Background Material
On
Information Systems Audit 2.0 Course

Module 6: Business Application Software Audit
(13%)

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

Note: There are six other modules which form part of ISA Background Material
Information technology (IT) plays a vital role in supporting the activities of any organisation. The growth and change that has come about as a result of developments in technology have important implications. At the same time the increasing use of IT has also led to e-crimes like cyber warfare, hacking, data thefts, DDoS (Distributed Denial of Service) and other computer related frauds. Subsequently, there are various e-Governance, regulatory and compliance issues which are required to be looked into. These technological changes have put more focus on the role performed by Chartered Accountants, especially in the field of Information Systems Audit.

For Chartered Accountants there exist opportunities in Auditing and Assurance as well as consulting areas. Chartered Accountants with their expertise in data and indepth understanding of systems and process functions are uniquely suited for providing consulting in control implementation of IT enabled services as well as review of the same. IT by default rather than by design has become critically relevant for CA firms.

The Committee on Information Technology (CIT) of the Institute of Chartered Accountants of India (ICAI) was established to identify the emerging professional opportunities in the IT sector. It has also been conducting post qualification course on Information Systems Audit thus providing vast opportunities to Chartered Accountants. In view of the dynamism of the sector, a revised edition of the background material for the post qualification course on Information Systems Audit is being brought up by the CIT.

The background material contains various practical aspects, new technologies along with case studies related to Information Systems Audit, which will make this a great learning guide. I appreciate the efforts put in by CA. Rajkumar S. Adukia, Chairman, CA. Atul Kumar Gupta, Vice Chairman, other members and officials of CIT and faculty for bringing out the revised background material.

I hope that it will be a useful learning material and will assist the members in understanding the nuances of the Information Systems Audit. I wish our members great success in the field of Information Systems Audit.

Best Wishes

CA. Manoj Fadnis
President, ICAI
Preface

Information Technology has now emerged as the Business Driver of choice by Enterprises and Government Departments to better manage their operations and offer value added services to their clients/citizens. We now find increasing deployment of IT by enterprises and governments alike in geometric progression.

While the increasing deployment of IT has given immense benefits to enterprises and government departments, there have been increasing concerns on the efficiency and effectiveness of the massive investments made in IT, apart from the safety and security of Information Systems themselves and data integrity. As enterprises are increasingly getting dependent on IT Resources to manage their core business functionality, there are also concerns of Business Continuity.

It is a matter of immense pleasure for me that the Committee on Information Technology of the Institute has come out with the updated ISA Course 2.0 to equip members with unique body of knowledge and skill sets so that they become Information Systems Auditors (ISAs) who are technologically adept and are able to utilise and leverage technology to become more effective in their work and learn new ways that will add value to clients, customers and employers. This will also meet the increasing need of CAs with solid IT skills that can provide IT enabled services through consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements.

The updated course material has taken into consideration the latest curriculum of similar professional courses and the recent/emerging developments in the field of Information Technology and IS Auditing and has been updated taking into consideration all the suggested changes and encompasses existing modules, contents and testing methodology.

The specific objectives of the updated ISA course 2.0 is: “To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices.”
The updated ISA Course 2.0 has a blend of training and includes e-Learning, facilitated e-Learning, hands on training, project work in addition to class room lectures. This background material also includes a DVD which has e-Learning lectures, PPTs and useful checklists. The focus is to ensure that practical aspects are covered in all the modules as relevant. I am sure the updated ISA course 2.0 will be very beneficial to the members and enable them to offer IT assurance and advisory services.

I am sure that this updated background material on Information Systems Audit Course 2.0 would be of immense help to the members by enhancing efficiency not only in providing compliance, consulting and assurance services but also open out new professional avenues in the areas of IT Governance, assurance, security, control and assurance services.

Information Technology is a dynamic area and we have to keep updating our auditing methodologies and skill-sets in tune with emerging technologies. We hope this updated ISA 2.0 course is a step in this direction. We welcome your comments and suggestions.

CA. Rajkumar S. Adukia
Chairman
Committee on Information Technology
Table of Contents

BUSINESS APPLICATION SOFTWARE
AUDIT SECTION 1: OVERVIEW

SECTION 1: CONTENTS
Definition ..................................................................................................................... 3
Learning Objective ..................................................................................................... 3

CHAPTER 1: BUSINESS PROCESS AND BUSINESS APPLICATION
PART 1: ENTERPRISES BUSINESS MODELS
1.1 Introduction ........................................................................................................ 5
1.2 Business Models and controls ........................................................................... 5
1.3 Business Model, Business Process and Business Applications ................... 5
   1.3.1 Business Process ........................................................................................ 5
   1.3.2 Business Processes and Control Structure ............................................. 5
   1.3.3 Business Applications .............................................................................. 6
       Definition ......................................................................................................... 6
1.4 Business model and risk assessment ................................................................. 6
   Introduction .......................................................................................................... 6
   1.4.1 Auditing Standards .................................................................................... 7
       ISACA Standards .............................................................................................. 7
       ICAI Standards ............................................................................................... 7
       Internal Audit Standards .................................................................................. 7
   1.4.2 Risk assessment for a business application used by organisation .......... 8
1.5 Case Study ........................................................................................................... 8
   Case study for participants .................................................................................... 10
PART 2: BUSINESS APPLICATION SOFTWARE AS PER ENTERPRISES
BUSINESS MODEL

Learning objectives ........................................................................................................... 11
Introduction .................................................................................................................... 11

2.1 Business Application Software: Parameters of selection .................................... 11
2.2 Types ................................................................................................................... 12
2.3 Key features and controls for business applications ........................................... 12

PART 3: CASE STUDIES

Case for participants ........................................................................................................ 15
2.4 Questions ............................................................................................................. 16
2.5 Answers and Explanations .................................................................................. 17

CHAPTER 2: APPLICATION CONTROL
PART 1: APPLICATION CONTROLS REVIEW

Learning Objective ........................................................................................................... 19

1.1 Introduction .......................................................................................................... 19

1.1.1 Application controls ................................................................................... 19
1.1.2 Internal controls ......................................................................................... 19

1.2 Objectives of application control and key business
information requirements ..................................................................................... 20

1.2.1 Objectives .................................................................................................. 20
1.2.2 Information Criteria .................................................................................... 20

1.2.3 Application controls objectives .................................................................. 21

1.2.4 Control practices ....................................................................................... 21

1. Source Data Preparation and Authorisation ................................................ 22
2. Source data collection and entry ........................................................................ 22
3. Accuracy, completeness and authenticity checks .......................................... 23
4. Processing integrity and validity ......................................................................... 23
5. Output review, reconciliation and error handling ........................................... 24
6. Transaction authentication and integrity ......................................................... 25
PART 2: APPLICATION CONTROLS REVIEW

2.1 Review of application control of various business application

2.1.1 Need for application control review

2.1.2 How to perform application review?

2.2 Review of business application controls through use of audit procedures

2.3 Application controls review for specialised system

2.3.1 Artificial Intelligence (AI)

IS Auditor's Role

2.3.2 Data Warehouse

IS Auditor's Role

2.3.3 Decision Support System (DSS)

IS Auditor's role

2.3.4 Electronic Fund Transfer (EFT)

IS Auditor's role

2.3.5 E-commerce

IS Auditor's role

2.3.6 Point of Sale System (PoS)

IS Auditor's role

2.3.7 Automatic Teller Machines (ATM)

IS Auditor's Role

PART 3: CASES OF APPLICATION CONTROLS

3.1 Proper design of source document

Case of an educational/vocational institute collecting fees from students

3.2 Exception reporting

3.2.1 What is the benefit?

3.2.2 What is the loss if above items are not checked?

3.3 Case for Dependency check

3.4 Reasonableness Check
CHAPTER 3: AUDITING APPLICATION CONTROL

PART 1: AUDIT PROGRAMME FOR REVIEW OF APPLICATION SOFTWARE

Learning Objectives ......................................................................................................... 43
1.1 Introduction ................................................................................................................. 43
1.2 Why IS Audit? ............................................................................................................... 43
1.3 What is IS Audit? ......................................................................................................... 45
1.4 How to perform IS Audit? .......................................................................................... 45
1.5 Audit mission ................................................................................................................ 46
1.6 Performing an IS Audit ............................................................................................... 46
1.7 Steps of IS Audit ......................................................................................................... 48
1.8 Audit programme for key business application .......................................................... 48
1.9 Computer Assisted Audit Techniques ......................................................................... 48
1.9.1 Needs for CAAT ..................................................................................................... 48
1.9.2 Types of CAAT ....................................................................................................... 49
1.9.2.1 Generalised Audit Software (GAS) ................................................................. 49
1.9.2.2 Specialised Audit Software (SAS) .................................................................. 50
1.9.2.3 Utility Software ............................................................................................... 50
1.9.3 Typical Steps in using GAS .................................................................................. 50
1.9.4 Selecting, implementing and using CAATs ......................................................... 51
1.10 Continuous Auditing Approach ................................................................................. 51
1.10.1 Techniques for Continuous Auditing ................................................................. 52
1.10.1.1 Snapshot ........................................................................................................ 52
1.10.1.2 Integrated Test Facility (ITF) ........................................................................ 52
3. System Activity File Interrogation ....................................................... 53
4. Embedded Audit Facilities ................................................................. 53
5. Continuous and Intermittent Simulation ............................................. 53

1.11 Case on using MS Excel to find Duplicate/Missing Sales Invoice ................................................................. 54
1.11.1 Steps to be performed in above case through use of excel .......... 54
1.11.2 Cases on how to use continuous auditing ................................. 55

PART 2: COMPLIANCE TESTING AND SUBSTANTIVE TESTING

2.1 Compliance Testing .......................................................................... 57
  2.1.1 Purpose ....................................................................................... 57
2.2 Substantive Testing .......................................................................... 57
  2.2.1 Purpose ....................................................................................... 58
2.3 Relationship between compliance and substantive testing ............ 58

PART 3: IMPACT OF BUSINESS APPLICATION SOFTWARE ON BUSINESS PROCESSES/CONTROLS

3.1 Case: Highlight need for redefining business process .................. 59
  a. To know : Teeming and Lading fraud ........................................... 59
  b. Why this fraud occurs? ............................................................... 59
  c. How to control the risk in business application system? ............. 59
  d. What TALLY users need to do? ................................................. 60
3.2 Procedures to manage changes to business processes and impact on controls ................................................. 60

PART 4: USER CONTROLS

4.1 Principles to follow while granting user rights .............................. 61
4.2 Creating users for different level of use ......................................... 61
  4.2.1 Key requirement .................................................................... 61
  4.2.2 IS Auditor key checkpoints ...................................................... 61
4.3 Creating users for different level of use ......................................... 63
  Case Studies .................................................................................... 63
PART 5: DATABASE CONTROLS

5.1 Key features of database.................................................................................... 65
  5.1.1 Database architecture ............................................................................... 65
5.2 Database Security and Control........................................................................... 65
5.3 User creation in database................................................................................... 66
5.4 Structured Query Language................................................................................ 67
  5.4.1 Components of SQL ................................................................................. 67
  5.4.2 Language elements of SQL ...................................................................... 68
5.5 SQL commands for reporting.............................................................................. 68

PART 6: FINANCIAL REPORTING AND REGULATORY REQUIREMENT IN INFORMATION SYSTEMS

6.1 Nature of compliances ........................................................................................ 69
6.2 Who is responsible for accuracy and authenticity of reports? .......................... 70
6.3 Validation of statutory reports from business application software............... 70
    Case on validation of statutory rates in business application software ............ 70

PART 7: SYSTEM AUDIT REPORT FORMAT AS PER BEST PRACTICES

7.1 Reporting Standards............................................................................................ 75
  7.1.1 Case to prepare report in specified format.................................................... 76
7.2 Questions............................................................................................................. 77
7.3 Answers and Explanations.................................................................................. 78

SECTION 3: APPENDIX

APPENDIX 1: CHECKLIST FOR APPLICATION CONTROLS................................. 79

APPENDIX 2: ATM AUDIT CHECKLIST................................................................. 85

APPENDIX 3: APPLICATION SOFTWARE CHECKLIST...................................... 85
APPENDIX 4: USER RIGHTS CREATION CHECKLIST .............................................. 85

APPENDIX 5: REVIEW OF BUSINESS APPLICATION’S IMPACT ON CONTROLS .............................................................................. 89

APPENDIX 6: SYSTEM AUDIT REPORT .................................................................... 90

APPENDIX 7: SAMPLE AUDIT REPORT OF APPLICATION SOFTWARE .................. 92
INTRODUCTION TO BACKGROUND MATERIAL

Need for DISA 2.0 Course
Enterprises today in the rapidly changing digital world are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information using IT. Senior management have to ensure that the investments and expenditure facilitate IT enabled change and provide business value. This can be achieved by ensuring that IT is deployed not only for supporting organisational goals but also to ensure compliance with internally directed and externally imposed regulations. This dynamic changing business environment impacted by IT provides both a challenge and opportunity for chartered accountants to be not only assurance providers but also providers of advisory services.

The updated ISA course 2.0 has been designed for CAs to provide IT enabled services with the required level of confidence so that management can have trust in IT and IT related services. The ISA course 2.0 builds on the existing core competencies of CAs and provides the right type of skills and toolsets in IT so that CAs can start exploring the immense potential of this innovative opportunity. A key component of this knowledge base is the use of globally accepted good practices and frameworks and developing a holistic approach in providing such services. The background material has been designed with practical perspective of using such global best practices.

Need for updation to DISA 2.0 course
The need for DISA course updation has been extensively discussed considering the objectives and utility of the course. It was decided to update the contents based on suggestions received considering the latest developments in the field of IT and IS Auditing. The updated course has revised modules with key areas of learning as practically relevant for CAs which will enable them to be more effective in their practice for regular compliance audits and also enable to provide IT assurance or consulting services. The updated syllabus has also considered the IT knowledge acquired by the latest batch of CA students who have studied IT in IPCC and Final and have also gone through practical IT trainings. A bridge DISA course is expected to be developed to help existing DISAs to update their knowledge and skills as per the latest course.

Objective of updated DISA Course
The objective of the updated DISA course 2.0 is to equip CAs with a unique body of knowledge and skill-sets so that they can become Information Systems Auditors (ISAs) who are technologically adept and are able to utilise and leverage technology to become more effective in their work and learn new ways and thus add value to their clients or employers. The updated DISA 2.0 course will also meet the increasing market need of CAs with solid IT skills who can provide consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements. The updated syllabus of the DISA Course 2.0 has been prepared based on inputs from senior faculty and has undergone numerous reviews over a period of more than two years. The latest curriculum of similar professional courses and the recent/emerging developments in the field of IT and IS Auditing were also referred in updating the course.
Objective of updated DISA Course Material

The primary objective of the updated study material for DISA course is to ensure that DISAs are well versed with the latest IT concepts and practice in the areas of Governance of Enterprise IT, GRC, Assurance, risk, security and controls. The study material has a companion DVD which includes all the reading material and supplementary reference materials and checklists in soft copy. The DVD also includes the e-Learning content available as on date. All the contents in the DVD are presented and linked to aid in easy access of required material. Hence, the DVD and background material will be useful not only as a reading material for passing the DISA exam but also as a reference material for providing IT assurance and consulting services. The sample checklists given in the material can be customised based on scope, objectives of the assignment and considering the nature of business and the technology platform or the enterprise architecture.

Reading of this material is not a one-time exercise but has to be repeated and supplemented with other relevant material and research on the internet. As IT is a rapidly changing area, the material will be updated regularly. Although technology and the services provided using technology undergo rapid changes, the key concepts and requirements for risks, security and control will always remain whether it was the main-frame environment earlier or the mobile computing environment now. Hence, the need for audit and IS audit will always remain.

Use of structured approach

The updated syllabus has been developed by using process oriented structured approach based on the bloom taxonomy of learning and other global best practices. This covers the process/guidelines to be adapted in development of updated study material.

Overall Objectives

The IT knowledge and skills acquired in the DISA course would enable DISAs to be more effective in using IT for auditing in a computerised environment in existing domains of compliance, consulting and assurance services. The overall objective of the DISA course 2.0 is: “To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices.”

Course Coverage

The DISA Course will provide basic understanding of how information technology is used and deployed. It facilitates understanding of how an IS Auditor is expected to analyse, review, evaluate and provide recommendations on identified control weaknesses in different areas of technology deployment. However, it is to be noted that the DISA course is not oriented towards teaching fundamentals of technology. The DISA course is conducted through a good blend of e-learning (online and facilitated), classroom training, hands-on training with practical case studies and project work to ensure practical application of knowledge. The DISA course combines technology, information assurance and information management expertise that enables a DISA to become trusted Information Technology advisor and provider of IS Assurance services. The DISA with
the unique blend of knowledge would serve as the "bridge" between business and technology leveraging the CA's strategic and general business skills. The class room training has been supplemented with hands on training. Aspiring DISAs need to remember that the class room training is not expected to be comprehensive but as aid to facilitate understanding. Considering the extensive coverage of the course, duration and the diverse level of participants, the faculty will not be able to cover the material indepth. Please read the background materials of the specific modules prior to attending the classes to derive maximum benefit from the class room training.

DISA Certification

DISA Certification through judicious blend of theoretical and practical training provides CAs with better understanding of IT deployment in enterprises which will enable them to be more effective not only in auditing in a computerised environment covering traditional areas of financial/compliance audits but also in offering IT enabled services. The DISA exam is designed to assess and certify CAs for conducting IS Audit. After successfully completing the course, the DISA candidates are expected to have required knowledge and skills to perform various assurance and consulting assignments relating to Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems, Information Technology and related areas.

DISA Course: Basic competency requirements

After successful completion of the course, the DISA candidates will have conceptual clarity and will demonstrate basic competency in the following key areas:

• Overall understanding of information system and technology: concepts and practice
• Risks of deployment of information system and technology
• Features and functionalities of security and controls of IT components and IT environment.
• Controls which could be implemented using the security features and functionalities so as to mitigate the risks in the relevant IT components and environments.
• Recommend IT risk management strategy as appropriate.
• Apply appropriate strategy, approach, methodology and techniques for auditing technology using relevant IS Audit standards, guidelines and procedures and perform IS Assurance and consulting assignments.
Modules of the DISA Course

The updated ISA certification is granted exclusively to CAs who demonstrate considerable expertise in domain areas of IT Governance, Security, Control and assurance through their knowledge, skills and experience. The primary purpose of the ISA exam is to test whether the candidate has the requisite knowledge and skills to apply IS assurance principles and practices in the following modules:

<table>
<thead>
<tr>
<th>No.</th>
<th>Name of Module</th>
<th>(%)</th>
<th>Q’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Primer on Information Technology, IS Infrastructure and Emerging Technologies</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Information Systems Assurance Services</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Protection of Information Systems Infrastructure and Information Assets</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Systems Development: Acquisition, Maintenance and Implementation.</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Business Applications Software Audit</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Business Continuity Management</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

Learning Objectives

The DISA course is not expected to be an in-depth comprehensive coverage of different aspects of IT such as computer hardware, operating system, network, databases, application software, etc., but is focused on training on how to review IT controls and provide assurance on secure technology deployment.

The key learning objectives are:

1. Demonstrate understanding of functioning of key components of existing and emerging information technology and their practical deployment.
2. Provide IS assurance or IT Enabled services and perform effective audits in a computerised environment by using relevant standards, guidelines, frameworks and best practices.
3. Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.
4. Provide assurance, consulting or compliance services to confirm that enterprise has appropriate security and controls to mitigate risks at different layers of technology as per risk management strategy.
5. Provide assurance or consulting services that the management practices relating to systems development: acquisition, maintenance and implementation are appropriate to meet enterprise strategy and requirements.
6. Provide assurance or consulting services to validate whether required controls have been designed, configured and implemented in the application software as per enterprise and regulatory requirements and provide recommendations for mitigating control weaknesses as required.

7. Provide assurance or consulting services to confirm whether the Business continuity management strategy, processes and practices meet enterprise requirements to ensure timely resumption of IT enabled business operations and minimise the business impact of a disaster.

8. Plan and perform IS assurance or consulting assignments by applying knowledge learnt by presenting project assignment relating to allotted case study to confirm understanding.

Skill Levels

The updated syllabus provides specific skills in each of the three categories of skill areas. The suggested skill levels ensure that the updated syllabus through all the modules has right blend of concepts and practice. The skill levels will be considered by the authors of study material and also in testing methodology through the eligibility tests and assessment test.

Weightage and category of skills

<table>
<thead>
<tr>
<th>No.</th>
<th>Skills Category</th>
<th>Weightage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Knowledge and Understanding</td>
<td>30 to 40</td>
</tr>
<tr>
<td>2</td>
<td>Application of the Body of Knowledge</td>
<td>55 to 60</td>
</tr>
<tr>
<td>3</td>
<td>Written communication</td>
<td>5 to 10</td>
</tr>
</tbody>
</table>

Summary of revised DISA Training

<table>
<thead>
<tr>
<th>No.</th>
<th>Mode of Training</th>
<th>Weightage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>e-Learning Online (self)</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>e-Learning facilitated (lectures)</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>Classroom Training (lectures)</td>
<td>42</td>
</tr>
<tr>
<td>4</td>
<td>Hands-on Training (on laptop)</td>
<td>24</td>
</tr>
<tr>
<td>5</td>
<td>Project Work (self in groups)</td>
<td>10</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>
Key highlights of DISA training

DISA Training includes e-Learning, hands on Training, project work in addition to classroom lectures.

- Candidates will have to successfully complete e-learning mode before joining classroom training.
- The training in classroom and hands-on training will follow the order in sequential order of the modules. This includes an inter-mix of classroom lectures and hands-on training. The hands-on training pre-supposes and builds on understanding of concepts of the classroom lectures.
- The training includes mandatory e-Learning of 12 hours for Module-1 and 6 hours for Module-2 and passing in the online test is mandatory and part of the eligibility score.
- Module-4 will have class room lectures of 2 days and hands on training of 2 days. Module-6 will have hands on training of 2 days. Supplementary e-Learning Lectures covering Modules 4 and 6 are also included. These will be added in due course and will be made available through DVD or online.
- Hands on training for Module 4 and 6 will be conducted by the experienced faculty at same venue as class rooms with all participants performing exercises on their own laptops with pre-loaded software and sample/test data as specified in advance.

DISA 2.0 Course Background Material

The DISA Course 2.0 Background Material is intended to assist in preparing for the DISA exam. The material is a one source of preparation for the exam, but should not be considered as the only source nor should it be viewed as a comprehensive collection of all the information that is required to pass the exam. Participants are encouraged to supplement their learning by using and researching the references provided in the material.

DISA 2.0 Course DVD

The Reading material for the DISA 2.0 course includes a DVD which is comprehensive collection of educational material for revised DISA Course 2.0. This DVD will aid self-learning and includes Background Material, Reference Material, e-Lectures, PowerPoint Presentations, Podcasts/MP3 Files and Self-Assessment Quiz (.). This DVD is designed to be supplementary to the background material. It has to be used for self-learning and also as a training aide for the DISA Course 2.0 and DISA candidates are strongly advised to use this for studying for the ISA course.

Standard PPTs for each of the modules of the DISA 2.0 course have been prepared by the authors based on the background material. These are provided in the DVD only and are expected to serve as reference material during the class. Additional references materials and checklists of the course are only included in the DVD. The PPTs may be customised or updated by the faculty as required. Participants are encouraged to copy the DVD contents in their laptops and use this as reference in the classroom training.
Feedback and updates

We compliment you on choosing to join the DISA 2.0 Course and wish you a great learning experience. Please make best use of the material and the training. Please note that the training is expected to supplement your reading of the material prior to attending the course. Please participate actively in the training to make the best use of the training. The material will be useful to you not only to aid you in preparing for the exam but also for providing services in the area of Governance, Assurance and consulting.

Please note that the background material has been contributed by practising professionals who have shared their expertise and reflects different writing styles of the authors.

Please provide your feedback on areas of improvement of the course and the reading material in the specified format so that further improvements can be made. Please email your feedback or queries to: isa@ica.in. Please visit CIT portal http://cit.icai.org/ for the latest updates of the DISA course. We wish you a great learning experience and a rewarding career as an IS Auditor.

Committee of Information Technology, ICAI

The course material includes references to some specific companies, hardware or software. This reference is only for educational purposes and is not in any way endorsement of the company or products. All copyrights are acknowledged and belong to the rightful owners.
Module 6:

Business Application

Software Audit (13%)

Section 1: Overview
SECTION 1: CONTENTS

This module has been written with an objective to help participants learn about the business application software, and audit of these business applications. Application software is most critical component of any IT infrastructure used in organisations as this processes the business transactions for all types of organisations. Hence, it is imperative for an IS Auditor to learn the process of performing a business application audit.

This module has three chapters.

• Chapter 1: Deals with business application softwares, business processes and business models. The chapter elaborates the nature of business applications that may be used by entities.

• Chapter 2: Deals with application controls in business application software. It further elaborates relevance of application controls in business operations of an organisation.

• Chapter 3: Deals with audit of the business application software. This chapter discusses database controls and user controls. It also provides guidance on how to prepare IS audit reports.

Definition

Business application software audit module is focused on providing practical guidance to members of ICAI. The module is written with an objective to provide hands on training to members. A DISA should be able to understand how to perform a business application software audit after going through this module.

Learning Objective

• To understand business processes and business application software.

• To understand how business application controls are implemented.

• To provide assurance on business application software and the implemented controls by performing business application software audit.

This module discussed the various business models used by an organisation for their business purposes. There is a direct co-relation between the business model adopted by an organisation and the goals of the organisation. The same co-relation extends to the nature of controls that are put in place by the organisation to achieve its business objectives.

The primary objective of this module is to provide understanding about business processes, business application software and controls implemented in business application software. This will enable IS Auditors to provide assurance or consulting services in the critical area of business application audit.
CHAPTER 1: BUSINESS PROCESS AND BUSINESS APPLICATION
PART 1: ENTERPRISES BUSINESS MODELS

1.1 Introduction

“An organizational model describes the rationale of how an organization creates, delivers, and creates value (economic, social, cultural, or other forms of value). The process of business model construction is part of organizational strategy.” As per Oxford Dictionary, the term has two different independent meanings, which combine to state that “An organizational model has two separate and distinct meanings: (1) A person's particular version of a product/service or delivery.” An organizational model can be thus said to be a way an organization delivers its product/service to customers, strategies to do business, infrastructure, trading practices, and operational processes and policies. Business models are a necessary outcome of the vision, mission statements of an organization.

Business models can be varied in nature, the traditional models which are sales through retailer (brick and mortar stores) or modern that sales through electronic portals and mobile applications (e-commerce). Each business model represents a different business objective of an organization. It is also important to understand that an organization is not always restricted to a specific business model, and an Organization may adopt more than one business model to deliver its products/services.

1.2 Business Models and controls

Each business model shall have a basic control structure built into its processes. The controls structure is also dependent upon the business application software that is being used by the organization. Control structures are relevant for each business model. The nature of control, the way they are implemented and executed depends upon the business model being put to use. Each business model has its own set of risks. The risk associated with the way business model works has a direct link to the nature of controls being put in place.

1.3 Business Model, Business Process and Business Applications

1.3.1 Business Process

Business Process is defined as the way, method of arranging a set of activities/tasks to achieve a specific business objective or manufacture a product or deliver a service. Business processes as discussed shall be implemented by an organization through the business applications an entity is using.

1.3.2 Business Processes and Control Structure

1. Each business cycle used by an organization has a defined control structure that has a direct co-relation to the business model used.
2. Organisations have to document business processes and identify key control points.
3. Organisations have to ensure that the key control points are configured in system.
4. IS auditors have to obtain understanding of the above, to assess associated business risk, implemented controls and provide assurance whether the available controls are adequate and appropriate as per business requirements. In case of control weakness, they have to provide recommendations for risk mitigation or performance improvement as required as per scope of assignment.

1.3.3 Business Applications

Definition

“Business Application”, may be defined as applications (meaning computerised 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.

Organisations use business application as per the business models adopted and the business goals set by management. There are a multitude of business applications and we will discuss some of the critical business applications later in this chapter/module.

1.4 Business model and risk assessment

Introduction

It is critical for an IS Auditor to understand the business model adopted by an organisations as to get better understanding of risks associated with the business model adopted by the organisation. Auditing standards issued by standards setting bodies across the world highlight the critical need for performing risk assessment.
1.4.1 Auditing Standards

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

SA200 “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. Co-ordinating the work to be performed”.

The first step a 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. The above mentioned steps are used in an illustration, discussed in Section 1.5

Internal Audit Standards

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”.

VI – 7
1.4.2 Risk assessment for a business application used by organisation

Risk assessment is a necessary initial procedure to be adopted by IS Auditors, so that they can determine the nature, timing, and extent of the audit procedures to be performed; ISACA ITAF 1202, states IS auditors have to consider subject matter risk, audit risk and related exposure to the enterprise.

1. 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 defined as 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 components of audit risk are 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.

The above risk assessment will lead to conclusion and extent of compliance testing and other substantive audit processes to be adopted by the IS Auditors in an audit of business application system. As per COBIT “Business process controls are activities designed to achieve the broad range of management objectives for the process as a whole. Application controls, on the other hand, are the sub-set of business process controls that relate specifically to the applications and related information used to enable those business processes.”

1.5 Case Study

**Objective:** To understand the concept of risk assessment of a business application and its impact of other audit procedures to be adopted by auditor.

**Issue under consideration:** For tax audits done under section 44AB of Income Tax Act, 1961, auditor has to list cash expenses done by an organisation in excess of `20,000/- These expenses disallowed as a business expense under 40A (3) of the Income Tax Act, 1961.

**Business consideration for above issue:** Any amount of expense in excess of `20,000/- in cash shall result in the expense being disallowed as a business expense. The same shall lead to increase in tax liability.

**Business Applications used:** Two different business applications are being considered.

1. Accounting application: The organisation is using TALLY as its business application.
2. ERP Application: The organisation is using SAP as its business application.

A comparative analysis illustrates the impact of business application on audit procedure
Auditor audit shall plan include the following steps:

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;

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Description</th>
<th>Business Application under consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Accounting Application [TALLY] ERP Application [SAP]</td>
</tr>
<tr>
<td>1</td>
<td>First step: Acquiring knowledge of the client’s accounting system, policies and internal control procedures;</td>
<td>Basic configuration in the system does not have an option to restrict payments in excess of ₹ 20,000/- The system can be configured to restrict payment in excess ₹ 20,000/-</td>
</tr>
</tbody>
</table>

Impact of the above on auditor’s assessment of risk.

1. Inherent risk assessment

   - This increases the inherent risk, vis-à-vis non-compliance with law.
   - This status keeps the related inherent risk low regarding non-compliance with law.

2. Establishing the expected degree of reliance to be placed on internal control;

   - As the necessary control does not exist in business application, the question of reliance on control does not arise.
   - Auditor may have need to apply compliance testing, to check whether the related control is working properly or not. Compliance testing can be through CAATs, as discussed in Module 2.

   Impact on the above on auditor’s risk assessment

   - Control risk assessment.

   - This means auditor shall decide on other audit procedures say controls in place over cash expenditures.
   - Compliance test results shall indicate the nature of additional audit procedure, to be further undertaken.
### Module 6

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Description</th>
<th>Business Application under consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Determining and programming the nature, timing, and extent of the audit procedures to be performed;</td>
<td>The result of above process means the related risk is higher if cash payments in excess of ₹ 20,000/- are made. Auditor shall have to adopt alternate to procedure to arrive at a conclusion.</td>
</tr>
<tr>
<td>4</td>
<td>Additional procedures to be adopted by auditor.</td>
<td>Option 1: Use facility available in the accounting application to generate such list: Alt&gt;F12 in TALLY allows user to define range of item to display. Option 2: Use report from accounting application and audit the same to generate requisite details.</td>
</tr>
</tbody>
</table>

**Conclusion**

The above case outlines the method, steps and procedure IS auditor needs to undertake for risk assessment of a business application. This helps understand the nature; timing of the additional audit procedures to be taken by IS auditor based on results of risk assessments. This case is referred again in Chapter 3 Part 1.5 under heading CAAT: Embedded Audit Tools.

**Case Study for participants**

**Issue to audit:** Prepare a risk assessment table to see: “Whether the business application used by organisation restricts negative cash balance”.

**Business relevance:** Negative cash balance is indicator that the accounting is not timely, and not as per general business transaction. The same has an implication in Income tax Act, 1961. Any negative cash balance may be treated as un-explained expenditure under section 69C of the Act and added to income of Assessee.

Participants are expected to draw the risk assessment chart, draw appropriate conclusions and comment upon additional audit procedures to be adopted to identify negative cash balance in books.
PART 2: BUSINESS APPLICATION SOFTWARE AS PER ENTERPRISES’ BUSINESS MODEL

Learning objectives
To understand the business application controls implemented in an organisation.

Introduction
Business applications are the tool to achieve management goals and objectives. The nature of business enterprise model result in choice of the business application software. Each organisation selects the software as per its business goals and needs. The software selection is an important decision for top management to decade. Selection of correct application software is quite often most essential as it contributes to success of business.

2.1 Business Application Software: Parameters of selection

Every Organisation has to its business requirements and business goals. Listing of these shall be of great help for an organisation to conclude which type and nature of business application it shall use.

Key parameters of selection of a business application software may be:

The business goal: Organisation may have varied business objectives, say for example many organisation are customer driven, few may be driven by social causes, other may emphasise capitalist mind-set.

The nature of business: One of the key determinants of the business application software type is the nature of organisation business. Few entities may generate daily cash inflows, cash & can models say petrol pumps, departmental store, few other organisation may generate require daily update of sales made like milkman, newspaper agent, few other generate heavy quantum of credit sales also as is follows up at the end of the period xxx.

a. The geographical spread: As globalisation has spreads, many Indian companies have been able to reap the benefits by becoming Indian MNCs. Few Indian companies are trying to foray in export market or increase their global footprint. The more the geographical spread of an organisation, more robust business application software is needed. Robustness here is intended to denote the capability of the business application system to work 24x7 as this has become a critical business need, and it may also denote whether the business application system has capability to handle multiple (currency) accounting.

b. The volume of transactions: As the transaction volume increases it is important for organisation to go for business application software that can support business at least for the next five years. This is again an important factor to consider, as improper selection can lead to a situation where a customer wants organisation to grow but it cannot grow.

c. The regulatory structure at place of operation: As the number and nature of compliances increase across the world, organisation shall prefer software which is capable to cater to the compliance requirements. A software company selling a product that is SOX compliant is likely to find more buyers than others.
2.2 Types

Business applications can be classified based on processing type (batch, online, real-time) or source (in-house, purchased/licenced) or based on function covered. The most important assessment for the management is based on the function perform. The discussion here is restricted to business applications based on function they perform.

a. 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. Banking Application

Today all public sector banks, private sector banks, including regional rural banks have shifted to core banking business applications (referred to as CBS). Reserve Bank of India guidelines mandae which all co-operative banks also to shift to core banking applications by December 2013, means 95% plus Indian banks today 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.

c. ERP Application

These have been created as 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 maximise E^3 i.e. economy, efficiency and effectiveness of business operations.

d. Payroll Application

Many companies across the world are outsourcing these activities to professionals, any India to expectation. ERP xx TALLY have a payroll application built into it. ICAI, has also made available for its members, a payroll application.

e. Other Business Applications

i. Office Management Software
ii. Compliance Applications
iii. Customer relationship Management Software
iv. Management Support Software
v. Logistics Management Software
vi. Legal Software Management
vii. Industry Specific Applications

The applications detailed above are those which constitute major audit areas for an is auditors.

2.3 Key features and controls for business applications

Each business application is selected and implemented for a specific business purpose. An IS Auditor has to verify whether the business objective from implementing the business application is achieved or even achievable.
PART 3: CASE STUDIES

Audit Objective: To review whether the application used by the organisation is appropriate for the business purpose.

User: Bank in co-operative sector

Business Application Software: Core banking solution.

Auditor has to obtain understanding of clients business.

As per 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.

Audit shall plan include the following steps: Acquiring knowledge of the client's accounting system, policies and internal control procedures.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Applicable laws</th>
<th>Sample list of guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>As client is a bank, guideline as specified by Reserve Bank of India (referred to as RBI) shall be applicable. All accounting system needs to be in compliance with the guidelines of RBI.</td>
<td>Reserve Bank of India Act, 1934 Banking Regulation Act, 1949 Companies Act, 1956. Co-operative Act, for State</td>
</tr>
</tbody>
</table>

Audit Process

Step 1  Understand the requirement of law

a. IRAC Norms

The guidelines state that once an account has been marked as NPA, no further interest charging to be done. Guidelines state that the classification shall be borrower-wise of not facility wise, meaning that once an account of a borrower has been marked as NPA all facilities extended to the borrower are classified as NPA.

b. ALM

Detailed guidelines issue require bank to create ALCO (Asset Liability Committee) and classify each item of balance sheet (both asset and liability), in terms of their maturity.

c. Investment Guidelines

Investments need to classified as “Held To Maturity” (HTM), Held For Trade (HFT) and Available For Sale (AFS) HTM investment can be up to limit specified by RBI. Present the limit being 5%.

d. CRR and SLR

As per RBI, banks need to keep specified percentage of their time and demand liabilities in form of cash, investments, bullion.
### Step 2 Understanding the system

<table>
<thead>
<tr>
<th>Area of operation</th>
<th>Requirement</th>
<th>Questions to get answers to?</th>
</tr>
</thead>
</table>
| **a. Income Recognition and Asset Classification** | No further interest Once NPA account. | Whether system has capability to tag an advance as NPA?  
Whether the system stops calculating interest on account once tagged as NPA? |
| | NPA borrower wise not facility wise. | To check whether at the time of creation of a new customer, duplicate check is done?  
To check customer report from system identifies all facilities of the customer in the bank?  
To check whether system generates an exception report for a customer with more than one facility, when one of the facilities is marked as NPA? |
| **b. Asset Liability Management** | Classify each item of balance sheet (both asset and liability), in terms of their maturity. | Whether the CBS used has ALM module?  
Whether chart of accounts for balance sheet as specified in master, have a field to specify the maturity pattern of account?  
Whether advance recovery schedule is updated in system?  
Whether the maturity report from system is as per required format? |
| **c. Investment Guidelines** | Classification of investment | Whether the CBS used has Investment module?  
Whether master data has a field to classify investment in specified category?  
Whether the report generated is as per required format? |
| | Investment as per RBI specified limits. | Whether system allows update of RBI limits in master data? |
| | | Whether system generates exception report when the investments made are not as per RBI guidelines? |
d. CRR and SLR. RBI guidelines to maintain CRR and SLR investment. Whether the CBS has capability to generate the requisite report for CRR and SLR compliance?

Step 3 Drawing conclusions for the audit objective in hand

Above is a sample checklist for a detailed audit of business application that an IS Auditor may undertake. Above checklist is focused only on the business validity of the application selected by the organisation. Whether the organisation has proper transaction processing system and control is part of next chapter.

Step 3 Drawing conclusions for the audit objective in hand

• Answers to the above checklist will help IS Auditor assess whether the CBS selected is appropriate to meet the business requirements of the organisation.
• Where the IS auditor reaches a conclusion that many of the requirements are not being met he/she may give any of the following recommendations.
• First option: Modify the system to meet requirements of law.
• Second option: Change the ending system.
• In case the management response to option 1 is that system cannot be modified then auditor reaches second option automatically.
• Any modifications made are to be validated by proper testing C regression testing.

Case Study for participants

Audit Objective: To check whether the application used by the organisation is appropriate for the business purpose.

Business Application: The one being used by your client for accounting purpose.

Area to check: Five key business requirements to be validated.

Audit programme for planning and performing audit of business application software is given in Appendix 1: Checklist for application control review.
Module 6

2.4 Questions

1. Initial adoption of Business Model adopted by an organisation is dependent upon:
   A. Business Applications
   B. Business Objective
   C. Controls in business applications
   D. Business Laws

2. Which of the following is to be reviewed first by an IS Auditor in audit of application software is to understand:
   A. Business Application
   B. Business Controls
   C. Business Model
   D. Business Laws

3. Arrange the following in chronological order
   A. Establishing the expected degree of reliance to be placed on internal control
   B. Determining and programming the nature, timing, and extent of the audit procedures to be performed
   C. Co-ordinating the work to be performed
   D. Acquiring knowledge of the client’s accounting system, policies and internal control procedures

   The correct serial order:
   A. A, B, C, D
   B. D, A, B, C
   C. D, C, B, A
   D. B, C, D, A

4. ISACA ITAF 1202, states IS auditor needs the following for an enterprise:
   A. Inherent Risk and Audit Risk
   B. Detection Risk and Control Risk
   C. Subject Matter Risk and Audit risk
   D. None of above

5. The best definition which fits ‘COBIT 5’ is that it is a:
   A. Business framework for the governance and management of enterprise IT.
   B. System Audit Tool
   C. Management tool for corporate governance
   D. IT management tool
2.5 Answers and Explanations

1. B. Business Objectives shall be the prime reason for adoption of business models. Other answers may be valid reasons but are never the first reason for adoption of a specific business model. “A **business model** describes the rationale of how an **organisation** creates, delivers, and captures value (economic, social, cultural, or other forms of value). The process of business model construction is part of **business strategy**.”

2. C. Business Model, needs to be assessed first by IS Auditor. Then, b and d, are assessment to be made later on. As an IS Auditor it becomes important to understand the business model adopted by an organisation for a better understanding of risk associated with business model adopted by an organisation.

3. B. As per SA00SA200 on “**OVERALL OBJECTIVES OF THE INDEPENDENT AUDITOR AND THE CONDUCT OF AN AUDIT IN ACCORDANCE WITH STANDARDS ON AUDITING**, the steps to audit as mentioned at point b.

4. C. ISACA ITAF 1202, states IS auditor needs to consider subject matter risk and audit risk. Subject matter risk, relates to business risk, control risk, contract risks. Audit risk, is defined as auditor reaching incorrect conclusion after an audit. The components of audit risk being **control risk**, **inherent risk** and **detection risk**.

5. A. COBIT 5 can be best described as “Business framework for the governance and management of enterprise IT by ‘a’. Other answers are part of COBIT framework but not full Framework.
CHAPTER 2: APPLICATION CONTROL
PART 1: APPLICATION CONTROLS REVIEW

Learning Objective
To understand the implemented business application controls by organisation

1.1 Introduction
Over the last several years, organisations around the world have spent billions of dollars upgrading or installing new business application systems for reasons ranging from tactical goals, such as year 000 compliance, to strategic activities, such as using technology to establish company differentiation in the marketplace. An application or application system is software that enables users to perform tasks by employing a computer's capabilities directly. These applications represent the interface between the user and business functions. For example, a counter clerk at a bank is required to perform various business activities as part of his job and assigned responsibilities. From the point of view of users, it is the application that drives the business logic. Application controls pertain to individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting. From an organisational perspective, it is important that application controls:

- Safeguard assets
- Maintain data integrity
- Achieve organisational goals effectively and efficiently

1.1.1 Application controls
As per COBIT's management guide: “Application controls are a subset of internal controls that relate to an application system and the information managed by that application. Timely, accurate and reliable information is critical to enable informed decision making. The timeliness, accuracy and reliability of the information are dependent on the underlying application systems that are used to generate process, store and report the information. Application controls are those controls that achieve the business objectives of timely, accurate and reliable information. They consist of the manual and automated activities that ensure that information conforms to certain criteria—what COBIT refers to as business requirements for information. Those criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.”

1.1.2 Internal controls
The Committee of Sponsoring Organisations of the Treadway Commission (COSO) defines internal control as: “Internal control is a process, affected by an organisation's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations”
COSO defines control activities as the policies and procedures that help ensure management directives are carried out.

1.2 Objectives of application control and key business information requirements

1.2.1 Objectives

COBIT states that application controls are intended to provide reasonable assurance that management’s objectives relative to a given application have been achieved. Management’s objectives are typically articulated through the definition of specific functional requirements for the solution, the definition of business rules for information processing and the definition of supporting manual procedures. Examples include:

i. **Completeness**: The application processes all transactions and the resulting information is complete.

ii. **Accuracy**: All transactions are processed accurately and as intended and the resulting information is accurate.

iii. **Validity**: Only valid transactions are processed and the resulting information is valid.

iv. **Authorisation**: Only appropriately authorised transactions have been processed.

v. **Segregation of duties**: The application provides for and supports appropriate segregation of duties and responsibilities as defined by management.

1.2.2 Information Criteria

Key business requirements for information also called as information criteria that these quality parameters need to be present in information generated. These are:

1. **Effectiveness**: Deals with information being relevant and pertinent to the process as well as being delivered in a timely, correct, consistent and usable manner

2. **Efficiency**: Concerns the provision of information through the optimal (most productive and economical) use of resources

3. **Confidentiality**: Concerns the protection of sensitive information from unauthorised disclosure

4. **Integrity**: Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations

5. **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.

6. **Compliance**: Deals with complying with the laws, regulations and contractual arrangements to which the process is subject, i.e., externally imposed business criteria as well as internal policies

7. **Reliability**: Relates to the provision of appropriate information for management to operate the organisation and exercise its fiduciary and governance responsibilities
The specific key quality requirements may vary for different organisations based on specific business needs.

1.2.3 Application controls objectives

COBIT provides best practices for application controls which can be used as a benchmark for implementing or evaluating application controls. The COBIT 4.1 control objectives and control practices provides the best collection of controls which are generic and can be customised and used as benchmark for implementation or used as assessment criteria for any application audit. COBIT defines six control objectives for application controls:

1. **Source Data Preparation and Authorisation**: Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input from design. Detect errors and irregularities so they can be reported and corrected.

2. **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.

1. **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.

2. **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.

3. **Output Review, Reconciliation and Error Handling**: Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient and protected during transmission; verification, detection and correction of the accuracy of output occur; and information provided in the output is used.

4. **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.

1.2.4 Control practices

Illustrative control practices for the control objectives as per COBIT 4.1 are given below. Under each of the control objectives, there are list of control practices which need to be implemented to meet the control objectives. The control practices are to be customised and implemented as per specific requirements of the organisation. Once the control practices of specific control objective are implemented, then it can be said that the application meets the required control objectives.
Module 6

1. Source Data Preparation and Authorisation
   i. Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents.
   ii. Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.
   iii. Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures.
   iv. Ensure that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management.
   v. Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction.
   vi. Return documents that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.

2. Source data collection and entry
   i. Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria.
   ii. Use only pre-numbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents.
   iii. Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions.
   iv. Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in a timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels.
v. Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processing should continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time.

vi. Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and, where necessary, incidents are raised for more senior-level attention. Automated monitoring tools should be used to identify, monitor and manage errors.

vii. Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.

3. Accuracy, completeness and authenticity checks

i. Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately to enable efficient remediation.

ii. Implement controls to ensure accuracy, completeness, validity and compliance to regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmation.

iii. Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data.

iv. Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements.

v. Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion and do not delay processing of valid transactions.

vi. Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.

4. Processing integrity and validity

i. Establish and implement mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used.
Module 6

ii. Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks and buffer overflow.

iii. Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or prevent errors.

iv. Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled.

v. Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing.

vi. Verify the unique and sequential identifier to every transaction (e.g., index, date and time).

vii. Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made.

viii. Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems. Any changes made should be reported and approved by the business owner before they are processed.

ix. Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry.

x. Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify report and act upon out-of-balance conditions.

5. Output review, reconciliation and error handling

i. When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output.

ii. At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents.
Chapter 2, Part 1 : Cases On Application Controls

iii. Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management.

iv. Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses.

v. Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and output is handled in line with the applicable confidentiality classification. Report potential errors; log them in an automated, centralised logging facility; and address errors in a timely manner.

vi. If the application produces sensitive output, define who can receive it, label the output so it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.

6. Transaction authentication and integrity

i. Where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.

ii. Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation and allow for content integrity verification upon receipt by the downstream application.

iii. Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.
<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Information Criteria</th>
<th>Effectiveness</th>
<th>Efficiency</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Compliance</th>
<th>Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Source Data Preparation and Authorisation</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Source Data Collection and Entry</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Accuracy, Completeness and Authenticity Checks</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>4</td>
<td>Processing Integrity and Validity</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>5</td>
<td>Output Review, Reconciliation and Error Handling</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>6</td>
<td>Transaction Authentication and Integrity</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

P = Primary  
S = Secondary

Table to the relationship between the information criteria and how achievement of those criteria can be enabled by various application control objectives. Primary and secondary are the relative importance of the information criteria.
PART 2: APPLICATION CONTROLS REVIEW

An IS auditor has to be aware of the controls that have been put in place in business applications. He / She may have to review the same as a part of auditor’s risk assessment procedure. As per SA200 on “Overall Objectives of the Independent Auditor and the conduct of an audit in accordance with standards on Auditing”, compliance procedures are tests designed to obtain reasonable assurance that those internal controls on which audit reliance is to be placed are in effect. As per ISACA ITAF 1001 “Assertions”, IS Audit and assurance professional shall review the assertions against the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

2.1 Review of application control of various business application

2.1.1 Need for application control review

The review is necessary for auditor to draw the following conclusion:

a. How much reliance he/she can put on entities business application system?
b. IS Auditor also to plan his/her other audit procedures.
c. In case application controls are found in effective to achieve the stated business objectives, then IS Auditor need to plan for alternate audit procedure?

2.1.2 How to perform application review?

As per ISACA ITAF 1205 “Evidences”, IS Auditor has to select most appropriate procedure to gather evidence depending on the subject matter being audited: The procedures used to obtain evidence include:

1. Inquiry and confirmation
2. Re-performance
3. Recalculation
4. Computation
5. Analytical Procedures
6. Inspection
7. Observation
8. Other Generally Accepted Methods

2.2 Review of business application controls through use of audit procedures

As per SA 500, “Audit Evidences”, auditor while designing tests of controls shall see whether the controls so put in place are effective.
Module 6

2.3 Application controls review for specialised system

Changes in technology are very fast. A separate section for these systems has been incorporated to help IS Auditor put a focused approach to audit of these systems.

2.3.1 Artificial Intelligence (AI)

A computer is an electromechanical machine that contains no live elements. However, it is used for simulating human working which involves thinking and reasoning, solving simple and complex problems, calculating, etc. Computer history shows that computers are good at making calculations of repetitive nature speedily. In fact, in the beginning, computers were used mainly for this purpose. The applications of AI can be classified into three major categories:

i. **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.

ii. **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.

**IS Auditor’s Role**

IS auditor has to be conversant with the controls relevant to these systems when used as the integral part of the organisation’s business process or critical functions and the level of experience or intelligence used as a basis for developing software. The errors produced by such systems would be more critical as compared to the errors produced by the traditional system.

2.3.2 Data Warehouse

Data warehouse is defined, “as a Subject-oriented, integrated, time-variant, non-volatile, collection of data in support of management’s decision making process. It is a Central Repository of clean, consistent, integrated & summarised information, extracted from multiple operational systems, for on-line query processing.”
Data warehousing system is used for getting valuable information for making management decisions. Generally, data is processed by TPS (Transaction Processing System), also known as operational systems. These systems are responsible for day-to-day functioning of business transactions.

Customers depositing and withdrawing money, applying for loans, opening accounts in a bank are examples of Transactions Processing System. The data associated with these transactions is stored in database management system and presented to users or programmes whenever required. These systems process data either in a batch mode or in a real-time manner (e.g., when we book a railway seat we are presented with a ticket immediately).

**IS Auditor’s Role**

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

**2.3.3 Decision Support System (DSS)**

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. Typical examples are:

1. Comparative sales figures between two consecutive months for different products with percentage variation to total sales.
2. Revenue and cost projections on the basis of a product mix.
3. Evaluation of different alternatives, leading to the selection of the best one.

**IS Auditor’s role**

As the system shall be used for decision making purpose of the management,

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
2.3.4 Electronic Fund Transfer (EFT)

The electronic mode of payment which has made a lot of impact to the way India does business. All big, medium and small businesses, banks, users, governments, government departments, logistics, customers, service receivers, service providers, exporters, importers, sellers, buyers, use EFT for their business and personal transaction. LIFE without EFT seems impossible. Immense growth of EFT has led to a new set of risk associated with such transactions. Reserve Bank of India (RBI) has issued detailed guidelines for banks to follow for EFT transactions. RBI has specified in its NEFT guidelines that, Banks need to create procedural guidelines, for the purpose of:

i. Verifying that a payment instruction, a communication authorising a payment instruction or an NEFT Data File is authorised by the person from whom it purports to be authorised; and

ii. For detecting error in the transmission or the content of a payment instruction, a communication or an NEFT SFMS message.

IS Auditor’s role

The major concern shall be:

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.

2.3.5 E-commerce

Other than buying and selling goods on the Internet, E-Commerce (Electronic Commerce) involves information sharing, payment, fulfilment and service and support.

Risks of E-commerce

1. Confidentiality of message
2. ID of organisation of the sender
3. Integrity of the message
4. Non Acceptance of confidentiality by receiver
5. Non Repudiation by sender of having sent the message

IS Auditor’s role

IS Auditor’s responsibility shall be to see whether the transactions have:

1. Authorisation
2. Authentication
3. Confirmation
2.3.6 **Point of Sale System (PoS)**

As the name indicates, 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. They provide significant cost and time saving as compared to the manual methods. They also eliminate errors that are inherent in manual system (when a user is subjected to make transcription error while entering data from a document into system). POS may involve batch processing or online processing. These are generally observed in the case of big shopping malls or departmental shops.

**IS Auditor’s role**

1. In case there is batch processing, the IS auditor should evaluate the batch controls implemented by the organisation
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.
6. RBI guidelines regarding ‘Cash withdrawal at Point of Sale (POs) - Prepaid Payment Instruments issued by banks: need to be validated in case such transactions are taking place.

2.3.7 **Automatic Teller Machines (ATM)**

An ATM (Automated Teller Machine) is a specialised form of the point of sale terminal. It is designed for unattended use by a customer of a financial institution. The ATMs generally allow cash deposits, cash withdrawals and a range of banking operations like requesting cheque books or account statements. ATMs are generally used for use after the closing hours of the financial institution and can be located either adjacent to the location of the financial institution or at a distant place. The facility of ATM can be within a bank, across local banks and amongst the banks outside a region. ATMs transfer information and money over communication lines. These systems provide a high level of logical and physical security for both the customer and the ATM machine.

**IS Auditor’s Role**

The following are the guidelines for internal controls of ATM system which the auditor shall have to evaluate and report:

a. Only authorised individuals have been granted access to the system.

b. The exception reports show all attempts to exceed the limits and reports are reviewed by the management.

c. The bank has ATM liability coverage for onsite and offsite machines

d. Controls on proper storage of unused ATM cards, Controls on their issue only against valid
Module 6

application form from a customer, Control over custody of unissued ATM cards, Return of old/ unclaimed ATM cards, Control over activation of PINs

e. Controls on unused PINs, Procedure for issue of PINs, Return of PINs of returned ATM cards.

f. Controls to ensure that PINs do not appear in printed form with the customer’s account number.

g. Access control over retrieval or display of PINs via terminals

h. Mail cards to customers in envelopes with a return address that do not identify the Bank. Mail cards and PINs separately with sufficient period of time (usually three days) between mailings.

As on date, there are more than 1,50,000 ATM machines installations in India. Government of India has already indicated that it wants to further enhance the usage of ATM in India, as this allows bank to reach remote corners without being physically present. This creates a scope to the IS Auditor for a separate ATM Audit. RBI has issued detailed set of instructions for bank to follow. Based on those a separate ATM audit program and checklist is being attached. Please see Appendix: Checklist for ATM audit to understand different areas of an ATM audit.
PART 3: CASES STUDY ON APPLICATION CONTROLS

3.1 Proper design of source document

Case of an educational/vocational institute collecting fees from students

Issue: Improper designed source document led to improper accounting.

Impact: A senior faculty left the Institute as incentives/payoffs were not calculated properly by accounts department.

Facts: The vocational institute was being run a PE Pvt. Ltd. (Referred to as PE). PE is engaged in educating CA / CS / CWA students. PE has implemented its fees collection on TALLY. Students while paying the fees were supposed to fill a pay-in slip and deposit the fees at the counter. Faculty payoffs are based on fees collected for the subject.

<table>
<thead>
<tr>
<th>Receipt No.</th>
<th>1111</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash / Cheque</td>
<td>Date</td>
</tr>
<tr>
<td>Name of student</td>
<td></td>
</tr>
<tr>
<td>Stream: CA / CS / ICWA</td>
<td></td>
</tr>
<tr>
<td>Tick CPT/ FOUNDATION/ IPCC/ FINAL/ EXECUTIVE / PROFESSIONAL</td>
<td></td>
</tr>
<tr>
<td>Level: Tick</td>
<td></td>
</tr>
<tr>
<td>SUBJECT:</td>
<td></td>
</tr>
<tr>
<td>Cheque Details</td>
<td></td>
</tr>
<tr>
<td>Name of Bank</td>
<td>1000X</td>
</tr>
<tr>
<td>Ch. Number</td>
<td>500X</td>
</tr>
<tr>
<td>Date</td>
<td>100X</td>
</tr>
<tr>
<td>10X</td>
<td></td>
</tr>
</tbody>
</table>

Based on the slip filled above, the cashier used to enter data in TALLY.

Problem: It was found, that one of the subjects in CA and CS has same name Direct Tax Law (DTL). Many students who paid fees for CA DTL got accounted in CS DTL. The result was that at the end of period when all payoffs were cleared TALLY data was used and calculations done. The fees paid by many CA students were credited of CS students. This resulted in payment dispute and CA Final faculty for PE left the institute in a grudge. The faculty was a respected person; this affected reputation of the Institute.

Action taken: PE management was worried about the development and sought help from an IS Auditor. IS Auditor’s mandate was to look for problem and provide a solution.

IS Auditor’s Report

The IS auditor went through the whole fees collection process, the people involved and the present problem. He/she gave a two-step solution to organisation.
Module 6

First Step: Modify pay-in-slip, to include the stream (CA/CS/CWA) as another field.
Second Step: Appoint an Internal Auditor to check whether the payments of fees made by the students have been properly accounted.

Suggested Pay-in-Slip

<table>
<thead>
<tr>
<th>Receipt No.</th>
<th>1111</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash / Cheque</td>
<td>Date</td>
</tr>
<tr>
<td>Name of student</td>
<td></td>
</tr>
<tr>
<td>Stream: CA / CS / ICWA</td>
<td></td>
</tr>
<tr>
<td>Tick</td>
<td></td>
</tr>
<tr>
<td>Level: Tick</td>
<td></td>
</tr>
<tr>
<td>SUBJECT: CPT/ FOUNDATION/ IPCC/ FINAL/ EXECUTIVE / PROFESSIONAL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Student signature</td>
<td>Receiver Signature</td>
</tr>
</tbody>
</table>

Benefit to PE
1. A big problem was set right with a simple solution i.e. proper design of source document.
2. PE was relieved that such issues won’t recur.
3. An Internal Auditor was also appointed to re-check the daily entries made.

3.2 Exception reporting

These are special reports generated by business application to highlight issues/items which are not the correct domain. For example: Exception reporting in TALLY:

How to generate the report? The command on GATEWAY OF TALLY: DISPLAY AND EXCEPTION REPORTS:

What items are displayed? The screen shot lists items that are reported as exception in TALLY. These include
- Negative Stock
- Negative Ledger and more.

What is the meaning of negative ledger? The word negative ledger means that the ledger account is not its correct domain. Correct domain means, for example the domain for CASH is debit, but if it is credit, the system shall show it as negative ledger. The same is true for a debtor’s ledger with credit balance or creditor’s ledger with debit balance.
3.2.1 What is the benefit?

Users, which include management, auditor's, IS Auditors can directly generate these reports and check as to accuracy of accounting.

3.2.2 What is the loss if above items are not checked?

a. Section 69C of Income Tax Act, 1961: Unexplained expenditure, etc.:

Where in any financial year an Assessee has incurred any expenditure and the offers no explanation about the source of such expenditure or part thereof, or the explanation, if any, offered by him is not, in the opinion of the Assessing Officer, satisfactory, the amount covered by such expenditure or part thereof, as the case may be, may be deemed to be the income of the Assessee for such financial year. **Above negative balance can be treated as Income.**

b. It reflects poor accounting controls, and can lead to losses due to frauds.

Exercise: Kindly comment upon: Q.1 The type of error?

a. Input
b. Process
c. Output
d. None of Above
Q.2. What is a better solution possible to the above problem?

2. Exception reporting in bank:

Case for participants

DISA participants are expected to comment on one of the items reported in bank's daily exception reports.

3.3 Case for Dependency check

Case of validating two related field of employee database

Facts: A company is held guilty of employing underage employees. The authorities send a notice to the company. The notice is based on data submitted by the company as a part of its annual return under labour laws.

The notice states that as per details made available by the company 10 employees have been found to be underage as the time difference between date of birth and date of employment is less than 18 years. Company responds by saying that it is basically a data entry problem in system from where the said return has been made. The company has to physically parade the 10 employees to the department to convince them that they are not underage.

Action Taken: After so much of embarrassment company decides to appoint an IS Auditor to find the problem and solution.
Report of IS Auditor
After studying the system and the problem faced IS auditor suggested the following:

1. System needs to be updated/modified so that it does not allow underage employee updates.
2. An internal system to validate each new addition to employee payroll.

Exercise
Q.1 The best way to define the error is:
   a. Input error
   b. Process error
   c. Output error
   d. Design error

3.4 Reasonableness Check
Case of Purchase Order in excess of five times vendor’s annual sale
Facts: The Company is engaged in manufacturing tyres. While issuing purchase order (PO) to a vendor, the clerk put 100 kgs as quantity instead of 1 kg. The result was that the PO to be made for ₹ 2/- lakhs was actually made for ₹ 200/- lakhs i.e. 100 times more. The same PO was signed by Purchase Manager and delivered to vendor by post. Looking at the PO vendor called back the company and informed that the PO is more than 5 times annual turnover of vendor himself.

Errors:
1. Lack of reasonableness check: The system must have been created to ensure that such a PO must not be released. It could be having a check on say:
   a. Maximum quantity that could be entered for purchase, or
   b. Maximum value a PO could be made.
   c. Maximum quantity PO that could be sent to a vendor, or
   d. A better definition by management.
2. Purchase Manager’s poor work.
3. No cross check system built in.

Exercise:
Q.1 Reasonableness verification control is a control at which part of application process?
   a. Input
   b. Process
   c. Output
   d. None of above
3.5 Case to highlight necessity of duplicate check

Case of double payment made to vendors against one purchase invoice.

**Facts:** A company using local made accounting software. While entering transactions, the software allowed user’s to create new ledgers by a command ALT+N. The system being used check duplicate ledgers for 100% same name. Any alteration in name or change in case was not tracked. While entering a purchase invoice the data entry operator created a new ledger without checking the existence of previous ledger. Later on it was found that a double payment was made to the vendor as the said purchase was against an advance payment and another payment was released based on new entry.

**Errors:**
1. Lack of user controls. Data entry operator can create ledger.
2. Lack of **duplicate check**.
3. Lack of internal controls, to see how duplicate entries are in system.

**Exercise:** Q.1 What is the best solution to the problem?

3.6 Obsolete stock reporting

In TALLY from gateway of tally through the following set of commands company can get report on non-moving/obsolete stock.

Gateway of TALLY: Press Display> Press Inventory books> Press Ageing Analysis: This shall show the following report:

How does the report help?
1. Helps assess the quality of inventory.
2. Basis for valuation of inventory, as non-moving/obsolete stock may be valued at net realizable value.
3.7 Report on Sales below cost price

From GATEWAY OF TALLY following command shall provide the above mentioned report:

a. Gateway of TALLY: Display>Inventory Books>Stock Item: Then select the item from list and press F7, which shows the profit/loss on items sold. Above details can also be seen through

b. Gateway of TALLY: Display>Account Books>Sales Register: Then select the month for which sales need to be displayed and press F7, which shows the profit/ loss on items sold.

Benefits of the report:
1. Management tool for performance analysis.
2. Any fraud done can be checked through the same.

3.8 Report on TDS deducted but not remitted on time

Gateway of TALLY: Display>Statutory Report>TDS Report>Outstandings>TDS Payables: The following report is displayed:

Benefits of the report:
1. Management tool for performance analysis.
2. Timely compliance can be ensured.
3.9 Questions

1. Application controls shall include all except
   A. Application controls are a subset of internal controls.
   B. The purpose is to collect timely, accurate and reliable information.
   C. It is part of the IS Auditor’s responsibility to implement the same.
   D. It is part of business application software.

2. As per Income tax Act, 1961 and banking norms, all fixed deposit holders of bank need to submit their PAN or Form 60/61 (a form as per Income Tax Act/Rules). Bank in its account opening form, has not updated the need for Form 60/61 in case PAN is not there. This defines which control lapse as per COBIT.
   A. Source Data Preparation and Authorisation:
   B. Source Data Collection and Entry
   C. Accuracy, Completeness and Authenticity Checks
   D. Processing Integrity and Validity

3. In a public sector bank while updating master data for advances given, the bank employee does not update “INSURANCE DATA”. This includes details of Insurance Policy, Amount Insured, Expiry Date of Insurance and other related information. This defines which control lapse as per COBIT.
   A. Source Data Preparation and Authorisation:
   B. Source Data Collection and Entry
   C. Accuracy, Completeness and Authenticity Checks
   D. Processing Integrity and Validity

4. E-mailed purchase order for 500 units was received as 5000 units. This defines which control lapse as per COBIT.
   A. Source Data Collection and Entry
   B. Accuracy, Completeness and Authenticity Checks
   C. Output Review, Reconciliation and Error Handling
   D. Transaction Authentication and Integrity

5. An IS Auditor, processes a dummy transaction to check whether the system is allowing cash payments in excess of ₹ 20,000/-. This check by auditor represents which of the following evidence collection technique?
   A. Inquiry and confirmation
   B. Re-calculation
   C. Inspection
   D. Re-performance
6. While auditing e-commerce transactions, auditor’s key concern includes all except:
   A. Authorisation
   B. Authentication
   C. Author
   D. Confirmation

7. RBI instructed banks to stop cash retraction in all ATMs across India from April 2013. This was result of few ATM frauds detected. This action by RBI can be best classified as:
   A. Creation
   B. Rectification
   C. Repair
   D. None of above

8. Non-repudiation relates to all terms except one:
   A. Right to deny withdrawal
   B. Digital Signatures
   C. E-commerce
   D. None of above

9. Company’s billing system does not allow billing to those dealers who have not paid advance amount against proforma invoice. This check is best called as:
   A. Limit Check
   B. Dependency Check
   C. Range Check
   D. Duplicate Check

10. While posting message on FACEBOOK, if user posts the same message again, FACEBOOK gives a warning. The warning indicates which control.
    A. Limit Check
    B. Dependency Check
    C. Range Check
    D. Duplicate Check
3.10 Answers and Explanations

1. C. Represents what auditor verifies but not that what he/she implements. Rest is part of definition and purpose of application controls.

2. A. is the correct answer as the source data capture is not proper. Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input from design.

3. C. This ensures 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.

4. D. is the correct answer. As per COBIT, where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.

5. D. IS Auditor may process test data on application controls to see how it responds.

6. C. Is correct. Others are key concerns of an IS auditor while auditing e-commerce transactions.

7. B. is the right answer. A, is not an answer as action by RBI is based on fraud detection. Repair is done to rectify an error which has occurred in a working system.

8. D. is the correct answer. The other options are related to non-repudiation. A, is definition of word. B, digital signatures create non-repudiation. E-commerce transactions need it (non-repudiation) for execution of contract.

9. B. Dependency check is one where value of one field is related to that of another.

10. D. is the answer as this is a duplicate check.
CHAPTER 3: AUDITING APPLICATION CONTROL
PART 1: AUDIT PROGRAMME FOR REVIEW OF APPLICATION SOFTWARE

Learning Objectives
To provide assurance on business application software and the controls put in place, through business application audit.

1.1 Introduction
The role of information System audit has become a critical mechanism for ensuring the integrity of information and the reporting of organisation finances to avoid and hopefully prevent future financial fiascos such as Satyam in recent years. Electronic infrastructure and commerce are integrated in business process around the globe. There is a need to control and audit using IS to avoid such kind of scam in near future. Today the business processes are tightly integrated to systems. In few organisations the level of integration is that when systems are off, business is off. In such a scenario it is important to ensure that systems are working properly and nothing is there to affect the working of system. The way businesses are integrated to system, any audit shall be preceded by system audit, as proper working of system is necessary to proper working of business. It shall be great risk being taken by a pure financial auditor to submit his/her report without going through the system audit report of the organisation for which financial audit is being done.

1.2 Why IS Audit?
Case to highlight “NPA provisioning in system may be wrong
Issue: NPA provisioning as per RBI guidelines.
Objective: To learn that system audit as an exercise needs to precede financial audit.
Location: Public Sector Bank using a CBS.
Reference: RBI guidelines for Income Recognition and Asset Classification.
[RBI/2013-14/62:DBOD.NO.BP.BC.1/21.01.048/2013-14/1.013]
Specific Point: Provision to be made for sub-standard assets, where the advance as per nature is unsecured. The guidelines state that a provision of @25% has to be made of total out standing. This is an exception to general rule of provision @15%. The exception is created as the advance is basically unsecured in nature. For example: Credit Card o/s turning sub-standard. This advance is unsecured in nature.
Point to remember: The provision is on total o/s, not on the amount of outstanding. As the advance is an unsecured advance.
Auditor observation:
Auditor observed that for credit card outstanding of ₹ 1,00,000/- the branch had made a provision @15% of outstanding amount, as reflected from system generated Non-Performing-Asset statement. The issue was brought to notice of branch manager. The interaction between the bank employees and the action taken by auditor is shown in the matrix below.

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Query Made to and nature of query.</th>
<th>Response from person at bank</th>
<th>Auditor Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Branch Manager (BM): The provision is not as per RBI guideline.</td>
<td>BM: The bank supplied data to regional office. The calculations have been made the regional office. No fault of branch.</td>
<td>Take to next level</td>
</tr>
<tr>
<td>2</td>
<td>Regional Manager (RM): The provision is not as per RBI guideline.</td>
<td>RM: The regional office only fed data in the software supplied by HO. No fault of regional office.</td>
<td>Take to next level.</td>
</tr>
<tr>
<td>3</td>
<td>Assistant General Manager (IT) of the bank: AGM (IT): The provision is not as per RBI guideline.</td>
<td>AGM (IT): Accepts the problem in software.</td>
<td>Qualify the main report.</td>
</tr>
</tbody>
</table>

Learning from the above
1. For Bank: Above means that if the banks unsecured sub-standard advances are to the tune of ₹ 10/- crore, bank shall be making short provision of ₹ 1/- crore against its NPAs.
2. For Auditor:
   a. Branch auditor had to qualify the main audit report.
   b. Branch auditor would be within his/her rights to ask bank to supply the system audit report of the software being used by the bank for calculating the NPA status and provisions thereon.
3. For us: Case helps us understand that 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.

IS auditing is an integral part of the audit function because it supports the auditor’s judgment on the quality of the information processed by computer systems. Initially, auditor with IT audit skills are viewed as the technological resource for the audit staff. The IS auditor’s role has evolved to provide assurance that adequate and appropriate controls are in place. The audit’s primary role, except in areas of management advisory services, is to provide a statement of assurance as to whether adequate and reliable internal controls are in place and are operating in an efficient and effective manner. Therefore, whereas the management is to ensure, auditors are to assure.
1.3 What is IS Audit?

An information technology audit, or information systems audit, is an examination of the controls within an Information technology (IT) infrastructure. An IS audit is the process of collecting and evaluating the evidence of an organisation's information systems, practices, and operations. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively and efficiently to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The IT audit's agenda may be summarised by the following questions:

1. Will the organisation's computer systems be available for the business at all times when required? (Availability)
2. Will the information in the systems be disclosed only to authorised users? (Confidentiality)
3. Will the information provided by the system always be accurate, reliable, and Timely? (Integrity)

The IS audit focuses on determining the risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. By implementing controls, the effect of risks can be minimised, but cannot completely eliminate all risks.

As per ISACA ITAF 1007 “Assertions”, IS Audit and Assurance professional shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

Information Systems Audit is often misunderstood as a mere technical audit and a domain of Information Technology professionals. On the contrary, Information Systems Audit involves evaluating the adequacy and efficiency of internal controls in business processes that are either partly or fully computerised. Hence, Audit and control professionals who have expertise in understanding of business processes and internal controls with exposure to information technology risks and controls are considered the most appropriate professionals to conduct information systems audits. Therefore, depending on the audit environment, objectives and scope, the audit could involve the audit of entire business processes, partially or fully automated, or audit of specified application, technology and related controls.

1.4 How to perform IS Audit?

The fundamental principles of audit do not change with change in the audit subject, however, the perspective of audit and the methods, tools and techniques to achieve the audit objectives do undergo a change. As in a financial audit, audit focus is on the risk arising from inadequate or inefficient controls on recording of transactions which could result in misstatement of financial statements. In an Information Systems Audit the focus is on the risks arising from the use of information technology in carrying out business processes.

ISACA ITAF 1008 “Criteria”, specifies that IS Audit assurance criteria should consider the source for which the IS Audit is being done and the potential audience. For example, when dealing with government regulations criteria based on assertions developed from legislation and regulations shall apply to the subject matter may be most appropriate. Sources of criteria may be:
1. Established by ISACA: These are publicly available criteria.
2. Those established by other expert bodies: Like those created by SYSTRUST certification body.
3. Established by laws and regulations: For example the one discussed in case above relating to RBI guidelines.
4. Developed specifically for IS Audit or Assurance engagement.

Above shall help decide on the key objective for an IS Audit.

Audit Objective: The entire audit programme and methodology depends upon the audit objective and scope. The objective of the IS audit is to evaluate an auditee’s computerised information system (CIS) in order to ascertain whether the CIS produces timely, accurate, complete and reliable information outputs as well as ensuring confidentiality, integrity, availability and reliability of the data.

1.5 Audit mission

Establishing an IS audit function may be critical in organisations that are specifically dependent on Information Technology. The IS audit function could be established either within the organisation as an internal department or the function could be fully or partly outsourced to an external agency. In either case there are certain fundamental principles that should be taken into consideration. The mission statement defines the primary purpose of the audit function and provides an overview of the focus, priorities, values and principles that will measure audit decisions. It also outlines the value addition that will be provided and clarifies the purpose and meaning for the audit function. IS audit function reviews the reliability and integrity of information, compliance with the policies and regulations, and the processes for safeguarding of assets, as well as to make suggestions for improvements in operating efficiencies and internal controls? It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The audit mission statement may vary between various organisations and audit functions.

1.6 Performing an IS Audit

The detailed concepts and practice of IS Audit are covered in detail in Module 3: IS Assurance services. However, some of the key concepts and practice are summarised here in the context of application audit. The standards of IS Audit provided by ISACA in ITAF 1200 on performance standards outline the following steps for performing an IS audit as under:

i. **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.

ii. **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.

iii. **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.

iv. **Materiality:** IS audit and assurance professionals shall consider potential weaknesses or absences of controls while planning an engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness. IS audit and assurance professionals shall consider materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures. IS audit and assurance professionals shall consider the cumulative effect of minor control deficiencies or weaknesses and whether the absence of controls translates into a significant deficiency or a material weakness.

v. **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.

vi. **Using the Work of Other Experts:** IS audit and assurance professionals shall consider using the work of other experts for the engagement, where appropriate. IS audit and assurance professionals shall assess and approve the adequacy of the other experts’ professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement. IS audit and assurance professionals shall assess, review and evaluate the work of other experts as part of the engagement, and document the conclusion on the extent of use and reliance on their work.

vii. **Irregularity and Illegal Acts:** IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement. IS audit and assurance professionals shall maintain an attitude of professional scepticism during the engagement. IS audit and assurance professionals shall document and communicate any material irregularities or illegal act to the appropriate party in a timely manner.
1.7 Steps of IS Audit

<table>
<thead>
<tr>
<th>Gather Information and Plan</th>
<th>Obtain Understanding of Internal Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Knowledge of business and industry</td>
<td>• Regulatory statutes</td>
</tr>
<tr>
<td>• Prior year’s audit results</td>
<td>• Inherent risk assessments</td>
</tr>
<tr>
<td>• Recent financial information</td>
<td>• Control risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Equate total risk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perform Compliance Tests</th>
<th>Perform Substantive Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify key controls to betested</td>
<td>• Analytical procedures</td>
</tr>
<tr>
<td></td>
<td>• Detailed tests of account</td>
</tr>
<tr>
<td></td>
<td>• Other substantive audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conclude the Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Create recommendations.</td>
</tr>
</tbody>
</table>

1.8 Audit programme for key business application

Detailed checklist for auditing business application software is given in Appendix 3.

1.9 Computer Assisted Audit Techniques

CAAT is a significant tool for auditors to gather evidences independently. It provides a mean to gain access and to analyse data for a predetermined audit objective, and report the audit findings with evidences. It helps the auditor to obtain evidence directly on the quality of records produced and maintained in the system. The quality of the evidence collected gives reassurance on the quality of the system processing such transactional evidences.

1.9.1 Needs for CAAT

During the course of the audit an IS auditor should obtain sufficient, relevant and useful evidence to effectively achieve the audit objectives. The audit findings and conclusions have to be supported by appropriate analysis and interpretation of this evidence. Computerised information processing environments pose a challenge to the IS auditor to collect sufficient, relevant and useful evidence, since the evidence exists on magnetic media and can be examined only by using CAATs. With systems having different hardware and software environments, different data structure, record formats, processing functions, etc., it is almost impossible for the auditors to collect evidence and analyse the records without a software tool. Owing to resource constraints and the ever changing audit objectives, it is almost impossible to quickly develop audit capabilities, without using audit software like CAATs.
Chapter 3, Part 1 : Audit program for review of application software

The ICAI Guidance note on CAAT describes CAATs as important tools for the auditor in performing audits. CAATs may be used in performing various auditing procedures including the following:

a. Tests of details of transactions and balances, for example, the use of audit software for recalculated interest or the extraction of invoices over a certain value from the computer records.

b. Analytical procedures, for example, identifying inconsistencies or significant fluctuations.

c. Tests of general controls, for example testing the set up or configurations of the operating system or access procedures to the programme libraries or by using code comparison software to check that the version of the programme in use is the version approved by management.

d. Sampling programmes to extract data for audit testing

e. Tests of application controls, for example, testing the functionality of a programmed control.

f. Re-performing calculations performed by the organisation’s accounting system.

1.9.2 Types of CAAT

While selecting the CAAT, IS Auditor is faced with certain critical decisions that he/she may be required to make, while balancing on the quality and cost of audit:

a. Use the audit software developed by the client.

b. Design and develop his /her own audit software.

c. Use a standard off the shelf Generalised Audit Software

The first two options require the auditor to be technically competent in programming and its methodology, which may not be his area of expertise. Computer audit software also known as Generalised Audit Programmes (GAS) is readily available off-the-shelf software with specific features useful for data interrogation and analysis. The auditors do not require much expertise knowledge to be able to use for auditing purpose

The various types of CAATs can be categorised as follows:

1. Generalised Audit Software

2. Specialised Audit Software

3. Utility Software

A brief description of the types of software is given below:

1. Generalised Audit Software (GAS)

Computer audit software may be defined as: “The processing of a client’s live files by the auditor’s computer programmes”. Computer audit software may be used either in compliance or substantive tests. Generalised Audit Software refers to generalized computer programmes designed to perform data processing functions such as reading data, selecting and analysing information, performing calculations, creating data files and reporting in a format specified by the auditor. The use of Generalised Audit Software is perhaps the most widely known computer assisted audit technique.
Module 6

GAS has standard packages developed by software companies exclusively for auditing data stored on computers. These are economical and extensively used by auditors the world over. Available off the shelf, GAS can be used for a wide range of hardware, operating systems, operating environments and database.

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. Totalling 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

2. Specialised Audit Software (SAS)

Specialised Audit Software, unlike GAS, is written for special audit purposes or targeting specialised 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 specialised audit software, the auditor should take care to get an assurance on the integrity and security of the software developed by the client...

3. Utility Software

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.

1.9.3 Typical Steps in using GAS

i. Define the audit objectives
ii. Identify the tests that the package can undertake to meet the objectives.
iii. Make out the package input forms for the tests identified.
iv. Compile the package on the computer, clearing reported edit errors.
v. If a programmer has been adding coded routines to the package to fill out the input forms or to advice, the programmer’s work must be tested.
vi. Obtain copies of the application filed to be tested.

vii. Attend the execution of the package against these copy files.

viii. Maintain security of the copy files and output until the tests have been fully checked out.

ix. Check the test results and draw audit conclusions.

x. Interface the test results with whatever subsequent manual audit work to be done.

Refer case at the end of chapter on the above steps:

1.9.4 Selecting, implementing and using CAATs

Computer Assisted Audit Techniques (CAATs) are a significant tool for auditors to gather evidence independently. CAATs provide a means to gain access and analyse data for a predetermined audit objective and to report audit findings with evidence. They help the auditor to obtain evidence directly on the quality of the records produced and maintained in the system. The quality of the evidence collected confirms the quality of the system processing. The following are some examples of CAATs, which can be used to collect evidence:

- ACL, IDEA etc.
- Utility Software such as Find, Search, flowcharting utilities
- Spreadsheets such as Excel
- SQL Commands, OS Commands
- Third party access control software
- Application systems
- Options and reports built in as part of the application/systems software
- Performance monitoring tools
- Network management tools, OS utilities
- High end CAATs
- RSAREF, DES, PGP
- TCP Wrapper, SOCKS, TIS Toolkit
- COPS, Tripwire, Tiger
- ISS, SATAN, etc.

1.10 Continuous Auditing Approach

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. In the traditional method, the scope for market influence on the information contained in the audit report is less due to

- The time gap between the audit and reporting
- The deficiencies identified in the control systems can be rectified even by the management during the time gap.
1.10.1 Techniques for Continuous Auditing

1. Snapshot

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.

Let us consider, for example, a banking transaction. Numerous transactions are effected and processed by various application systems in a banking environment. While all applications are tested before being deployed, in an integrated computing environment, a cash withdrawal at the ATM may be processed by more than one software working in an integrated manner. In the event of some errors in transactions being detected or suspected, snapshot software installed as part of the production environment would continuously take pictures of transactions passing a particular control point e.g. instruction set executed in the memory of the ATM machine for processing withdrawal. Hence the error in code/ instruction can be pinpointed and identified by the snapshot software.

Snapshots are employed in the following:

- They are used for analysing and tracking down the flow of data in an application programme, so as to know the underlying logic of the data processing software.
- For documenting the logic, input/output controls (or conditions) of the application programme and the sequence of processing.

Snapshots are generally deployed for tracking down the reasons for any disruption in the functioning of application or system software like operating system or database system.

Case at the end of this part: SNAPSHOT for payroll process.

2. Integrated Test Facility (ITF)

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. The approach could also involve setting a separate dummy organisation using the application software in the live environment. ITF is useful in identifying errors and problems that occur in the live environment and that cannot be traced in the test environment. However the disadvantage in using ITF is that the dummy transactions also append to the live database and hence will impact the results and reports drawn from the live database. It will therefore, be necessary to delete the test transaction from the system once the test is performed. As with all test packs, the output produced is compared with predicted results. This helps to determine whether the programmed procedures being tested are operating correctly.
Case at the end of this part: Stores and Purchase programme testing through ITF.

3. System Activity File Interrogation

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. Where a suitable system activity file is retained on magnetic media, one can select and report exceptional items of possible audit interest such as unauthorised access attempts, unsuccessful login attempts, changes to master records and the like. Similar implementation is also possible by embedding special audit software in application software that maintains continuous transaction logs at various points in the application software. This technique is also referred to as the Systems Control Audit Review File. The files can be further analysed to determine deviations and improper transactions.

4. Embedded Audit Facilities

Embedded audit facilities consist of programme 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.

This technique generally uses one or more specially designed modules embedded in the computer application system to select and record data for subsequent analysis and evaluation. The data collection modules are inserted in the application system or programme at points predetermined by the auditor. The auditor also determines the criteria for selection and recording. Automated or manual methods may be used to analyse the data later. This is intended to highlight unusual transactions, which can be later taken up for scrutiny. Please refer to the case of listing cash payments in excess of ₹ 20,000/- through use of range function in TALLY discussed in detail in Chapter 1.

5. Continuous and Intermittent Simulation

With significant advancements in technologies, business systems are increasingly driven by client-server systems with distributed computing and databases. The components of such systems are networked generally over geographically disparate locations. This has resulted in the need for auditing systems that not only enable continuous auditing of transactions but also have a low overhead on the IT resources of the auditee but without compromising on the independence of such systems. This has resulted in the use of continuous auditing techniques that the client-server environment to enable independent simulation of “suspect” transactions independently by the simulation audit software under the control of the auditor but using the online data of the auditee waiting to be written to the database. Please note this case is part of PT. Please refer to reference material which includes the publication: Data analysis for an auditor which has detailed case studies on using CAATs. Please also refer to Module-2 which has explanation on CAATs.
1.11 Case on using MS Excel to find Duplicate/Missing Sales Invoice

Objective: The case is to help understand the steps of using CAATs.

Facts: Company using TALLY has selected manual invoice numbering as an option in TALLY. The option is available when user creates/configures Vouchers.

Problem: Management action of selecting manual invoice numbers, for data entry purpose raises the following risks:
- Duplicate
- Missing invoice number.

IS Auditor’s concern: To identify a mechanism to track the missing/duplicate invoice number.

Using Audit tools to achieve the above audit objectives:

a. Through use of Excel: Discussed here
b. Through use of IDEA, the generalised audit tool: Part of online demo in PT.

1.11.1 Steps to be performed in above case through use of excel

i. Define the audit objectives: To identify duplicate/missing invoice number.

ii. Identify the tests that the package can undertake to meet the objectives. The objective is to identify duplication/missing invoice number through use of excel.

iii. Make out the package input forms for the tests identified. No separate input form required. TALLY exports data directly in excel. This is a good control as it reduces the risk of discrepancy occurring during the system hand over process.

iv. Compile the package on the computer, clearing reported edit errors. Display the sales register from TALLY and export the same to excel.

v. If a programmer has been adding coded routines to the package to fill out the input forms or to advice, the programmer’s work must be tested. Not applicable in the instant case.

vi. Obtain copies of the application file to be tested. Before testing on excel a copy of report kept separately.

vii. Attend the execution of the package against these copy files.: Execution includes the following steps:
- Index the excel sheet in ascending order, based on Invoice number.
- Insert an additional column to the right side of invoice number.
- Put the rule Invoice number (Row Next) - Invoice number (current row). The same shall appear like:
### Chapter 3, Part 1: Audit program for review of application software

<table>
<thead>
<tr>
<th></th>
<th>Invoice number</th>
<th>Inserted column</th>
<th>Result of command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10001</td>
<td>=A3-A2</td>
<td>1.00</td>
</tr>
<tr>
<td>3</td>
<td>10002</td>
<td>=A3-A4</td>
<td>1.00</td>
</tr>
<tr>
<td>4</td>
<td>10003</td>
<td>=A4-A5</td>
<td>2.00</td>
</tr>
<tr>
<td>5</td>
<td>10005</td>
<td>=A5-A6</td>
<td>1.00</td>
</tr>
<tr>
<td>6</td>
<td>10006</td>
<td>=A6-A7</td>
<td>0.00</td>
</tr>
<tr>
<td>7</td>
<td>10006</td>
<td>=A7-A8</td>
<td>1.00</td>
</tr>
<tr>
<td>8</td>
<td>10007</td>
<td>=A8-A9</td>
<td>1.00</td>
</tr>
<tr>
<td>9</td>
<td>10008</td>
<td>=A9-A10</td>
<td></td>
</tr>
</tbody>
</table>

*Reading the above: Where the value of column C is other than ‘1’, it means there is a problem with invoice numbering. Above is one way of doing the same in excel, there could be multiple ways of getting the audit conclusions in excel.*

viii. Maintain security of files and output until the tests have been fully checked out: *Important to remember.*

ix. Check the test results and draw audit conclusions. *Based on above results auditor can draw conclusions.*

x. Interface the test results with whatever subsequent manual audit work to be done.

### 1.11.2 Cases on how to use continuous auditing

1. **Snapshot**

   **Facts:** A software company with more than 1,00,000 employees. Organisation uses payroll software to process salary. The payroll is processed in four distinct steps in system. They are:
   - Calculate basic salary: Based on basic input data, like attendance and master data is used here
   - Calculate Allowance: Based on basic salary calculated allowances like House Rent Allowances, calculated.
   - Calculate deductions: Once Basic Salary and Allowances calculated deductions like TDS, PF etc. made.
   - Calculate the net salary: Same based on above calculation.

   **Audit objective:** Management has appointed a system auditor to check whether the payroll system is working properly.

   Auditor’s use of **SNAPSHOT** as a technique:
   - This technique allows auditor to capture images of transactions as the same is processed in system.
2. Auditor identifies the transactions for which snapshot shall be taken.
3. Based on the snapshot auditor is able to come to a conclusion about the nature and location or error in payroll process if any.

2. Integrated Test Facility (ITF)

**Facts:** Company has linked its stores system to its purchase system. In the stores system whenever an items level comes to re-order level, system automatically generates a purchase order.

**Objective:** Company appoints an IS Auditor to check whether the same system is working properly or not.

**IS Audit process:** IS auditor uses the technique of ITF.

**IS Audit Steps:**

1. Create a dummy organisation. In the given case the dummy organisation is an issue slip. The objective is to reduce an items balance below re-order level.
2. Once the dummy organisation is processed in system, auditor checks whether the system triggers a purchase order.
3. If the answer is ‘yes’, it means the system is working properly.

**Points to remember**

1. Items selected for the above test shall be material.
2. Effect of dummy organisation need to be reversed.
PART 2: COMPLIANCE TESTING AND SUBSTANTIVE TESTING

Business application software controls has to be analysed through compliance and substantive testing. These tests are necessary for risk assessment. The evaluation of internal control is accomplished through compliance and substantive testing. The purposes for compliance and substantive testing differ and will be achieved during the fieldwork.

2.1 Compliance Testing

ISACA ITAF201 Performance Guidelines on “Engagement Planning” states as follows: “Audit and assurance projects should include consideration of internal controls either directly as a part of the project objectives or as a basis for reliance upon information being gathered as a part of the project. Where the objective is evaluation of internal controls, IT audit and assurance professionals should consider the extent to which it will be necessary to review such controls. When the objective is to assess the effectiveness of controls over a period of time, the audit plan should include procedures appropriate for meeting the audit objectives, and these procedures should include compliance testing of controls. When the objective is not to assess the effectiveness of controls over a period of time, but rather to identify control procedures at a point in time, compliance testing of controls may be excluded”.

SA00 issued by ICAI, “Basic Principles Governing an Audit”, defines compliance procedures as tests designed to obtain reasonable assurance that those internal controls on which audit reliance is to be placed are in effect. A compliance test determines if controls are being applied in a manner that complies with management policies and procedures. The broad objective of compliance test is to provide the IS auditors with reasonable assurance that the particular control on which the IS auditor plans to rely is operating as the IS auditor perceived in the preliminary evaluation. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary and/or automated evidence, for example to provide assurance that only authorised modifications are made to production programs.

2.1.1 Purpose

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. It is achieved through compliance testing. Compliance testing helps an auditor determine that

- The controls exist and are working as expected
- The controls are applied in a manner that complies with policies and procedures.

2.2 Substantive Testing

To obtain evidence of the validity and propriety of accounting treatment of transactions and balances or, conversely, of errors or irregularities therein
SA00 issued by ICAI, “Basic Principles Governing an Audit”, defines substantive procedures are designed to obtain evidence as to the completeness, accuracy and validity of the data produced by the accounting system. A substantive test substantiates the integrity of actual processing and the outcome of compliance testing. Substantive testing is the testing of individual transactions. It provides evidence of the validity and integrity of the balances in the financial statements and the transactions that support these balances. The IS auditors use substantive tests to test for monetary errors directly affecting financial statement balances.

2.2.1 Purpose
Substantive testing procedures focus on broadly two types of tests:

i. Tests of details of transactions and balance such as recalculating interest to ensure the accuracy of process and effectiveness of controls over the process of the calculation of interest.

ii. Analysis of significant ratios and trends including the resulting enquiry of unusual fluctuations and items in exceptions e.g. debit balance in deposit accounts, pending items to ensure the controls to prevent or detect such transactions or balances are in place.

2.3 Relationship between compliance and substantive testing
There is a direct correlation between the effectiveness of controls and the extent of substantive testing required. If the auditor after compliance testing concludes that the controls are adequate and are working effectively as expected, then he is justified in reducing the size of his sample for substantive testing. If testing of controls reveals weak controls, he might decide to go for increasing his sample for substantive testing.

Please refer to chapter 2 of module 2: IS Assurance services for more details of compliance testing and substantive testing.
PART 3: IMPACT OF BUSINESS APPLICATION SOFTWARE ON BUSINESS PROCESSES/CONTROLS

As discussed in previous sections, an organisation selects business application to achieve its business goals and objectives. In part 1 of the chapter, the case study has highlighted the importance of selecting the correct business application software. Once an organisation has selected a business application, it needs to implement appropriate business processes or re-define its way of working to ensure that business application software process and organisation own business operations are in sync.

3.1 Case: Highlight need for redefining business process

Objective: To highlight importance of re-defining the business process to suit the requirements of the business application selected to be used.

a. To know : Teeming and Lading fraud

Definition: It is a type of fraud that involves the crediting of one account through the abstraction of money from another account. It can happen when one customer's payment is stolen and another customer's payment is posted to hide the theft.

b. Why this fraud occurs?

If the internal check is lacking then the fraud perpetrator can divert the cash cheque for his/her personal use. As we have read that person in possession must not possess the record of asset. This fraud occurs when a person acts as cashier as well as ledger writer or enters data.

c. How to control the risk in business application system?

1. Organisation using TALLY

In TALLY, as soon as a cash voucher is entered in system, it immediately updates ledger and related financial statements also. The issue to resolve is safeguarding against occurrence of fraud.

Safeguards put in place: In TALLY it is preferred that better input controls be put in place to prevent occurrence of fraud by creating specific users with access for specific functions.

2. Organisation using ERP system like SAP

In SAP, the transaction processing follows a two-step process:

i. Park of entry: This step is used to enter and store (park) incomplete documents in the SAP System without carrying out extensive entry checks.

ii. Posting of entry: Parked documents can be completed, checked, and then posted at a later date – if necessary by a different accounting clerk.

This ensures that same accounting clerk does not receive the cash and also update the records.
d. What TALLY users need to do?

They need to redefine their business process in a manner to prevent the occurrence of above frauds. The redefined business process needs to address the following propositions:

1. There are proper internal check is established, and
2. The business process shall be as per the nature of business of organisation.

3.2 Procedures to manage changes to business processes and impact on controls

During the procedure conversion performed in the implementation phase of system development life cycle approach, an organisation needs to prepare a control impact assessment chart. This documentation is important to help identify the following:

**Step 1:** What is the impact of new business application on the internal controls? This assessment has to be done for all items specified in the “Checklist for Application Control Review of Business Application” (Annexure ‘1’ of this module). An evaluation checklist for impact assessment is given in Appendix-5 “Business Application’s impact on internal controls”.

**Step 2:** Based on the assessment made at step ‘1’ IS auditor shall check how management has addressed the shortcoming. Management may address the concerns raised by specifying new business process, approval process. All such new business process, approval process need to be validated. For validation IS auditor shall use the checklist given in Appendix 1.
PART 4: USER CONTROLS

The most important aspect of a business application is the user controls. User controls are defined as the rights given to users as per job profile and their rights and duties within the organisation. Entitlement of access to an information resource and degree of access is determined according to the job description, functions and role of the user in the organisation.

The “rights of access” is to ensure that user does not gain access to undesired information resources or an undesired mode of access to the information. This is governed by philosophy “need to know and need to do basis” or the principle of least privilege. Principle of least privilege is an important concept in information security. It advocates minimal user profile privileges on computers, based on user’s job necessities. It can also be applied to processes on the computer; each system component or process should have least authority necessary to perform its duties. This is also called the “default deny” principle. All these terms imply that access is available only to users after it has been specifically granted to them, only to perform the job function that has been granted to them. Please refer to the chapter on Logical access controls in Module-4 for more details.

4.1 Principles to follow while granting user rights

User rights are to be assigned based on following guiding principles:

1. Rights are allocated on the basic philosophy of, “NEED TO KNOW and NEED TO DO
2. Rights need to be allocated based on user’s job profile.
3. Maker and checker distinction need to be followed, for example a user who creates a cash voucher must not be able to modify the same.
4. Asset recorder must be different from person physically holding asset.

4.2 Creating users for different level of use

4.2.1 Key requirement

Proper user rights definition in system has two key requirements.

- Well defined structure
- Application software capability

a. Well defined management structures with employee roles and responsibility.
b. Capability of the business application to allow user rights creation

The job of user rights creation, modification and deletion is a critical from internal control perspective.

4.2.2 IS Auditor key checkpoints

It is important for an IS Auditor to check:
Module 6

i. 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.

Case at the end of this part: An accounting software's USER RIGHTS AUDIT.

ii. 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?

iii. 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?

iv. 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?
c. Whether the alterations are done through proper validated USER RIGHTS ALTERATION FORMS?
d. Whether these forms follow the similar authorisation process as done during initial creation of user rights?

v. Keeping track of user actions?
This shall be part audit trail review, dealt in detail at other location in this module.
4.3 Creating users for different level of use

A checklist from TALLY to allow creation of user rights is explained in the case which follows.

**Case Studies**

1. User rights review Audit

An Internal Auditor asked the company to make available user rights lists as provided by the company in accounting software. Internal Auditor also asked the HR department to make available the hierarchy chart and job profile of the individuals. On comparison of the two documents auditor found the following: There were 50 employees in the company. Details of two employees are:

<table>
<thead>
<tr>
<th>Designation</th>
<th>HR department profile</th>
<th>Accounting Software rights: Allowed Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Major responsibility as defined by company</td>
<td>Name of Document / Master</td>
</tr>
<tr>
<td>Stores Clerk</td>
<td>Prepare Material Receipt Note</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Material Vendor Master</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Receipt Note VAT Rate Master</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>after validation with PO for quantity, rate, and other terms.</td>
<td></td>
</tr>
<tr>
<td>Manager Accounts</td>
<td>Timely and accurate accounting, statutory compliances, timely preparation of financial statements, timely submission of MIS to management.</td>
<td>Vouchers</td>
</tr>
<tr>
<td></td>
<td>Account Masters, including debtors and creditors master.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**The person was allowed to do back dated entries 365 days in past.**

**Exercise for participants:** What are the risks and what are the remedies?
Module 6

2. GM (F) who left the company.

**Facts:** The Company had a policy of allocating the super-user password to General Manager (Finance). The same defined in the job profile of the GM (F). GM (F) shall be responsible to ensure for allocation, deletion, modification and suspension of user rights based on approvals made available by HR department.

**Problem:** The GM (F) left the organisation. Another one joined. The new joinee was given another super-user password. Six months after the new joinee, it came to notice of Internal Auditor that all employees of the accounts department have been using the super-user password of the previous GM (F).

**Exercise for the participants:** What was wrong and how these could be corrected for future?
PART 5: DATABASE CONTROLS

In this chapter we will understand database structure and tables, user creation, access levels and user management. We will also understand how to evaluate internal control systems in application software relating to system design, data creation/input, data processing, data flow, data transmission and data storage. How to use reporting, query and SQL features as required for reviewing controls are briefly discussed.

5.1 Key features of database

5.1.1 Database architecture

Data is defined as collection of different data. Database is like an electronic file cabinet i.e. a collection of computerised data files. Database being a critical system resource needs elaborate controls to be put in place. Data architecture is composed of models, policies, rules or standards that govern which data is collected, and how it is stored, arranged, integrated, and put to use in data systems and in organisations. They are namely;

(i) **External or user view**: It is at the highest level of the database abstraction. It includes only that portion of database or application programmes 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.

(ii) **Conceptual or global view**: This 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,

(iii) **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.

5.2 Database Security and Control

Database Controls could be in terms of:

1. **Database Roles and Permissions**
   - Segregation of duties
   - Roles & Permissions allow control of operations that a user can perform on database,

2. **Concurrent Control**: Addresses conflicts relating to simultaneous accesses

3. **Views**: Views enable data access limitations. A view is a content or context dependent subset of one or more tables. E.g. – A view might be created to allow a sales manager to view only the information in a customer table that is relevant to customers of his own territory. Restrict user views of the database.

4. **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). This is discussed later.
5.3 User creation in database

Please refer to the eLearning part of Module 1 for more details on concepts of database. The objective of Database security would be Authorised people should be given Right access to the Right data. In this context user management becomes very important. There could be different types of database users:

1. Application programmers
2. Sophisticated users
3. Specialised users
4. Naive users

This user management is achieved through Authorisation and access control

Basic model for accessing control involves:

a. Subjects (Right People)
b. Objects (Right data)
c. Access Rights (Right Access)

Subject is allowed access rights to objects.

To access the database, a user must specify a valid database user account and successfully authenticate as required by that user account. 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.

Data base Administrator will then grant access rights or privileges to user as shown below.
5.4 Structured Query Language

A query language is a set of commands to create, update and access data from a database allowing users to raise ad hoc queries/questions interactively without the help of programmers. Structured Query Language (SQL) is a programming language used to manipulate information in relational database management systems (RDBMS).

5.4.1 Components of SQL

a. DML or data manipulation language: DML consist of SELECT, UPDATE, INSERT, and DELETE statements.

b. DDL or data definition language: DDL is made up of CREATE and ALTER statements.

c. DCL or data control language: DCL is comprised of GRANT and REVOKE statements. In recent years DML, has been expanded to include the MERGE statement and DDL has had the APPEND statement added.
5.4.2 Language elements of SQL

a. Clauses, which are in some cases optional, constituent components of statements and queries.

b. Expressions which can produce either scalar values or tables consisting of columns and rows of data.

c. Predicates which specify conditions that can be evaluated to Boolean (true/false/unknown) truth values and which are used to limit the effects of statements and queries, or to change programme flow.

d. Queries which retrieve data based on specific criteria.

e. Statements which may have a persistent effect on schemas and data, or which may control transactions, programme flow, connections, sessions, or diagnostics.

5.5 SQL commands for reporting

SELECT Statement Syntax

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Action</th>
<th>Target</th>
<th>Options to specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select</td>
<td>Columns</td>
<td>i. Specific columns by name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ii. All columns through wildcard</td>
</tr>
<tr>
<td>2</td>
<td>From</td>
<td>Tables</td>
<td>Lists &quot;qualified table name&quot;</td>
</tr>
<tr>
<td>3</td>
<td>Where</td>
<td>Criteria are met</td>
<td>i. Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ii. Conditions that limit the records to be displayed</td>
</tr>
<tr>
<td>4</td>
<td>Group by</td>
<td>Summarise</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Order By</td>
<td>Order Results</td>
<td>i. Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ii. Sorts the query results</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASC – ascending order</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DESC – descending order</td>
</tr>
</tbody>
</table>

The above can be used to generate specified reports directly from database. These are covered in more detail through practical examples in the hands on training of this module.
PART 6: FINANCIAL REPORTING AND REGULATORY REQUIREMENT IN INFORMATION SYSTEMS

6.1 Nature of compliances

As the usage of business application has been increasing in business, so has been the increase of regulatory compliances. Today businesses rely on reports generated from business applications for their statutory compliances. The list of compliances may include:

i. **Taxation related:** TDS, TCS, Excise Duty, Service Tax, VAT, PF, etc.

ii. **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.

iii. **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.

iv. **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.

v. **Compliances as specified in the newly notified Companies Act, 2013:**

   - Maintenance of books in e-form. (Section 128)
   
   - Compulsory Internal Audit: Prescribed companies to have an Internal Auditor. **This provision makes it more important for company to implement proper controls in business application used.** (Section 138)
   
   - Constitution of National Financial Reporting Authority (NFRA). This body has been entrusted with task of framing auditing and accounting standards. (Section 132)

vi. **Compliances requirements from industry specific statutes**

   - Banking industry compliances
   
   - Insurance Industry
   
   - Stock market industry
6.2 Who is responsible for accuracy and authenticity of reports?

The responsibility may be defined through the following chart:

- **i.** The prime responsibility for accuracy of report generated from the business applications lies with the management.
- **ii.** The role of internal auditor is to see whether established controls ensure the accuracy of reports.
- **iii.** Where statutory auditor wishes to use the above reports for his/her documentation, or forms and opinion based on such reports.

SA 580 on “Written Representations”, issued by ICAI, state that auditor when decides to obtain written representations as assertions, and to respond appropriately to written representations provided by management or if management does not provide the written representations requested by the auditor.

6.3 Validation of statutory reports from business application software

This requires IS auditor to have an understanding of system, this includes the way it is configured and the way it generates reports. To highlight the above issue two cases are given here.

Case on validation of statutory rates in business application software

1. **PF rates are not properly defined**
   - **Facts:** Employee’s PF Contribution @10% Pay Head Creation. If rate of % defined incorrectly in master configuration, then salary calculated and report will also be affected and shown incorrectly.
b. How to define the rate?

Go to Gateway of Tally > Payroll Info. > Pay Heads > Create > In the Pay Head Creation screen,

- Type Employee’s PF Contribution @ 10% as the Name of the Pay Head
- Select Employees’ Statutory Deductions in the field Pay Head Type
c. **What shall be the impact?**
   - Deduction of PF at wrong rates
   - Other liabilities associated with the above.

2. **TDS rates are not correctly specified**
   
a. **Wrong classification of payments and the related section under which payment is to be made.**

   Default Nature of Payment for professional fees is entered as payment to contractors instead of Fees for Technical Services u/s 194-J.
b. Improper classification regarding exemptions

Income Tax Exemption Limit: Income tax exemption limit is ignored which results in deduction of tax from the first voucher ignoring the basic exemption limit. For example, TDS on interest is deducted only if the amount of interest exceeds ₹ 10000.

c. What shall be the impact?
- Deduction of TDS at wrong rates
- Other liabilities associated with the above
PART 7: SYSTEM AUDIT REPORT FORMAT AS PER BEST PRACTICES

7.1 Reporting Standards

Report is the output of effort taken. Quality of report is the key to success of audit effort. ISACA ITAF 401 guidance on reporting standards states: “The reports produced by IS audit and assurance professionals will vary, depending on the type of assignments performed. Considerations include the levels of assurance, whether IS audit and assurance professionals were acting in an audit capacity, whether they are providing direct reports on the subject matter or reporting on assertions regarding the subject matter, and whether the reports are based on work performed at the review level or the examination level”.

1. Audit report format ISACA ITAF 401 on “Reporting” and SA 700 on “Forming an opinion and Reporting on Financial Statements”, the audit report need to cover the following.

   i. Title
   ii. Addressee
   iii. Description of the scope of the audit, the name of the organisation or component of the organisation to which the subject matter relates, including:

      a. Identification or description of the area of activity.
      b. Criteria used as a basis for the IS audit and assurance professional’s conclusion.
      c. The point in time or period of time to which the work, evaluation or measure of the subject matter relates.
      d. A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management.

   iv. A statement that the IT audit and assurance professional has conducted the engagement to express an opinion on the effectiveness of control procedures.
   v. Identification of the purpose for which the IT audit and assurance professional’s report has been prepared and of those entitled to rely on it, and a disclaimer of liability for its use for any other purpose or by any other person.
   vi. Description of the criteria or disclosure of the source of the criteria.
   vii. Statement that the audit has been conducted in accordance with specified IT Audit and Assurance Standards or other applicable professional standards.
   viii. A paragraph stating that because of the inherent limitations of any internal control, misstatements due to errors or fraud may occur and go undetected.
   ix. An expression of opinion about whether, in all material respects, the design and operation of control procedures in relation to the area of activity were effective.
Module 6

x. IT audit and assurance professional’s signature.
xii. Date of the IT audit and assurance professional’s report. In most instances, the dating of the report is based upon applicable professional standards. In other instances, the date of the report should be based on the conclusion of the fieldwork.

7.1.1 Case to prepare report in specified format

Objective: to help document a system audit report for a company’s password management policy.

Facts: “Password Management Policy” has been framed as a part of main security policy of the company.

Policy details
1. Policy Name: “Password Management Policy”. The objective is to ensure that the company has no loss due to password mismanagement.
2. Policy Guidelines
   • Password length to be minimum 8 characters
   • Password to be alpha-numeric
   • Password to be changed every 30 days
   • Password not to be shared
3. Policy design and implementation: Management informed its system developers to implement the above policy as a part of system design.
4. Policy monitoring: Manager (PW) appointed by the company in HR department, having access to password log of system reports to System Administrator. At the end of year management appointed an IS Auditor with the following scope:
   1. To review policy compliance.
   2. To suggest:
      i. Modification in policy
      ii. Any other aspect for better implementation.

IS Audit steps: The basic audit steps including those mentioned at Chapter 1, IS Auditor used the audit procedures including compliance and substantive procedures. IS Auditor uses the following audit techniques to collect audit evidence.

i. Inquiry: Interacting with the stakeholders to confirm understanding of the policy and level of compliance by the users.

ii. Documentation: Reviewing the Audit Logs in system. These logs inform which employee logged in on a specific date. Reviewing the attendance records of staff.

iii. Observation: Validating the process by which staff enters their passwords in system.

iv. Re-performance: With the permission of management, IS Auditor tries to create passwords which were not in line with the policy.
B. IS Auditor’s Findings: Based on the audit done auditor came across the following.

1. There were 200 employee data available. Of these 175 are working and 5 have left.
2. The password of employee who had left had not been disabled.
3. 20 employees did not change their password every 30 days, as defined in policy. 5 were repeat offenders.
4. 50 instances of employee passwords being used when they were absent have been observed.

Please refer to Appendix 6: System Audit Report.

7.2 Questions

1. The best way to define the purpose for an IS Audit in one word:
   A. Assurance
   B. Activity
   C. Review
   D. Performance

2. What is the primary basis of audit strategy? It should be based on:
   A. Knowledge.
   B. Life-cycle.
   C. User-request
   D. Risk assessment.

3. Which of the following audit tools is MOST useful to an IS auditor when an audit trail is required?
   A. Integrated Test Facility (ITF)
   B. Continuous and Intermittent Simulation (CIS)
   C. Audit hooks
   D. Snapshots

4. Which of the following is the first step in compliance testing? To review:
   A. Access Security Controls
   B. Input Controls
   C. Processing Controls
   D. Output Controls.

5. The cashier of a company has rights to create bank master in TALLY. This error is a reflection of poor definition for which type of control:
   A. User Controls
   B. Application Control
   C. Input Control
   D. Output Control
6. An employee has left the company. The first thing to do is to:
   A. Hire a replacement employee
   B. Disable his/her access rights
   C. Ask the employee to clear all dues/advances
   D. Escort employee out of company premises

8. Common features in ISACA ITAF 401, SA 700 and NFRA (National Financial Reporting Authority) is.
   A. Reporting
   B. Auditing
   C. Accounting
   D. Standard

7.3 Answers and Explanations

1. A. The IS audit focuses on determining the risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. Management gets an assurance about the functioning of controls.

2. D. Audit Strategy is based on risk assessment done by the auditor. Other answers do not represent basis for deciding audit strategy.

3. D. Snapshots is the right answer as in this technique IS auditor can create evidence through IMAGE capturing. A snapshot tool is most useful when an audit trail is required. ITF can be used to incorporate test transactions into a normal production run of a system. CIS is useful when transactions meeting certain criteria need to be examined. Audit hooks are useful when only select transactions or processes need to be examined.

4. A. Is the first step towards compliance test. Other steps are more part of application system transaction audit.

5. A. User controls are not properly defined. User controls need to be defined based on NEED TO DO and NEED TO DO basis. The above is reflection of a greater problem of improper assessment user profiles created in the system.

6. B. The first thing to do as soon as an employee leaves the company is to disable his/her access rights in system. This needs to be done to prevent frauds being committed. Other answers may be valid but are not the first thing to do.
   C is the correct answer other options are components of SQL.

7. D. ISACA ITAF is a reporting standard by ISACA. SA 700 is a reporting standard by ICAI. NFRA is an authority created in the new Companies Act, to prescribe standard for accounting and auditing.
### SECTION 3: APPENDIX

**APPENDIX 1: CHECKLIST FOR APPLICATION CONTROLS**

<table>
<thead>
<tr>
<th>IS Auditor Review of Application Controls</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Process/Application Name:</td>
<td></td>
</tr>
<tr>
<td>Business Process Owner:</td>
<td></td>
</tr>
<tr>
<td>Date of review:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Objective and Control Practices</th>
<th>Description</th>
<th>Information Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Completeness</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ref</th>
<th>Source Data Preparation and Authorisation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Check whether the source document is a well-designed input form. Detect errors and irregularities so they can be reported and corrected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Completeness</th>
<th>Accuracy</th>
<th>Validity</th>
<th>Authorisation</th>
<th>Segregation of Duties</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Whether the source documents is designed in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Where appropriate, include completeness controls in the design of the source documents.]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a</td>
<td>Whether the procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel? [These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Source Data Preparation and Authorisation

Establish 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.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Source Data Preparation and Authorisation</strong></td>
<td></td>
</tr>
<tr>
<td>Establish 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>a</strong></td>
<td>Whether criteria for timeliness, completeness and accuracy of source documents have been communicated?</td>
</tr>
<tr>
<td></td>
<td>Whether mechanisms are there to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria?</td>
</tr>
<tr>
<td><strong>b</strong></td>
<td>Whether pre-numbered source documents for critical transactions are used? Whether application allows identification and listing of missing source documents?</td>
</tr>
<tr>
<td><strong>c</strong></td>
<td>Whether definition for who can input, edit, authorise, accept and reject transactions, and override errors is there? Whether the same is as per roles and responsibilities of individual and record supporting evidence to establish accountability is maintained?</td>
</tr>
</tbody>
</table>
### Section 3

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>d</strong></td>
<td>Whether procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in timely manner are defined?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>e</strong></td>
<td>Whether application system generates error messages in a timely manner and as close to the point of origin as possible? Whether the transactions are processed without errors being corrected or appropriately overridden or bypassed? Whether the errors that cannot be corrected immediately logged in an automated suspense log? Whether error logs are reviewed and acted upon within a specified and reasonable period of time?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>f</strong></td>
<td>Whether errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and that, where necessary, incidents are raised for more senior attention? Whether automated monitoring tools are used to identify, monitor and manage errors?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>g</strong></td>
<td>Whether all source documents are safe stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Accuracy, Completeness and Authenticity Checks

Establish 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.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a</strong></td>
<td>Whether the transaction data are verified as close to the data entry point as possible and interactively during online sessions? Whether the transaction data, whether people-generated, system generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>b</strong></td>
<td>Whether controls to ensure accuracy, completeness, validity and compliance to regulatory requirements of data input put in place? Whether validation criteria and parameters should be subject to periodic reviews and conformation?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>Whether access control and role and responsibility mechanisms are established so that only authorised persons input, modify and authorise data?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td>Whether requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules defined?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e</td>
<td>Whether report of transactions failing validation generated? Whether report all errors are generated in a timely fashion?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f</td>
<td>Whether transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated? Whether information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 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.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Whether mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used defined and put in place?</td>
</tr>
<tr>
<td>b</td>
<td>Whether processing is completed and accurately performed with automated controls? [For example: Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks, and buffer overflow.]</td>
</tr>
<tr>
<td>c</td>
<td>Whether transactions failing validation routines are reported and posted to a suspense file? Whether the errors are reported in timely fashion? Whether the information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or to prevent errors?</td>
</tr>
<tr>
<td>d</td>
<td>Whether the transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled?</td>
</tr>
</tbody>
</table>
Whether there is a unique and sequential identifier to every transaction (e.g., index, date and time)?

Whether an audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction maintained?

Whether there is a listing of sensitive transactions and before and after images maintained, to check for accuracy and authorisation of changes made?

Whether integrity of data during unexpected interruptions in data processing with system and database utilities, maintained? Whether controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems?

Whether any adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry?

Whether reconciliation of file totals done? [For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify report and act upon out-of-balance conditions.]

Output Review, Reconciliation and Error Handling

Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.

Whether the handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements?

Whether procedures for communicating and follow-up defined for distribution of output?

Whether physical inventory of all sensitive output, such as negotiable instruments taken and compared it with inventory records?

Whether there are procedures with audit trails to account for all exceptions and rejections of sensitive output documents?
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>Whether out-of-balance control totals exist and exceptions reported to the appropriate level of management?</td>
</tr>
<tr>
<td>d</td>
<td>Whether procedure exists to check completeness and accuracy of processing before other operations are performed? Whether reuse of electronic output subject to validation check before re-use?</td>
</tr>
<tr>
<td>e</td>
<td>Whether procedures are defined to ensure that the business owners review the final output for reasonableness, accuracy and completeness? Whether the output is handled in line with the applicable confidentiality classification? Whether the potential errors are logged in a timely manner?</td>
</tr>
<tr>
<td>f</td>
<td>Whether for sensitive output, definition exists as to who can receive it? Whether such output is properly labelled for reorganisation?</td>
</tr>
</tbody>
</table>
### APPENDIX 2: ATM AUDIT CHECKLIST
This is provided as soft copy.

### APPENDIX 3: APPLICATION SOFTWARE CHECKLIST
This is provided as soft copy.

### APPENDIX 4: USER RIGHTS CREATION CHECKLIST

#### EMPLOYEE ACCESS RIGHT'S FORM

<table>
<thead>
<tr>
<th>Form Sl. No.</th>
<th>1</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department / Designation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name of Security Level:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Days allowed for Back Dated Entry:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cut-off Date for Back Dated Vouchers:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Put Y/N only

#### Reports / Items to ALLOW / DISALLOW

<table>
<thead>
<tr>
<th>ACCOUNTING STANDARDS</th>
<th>CREATE</th>
<th>ALTER</th>
<th>DISPLAY</th>
<th>PRINT</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNT MASTERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANNEXURE TO AUDIT REPORT CARO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATTENDANCE VOUCHERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDITING AND ASSURANCE STANDARDS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIT JOURNALS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIT LISTINGS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIT PROGRAMMES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIT WORKING PAPERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BACK DATED VOUCHERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>BALANCE SHEET</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BANK BOOKS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BANK RECONCILIATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BATCH GOWDOWN SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BATCH SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CASH FLOW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHEQUE PRINTING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHEQUE REGISTER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLIENT/ SERVER RULE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMMODITY WISE PURCHASE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMMODITY WISE SALES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMPANY FEATURES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONNECT COMPANY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COST CENTRE DETAILS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CST PURCHASE REGISTER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CST REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CST SALES REGISTER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAY BOOK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEALER EXCISE REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEPOSIT SLIP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMPLOYEE VOUCHERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXCISE COMPUTATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXCISE ER-1 REPORT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXCISE REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FBT REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FORM 3CA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FORM 3CB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FORM 3CD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUNDS FLOW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GROUP MONTHLY SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GROUP OUTSTANDING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GROUP SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GROUP VOUCHER DETAILS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMPORT DATA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INTEREST CALCULATIONS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVENTORY MASTERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVOICE CONFIGURATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JOB WORK ANALYSIS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JOB WORK ORDER DETAILS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JOB WORK REGISTERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JOB WORK STOCK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEDGER MONTHLY SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEDGER OUTSTANDING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEDGER VOUCHER DETAILS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOCATION-WISE SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCA REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOTE SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ORDER DETAILS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUTSTANDINGS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OVERRIDE INVOICE CLASS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OVERRIDE INVOICE DEFAULTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAYMENT ADVICE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAYROLL MASTERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAYROLL REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAYROLL VOUCHERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRICE LIST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROFIT &amp; LOSS A/c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PURCHASE REGISTER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QUICK SETUP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECEIPTS &amp; PAYMENTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SALES REGISTER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCHEDULE VI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SERVICE TAX REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STATUTORY AUDIT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STOCK CATEGORY OUTSTANDING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STOCK CATEGORY SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STOCK GROUP OUTSTANDING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STOCK ITEM MONTHLY DETAILS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STOCK ITEM OUTSTANDING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STOCK QUERY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STOCK SUMMARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STOCK VOUCHER DETAILS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYNCHRONISATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYNC REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TALLY.NET FEATURES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAX AUDIT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCS REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TDS REPORTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRACKING NUMBER DETAILS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRIAL BALANCE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAT COMPUTATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAT PURCHASE REGISTER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAT SALES REGISTER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VOUCHER REGISTER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VOUCHERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VOUCHING DONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Prepared by
Checked by
Approved by
Date of Approval
APPENDIX 5: REVIEW OF BUSINESS APPLICATION’S IMPACT ON CONTROLS

<table>
<thead>
<tr>
<th>Process/Application Name: Business Process Owner:</th>
<th>Date of review:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes made to business process due to implementation of business application software. Matrix to evaluate whether the new business application has impact on key information objectives to be achieved.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Information Objective. Put Y, to denote negative impact, and N to denote NO / Positive Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Changes to Source Data Preparation and Authorisation.</td>
</tr>
<tr>
<td>2</td>
<td>Changes to Source Data Preparation and Authorisation.</td>
</tr>
<tr>
<td>3</td>
<td>Accuracy, Completeness and Authenticity Checks</td>
</tr>
<tr>
<td>4</td>
<td>Processing Integrity and Validity.</td>
</tr>
<tr>
<td>5</td>
<td>Output Review, Reconciliation and Error Handling</td>
</tr>
</tbody>
</table>

For all items labelled as ‘Y’, IS auditor needs to check how the issue has been addressed.
# APPENDIX 6: SYSTEM AUDIT REPORT

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Description</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Title: REPORT ON PASSWORD MANAGEMENT SYSTEM</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Addressee CHIEF INFORMATION OFFICER, XYZ LTD.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Description of the scope of the audit, the name of the organisation or component of the organisation to which the subject matter relates, including:</td>
<td>Scope: System Audit of the Password Management Policy. User rights department in HR department.</td>
</tr>
<tr>
<td></td>
<td>a. Identification or description of the area of activity</td>
<td>Password Management Policy: Implementation and Compliance</td>
</tr>
<tr>
<td></td>
<td>b. Criteria used as a basis for the IS audit and assurance professional’s conclusion</td>
<td>The mandate of management to comment on compliance, suggest methods to improve compliance</td>
</tr>
<tr>
<td></td>
<td>c. The point in time or period of time to which the work, evaluation or measure of the subject matter relates</td>
<td>Audit period starts from April 1st, 2013 and ends on December 31st, 2013.</td>
</tr>
<tr>
<td></td>
<td>d. A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management</td>
<td>The responsibility of implementing proper and effective internal controls in general and specifically in terms of the policy under audit lies with the management.</td>
</tr>
<tr>
<td>4</td>
<td>A statement that the IT audit and assurance professional has conducted the engagement to express an opinion on the effectiveness of control procedures.</td>
<td>The IS Audit method and approach is to express an opinion on existence, effectiveness and continuity of internal controls put in place by the management.</td>
</tr>
<tr>
<td>5</td>
<td>Identification of the purpose for which the IT audit and assurance professional’s report has been prepared and of those entitled to rely on it, and a disclaimer of liability for its use for any other purpose or by any other person</td>
<td>The IS Audit has been conducted to help management identify lacunae in policy implementation. It does not provide any assurance as to the future viability but is a comment on the present state of affairs. The report is for use by management not for external agency.</td>
</tr>
<tr>
<td>6</td>
<td>Description of the criteria or disclosure of the source of the criteria</td>
<td>The report is based on management request to perform an audit of Password Management System, its effective implementation and monitoring.</td>
</tr>
<tr>
<td>Sl. No.</td>
<td>Description</td>
<td>Report</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Statement that the audit has been conducted in accordance with specified IT Audit and Assurance Standards or other applicable professional standards.</td>
<td>The IS Audit has been conducted as per the ISACA ITAF Standards on System Audit and ICAI SA on Audit.</td>
</tr>
<tr>
<td>8</td>
<td>A paragraph stating that because of the inherent limitations of any internal control, misstatements due to errors or fraud may occur and go undetected.</td>
<td>The audit is done as per mentioned standards. The expression on an opinion is subject to inherent limitation of internal controls. These arising from the fact that implemented controls may fail to prevent, detect misstatement due to errors and frauds. Audit is subject to its limitation, arising from the fact that audit is done on test basis, leaving a possibility of error or fraud going undetected.</td>
</tr>
<tr>
<td>9</td>
<td>An expression of opinion about whether, in all material respects, the design and operation of control procedures in relation to the area of activity were effective.</td>
<td>Based on the information, explanations provided, we comment that: A Password Management System has not been implemented properly. B. It fails to achieve the purpose. C. Management needs to take the following actions to improve its performance:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>i. Policy modification: Policy needs to specifically state, that as employee leaves and organisation his/her password shall be immediately disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ii. The attendance system of the organisation needs to be joined to the password system. This is necessary to ensure that a password of absent employee is not misused.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iii. Employee training is a must, for proper understanding and implementation of policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Basis of our recommendation as findings during the audit. Findings are enclosed as an annexure to the report.</td>
</tr>
<tr>
<td>10</td>
<td>IT audit and assurance professional’s signature</td>
<td>ABC</td>
</tr>
<tr>
<td>Sl. No.</td>
<td>Description</td>
<td>Report</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>11</td>
<td>IT audit and assurance professional’s address</td>
<td>ICAI BHAWAN, NEW DELHI</td>
</tr>
<tr>
<td>12</td>
<td>Date of the IT audit and assurance professional’s report. In most instances,</td>
<td>01-Jan-14</td>
</tr>
<tr>
<td></td>
<td>the dating of the report is based upon applicable professional standards.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In other instances, the date of the report should be based on the conclusion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the fieldwork.</td>
<td></td>
</tr>
</tbody>
</table>

### Annexure to System Audit Report

1. There were 200 employee data available. of these 175 are working and 5 have left.

2. The password of employee who had left had not been disabled.

3. 20 employees did not change their password every 30 days, as defined in policy. 5 were repeat offenders.

4. 50 instances of employee passwords being used when they were absent have been observed.

   [IS Auditor may add name and detail of employees]

5. IT audit and assurance professional’s signature. ABC

6. IT audit and assurance professional’s address. ICAI BHAWAN, NEW DELHI

7. Date of the IT audit and assurance professional’s report. In most instances, the dating of the report is based upon applicable professional standards. In other instances, the date of the report should be based on the conclusion of the fieldwork. 01-Jan-14

---

**APPENDIX7: SAMPLE AUDIT REPORT OF APPLICATION SOFTWARE**

This is provided as soft copy.
ISA
INFORMATION SYSTEMS AUDIT 2.0 COURSE

PRIMER ON INFORMATION TECHNOLOGY, IS INFRASTRUCTURE AND EMERGING TECHNOLOGIES

BACKGROUND MATERIAL

₹ 750/- (For Modules I to VII) with DVD

http://cit.cai.org
www.cai.org

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

July 2015