEY A

A is correct - **Cross-Site Request Forgery (CSRF):** A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

B is incorrect - **Missing Function Level Access Control**: Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

C is incorrect - **Sensitive Data Exposure**: Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

D is incorrect – **Using Components with Known Vulnerabilities**: Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

880. In case of advanced persistent threat why is an antivirus unable to detect the malware?

A. The attack is on an identified subject

B. Social engineering methods are used

C. Malware is specifically written for this purpose

D. The attack continues for a longer duration

KEY C

C is correct - In case of Advanced Persistent threat, since the malware is specifically written for this purpose, it cannot be detected by an antivirus

A, B and D are incorrect – These are the other characteristics of advanced persistent threat

881. In order to limit the amount of damage a single vulnerability can allow, it is important to:

A. All servers reside on a single segment

B. There should be different segments for different servers

C. Having a single web server

D. Eliminating single points of failure

KEY B

B is correct - **Segmentation / Zoning:** Segmentation / Zoning can limit the potential for harm in a network in two important ways. Segmentation reduces the number of threats, and it limits the amount of damage a single vulnerability can allow. A web server, authentication server, applications and database are residing on a single server or segment for facilitating electronic commerce transactions are a very insecure configuration. A more secure design will use multiple segments. Since the web server has to be exposed to the public, that server should not have other more sensitive, functions on it or residing on the same segment such as user authentication or access to the database. Separate segments and servers reduce the potential harm should any subsystem be compromised.

A is incorrect – for the same reason as mentioned above

C is incorrect – This is a redundancy vulnerability

D is incorrect – This does not relate to segmentation

882. Where does encryption occur when data is encrypted in link encryption?

A. Data link layer of the receiving host

B. Network layer

C. Data link layer in the OSI model

D. In transit between two computers

KEY C

C is correct - In link encryption, data are encrypted just before the system places them on the physical communications link, that is, encryption occurs at the Data Link layer in the OSI model.

A, B and D are incorrect – decryption occurs at the Data Link layer of the receiving host. Link encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts (above the data link layer). Headers added by the network layer (which includes addresses, routing information and protocol) and above are encrypted, along with the message/data. The message is, however, exposed at the Network layer and thus all intermediate nodes through which the message passes can read the message. This is because all routing and addressing is done at the Network layer. Link encryption is invisible to user and appropriate when the transmission line is the point of greatest vulnerability. Link encryption provides protection against traffic analysis.

Module 5

Systems Development-Acquisition, Maintenance and Implementation

883. Business application system/software is designed to support a specific organisational service, function or process, such as inventory management, payroll, market analysis or e-commerce. What is the goal of such a business application?

A. To enhance the targets and goals of an organisation

B. To deal with problems relating to business processes

C. To enhance quality of services

D. To turn data into information

KEY D

D is correct - The goal of an application system is to turn data into information.

A, B and C are incorrect – These are situations under which the need for business development or acquisition of new applications may arise

647. What is the intent of SDLC?

A. To process data of relevant business processes

B. To enhance the targets and goals of an organisation

C. To improve the quality of services

D. To examine a business situation and improve it

KEY D

D is correct - SDLC refers to the process of examining a business situation with the intent of improving it through better procedures and methods. This is required when there is need to change business processes due to requirements arising out of customers/stakeholders expectations and business strategy.

A, B, and C incorrect – These are situations under which the need for business development or acquisition of new applications may arise

884. Which of the following is the role of an IS Auditor in Phase 3 (System Analysis) of SDLC?

A. Review cost justification/ benefits

B. Review detailed requirement definition documents

C. Verify that the management has approved the initiation and cost of the project

D. Review existing data flow diagrams and other related specifications

KEY C

C is correct - Role of IS Auditor in system analysis phase:

- Verify that management has approved the initiation of the project and the cost.
- In case of acquisition, determine that an appropriate number of vendors have been given proposals to cover the true scope of the project and requirements of the users.
- Determine whether the application is appropriate for the user of an embedded audit routine and if so request may be made to incorporate the routine in conceptual design of the system.

is correct -

A is incorrect – This is the role of an IS Auditor in the feasibility phase

B and D are incorrect – These are the roles of an IS auditor in the System Analysis phase

885. Which of the following is the role of an IS Auditor in the detailed design phase of SDLC?

A. Analyse the justification for going in for a development or acquisition

B. Review input, processing and output controls

C. Ensure that the documentation is complete

D. Review QA report on adopting coding standards by developers.

KEY B

B is correct - Role of IS Auditor in detailed design phase:

- Review system flowcharts for adherence to the general design
- Review input, processing and output controls have been appropriately included in the system.
- Assess adequacy of the audit trails which provide traceability and accountability.
- Verify key calculations and processes for correctness and completeness.
- Interview users to ascertain their level understanding of the system design, input to the system, screen formats and output reports.

- Verify that system can identify erroneous data correctly and can handle invalid transactions.
- Review conceptual design to ensure the existence of appropriate controls.
- Review quality assurance and quality control results of programs are developed.
- Verify the design for its completeness and correctness and it meets the defined requirements.
- Verify that functional data created during requirement phase is complete and test plans are developed.

A is incorrect – This is the role of an IS Auditor in the feasibility phase

C and D are incorrect – These are the roles of an IS Auditor in the development phase

886. What are the characteristics of a very well coded application program?

A. Good coding standards, Accuracy and Speed

B. Reliability, Robustness, Accuracy, Efficiency, Usability, Readability

C. Flexibility, Speed, Coding Standards

D. Reliability, Flexibility and Speed

KEY B

B is correct - A very well coded application program should have the following characteristics:

- **Reliability:** It refers to the consistency with which a program operates over a period of time. However, poor setting of parameters and hard coding of some data subsequently could result in the failure of a program after some time.
- **Robustness:** It refers to the applications' strength to perform operations in adverse situations by taking into account all possible inputs and outputs of a program considering even the least likely situations.
- **Accuracy:** It refers not only to 'what program is supposed to do', but also the ability to take care of 'what it should not do'. The second part is of great interest for quality control personnel and auditors.
- **Efficiency:** It refers to the performance per unit cost with respect to relevant parameters and it should not be unduly affected with the increase in input values.
- **Usability:** It refers to a user-friendly interface and easy-to-understand internal/external documentation.
- **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.

A, C and D are incorrect – These are not the major characteristics of a well coded application program

887. What is the role of an IS Auditor in the testing phase of SDLC?

A. Review the test plan for completeness and correctness

B. Ensure test plans, test data nd test results are maintained for reference

C. Verify that the system has been installed according to the organisation's change control procedures.

D. Review programmed procedure used for scheduling and running the system along with the system parameters are used in executing the production schedule.

KEY A

A is correct - Role of IS Auditor in testing phase:

- Review the test plan for completeness and correctness.
- Review whether relevant users have participated during testing phase.
- Review error reports for their precision in recognizing erroneous data and for resolution of errors.
- Verify cyclical processes for correctness(example: year-end process, quarter-end process)
- Interview end-users of the system for their understanding of new methods, procedures and operating instructions.
- Review the system and end-user documentation to determine its completeness and correctness.
- Review whether reconciliation of control totals and converted data has been performed to verify the integrity of the data after conversion.
- Review all parallel testing results.
- Test the system randomly for correctness.
- Review unit test plans and system test plans to determine that tests for internal control are addressed.
- Verify that the system security is functioning as designed by developing and executing access tests.
- Ensure test plans and rest results are maintained for reference and audit

B, C and D are incorrect – These are the roles of an IS Auditor in the UAT or final testing phase

888. What are the security steps involved in the development phase of SDLC?

A. To identify possible attacks and design controls

B. To train developers on security coding practices.

C. To ensure security requirements are tested during testing.

D. To perform security scan of application after implementation.

KEY B

B is correct - Security steps involved during the development phase are:

To develop and implement security coding practices such as input data validation and avoiding complex coding.

To train developers on security coding practices.

A, C and D are incorrect – These are security steps involved during the design, testing and implementation phases.

889. Which of the following is a mitigation plan for risk associated with compromising on quality and testing?

A. Understand organisation baseline for infrastructure and incorporate in design.

B. Ensure standard coding practices are adopted.

C. Ensure completion of documentation along with design and development.

D. Ensure documentation experts and technical writers are part of team.

KEY B

B is correct - The following are the mitigation plans for risk associated with compromising on quality and testing:

Ensure standard coding practices are adopted.

Provide enough time for building test cases to cover all function, performance and security requirements.

Build test cases along with design.

A is incorrect – This is a mitigation plan associated with the risk of inappropriate selection of platform

C and D are incorrect – These are mitigation plans for risk associated with missing or inadequate documentation

890. What is the mitigation plan for risk associated with absence of skilled resources?

A. Consider outsourcing or hiring skilled resources on contract.

B. Develop and implement standard coding practices

C. Perform scope base lining.

D. Introduce change management process to evaluate and adopt changes in requirements

KEY A

A is correct - Mitigation plan for risk associated with absence of skilled resources is to consider outsourcing or hiring skilled resources on contract

B, C and D are incorrect – these are mitigation plans for risks associated with poor coding techniques and lack of proper change control

891. Who is responsible for delivery of a project within the time and budget?

A. Module/Team leader

B. System Analyst

C. Project Manager

D. Database Administrator

KEY C

C is correct - A project manager is normally responsible for more than one project and liaisons with the client or the affected functions. This is a middle management function. The Project manager is responsible for delivery of the project within the time and budget.

A is incorrect – A project is divided into several manageable modules and the development responsibility for each module is assigned to module leaders.

B is incorrect - The system analyst also has a responsibility to understand existing problem/system/data flow and new requirements. System analysts convert the user's requirements in the system requirements to design new system.

D is incorrect – The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The database administrator handles multiple projects; and ensures the integrity and security of information stored in the database.

892. Which of the following is the role of a programmer?

A. Approve, supervise and direct IT projects

B. Convert design into programs by coding

C. Checking compliance with SDLC standards

D. Testing programs and sub programs

KEY B

B is correct - Programmers convert design into programs by coding using programming language. They are also referred to as coders or developers

A is incorrect - This is the role of a steering committee

C is incorrect – this is the role of the quality assurance team

D are incorrect – This is the role of testers

893. The technical feasibility study for automating a business process using information technology includes which of the following?

A. Is the cost of hardware and software for the class of applications being considered.

B. Are the benefits derived from new application such as improved efficiency, reduced costs, business growth, and customer and user satisfaction.

C. Is the cost of conducting a full systems development/acquisition, implementation and operation.

D. Is system scalable and can it handle the expected business and data growth?

KEY D

D is correct - The technical feasibility includes evaluation of the following factors:

- Can the solution work on existing infrastructure or does organisation need to acquire new hardware or software? If currently the organisation is not using an automated solution, they may have to invest in acquiring technology and solution.
- Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users? Currently there are many organisations that have deployed such solutions and hence we can conclude that the technical solutions can be made available to meet the response requirements.
- Is system scalable and can it handle the expected business and data growth? There are multiple training courses and those can be deployed using scalable infrastructure.
- Does the technology offer adequate security? Those requirements need to be considered while developing or acquiring solution. However since many organisations have already implemented similar solution, the required security can be embedded.

A, B, C are incorrect – These factors are evaluated by the study of economic feasibility.

894. The business case is a KEY element of the decision making process throughout the life cycle of project. What information does a business case provide to an organisation?

A. decide whether the SDLC project should be undertaken

B. Explore solutions and make a recommendation

C. Develop a new application system

D. Outline and calculate of benefits

KEY A

A is correct - A business case is normally derived from the benefit realization plan and feasibility study. A business case provides the information required for an organisation to decide whether the SDLC project should be undertaken and if approved, becomes the basis for a project execution and assessment.

B is incorrect – this is the objective of a feasibility study

C and D are incorrect – these are also the objectives of a feasibility study

895. What does study of history, structure and culture of information involve?

A. Identifying stakeholder expectations

B. Types of useful systems, issues that have not been addressed and require attention

C. Identifying how the system needs to interact with its environment

D. Study of business processes, underlying activities, and actors that perform these activities

KEY B

B is correct - The study of the history of systems in an organisation gives an idea about the types of systems that have been extremely useful, issues that have not been addressed over a period and new issues that require attention. It is essential to understand organisational structure and culture as the solutions that are not consistent with the culture often fail.

A and C are incorrect – These are the activities that come under understanding requirements

D is incorrect – These is an activity associated with the study of information flows

896. t is important to record requirements after they have been analysed. Under which phase of requirement Engineering does this fall?

A. Elicitation

B. Analysis and Negotiation

C. Documentation

D. Validation

KEY C

C is correct -

Documentation: Once the requirements have been analyzed, it is important to record them in order to make them formal through proper specification mechanism. During this phase, the team organizes the requirements in such a way that ascertains their clarity, consistency, and traceability etc. This phase is extremely important because often 'the document produced during specification is what the rest of the development stages will be based upon'.

A is incorrect – **Elicitation:** The RE process is normally considered as the process of finding out 'what are the real needs of the customers as well as of the system'. It also includes activities to explore 'how the software can meet the stakeholders' goals' and 'what alternatives might exist'.

B is incorrect - **Analysis and Negotiation:** This phase consists of a set of activities aimed to discover problems within the system requirements and achieve agreement on changes to satisfy all system stakeholders. If an analyst discovers some problems with the requirements during the analysis phase, such requirements are referred back to the elicitation phase. This process is related to the requirements that are incomplete, ambiguous and/or conflicting. Negotiation part is known as 'the process of discussing conflicts in requirements and finding some compromise which all of the stakeholders can live with'. The principle of this process should be objective, where the judgments and the compromise for the system requirements should be based on technical and organisational needs. All the conflict requirements identified during the analysis process should be negotiated and discussed individually with the stakeholders in order to resolve the conflicts.

D is incorrect – **Validation:** This phase ensures that models and documentation accurately express the stakeholders' needs along with checking the final draft of requirements document for conflicts, omissions and deviations from different standards.

897. Which aspect related to Project Planning does process of handing over deliverables come under?

A. Project execution

B. Project execution

C. Project monitoring and controlling

D. Project closing

KEY D

D is correct - **Project closing** has processes for handing over deliverables or terminating project.

A is incorrect – **Project planning** consists of processes related to developing project execution plan, finalizing requirements, defining work breakdown structure and modules to be developed, estimating efforts and cost, resource planning, risk management, procurement planning and plan for communications with stakeholders.

B is incorrect - **Project execution** consists of processes related to direct project teams, ensuring quality assurance and testing, managing requirements and changes in requirements, ensuring timely procurements and manage resources.

C is incorrect - **Project controlling and monitoring** consists of processes related to monitoring risks, scope creeps, quality of deliverables, costs and budgets, performance reporting.

898. What does Work Breakdown Structure (WBS) represent?

A. The project in terms of manageable and controllable units of work

B. Detailed specifications with objectives

C. Assigned responsibilities and deadlines

D. Work documents containing the start and finish dates

KEY A

A is correct - A commonly accepted approach to define project objectives is to start with a work breakdown structure (WBS) with each work module having its own objectives derived from main objectives. The WBS represents the project in terms of manageable and controllable units of work and forms the baseline for cost and resource planning.

B, C and D are incorrect – Detailed specifications regarding the WBS can be used to develop work packages (WP). Each WP must have a distinct owner and a list of main objectives, and may have a list of additional objectives. The WP specifications should include dependencies on other WPs and a definition of how to evaluate performance and goal achievement. A task list is a list of actions to be carried to complete each work package and includes assigned responsibilities and deadlines. The task list aids the individual project team members in operational planning and scheduling, that when merged together forms a project schedule. Project schedules are work documents containing the start and finish dates, percentage completed, task dependencies, and resource names of individuals planned to work on tasks.

899. Half way through a project development, on which phase should an IS auditor focus in order to ensure that there is no deviation from the primary objectives of the projects?

A. Project Planning

B. Project Controlling

C. Resource Management

D. Risk Management

KEY B

B is correct - During mid-term project review IS auditor should focus on project planning and controlling activities to ensure that these are not deviating from primary objectives of the project.

A is incorrect –

A and C are incorrect – These phases do not require much review during this stage.

D is incorrect – Focus on risk management process provides detailed insight on the effectiveness of the project management

900. What is the tool used to verify that deployed resources are capable of finishing a task within the set time limit and with the expected quality level?

A. Earned value analysis

B. Work Breakdown structure

C. Work Package

D. Qualitative Analysis of Risks

KEY A

A is correct - **Earned Value Analysis** consists of comparing expected budget till date, actual cost, estimated completion date and actual completion at regular intervals during the project.

B and C are incorrect – A commonly accepted approach to define project objectives is to start with a work breakdown structure (WBS) with each work module having its own objectives derived from main objectives. The WBS represents the project in terms of manageable and controllable units of work and forms the baseline for cost and resource planning. Detailed specifications regarding the WBS can be used to develop work packages (WP). Each WP must have a distinct owner and a list of main objectives, and may have a list of additional objectives. The WP specifications should include dependencies on other WPs and a definition of how to evaluate performance and goal achievement. A task list is a list of actions to be carried to complete each work package

and includes assigned responsibilities and deadlines. The task list aids the individual project team members in operational planning and scheduling, that when merged together forms a project schedule. Project schedules are work documents containing the start and finish dates, percentage completed, task dependencies, and resource names of individuals planned to work on tasks.

D is incorrect – Qualitative Analysis of Risks is a part of project planning.

901. During risk management process, how is risk assessed and evaluated?

A. Creating an inventory of possible risk

B. Quantify the likelihood and impact of risk

C. Create a risk management plan

D. Discover risk that materializes

KEY B

B is correct - **Assess and evaluate risk:** Quantify the likelihood (expressed as a percentage) and the impact of the risk (expressed as an amount of money). The "insurance policy" (total impact) that needs to be in the project budget is calculated as the likelihood multiplied by the impact.

A is incorrect – This step is to identify the risk\

C is incorrect – This is a part of managing the risk after it has been assessed

D is incorrect – This forms a part of monitoring the risk process

902. Which of the following is the feature of a waterfall model?

A. The designers create an initial base model and give little or no consideration to internal controls, but instead emphasize system characteristics such as simplicity, flexibility, and ease of use.

B. Project is divided into sequential phases, with some overlap and splash back acceptable between phases.

C. This is an iterative model where each iteration helps in optimizing the intended solution.

D. This model of development helps to ease the traumatic effect of introducing completely new system all at once

KEY B

B is correct - The characterizing features of the waterfall model have influenced the development community in big way. Some of the KEY characteristics are:

- Project is divided into sequential phases, with some overlap and splash back acceptable between phases.

- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

A, C and D are incorrect – These are the features of prototype model, spiral model and the incremental model respectively.

903. In this model, a series of mini-waterfalls are performed, where all phases of the waterfall development model are completed for a small part of the system, before proceeding to the next increment. What SDLC model is this?

A. Waterfall model

B. Prototype model

C. Spiral model

D. Incremental model

KEY D

D is correct - A few pertinent features of incremental model are listed as follows:

A series of mini-waterfalls are performed, where all phases of the waterfall development model are completed for a small part of the system, before proceeding to the next increment.

- Overall requirements are defined before proceeding to evolutionary, mini – Waterfall development of individual increments of the system.
- The initial software concept, requirement analysis, and design of architecture and system core are defined using the Waterfall approach, followed by iterative Prototyping, which culminates in installation of the final prototype (i.e. working system).

B, C and D are incorrect – This is not a feature of any of these models.

904. This model is especially useful for resolving unclear objectives and requirements; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.

A. Waterfall model

B. Prototyping model

C. Spiral Model

D. Incremental model

KEY B

B is correct - Strengths **of Prototyping Model:**

- It improves both user participation in system development and communication among project stakeholders.
- It is especially useful for resolving unclear objectives and requirements; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.
- Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
- It helps to easily identify, confusing or difficult functions and missing functionality.
- It enables to generate specifications for a production application.
- It encourages innovation and flexible designs.
- It provides for quick implementation of an incomplete, but functional, application.
- It typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.
- A very short time period is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
- Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

A, C and D are incorrect – this is not strength of any of these models

905. Which of the following is a weakness of the spiral model?

A. It is criticized to be Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.

B. Approval process and control are not formal.

C. Sometimes there are no firm deadlines, cycles continue till requirements are clearly identified.

D. Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.

KEY C

C is correct – **Weaknesses of the spiral model are:**

- It is challenging to determine the exact composition of development methodologies to use for each of the iterations around the Spiral.
- A skilled and experienced project manager is required to determine how to apply it to any given project.
- Sometimes there are no firm deadlines, cycles continue till requirements are clearly identified. Hence has an inherent risk of not meeting budget or schedule.

A, B and D are incorrect – These are the weaknesses of the waterfall model, prototype model and incremental model respectively

906. Which of the following is a KEY feature of Rapid Application Development?

A. fast development and delivery of a high quality system at a relatively low investment cost,

B. Use of small, time-boxed subprojects or iterations where each iteration forms basis for planning next iteration.

C. Customer satisfaction by rapid delivery of useful software;

D. ☐ Welcome changing requirements, even late in development;

KEY A

A is correct - The KEY features of RAD are:

- KEY objective is fast development and delivery of a high quality system at a relatively low investment cost,
- Attempts to reduce inherent project risk by breaking a project into smaller segments and providing more ease-of-change during the development process.
- Aims to produce high quality systems quickly, primarily through the use of iterative Prototyping (at any stage of development), active user involvement, and computerized development tools like Graphical User Interface (GUI) builders, Computer Aided Software Engineering (CASE) tools, Database Management Systems (DBMS), Fourth generation programming languages, Code generators and object-oriented techniques.
- KEY emphasis is on fulfilling the business need while technological or engineering excellence is of lesser importance.
- Project control involves prioritizing development and defining delivery deadlines or “time boxes.” If the project starts to slip, emphasis is on reducing requirements to fit the time box, not in increasing the deadline.
- Generally includes Joint Application Development (JAD), where users are

intensely involved in system design, either through consensus building in structured workshops, or through electronically facilitated interaction.

B, C and D are incorrect – These are the KEY features of Agile Software development methodology

907. Which of the following is the weakness of the Agile Software development methodology?

A. Fast speed and lower cost may affect adversely the system quality.

B. The project may end up with more requirements than needed (gold-plating).

C. Potential for feature creep where more and more features are added to the system during development.

D. There is lack of emphasis on necessary designing and documentation due to time management and generally is left out or incomplete.

KEY D

D is correct - **Weaknesses of Agile methodology:**

- In case of some software deliverables, especially the large ones, it is difficult to assess the efforts required at the beginning of the System Development life cycle.
- There is lack of emphasis on necessary designing and documentation due to time management and generally is left out or incomplete.
- Agile increases potential threats to business continuity and knowledge transfer due to verbal communication and weak documentation.
- Agile requires more re-work and due to the lack of long-term planning and the lightweight approach to architecture.
- The project can easily get taken off track if the customer representative is not clear about the requirements and final outcome.
- Agile lacks the attention to outside integration.

A, B and C are incorrect – These are the weaknesses of RAD

908. This is the process of studying and analyzing an application, a software application or a product to see how it functions and to use that information to develop a similar system.

A. Software Reengineering

B. Reverse Engineering

C. Agile processes

D. Rapid Application Development

KEY B

B is correct - Reverse engineering is the process of studying and analyzing an application, a software application or a product to see how it functions and to use that information to develop a similar system.

A, C and D are incorrect – This is not part of any of these processes

909. How is a product for which software is available and can be implemented without customisation classified as?

A. Generic products without customisation

B. Commercial product with customisation

C. Outsourced development

D. Commercial product without customisation

KEY A

A is correct - **Generic products without customization**: Software is available and can be implemented without customization. These products are also known as Plug-and-play or COTS (Commercial of the shelf) for example MS Office, MS projects etc.

B is incorrect – **Commercial product with customization**: Software needs to be customized like ERP or core banking products or at lower level customization like Tally.

C is incorrect – **Outsourced development**: Ready-made software as required is not available. Hence, the organisation intends to outsource development activities based on cost benefit analysis.

D is incorrect – There is no such classification

910. In achieving the objectives of requirement analysis, the process of understanding the present system and its related problems comes under which of the following steps?

A. Fact finding

B. Analysis

C. Requirements of proposed systems

D. Identifying rationale and objectives

KEY B

B is correct - **Analysis to understand Present process:** Understanding present system and its related problems helps in confirming the requirements from new application/software.

A is incorrect – **Fact Finding:** Application system focuses on two main types of requirements. The first one is service delivery and second one is operational requirements. These may include lower operational costs, better information for managers, smooth operations for users or better levels of services to customers. To assess these needs, the analysts often interact extensively with stakeholders, to determine 'detail requirements'. The fact-finding techniques/tools used by the system analyst include document verification, interviews, questionnaire and observation.

C is incorrect - **Requirements for Proposed Systems:** Analysis of functional area and process, the proposed expectations can be clearly defined considering the issues and objectives.

D is incorrect – Analysis also include identifying rationale and objectives, inputs and data sources, decision points, desired outcomes from application, mandatory and discretionary controls.

911. The process of allotting weight-age for each requirement and then allotting score to the software that meets that requirement is called as:

A. Point scoring Analysis

B. Agenda based presentations

C. Public evaluation reports

D. Benchmarking solutions

KEY A

A is correct - **Point-Scoring Analysis (Functional gap analysis):** Point-scoring analysis provides an objective means of selecting software. This is performed by allotting weight-age for each requirement and then allotting score to the software that meets that requirement.

B is incorrect - **The agenda-based presentations** are scripted business scenarios that are designed to show how the software will perform certain critical business functions. Vendors are typically invited to demonstrate their product and follow the sample business scenarios given to them to prepare.

C is incorrect – **Public Evaluation Reports:** Organisation may refer to independent agencies that evaluate various software products of different vendors and publish comparison along with rating based on various predefined parameters including survey

of current users. (For example, magic quadrant for similar software product by Gartner, Forester etc.). This method has been frequently and usefully employed by several buyers in the past.

D is incorrect – **Proof of Concept (PoC) or Benchmarking Solutions:** Organisations may request vendor to provide a proof of concept (by implementing product in small pilot area within organisation) that the software meets the expected requirements. This helps organisation in evaluating best product that meets the requirements. This is particularly useful for products that has high-cost and requires high level of efforts that it may not be possible to roll back.

912. While preparing the request for proposal, what should an organisation do to ensure vendor viability and financial stability?

A. Compare product functionalities against requirements

B. Validate vendor claims about their product performance

C. Get feedback from existing customers of the vendor on supporting documents of the vendor

D. Evaluate what king of support the vendor provides

KEY C

C is correct - Evaluate the vendor's viability with reference to period for which the vendor is in operation, the period for which the desired product is being used by the existing customers and the Vendor's financial stability on the basis of the market survey and the certification from the customers and on certain supporting documentation from the Vendor

A is incorrect – This is part of software and system requirements

B is incorrect – This is part of customer references

D is incorrect – This is part of vendor support

913. Out of the tests performed on a program unit, what does a performance test check?

A. whether programs do, what they are supposed to do or not

B. verify the expected performance criteria of program

C. determines the stability of a given system or entity

D. examines the internal processing logic of a software system

KEY B

B is correct - Performance tests are designed to verify the expected performance criteria of program.

A, C and D are incorrect – These are the functions of a function test, stress test and structural test respectively

914. Which of the following is a feature of top down integration?

A. The testing will start from opening login screen and then login, then selecting function one by one

B. It is the traditional strategy used to integrate the components of a software system starting from smallest module/function/program.

C. It consists of unit testing, followed by sub-system testing.

D. Bottom-up testing is easy to implement as at the time of module testing, tested subordinate modules are available.

KEY A

A is correct - **Top-down Integration:** This starts with the main routine followed by the stubs being substituted for the modules which are directly subordinate to the main module. Considering above example, the testing will start from opening login screen and then login, then selecting function one by one. An incomplete portion of a program code is put under a function (called stub) to allow the function. Here a stub is considered as black box and assumed to perform as expected, which is tested subsequently. Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested. This process continues till the atomic (smallest) modules are reached. Since decision-making processes are likely to occur in the higher levels of program hierarchy, the top-down strategy emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes. The difficulty arises in the top-down method, because the high-level modules are tested with stubs and not with actual modules.

B, C and D are incorrect – These are the features of bottom up integration

915. With respect to System testing, what is the objective of performance testing?

A. To assess how well the application is able to recover from crashes, hardware failures and other similar problems

B. To determine that an Information System protects data and maintains functionality as intended.

C. to determine the stability of a given system or entity based on the requirements

D. to assess various parameters like response time, speed of processing, effectiveness use of a resources (RAM, CPU etc.), network, etc.

KEY D

D is correct - **Performance Testing:** Software performance testing is performed on various parameters like response time, speed of processing, effectiveness use of a resources (RAM, CPU etc.), network, etc. This testing technique compares the new system's performance with that of similar systems using available industry benchmarks.

A,B, C are incorrect – These are the objectives of Recovery Testing, Security testing and Stress testing respectively.

916. What does User Acceptance Testing focus on?

A. Ensuring that the system is production-ready and satisfies all accepted (baselined) requirements

B. Conforming to the quality standards of the organisation accepted before development

C. Documenting specifications, technology employed, use of coding standards

D. Controlling the execution of tests and the comparing of actual outcomes with predicted outcomes

KEY A

A is correct - **User Acceptance Testing (UAT):** It is a user extensive activity and participation of functional user is a primary requirement for UAT. The objective of UAT is to ensure that the system is production-ready and satisfies all accepted (baseline) requirements.

B and C are incorrect – These are the features of Quality Assurance Testing

D is incorrect – This is the feature of automated testing

917. In this strategy, implementation can be staged with conversion to the new system taking place gradually.

A. Phased Changeover

B. Abrupt Changeover

C. Pilot Changeover

D. Parallel Changeover

KEY A

A is correct - **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually. This is done based on business operations. For example, converting one function (e.g. marketing) on new system, wait for the same be stabilized and then take another function (Finance/HR/production etc.)

B is incorrect – **Cut-off or Direct Implementation / Abrupt Change-Over:** This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. Fig 6.1 depicts Direct Implementation, which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.

C is incorrect – **Pilot Changeover:** With this strategy, the new system replaces the old one in one operational area or with smaller scale. Any errors can be rectified and new system is stabilized in pilot area, this stabilized system is replicated in operational areas throughout the whole system. For example converting banking operations to centralized systems are done at one branch and stabilized. The same process is replicated across all branches.

D is incorrect – **Parallel Changeover:** This is considered the most secure method, time and resource consuming implementation. The new systems is implemented, however the old system also continues to be operational. The output of new system is regularly compared with old system. If results matches over period of time and issues observed with new system are taken care of, the old system is discontinued.

918. Which of the following is a requirement to be considered with respect to cloud computing and sourcing options?

A. The development team needs to define backup procedures

B. Client needs to be tested for all known browsers

C. Evaluation of vendors for acquisition of tools and software

D. Developers to test their code before releasing to testing team

KEY B

B is correct - The lists of requirements that must be considered are discussed below:

- Application on cloud uses platform independent web based technology like Java, Net, XML, PHP etc. Deployment of services may happen in phased manner, the project manager may consider agile development method to develop and deploy services.
- Client is executed using internet browsers like internet explorer, Google chrome, Mozilla etc. and hence need to be tested for all known browsers. It is necessary to consider security while developing the software, users may or may not use security settings in their browsers. Also not all browsers offer same level of security settings.
- Web application security requirements need to be considered while designing and testing the application.

- Non-functional requirements of performance and response have to be considered while developing the software.
- Licensing issues for utilities and middleware are complex and should be considered.

A, C and D are incorrect – These are the characteristics for virtualisation

919. Which of the following is a risk with respect to security of big data?

A. When an employee leaves the company, data may still be present on their employees' device.

B. Requires data to be stored in denormalized form i.e. schema-less in distributed environments

C. Propagation of malware resulting in data leakage, data corruption and non-availability of required data.

D. Possibility of fraud through remote access and inability to prevent/detect it.

KEY B

B is correct - Big data requires data to be stored in denormalized form i.e. schema-less in distributed environments, where data from multiple sources can be joined and aggregated in arbitrary ways, make it challenging to establish access controls

- As the big data consist of high volume, high variety and high velocity data, it makes difficult to ensure data integrity
- Since it is aggregation of data from across the organisation, it also includes sensitive data
- Most existing data security and compliance approaches will not scale to handle big data security.

A, C and D are incorrect – These are the disadvantages of using mobile devices in SDLC

920. Which of the following is the role of an IS Auditor during post implementation review?

A. suggest appropriate controls to be included in proposed solution

B. Interview project team and stakeholders to understand expectations

C. Ensure 'what project control standards are to be complied with

D. Evaluation of system for information security and privacy controls

KEY D

D is correct - **Information Security:** System should also need to be evaluated for information security and privacy controls. This aspect of system evaluation is based on the security requirements documented during information gathering, security of infrastructure on which the application is hosted (e.g. hardware baselining, network security, access controls and vulnerability scanning). Evaluation may also include the availability aspect required for continuity (e.g. in case of high availability requirements redundant infrastructure in cluster or replication and readiness of alternate site, updating of BCP documents etc.)

A, B, C are incorrect – These are the reviews to be done by the auditor as a team member and during mid project

Module 6
Business Application Software Audit

921. In an organisation, business processes and related controls are put in place through:

A. Business Applications

B. Control Structure

C. Business Cycle

D. Business Model

KEY A

A is correct - "Business Application", may be defined as applications (meaning computerized software) used by organisation to run its business. The consideration is whether the said application covers / incorporates the KEY business processes of the organisation. Another important consideration is whether the control structure as available in the Business Application is appropriate to help organisation achieve its goals. Business applications are where the necessary controls needed to run business are put in place. The business processes and related controls are put in place through business applications used by an organisation.

B, C and D are incorrect –

Each business cycle used by an organisation has a defined control structure that has a direct co-relation to the business model used. Organisations have to document business processes and identify KEY control points. Organisations have to ensure that the KEY control points are configured in system.

922. The ICAI has issued standards on Internal Audit in Information Technology Environment. According to this, an auditor has to:

A. Consider subject matter guidance or direction, as afforded through legislation, regulations, rules, directives and guidelines issued by government or industry.

B. Establish the expected degree of reliance to be placed on internal control;

C. Determine the nature, timing, and extent of the audit procedures to be performed; and

D. Consider the extent to which the IT environment is used to record, compile, process and analyse information

KEY D

D is correct - SIA 14, on INTERNAL AUDIT IN INFORMATION TECHNOLOGY ENVIRONMENT, as issued by ICAI, states that; "The internal auditor should consider the effect of an IT environment on the internal audit engagement, inter alia:

a. The extent to which the IT environment is used to record, compile, process and analyse information; and

b. The system of internal control in existence in the organisation with regard to: the flow of authorised, correct and complete data to the processing centre; the processing, analysis and reporting tasks undertaken in the installation".

A, B and C are incorrect – ISACA Standards

ISACA ITAF, 1201 "Engagement Planning", identifies risk assessment as one of the KEY aspects and states that IS audit and assurance professionals, have to;

- Obtain an understanding of the activity being audited. The extent of the knowledge required should be determined by the nature of the enterprise, its environment, areas of risk, and the objectives of the engagement.
- Consider subject matter guidance or direction, as afforded through legislation, regulations, rules, directives and guidelines issued by government or industry.
- Perform a risk assessment to provide reasonable assurance that all material items will be adequately covered during the engagement. Audit strategies, materiality levels and resource requirements can then be developed.
- Develop the engagement project plan using appropriate project management methodologies to ensure that activities remain on track and within budget.

ICAI Standards

SA 200 "Overall Objectives of the Independent Auditor and the conduct of an audit in accordance with standards on Auditing", Issued by ICAI, requires an auditor to plan an audit and get following information: "The auditor should plan his work to enable him to conduct an effective audit in an efficient and timely manner. Plans should be based on knowledge of the client's business. Plans should be made to cover, among other things:

a. Acquiring knowledge of the client's accounting system, policies and internal control procedures;

b. Establishing the expected degree of reliance to be placed on internal control;

c. Determining and programming the nature, timing, and extent of the audit procedures to be performed; and

d. Coordinating the work to be performed.

The first step to by an IS auditor is to obtain knowledge about the business of the organisation, do risk assessment and decide on the specific and additional audit procedures to complete the audit.

923. What is control risk with respect to risk assessment for a business application?

A. Relates to business risks, country risks and contract risks

B. Failure of a control to prevent or detect a material error that exists in system.

C. risk arising without taking into account a planned action by management

D. failure of an audit procedure to detect an error that might be material

KEY B

B is correct - Control risk is defined as failure of a control to prevent, detect a material error that exists in system.

A, C and D are incorrect –

Subject matter risk, relates to business risk, country risk, contract risks. These are important for an IS auditor to consider but merged with inherent risk (discussed later).

2. Audit risk, is define as auditor reaching incorrect conclusion after an audit. The components of audit risk being *control risk, inherent risk and detection risk.*

- Control risk is defined as failure of a control to prevent, detect a material error that exists in system.
- Inherent risk is defined as risk arising without taking into account a planned action by management to reduce the risk. Simply said it related to nature of transaction / business.
- Detection risk is defined as failure of an audit procedure to detect an error that might be material individually or in combination of other errors.

924. Business applications used by entities to manage resources optimally and to maximize economy, efficiency and effectiveness of business operations is known as:

A. Accounting Applications

B. Banking Applications

C. ERP Applications

D. Payroll Application

KEY C

C is correct -

ERP Application: These have been created a separate category of business application systems, due to their importance for an organisation. These software called as enterprise resource planning software are used by entities to manage resources optimally and to maximize E^3 i.e. economy, efficiency and effectiveness of business operations.

A is incorrect -

Accounting Applications: Applications like TALLY, TATA EX, UDYOG, used by business entities for purpose of accounting for day to day transactions, generation of financial information like balance sheet, profit and loss account, cash flow statements, are classified as accounting applications.

B is incorrect –

Banking Application: Today all public sector banks, private sector banks, and including regional rural banks have shifted to **core banking business applications (referred to as CBS).** Reserve Bank of India guidelines mandating all co-operative banks also to shift to core banking applications by December 013, means 95% plus Indian banks use CBS. CBS used by Indian banks include, FINACLE (by Infosys Technologies Ltd.), FLEXCUBE (By Oracle Financial Services Software Limited, formerly called i-flex Solutions Limited), TCS BaNCS (By TCS Limited), and many more CBS.

D is incorrect –

Payroll Application: Many companies across the world are outsourcing these activities to professionals. In India also many CA firms are doing good job on payroll outsourcing. TALLY has a payroll application built into it. ICAI, has made available for its members a payroll application.

925. Key business requirements for information specify 'integrity' as a parameter that needs to be present in information generated. By integrety we mean:

A. protection of sensitive information from unauthorised disclosure

B. accuracy and completeness of information as well as its validity

C. information being available when required

D. information being delivered in a timely, correct, consistent and usable manner

KEY B

B is correct - **Integrity:** Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations

A is incorrect – **Confidentiality:** Concerns the protection of sensitive information from unauthorised disclosure

C is incorrect - **Availability:** Relates to information being available when required by the process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

D is incorrect – **Effectiveness:** Deals with information being relevant and pertinent to the process as well as being delivered in a timely, correct, consistent and usable manner

926. COBIT defines six control objectives for application controls. Under which of the following objectives does validating input data classify?

A. Data collection and entry

B. Completeness and Authenticity checks

C. Processing integrity and validity

D. Transaction Authentication and Integrity

KEY B

B is correct - **Accuracy, Completeness and Authenticity Checks**: Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.

A is incorrect - **Source Data Collection and Entry**: Ensure that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.

C is incorrect - **Processing Integrity and Validity:** Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.

D is incorrect – **Transaction Authentication and Integrity**: Before passing transaction data between internal applications and business/operational functions (within or outside the enterprise), check the data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport

927. Neural Networks and Fuzzy Logics are classified under which category of Artificial intelligence?

A. Cognitive Science

B. Robotics

C. Natural Sciences

D. Virtual Reality

KEY A

A is correct - Cognitive **Science**: This is an area based on research in disciplines such as biology, neurology, psychology, mathematics and allied disciplines. It focuses on how human brain works and how humans think and learn. Applications of AI in the cognitive science are Expert Systems, Learning Systems, Neural Networks, Intelligent Agents and Fuzzy Logic

B, C and D are incorrect – **Robotics**: This technology produces robot machines with computer intelligence and human-like physical capabilities. This area includes applications that give robots visual perception, capabilities to feel by touch, dexterity and locomotion.

iii. **Natural Languages**.

Being able to 'converse' with computers in human languages is the goal of research in this area. Interactive voice response and natural programming languages, closer to human conversation, are some of the applications. Virtual reality is another important application that can be classified under natural interfaces.

928. What are decision support systems (DSS)?

A. System used for getting valuable information for making management decisions

B. systems that provide interactive information support to managers with analytical models

C. **s**ystem which allows buying and selling goods on the internet and involves information sharing, payment, fulfillment, service and support

D. system intended to capture data at the time and place of a transaction

KEY B

B is correct - DSS are information systems that provide interactive information support to managers with analytical models. DSS are designed to be ad hoc systems for specific decisions by individual-managers. These systems answer queries that are not answered by the transactions processing systems.

A, C and D are incorrect – Data warehousing system is used for getting valuable information for making management decisions.

Other than buying and selling goods on the Internet, E Commerce (Electronic Commerce) involves information sharing, payment, fulfillment and service and support.

a PoS is intended to capture data at the time and place of transaction which is being initiated by a business user. It is often attached to scanners to read bar codes and magnetic cards for credit card payment and electronic sales.

929. Which of the following should an IS auditor consider while auditing data warehousing systems?

A. Network capacity for speedy access

B. Accuracy and correctness of outputs generated

C. Validation of receivers details for correctness and completeness

D. Review of exceptional transaction logs

KEY A

A is correct - IS Auditor should consider the following while auditing data warehouse:

1. Credibility of the source data
2. Accuracy of the source data
3. Complexity of the source data structure
4. Accuracy of extraction and transformation process
5. Access control rules
6. Network capacity for speedy access

B is incorrect – IS Auditors role with respect to Decision Support System:

1. Credibility of the source data
2. Accuracy of the source data
3. Accuracy of extraction and transformation process
4. Accuracy and correctness of the output generated
5. Access control rules

C is incorrect – The IS Auditors role with respect to EFT will be with respect to:

1. Authorisation of payment.
2. Validation of receivers details, for correctness and completeness.
3. Verifying the payment made.
4. Getting acknowledgement from the receiver, or alternatively from bank about the payment made.
5. Checking whether the obligation against which the payment was made has been fulfilled.

D is incorrect – IS Auditors role for PoS systems:

1. In case there is batch processing, the IS auditor should evaluate the batch controls implemented by the organization.

2. Check if they are in operation,
3. Review exceptional transaction logs.
4. Whether the internal control system is sufficient to ensure the accuracy and completeness of the transaction batch before updating?
5. The relevance of controls is more In the case of online updating system, the IS auditor will have to evaluate the controls for accuracy and completeness of transactions.

930. Why is IS Audit performed?

A. It safeguards assets, maintains data integrity and achieves the organisations goals and objectives

B. To ensure that the organisations computer systems are available for the business at all times when required

C. Business processes have been integrated into system and decisions are being taken through this integrated system

D. To ensure that the information provided by the system is accurate, reliable and timely

KEY C

C is correct - **IS Audit is necessary** in today's business environment as business processes have been integrated into system and lot of decision is being taken through these integrated system.

A, B and D are incorrect – These are the agenda to be followed for an IS Audit

931. While performing an IS audit which of the following comes under risk assessment and planning?

A. conclusions on objective(s), scope, timeline and deliverables, compliance with applicable laws and professional auditing standards

B. provide supervision to IS audit staff for whom they have supervisory responsibility, to accomplish audit objectives

C. use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan

D. obtain sufficient and appropriate evidence to achieve the audit objectives.

KEY C

C is correct - **Risk Assessment in Planning:** The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit

resources. IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements. IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.

A, B and D are incorrect –

Engagement Planning: This includes conclusions on objective(s), scope, timeline and deliverables, compliance with applicable laws and professional auditing standards, use of a risk-based approach, where appropriate, engagement-specific issues, documentation and reporting requirements.

Performance and Supervision: IS audit and assurance professionals shall conduct the work in accordance with the approved IS audit plan to cover identified risk and within the agreed-on schedule. IS audit and assurance professionals shall provide supervision to IS audit staff for whom they have supervisory responsibility, to accomplish audit objectives and meet applicable professional audit standards. IS audit and assurance professionals shall accept only tasks that are within their knowledge and skills or for which they have a reasonable expectation of either acquiring the skills during the engagement or achieving the task under supervision. IS audit and assurance professionals shall obtain sufficient and appropriate evidence to achieve the audit objectives. The audit findings and conclusions shall be supported by appropriate analysis and interpretation of this evidence. IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions. IS audit and assurance professionals shall identify and conclude on findings.

Evidence: IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

932. The type of CAAT which is written for special audit purposes or targeting specialized IT environments is known as:

A. Specialised Audit Software

B. Generalised Audit Software

C. Utility Software

D. Computer Audit Software

KEY A

A is correct - Specialised Audit software, unlike GAS, is written for special audit purposes or targeting specialized IT environments.

B, C and D are incorrect – Generalised Audit software refers to generalized computer programs designed to perform data processing functions such as reading data, selecting and analyzing information, performing calculations, creating data files and reporting in a format specified by the auditor.

Utility software or utilities though not developed or sold specifically for audit are often extremely useful and handy for conducting audits.

Computer audit software is also known as Generalised Audit Programs (GAS)

933. Which of the following pertains to an operation using GAS?

A. Testing for UNIX controls

B. Comparing an input file with a processed file

C. Production of circularisation letters

D. Random sampling plan

KEY D

D is correct - Typical operations using GAS include:

a. Sampling Items are selected following a value based or random sampling plan.

b. Extraction Items that meet the selection criteria are reported individually.

c. Totaling the total value and number of items meeting selection criteria are reported.

d. Ageing Data is aged by reference to a base date

e. Calculation Input data is manipulated prior to applying selection criteria

A, B and C are incorrect – Specialised Audit software, unlike GAS, is written for special audit purposes or targeting specialized IT environments. The objective of these software to achieve special audit procedures which may be specific to the type of business, transaction or IT environment e.g. testing for NPAs, testing for UNIX controls, testing for overnight deals in a Forex Application software etc. Such software may be either developed by the auditee or embedded as part of the client's mission critical application software. Such software may also be developed by the auditor independently. Before using the organisation's specialized audit software, the auditor should take care to get an assurance on the integrity and security of the software developed by the client...

Utility software or utilities though not developed or sold specifically for audit are often extremely useful and handy for conducting audits. These utilities usually come as part of office automation software, operating systems, and database management systems or may even come separately. Utilities are useful in performing specific system

command sequences and are also useful in performing common data analysis functions such as searching, sorting, appending, joining, analysis etc. Utilities are extensively used in design, development, testing and auditing of application software, operating systems parameters, security software parameters, security testing, debugging etc.

a. File comparison: A current version of a file for example, is compared with the previous year's version, or an input file is compared with a processed file.

b. Production of circularisation letters.

934. What is continuous auditing?

A. Process of obtaining evidence directly on the quality of the records produced and maintained in the system.

B. Process of reviewing the computer logs generated at various points to build an audit trail

C. Process through which an auditor evaluates the particular system(s) and thereby generates audit reports on real time basis.

D. Process of reviewing transactions as they are processed and select items according to audit criteria specified in the resident code

KEY C

C is correct - Continuous auditing is a process through which an auditor evaluates the particular system(s) and thereby generates audit reports on real time basis. Continuous auditing approach may be required to be used in various environments. Such environments usually involve systems that are 4*7 mission critical systems.

A is correct – This forms part of selecting, implementing and using CAAT's

B and D are incorrect – These are different techniques of continuous auditing

935. Procedure of continuous auditing whereby digital pictures of procedures are saved and stored in the memory:

A. Snapshot

B. Integrated Test facility

C. System activity file interrogation

D. Embedded audit facilities

KEY A

A is correct - Most applications follow a standard procedure whereby, after taking in the user input they process it to generate the corresponding output. Snapshots are digital pictures of procedures of the console that are saved and stored in the memory. Procedures of the console refer to the application procedures that take input from the

console i.e. from the keyboard or the mouse. These procedures serve as references for subsequent output generations in the future. Typically, snapshots are implemented for tracing application software and mapping it. The user provides inputs through the console for processing the data. Snapshots are means through which each step of data processing (after the user gives the input through) is stored and recalled.

B is incorrect - Integrated Test Facility (ITF) is a system in which a test pack is pushed through the production system affecting "dummy" entities. Hence this requires dummy entities to be created in the production software. For example, the auditor would introduce test transactions that affect targeting dummy customer accounts and dummy items created earlier for this testing purpose.

C is incorrect – Most computer operating systems provide the capability of producing a log of every event occurring in the system, both user and computer initiated. This information is usually written to a file and can be printed out periodically. As part of audit testing of general controls, it may be useful for the auditor to review the computer logs generated at various points to build an audit trail. Wherever possible, unauthorised or anomalous activity would need to be identified for further investigation.

D is incorrect – Embedded audit facilities consist of program audit procedures, which are inserted into the client's application programs and executed simultaneously. The technique helps review transactions as they are processed and select items according to audit criteria specified in the resident code, and automatically write details of these items to an output file for subsequent audit examination.

936. Compliance testing helps an auditor:

A. substantiate the integrity of actual processing and the outcome of compliance testing

B. to test for monetary errors directly affecting financial statement balances

C. To obtain evidence of the validity and propriety of accounting treatment of transactions

D. Determine that controls are applied in a manner that complies with policies and procedures

KEY D

D is correct - Compliance tests are used to help determine the extent of substantive testing to be performed, as stated in Statement of Auditing Standards. Such tests are necessary if the prescribed procedures are to be relied upon in determining the nature, time or extent of substantive tests of particular classes of transactions or balances. Once the KEY control points are identified, the auditor seeks to develop a preliminary understanding of the controls to ensure their existence and effectiveness.

B, C and D are incorrect – These are the features of Substantive Testing

937. While reviewing authorisation procedure before creating user rights, an IS auditor has to:

A. Evaluate how the user rights have been granted and monitored

B. Check who triggers the request for user rights creation

C. Check Whether there is a proper cross check mechanism to validate the user rights

D. Check Whether user right alteration process is linked to the job profile of the individual

KEY B

B is correct - Authorisation procedure before creating user rights?

IS Auditor needs to check whether there is a formal user rights approval form/document. The question that need to be answered being

a. Who triggers the request for user rights creation? Ideally this request has to be generated through HR department.

b. Whether the form contains all relevant information for the specific user?

c. Whether the form has been properly filled?

d. Whether the form has valid authorisation?

e. Whether forms are marked once user rights are created in system?

A is incorrect – Who has the authority to create user rights?

IS auditor is also concerned to know the person who has the authority to create users in system. IS auditor needs to evaluate the rights of persons doing this job and how these rights have been granted and monitored.

C is incorrect - Validation of user rights created in system?

IS Auditor needs to evaluate the process how user rights created at step (ii) are validated once they have been put in system. IS Auditor may seek answers to the following questions.

a. Whether there is a proper cross check mechanism build in organisation to validate the user rights of employee once they have been created?

b. Whether there is timely validation of user rights and user job profiles? For example this is a cyclical process to be done once each year to see whether the job profile of individual is appropriately reflected in his/her user rights?

D is incorrect - Process of alteration of user rights?

IS Auditor is concerned with the process of alteration of rights. The IS Auditor seeks answers to the following questions.

a. Whether the user right alteration process is linked to job profile of individual?

b. Who triggers the request for user rights alteration?

938. This is the highest level of database abstraction which is of concern to the users is:

A. Conceptual or global view

B. Physical view

C. Internal view

D. External or user view

KEY D

D is correct - **External or user view**: It is at the highest level of the database abstraction. It includes only that portion of database or application programs which is of concern to the users. It is defined by the users or written by the programmers. It is described by the external schema.

A is incorrect – **Conceptual or global view**: This is reflection of a database is viewed by database administrator. Single view represents the entire database. It describes all records, relationships and constraints or boundaries. Data description to render it independent of the physical representation. It is defined by the conceptual schema,

B and C are incorrect – **Physical or internal view**: It is at the lowest level of database abstraction. It is closest to the physical storage method. It indicates how data will be stored, describes data structure, and the access methods. It is expressed by internal schema.

939. What control does a 'view' function offer with respect to database security?

A. Segregation of duties

B. Addresses conflicts relating to simultaneous access

C. Enables data access limitations

D. Ability to create and reuse SQL code

KEY C

C is correct - **Views**: Views enable data access limitations. A view is a content or context dependent subset of one or more tables.

A, B and D are incorrect – **Database Roles and Permissions**

- Segregation of duties
- Roles & Permissions allow control of operations that a user can perform on database,

Concurrency Control: Addresses conflicts relating to simultaneous accesses

Stored Procedures: Database servers offer developers the ability to create & reuse SQL code through the use of objects called as Stored Procedures (Group of SQL statements).

940. User Creation and Access rights are done by _____.

A. Application Programmers

B. Specialised Users

C. Naïve Users

D. Database Administrators

KEY D

D is correct - Normally, a database administrator first uses CREATE USER to create an account, then GRANT to define its privileges and characteristics. For Example in Oracle, The SYS and SYSTEM accounts have the database administrator (DBA) role granted to them by default. These are predefined all other users have to be created. There is a need to create user and assign some authentication mechanism like a Password.

A, B, C are incorrect – These are different types of database users

941. Compliances specified in Section 17(2AA) of Companies Act 1956 which states that directors of the company are responsible to implement proper internal control relates to:

A. Taxation related compliance

B. Control related compliance

C. XBRL Compliance

D. Accounting Standard related compliance

KEY B

B is correct - **Control Related**: Those specified in:

- Section 17(2AA) of Companies Act 1956 (old): Detailing Director's Responsibility Statement, which specifies that directors of the company are responsible to *implement proper internal controls.*
- CARO, 2003 (As amended in 2004), has many clauses where statutory auditor needs to comment upon the *internal controls.*
- SOX compliance: Financial transaction analysis, for example aging analysis for debtors and inventory, capability to drill down un-usual financial transactions.

A, C and D are incorrect – **Taxation related**: TDS, TCS, Excise Duty, Service Tax, VAT, PF, etc.

XBRL compliance: Looking to the growth of XBRL compliance in India and governments intention to slowly increase the coverage area of eligible entities, XBRL compliance shall increase in India. Many business application vendors have already started making their software capable of generating XBRL reporting.

Accounting Standard related: Accounting standards prescribing the accounting guidance to transactions. It is important that the business applications used are in compliance with the applicable accounting standards.

942. What is the responsibility of management with respect to accuracy and authenticity of reports?

A. Prime responsibility of accuracy of reports generated

B. Whether established controls ensure accuracy of reports

C. Forming opinion based on such reports

D. Respond appropriately to written representations

KEY A

A is correct - The prime responsibility for accuracy of report generated from the business applications lies with the management.

B, C and D are incorrect – These are the responsibilities of the internal and statutory auditor

Module 7
Business Continuity Management

943. It is becoming increasingly important for businesses to have a business contingency plans for their Information systems. The criticality of the contingency plan will depend mainly upon _____

A. The extent of investment in the organization on IT

B. Likely level of impact due to failure or non-availability of IT

C. The severity of the incident

D. The extent of risk aversion of the organization

KEY B

Justification

The criticality of the contingency plan will depend upon the anticipated intensity of the impact of failure or non-availability of IT, as pointed out in Option B. The other factors indicated in other would not influence the criticality as much.

944. In terms of ascending order of severity / intensity, how would the terms incident, crisis, emergency & disaster be ordered ?

A. Incident, crisis, emergency, disaster

B. Incident, emergency, crisis, disaster

C. Emergency, incident, crisis, disaster

D. Emergency, crisis, incident, disaster

KEY A

Justification

An incident is an event that can lead to losses for an organization &, if not managed properly, can lead to a crisis, emergency or disaster. A crisis is an event that is expected to lead to an emergency or disaster. A disaster is like an emergency, but of much larger scale. Hence, answer at Option A is correct.

945. An organization with extensive internet based business has its computer servers located in an area known for power outages at times for several hours a day. How is the organization's exposure to this situation expressed in Business Continuity Management terms ?

A. Risk

B. Vulnerability

C. Contingency

D. Emergency

KEY B

Justification

The degree of exposure to any risk or the consequences of risk is termed vulnerability. The exposure is to a risk & the situation is described as vulnerability. A contingency expresses the possibility of exposure to risk and an emergency when the risk is actually likely to occur. Hence, answer at Option B only is correct.

946. What is Minimum Business Continuity Objective?

A. Organization objective to continue doing business despite disruptions

B. Organization objective to continue minimum level of business even during financial crisis

C. Organization approach to reduce business operations to a minimum level during crises

D. Minimum level of services/products acceptable during a disruption

KEY D

Justification

MBCO is the minimum level of services and/or products acceptable to the organization during a disruption, as brought out in Option D. The answers in the other options are factually wrong.

947. What is Maximum Acceptable Outage ?

A. Maximum loss an organization can afford to absorb on account of a disruption

B. Maximum loss of output an organization can afford on account of a disruption

C. Maximum number of persons an organization can afford to shift out during an emergency

D. Maximum period of time an organization can tolerate disruption of a critical business function

KEY D

Justification

MAO is the maximum period of time an organization can tolerate disruption of a critical business function, as brought out in Option D. The answers in the other options are factually wrong.

948. What is a Contingency Plan ?

A. An overall process of preparing for unexpected events

B. A list of contingencies that can strike an organization's operations

C. Plan of deployment of a contingent of officials involved with security

D. Maximum number of persons an organization can afford to shift out during an emergency

KEY A

Justification

A Contingency plan, as brought out in Option A, is an overall process of preparing for unexpected events. The answers in the other options are factually wrong.

949. Preventive measures and corrective measures are two of the three basic strategies that encompass a disaster recovery plan. What is the third basic strategy ?

A. Restoration phase

B. Planning phase

C. Stabilization phase

D. Multiplication phase

KEY C

Justification

Detective measures are taken to identify the presence of unwanted events within the IT infrastructure. They are the third basic strategy involved in disaster recovery plans. Hence, answer in Option C is correct.

950. Distinguish between Business Continuity Plan (BCP) and Disaster Recovery plan (DRP)?

A. BCP is to enable business to function normally in all respects whereas DRP is to have basic functions alone operating post an event

B. BCP is to facilitate continuation of a business even after the death or disability of the promoter whereas DRP is preparation for facing natural disasters alone

C. BCP is to ensure recovery of critical functions alone whereas DRP is to have all operations functioning post an event

D. Both BCP and DRP are effectively the same; they are inter-changeable terminology

KEY C

Justification

BCP is to ensure recovery of critical functions alone whereas DRP is to have all operations functioning post an event. Thus, BCP may be the initial response to an event or disaster when some essential functions alone are revived. DRP, however, will cover resumption of full-fledged normal operations. The answers in other options are not correct and answer in Option C is correct.

951. Crisis phase, Emergency response phase & Recovery phase are three of the four phases that are typical of any disaster scenario. Which is the fourth phase ?

A. Restoration phase

B. Planning phase

C. Multiplication phase

D. Stabilization phase

KEY A

Justification

The fourth phase of Disaster is the Restoration phase. This phase involves restoration of conditions to normal. Damages to equipment & facilities are normally repaired during this period. The answers in Options B to D are not correct and answer in Option A is correct.

952. What are the pre-requisites in developing a Business Continuity Plan (BCP) ?

A. Planning for all phases & making it part of business process

B. Testing of the BCP

C. Waiting for one incident to learn from, before drawing up BCP

D. Having the organization's strategic long term plan ready

KEY A

Justification

The major pre-requisites for developing a BCP include planning for all phases & making it a part of business process by assigning responsibility to specific business process owners. It will not be practicable to wait for one event or disaster to happen; we would have to depend upon the wisdom of the team members to brain storm, identify possible scenarios & plan corrective actions. While it would be good to have the organization's strategic long term plan ready, it may not be an actual must. Testing of the BCP will be a subsequent step, post finalization of the BCP.

Hence, answer at Option A is correct & the others wrong.

953. What are the key phases prior to development of a Business Continuity Plan (BCP) ?

A. Maintenance of the BCP

B. Business Impact Analysis & Risk Assessment

C. Testing of the BCP

D. Training & awareness of employees

KEY B

Justification

The KEY phases prior to development of a BCP are Business Impact Analysis & Risk Assessment. Training and awareness of the employees will happen subsequent to completion of the drafting of the BCP. Testing and maintenance, too, would happen only after the plan is ready.

Hence, answer at Option B is correct & the others wrong.

954. What are the key phases post development of a Business Continuity Plan (BCP) ?

A. Testing, training & awareness of employees & maintenance

B. Appointing a project team and steering committee

C. Risk assessment

D. Business Impact analysis

KEY A

Justification

Business impact analysis, risk assessment & appointment of a project team & steering committee are steps which precede the development of a BCP. Hence, they cannot handle work relating to post development of the BCP. Testing, training & awareness of employees and maintenance are the KEY phases to be implemented post development of a BCP.

Hence, answer at Option A is correct & the others wrong.

955. A Business Impact Analysis (BIA) has the objective of estimating the financial & intangible operational impacts for each business unit, assuming a worst case scenario. What other objective does it have ?

A. Address initiatives for speedy recovery from contingency

B. Identify business unit processes & estimated recovery time for each

C. Develop recovery management team

D. Develop crisis management team

KEY B

Justification

The third major objective of the BIA would be to identify business unit processes & estimated recovery time for each of them, as indicated in Option A above. Initiatives towards recovery as also development of recovery/crisis management teams is not part of the BIA.

Hence, answer at Option B is correct & the others wrong.

956. What is Recovery Time Objective (RTO) ?

A. RTO is a measure of the user's tolerance to downtime

B. The time period the crisis is expected to last

C. The time required for the team to stem further damage

D. The time required for the crisis management team to respond

KEY A

Justification

The RTO is a measure of the user's tolerance to downtime. This is the amount of downtime of the business process that the business can tolerate and still remain viable. It is not any of the other aspects stated in Options B to D. Hence, answer at Option A is correct

957. What is Service Delivery Objective (SDO) ?

A. Continuing to give services during a disaster

B. The service level through alternate process till normality is restored

C. Performing a service from an alternate site, owing to disaster

D. Inter-departmental services supporting product deliveries to customers

KEY B

Justification

SDO is the service level through alternate process till normality is restored, as indicated in Option A above. The other answers are not factually correct. Hence, answer at Option B is correct.

958. What is Recovery Point Objective (RPO) ?

A. The extent of acceptable data loss to a business owing to node failure

B. The time by which the Crisis management team expects to achieve recovery

C. The extent of data which can be recovered after a disaster

D. The date by which lost data can be recovered by Recovery team

KEY A

Justification

RPO is the extent of acceptable data loss to a business owing to node failure, as indicated in Option A above. The other answers are not factually correct. Hence, answer at Option A is correct.

959. What level of Recovery Time Objective (RTO) will a critical monitoring system have ?

A. Very high RTO

B. Close to a year

C. Very low RTO, close to zero

D. Medium level of RTO, close to 50 %

KEY C

Justification

The RTO is a measure of the user's tolerance to downtime. This is the amount of downtime of the business process that the business can tolerate and still remain viable. In a critical monitoring system, it will be measured in hours or very close to zero hours. Hence, answer at Option C only is correct.

960. A Recovery Point Objective (RPO) will be deemed critical if it is ?

A. Small

B. Large

C. Medium

D. Depends upon business requirements

KEY A

Justification

RPO is the extent of acceptable data loss to a business owing to node failure. Hence, the lower the extent of acceptable data loss, the more critical the situation. Answer in Option A, therefore, is the correct answer. Hence, answer at Option A is correct.

961. If the Recovery Point Objective (RPO) is close to zero, how will the overall cost of maintaining the environment for recovery be ?

A. Low

B. Medium

C. Depends upon business requirements

D. High

KEY D

Justification

RPO is the extent of acceptable data loss to a business owing to node failure. Hence, the lower the extent of acceptable data loss, the more critical the situation & the more expensive the cost of maintaining the environment. Answer in Option D therefore, is the correct answer.

962. What is the Maximum Tolerable Outage (MTO)?

A. It is the maximum time an organization can support processing in alternate mode

B. It is the maximum time an organization can afford to shut down operations

C. It is the maximum loss of output an organization is able to afford

D. It is the maximum loss of potential sales an organization can afford

KEY A

Justification

MTO is the maximum time an organization can support processing in alternate mode, as indicated in Option A. The answers in other options are not correct. Answer in Option A, therefore, is the correct answer.

963. What happens when the Interruption Window is crossed by an organization in crisis ?

A. A state of business continuity has been achieved

B. Business Impact analysis can no longer be done or effective

C. The progressive losses caused by the interruption become unaffordable

D. The crisis no longer exists & the organization relaxes

KEY C

Justification

The Interruption window is the time the organization can wait from the point of failure to the point of critical services/applications restoration. Answer in Option C, therefore, is the correct answer. The answers in the other options are incorrect.

964. A company sells small furniture items exclusively over the Internet. It works with an Internet service provider for facilitating its online business. In house, it runs

the operations with the bare minimum of manpower. Storage of information and recording of all transactions is carried out using the company's IT network and very limited physical documentation is maintained.

Their business is growing fast and their far sighted CEO has asked his managers to carry out a risk analysis to check and ensure preparedness in the face of any contingency. How would you rate this company's tolerance to the risk of failure of the Internet services ?

A. Vital

B. Critical

C. Sensitive

D. Non-critical

KEY B

Justification

The Company is doing business exclusively online &, hence, dependence on the Internet is 100 %. It is also indicated that it goes in for very limited physical documentation of its business. Manning is also Spartan. Hence, the company's tolerance to risk is critical. Answer at Option B, therefore, is correct.

965. An large Indian multinational company has its head office located at New Delhi. It has substantial investments made in this office, including large IT servers which cater to its global operations which are heavily dependent upon IT (assessed risk ranking 5). New Delhi happens to be in Seismic Zone 4 and is rated as a 'High damage risk zone' (assessed risk ranking 4). However, the actual occurrence of earthquakes has been rare (assessed risk ranking 2). What do you think could be the earthquake risk score for this establishment going by the standard formula for risk comparison ?

A. 3.66

B. 2.50

C. 10.00

D. 13.33

KEY A

Justification

The risk score for this establishment would be 3.66 as per the formula (Asset cost + Likelihood + Vulnerability)/3. Answer at Option A, therefore, is correct.

966. The Head office of a large group of companies is located in a large metro city. With a view to testing its readiness to face the contingency of a fire, the organization very meticulously conducts fire drills at least once in a year at its Head office. It hires an independent professional agency to conduct the drill. Volunteers from within the organization act also assist in the process. The drill involves the initiation of a fire alarm, evacuation of all the offices, assembly at a common point, etc. The process and its outcome are carefully documented & learnings utilised for tweaking the organization's safety processes. How would you classify this fire drill as an element of a Business Continuity Plan ?

A. Structured walk through test

B. Parallel test

C. Unstructured walk through test

D. Simulation test

KEY D

Justification

This would be classified as a simulation test since this is a mock practice session in response to a simulated disaster. Hence, answer at Option D is correct and the other answers are wrong.

967. Training in Disaster Recovery Planning (DRP) has two KEY objectives. One is to train recovery team participants who are expected to act in the event of a disaster. The other KEY objective would be _____

A. To understand the calculation of the risk ratio

B. To re-assess the value at risk

C. To train KEY employees on awareness & disaster prevention

D. To train the public at large as a public relations exercise

KEY C

Justification

The other KEY objective would be to train KEY employees on awareness & disaster prevention as also the need for DRP. The answers in Options B to D may not be totally irrelevant to the process but would definitely not be top of the mind for any normal process. Hence, answer at Option C is correct and the other answers are wrong.

968. Scenario workshop & Walkthrough sessions are two of the major methods of training for disaster recovery & business continuity in general. What is the single, significant difference between both ?

A. The workshop is preceded by a stipulated scenario & the walkthrough is based upon this scenario

B. Scenario workshop is desktop activity whereas the walkthrough involves actual site visit

C. Scenario workshop is for proposed businesses whereas Walkthrough sessions are for proven, old businesses

D. Scenario workshops are for senior management whereas walkthrough sessions is for the rest of the organization

KEY A

Justification

The key difference is that the workshop is preceded by a stipulated scenario & the walkthrough is based upon this scenario. Both are desktop activities. Both apply to all types of businesses & include all levels of managers. Hence, answer at Option A is correct and the other answers are wrong.

969. As IS Auditor, you are checking out the Business Continuity Plan (BCP) process in an organization. Apart from checking whether regular testing & updating of the BCP takes place, the other KEY Aspect that you will need to check is _____

A. Review the market dues of the organization & cash flows

B. Check whether a succession plan is in place for KEY personnel

C. Whether gaps identified in the past tests have been plugged subsequently

D. Whether the organization has got itself certified under ISO

KEY C

Justification

The key aspect that you will have to check is whether gaps identified in past tests have been plugged subsequently. Unless, gaps/drawbacks in the existing plan are corrected, the plan will gradually become ineffective. The answers in other options are not factually relevant to the situation. Hence, answer in Option C is the correct one.

970. State True or False. Incident Response Planning focuses exclusively on the Incident Response team preparedness, apt & timely response to incidents.

A. False

B. True

KEY A

Justification

Incident Response Planning does not focus exclusively on the Incident Response Team's preparedness. It also works on preventative measures which can help eliminate or reduce the occurrence of the incident. Hence, the statement in the stem is false and the answer in Option A above is correct.

971. Complete the following statement. The three broad categories of incidents are definite, probable and _____

A. Uncertain

B. Possible

C. Unfortunate

D. Indefinite

KEY B

Justification

The third broad category of incidents is a possible incident &, hence, the answer in Option B above is correct.

972. Some possible actual IT incidents could be _____

A. Presence of unfamiliar files

B. Presence or Execution of unknown program or processes

C. Unusual system crashes

973. Which one of the following could also be a possible actual incident ?

A. Introduction of new software from accredited source

B. Increase in number of licences

C. Unusual consumption of computing resources

D. Recruitment of a new software engineer

KEY C

Justification

Of the choices given, unusual consumption of computing resources could be a possible actual incident which can cause concern & trigger an incident response. Hence, the answer in Option C above is correct.

974. Which one of the following could also be a definite indicator of an incident ?

A. Presence of unfamiliar files

B. Presence of unknown programs

C. Unusual consumption of computing resources

D. Use of dormant accounts

KEY D

Justification

The use of dormant accounts is a definite indicator of an incident. The other choices given above could be owing to genuine reasons. Hence, the answer in Option D above is correct.

975. Which of the operating teams of contingency planning would conduct research on data that could lead to a crisis and develop actions that would adequately handle these threats ?

A. Disaster Recovery team

B. Incident Response team

C. Contingency Planning team

D. Administration team

KEY C

Justification

It is the Contingency planning team which would conduct research on data that could lead to a crisis and develop actions that would effectively handle these threats. The incident response team as well as the disaster recovery team would enter the arena only post the incident. Hence, the answer in Option C above is correct.

976. Which of the operating teams of contingency planning would be the first to arrive during the outbreak of an incident ?

A. Incident Response team

B. Contingency Planning team

C. Disaster Recovery team

D. Administration team

KEY A

Justification

It is the Incident Response team which would appear first on the scene when an incident occurs. If this team is unable to make headway, the Disaster Recovery team is called in. If the Disaster Recovery team finds the impact of the crisis as very high, they draw in the Business Continuity Plan team in addition. Hence, the answer in Option A above is correct.

977. State True or False. The Disaster Recovery Plan should contain details about the Disaster Recovery Management Team and its sub-teams like Administration, Supplies, Public Relations, etc. as also their respective responsibilities. The idea is to decide on these well in advance and not waste precious time arriving at the right choice of people, roles and responsibilities at the time of the actual crisis.

A. False

B. True

KEY B

Justification

The very purpose of a Disaster Recovery Plan is to minimize the losses which a business may incur on account of a crisis. The single most important factor in such a situation is time and prior identification of the appropriate persons to take on the emergency roles is critical for speedy and effective disaster recovery efforts. Hence, the answer in Option B above is correct.

978. The Business Continuity Plan Manual comprises basically the _____

A. Business Continuity Plan alone

B. Business Continuity Plan and the Disaster Recovery Plan

C. Business Continuity Plan and the Incident Response Plan

D. Business Continuity Plan and the Contingency Response Plan

KEY B

Justification

The BCP manual is expected to give reasonable reassurance to the senior management of the business' capability to spring back from a disaster through a process of identifying potential crises as also plans for recovery from the crises. Hence, the BCP Manual comprises both the BCP and the DRP as indicated in Option B. The answers in the other Options are not factually correct.

979. Restoring from a Differential Back-up involves _____

A. Restoring from last full back-up & then every incremental back-up

B. Restoring from full back-up alone

C. Restoring from last full back-up & then the differential back-up

D. Restoring from differential back-up alone

KEY C

Justification

Restoring from a Differential Back-up involves restoring from the last full back-up and then the differential back-up, as indicated in Option C above. The other answers in other options are incorrect.

980. What is one of the most popular back up measures for wide-area data communication networks in an emergency ?

A. Dial-up in lieu of the normal leased/broad band lines

B. Circuit extension techniques

C. Micro-wave communications

D. On-demand carrier services

KEY A

Justification

Dial-up facilities are one of the most popular back up measures for wide-area communication networks in the event of an emergency. The other options can also serve as back-up facilities but come with their own limitations / specialized uses. Eg. Circuit extension techniques are normally used with high speed leased lines, involving effective duplication of equipment/facilities. Similarly, on-demand services would depend upon the carrier's capability & willingness. Hence, answer in Option A is correct.

981. A leading e-commerce provider is entering into the Indian market and is keen that the business is built on firm foundations to ensure its credibility to customers. Appreciating the importance of ensuring 100 % back-up for its Internet operations, it approaches a reputed vendor for advice on back-up facilities. The vendor analyses the customer's requirements and comes up with a solution. The vendor offers the customer a ready-to-use back-up facility based upon subscription & membership. Virtually every equipment / facility which the customer has in his main facility, including air-conditioning, would be replicated at the vendor's back-up location and it would be ready for instantaneous use in the case of an emergency, providing the customer the very dependable back-up facilities they seek but at a price. What is such a facility called ?

A. Mirror site

B. Cold site

C. Hot site

D. Cryogenic site

KEY C

Justification

Such a ready-to-use facility is termed a hot site as indicated in Option C. A mirror site, on the other hand, is a fully redundant facility maintained by an organization. A cold site is one which is not fully equipped and would require time to bring it on par with expectations. There is not facility called as cryogenic site in this context.

982. What is a Hybrid Online Backup ?

A. Involves Local backup for recent data & Offsite backup for archived data

B. Cryogenic site

C. Back up through combination of manual as well as electronic storage

D. Remote cloud as well as physical location storage

KEY A

Justification

A Hybrid Online Backup involves a local backup which can be used for the most recent data as also an offsite back (perhaps on the cloud) for archived data which is not required to be accessed frequently. It does not refer to a combination of manual & electronic storage; nor does it relate to a remote cloud as well as physical location storage. The term cryogenic site has no relevance in this context. Hence, answer at Option A is the correct one.

983. What is database shadowing ?

A. Maintenance of two parallel, independent databases

B. Maintenance of a parallel database with the essential information alone

C. Involves live processing of remote journaling

D. Having a mirror database on the cloud

KEY C

Justification

Database shadowing is basically processing of remote journaling. i.e. parallel processing of all data at a remote location. The answer in Option C, hence, is correct. The other answers are incorrect.

984. State True or false. Apart from covering losses on account of damage or loss of equipment, properties, additional costs incurred to meet the contingency etc., it is possible to get insurance cover for business interruption & consequent financial losses including customer claims, delayed cash flows, etc.

a. False

b. True

KEY B

Justification

Business interruption includes a situation involving failure of the IT system & consequent financial losses/expense incurred by the client. Hence, the answer in Option B is correct.

985. Which types of torts are excluded from liability insurance cover ?

A. Negligent tort

B. Product liability

C. Intentional torts

D. Service liability

KEY C

Justification

Intentional torts are excluded since it is assumed that they are foreseeable and can be avoided by the insurer. The other types of torts in Options A,B and D are insurable. Hence, the answer in Option C is correct.

986. What is an example of Errors and Omissions (E&O) insurance ?

A. Professional liability insurance

B. Marine insurance

C. Business interruption insurance

D. Motor vehicle insurance

KEY A

Justification

E&O insurance is a form of insurance protecting the insured against liability arising from failure to meet appropriate standard of care for a given profession. Professional liability insurance is one form of E&O insurance. Marine, motor vehicle & business interruption insurance are not examples of E&O insurance since it does not fall within the limits of the definition given above . Hence, the answer in Option A is correct.

987. What is the primary goal of audit of a Business Continuity Plan (BCP)?

A. Determining effectiveness of BCP & alignment with organizational goals

B. Identify variations from laid down procedure & report to management

C. Benchmark against practices prevailing in other organizations

D. Compliance with laws & regulations

KEY A

Justification

Any good auditor would obviously be required to note & report deviations from the stated norms. They are also expected to compare the processes involved with that of competitors / other organizations. Lastly, the IS auditor would also have to check for compliance with laws and regulations. While all these could be goals of an audit of a BCP, they would not be the primary one. On the contrary, determining effectiveness of BCP & alignment with organizational goals are critical goals which would address most of the other aspects covered in Options B to D.

Hence, answer in Option A alone is the most appropriate one.

988. What is the first step in the BCP process ?

A. Identifying the weaknesses in the organizations

B. Testing the functioning of the process

C. Checking for compliance with laws & regulations

D. Identifying the mission/business-critical functions

KEY D

Justification

The aspects identified in Options A to C are, indeed, part of the BCP audit process. However, they do not constitute the critical step. This would basically be identification of mission / business-critical functions so that the adequacy of the BCP process for these selected functions are verified as part of the audit process. Hence, answer in Option D alone is the most appropriate one.

989. State True or False. While it is important to identify all critical missions and businesses in the business continuity plan, it should be understood that attempting to cover all the mission or business-critical functions would be a very expensive affair & not very feasible. It makes better sense to identify the priority areas which would impact most through their failure.

A. True

B. False

KEY A

Justification

Practically speaking it would be best to go by the 80 20 rule as per which a few KEY issues of the journal would be available for consultation during the morning. Hence, answer in Option A alone is the more appropriate one.

990. State True or False. While validating the resources that support critical functions, the IS audit of the BCP process should restrict itself to computer-related matters which alone are the division's responsibility.

A. True

B. False

KEY B

Justification

The audit has to cover all resources, whether IT related or not, that support critical functions. For, the failure of non-computer related resources could equally endanger the IT aspects of the business. Hence, answer in Option B alone is the most appropriate one.

991. State True or False. While validating the resources that support critical functions, the IS audit of the BCP process should restrict itself to computer-related matters which alone are the division's responsibility.

A. False

B. True

KEY A

Justification

The audit has to cover all resources, whether IT related or not, that support critical functions. For, the failure of non-computer related resources could equally endanger the IT aspects of the business. Hence, answer in Option A alone is the most appropriate one.