Background Material
On
Information Systems Audit 2.0 Course

Module-3 Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews (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

DISCLAIMER

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

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

Revised Edition	:	July 2015
Committee/Department	:	Committee of Information Technology
E-mail	:	cit@icai.org
Website	:	www.icai.org/http://cit.icai.org
Price	:	₹ 750/- (For Module - I to Module VII, Including DVD)
ISBN	:	978-81-8441-335-9
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.
Printed by	:	Finesse Graphics & Prints Pvt. Ltd. Tel.: 022-4036 4600 Fax : 022-2496 2297

Foreword

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

GOVERNANCE AND MANAGEMENT OF ENTERPRISE INFORMATION TECHNOLOGY, RISK MANAGEMENT AND COMPLIANCE SECTION 1: OVERVIEW

CHAPTER 1: CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

CHAPTER 2: GRC FRAMEWORKS AND RISK MANAGEMENT PRACTICES

CHAPTER 3: GEIT AND GRC

CHAPTER 4: KEY ENABLERS OF GEIT

CHAPTER 5: PERFORMANCE MANAGEMENT SYSTEMS

CHAPTER 6: IMPLEMENTING GOVERNANCE AND MANAGEMENT PRACTICES

SECTION 2: APPENDIX

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:

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

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

No.	Skills Category	Weightage (%)
1	Knowledge and Understanding	30 to 40
2	Application of the Body of Knowledge	55 to 60
3	Written communication	5 to 10

Summary of revised DISA Training

No.	Mode of Training	Weightage (%)
1	e-Learning Online (self)	12
2	e-Learning facilitated (lectures)	12
3	Classroom Training (lectures)	42
4	Hands-on Training (on laptop)	24
5	Project Work (self in groups)	10
	Total	**100**

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 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@icai.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 3:

Governance and Management of Enterprise Information Technology, Risk Management and Compliance (13%)

Section 1: Overview

SECTION 1: CONTENTS
CHAPTER 1: CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

Learning Objectives

The objective of this chapter is to provide an overview of the concepts and practice of governance and management of information systems from the perspective of corporate and business governance. Governance is built on the premise the effective enterprise risk management is implemented encompassing all key IT risks adapting a holistic approach and internal control process is used for effective risk management. Regulations require mandatory certification of such implementation by management as well as auditors. Governance also facilitates achieving enterprise objectives with much more certainty. The linkage of governance with enterprise risk management, governance of enterprise IT (GEIT) and internal controls is explained. A step by step methodology for implementing GEIT is outlined. IS Auditors need to review whether the implementation of GEIT has been done followed a structured approach and whether this has resulted in envisaged value to the enterprise.

1.1 Introduction

The need for governance and management of information systems can be assessed from the simple fact that today technology is all pervasive. Organisations are so dependent on Technology that its failure will bring all key operations to a complete halt. On the positive side, technology facilitates organisations to offer products or services to anyone across the globe. The fundamental principle in the current business environment is to use technology to enable users to access information anytime, anywhere, anyhow by anyone. The objective is to provide information access to all stakeholders online with real-time access and update. This is done using enabling technology such as the network, Internet, hardware, operating system software, database, applications and browser. Modern Technology is empowered by the cloud and internet access through wireless broadband. Technology is only an enabler but the backbone for this has to be robust systems and processes for the information systems. Hence, it is critical to ensure that organisations embed Governance and management processes and other enablers in the technology deployed. This will ensure that various stakeholder requirements are met and the management at all levels are able to use technology to perform their responsibilities. It is important to comply with the requirements of corporate governance or enterprise governance by implementing Governance of Enterprise IT, enterprise risk management using appropriate risk management strategy and internal control systems. This chapter outlines these concepts and provides overview of how to implement GEIT

1.2 Organisation of chapters

The chapters (1 to 6) in Section 2 of this module are organised in a logical sequence to enable understanding of the subject of Governance and Management of Information Systems in a simple and structured manner. It is advisable to read the chapters in the same sequence as the chapters are arranged with a logical flow and move from concepts to practice with specific examples. The objective of this module is to: "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". It is critical to adopt and adapt best practices to cover these key areas. Hence, there is heavy reliance on best practice frameworks. As the primary focus of this module is on Governance of Enterprise IT (GEIT) and its implementation at macro to micro level covering GRC and related management practices, the best practices guidance from COBIT 5 has been extensively referenced in this module as it is only framework for GEIT.

Chapter 1 titled: "Governance and Management of Information systems" provides an overview of the concepts and practice of governance and management of information systems from the perspective of corporate and business governance and explains the relationship between corporate governance, enterprise governance, GEIT, Enterprise Risk Management, IT risk management and internal controls. It also provides generic guidance on implementing GEIT.

Chapter 2 titled: "GRC frameworks and Risk Management Practices" provides an overview of key GRC frameworks and also elaborates key concepts of risk management from strategy to operations. It explains the relationship between GEIT and GRC and how implementing GEIT will help in meeting GRC requirements. The principles and enablers of COBIT 5 with specific relevance to how it meets risk management have been explained. Understanding concepts and practice of risk management is critical for implementing any GRC framework and also to meet compliance requirements. Hence, all the key concepts of risk management have been explained.

Chapter 3 titled: "GEIT and GRC" provides an overview of the need for GEIT and how GRC requirements of compliance can be implemented using GEIT framework such as COBIT 5 and other related best practices.

Chapter 4 titled: "Key enablers of GEIT" discusses the seven key enablers of GEIT which facilitate the successful achievement of enterprise goals and IT enabled goals. Each of the seven enablers have been discussed in terms of the characteristics and components so that implementation as required is easier. The relevance and relationship of each of these enablers and how they can be implemented in an integrated manner have been explained.

Chapter 5 titled: "Performance Management Systems" provides an overview of performance management systems with specific details of goals cascade from COBIT 5 and also explains the principles of Balanced Scorecard and Strategic Scorecard. It explains the concepts of goal setting, various types of goals and linkage of goals from enterprise goals to IT related goals and process goals. Further, principles of Balanced Scorecard have been explained. An overview of strategic scorecard, maturity model and quality management are also provided.

Chapter 6 titled: "Implementing Governance and Management practices" outlines the systematic approach to implementing GEIT detailing the phases and what is required to be done in each of the phases. Further, it highlights the distinction between Governance and Management. This chapter also explains and illustrates how to implement identified Governance and Management practices in specific areas. It also provides methodology for scoping IS assurance and consulting assignments using COBIT 5 processes.

1.3 Key Concepts of Governance

Enterprises whether they are commercial or non-commercial, exist to deliver value to their stakeholders. Delivering value is achieved by operating within value and risk parameters that are acceptable and advantageous, and by using resources including IT responsibly. In the rapidly changing environment that most enterprises operate in, swift direction setting and agility to change are essential. Senior management is responsible for ensuring that the right structure of decision-making accountabilities are shared among many people in the enterprise and when accountability is shared, governance comes into play. Governance is “the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organisation toward the achievement of its objectives.” Governance should be in place to ensure IT supports the strategies and objectives of the organisation. The relationship of enterprise Governance and Corporate Governance with IT governance (GEIT is depicted below.

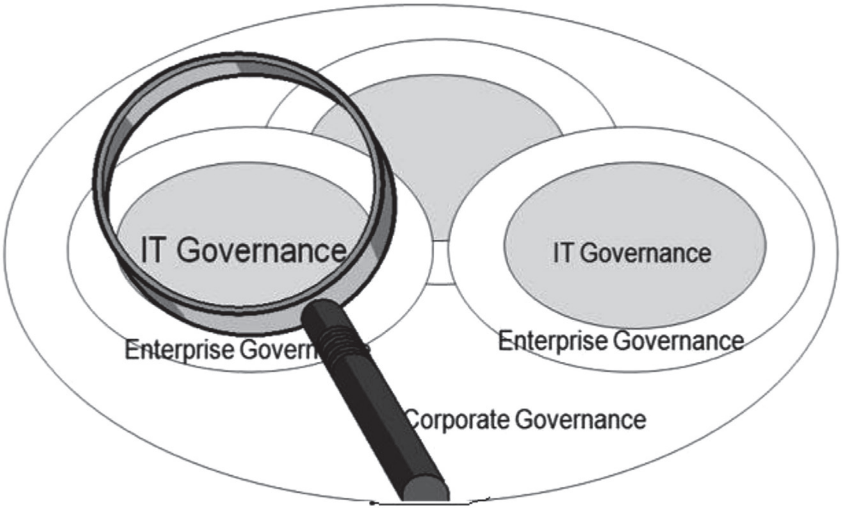


Figure 1.1: Relationship of types of Governance

1.3.1 Enterprise Governance

ISO/IEC 38500 defined Governance as: “The system by which organisations are directed and controlled”. A governance system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organised mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives. Enterprise governance can be defined as: ‘The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organisation’s resources are used responsibly.’ Enterprise governance is an overarching framework into which many tools and techniques and codes of best practice can fit. Examples include codes on corporate governance and financial reporting standards.

1.3.2 Corporate Governance

Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business by ensuring compliance and protecting shareholders' interest.

Good corporate governance requires sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of audit committee, risk management and compliance with the relevant laws and standards including corporate disclosure requirements. These are intended to guide companies to achieve their business objectives in a manner such that this those who are entrusted with the resources or power to run the companies to meet stakeholder needs without compromising the shareholders' interest. Legally, the directors of a company are accountable to the shareholders for their actions in directing and controlling the business, and for the actions of the company's employees, who are in the position of trust to discharge their responsibilities in the best interest of the company. Corporate governance is thus necessary for the purpose of monitoring and measuring their performance and is mandated by regulations across the world and across various industries.

1.3.3 Need for Corporate Governance

Although Governance is not new for enterprises, a spate of frauds in the corporate sector involving large enterprises across the world including India in the last two decades have awakened regulators to the need for mandating the implementation of corporate governance integrated with Enterprise Risk Management and Internal controls. The concept of Corporate Governance has succeeded in attracting a great deal of public interest because of its importance for the economic health of companies, protecting the interest of stakeholders including investors and the welfare of society, in general.

Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as, the Board, management, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. The requirements for corporate governance are built on the principles of governance and encompass all levels of management including specific responsibility of board and senior management. Corporate Governance is focused on protecting the interests of various stakeholders and is compliance oriented. Although the terms corporate governance and enterprise governance are quite often used inter-changeably, it can be said that corporate governance is applying the principles of enterprise governance to corporate structure of enterprises. Some of the key concepts of corporate governance are:

- Clear assignment of responsibilities and decision-making authorities, incorporating an hierarchy of required approvals from individual employees to the board of directors;
- Establishment of a mechanism for the interaction and co-operation among the board of directors, senior management and the auditors;

- Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;
- Special monitoring of risk exposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. vendors);
- Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition; and
- Appropriate information flows internally and to the public. For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly understood, appreciated and implemented.

1.4 Corporate Governance and Regulatory requirements

Corporate governance in India is evolving, primarily due to regulatory requirements, but also, to some extent, due to each enterprises specific needs and context. The objectives of corporate governance are fulfilled by setting up an appropriate structure and functioning mechanisms for the board of directors and audit committees, as laid down by the Companies Act, 1956. It is critical for each enterprise to establish its own specific governance system based on its own specific constraints and business culture.

The Companies Act, 2013 outlines the need for mandatory Internal Audit and reporting on Internal Financial Controls [section 138]. The Act requires certain new aspects which need to be covered in an auditors' report which include: "whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls [section 143(3)(i) of the 2013 Act]. Further, the Act deals extensively on the issue of fraud (section 447) and has for the first time defined fraud. The new regulations make it more imperative for management to implement a system of governance integrated with risk management and internal control systems. As IT is a key enabler of enterprise processes, risk management and controls has to consider technology and hence the need for implementing a holistic approach of Governance of enterprise IT (GEIT) using global best practices and frameworks.

The Information Technology Act amended in 2008 introduced new provisions which are specifically applicable to corporates, provisions relating to maintaining privacy of information and imposed compliance requirements on management with penalties for non-compliance. These requirements have to be considered as part of compliance by corporates and individuals as applicable. Please refer to module-2 for more details of these requirements. A copy of the IT Act 2000, amendments of 2008 and the related rules are provided as reference material in the DVD of the course.

Corporate Governance is a system by which companies are directed and controlled by the management in the best interest of the stakeholders and others ensuring greater transparency and better and timely financial reporting. The Board of Directors are responsible for governance of their companies. SEBI introduced a mandatory audit to ensure that this is maintained as per its norms by all listed companies as part of corporate governance and came up with an updated Clause 49 to address this requirement. Although Clause 49 primarily focuses on corporate governance, there are two key sections: Clause 49 IV(C) and Clause 49V that make it imperative for listed companies to implement Governance of Enterprise IT.

Clause 49IV(C) Board Disclosures on Risk Management requires every listed company to lay down procedures to inform board members about the risk assessment and minimisation procedures. These procedures must be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework. Indian companies often adopt a combination of home-grown, in-house practices and globally recognised frameworks for risk management. The ideal approach would be to adopt a globally accepted risk management framework such as COSO, which provides a framework for enterprise risk management, and then integrate the local practices as relevant. The amendments effected in Clause 49V(C) and (D) clearly bring out:

- The responsibility entrusted to the CEO/CFO is in relation to establishing and maintaining internal controls for financial reporting.
- The CEO/CFO has to assert that he/she has evaluated the effectiveness of internal control systems of the company pertaining to financial reporting.
- The CEO/CFO certificate will further state the manner in which deficiencies (if any) in the design or operation of such internal controls have been disclosed to the auditors and the audit committee.
- The CEO/CFO certification will also state the steps they have taken or proposed to take to rectify these deficiencies in the design or operation of such internal control pertaining to financial reporting.

As the management is vested with responsibility of running the business, it implies that they have to take reasonable steps to ensure the implementation of the conditions of corporate governance as stipulated in clause 49 of the Listing Agreement. The auditors' responsibility in certifying conditions of corporate governance relate to verification and certifying factual implementation of conditions of corporate governance as stipulated in the above clause. Such certification is neither an audit nor an expression of opinion on financial statements of the entity. In the US, The Sarbanes Oxley Act (SOX) focuses on the implementation and review of internal controls as relating to financial audit. It highlights the importance of evaluating the risks, security and controls as related to financial statements. In an IT environment, it is important to understand whether the relevant IT controls are implemented in the relevant computerised information systems. The overall reliability of these controls would be dependent on the overall risk management strategy, risk appetite of the management, use of best practices and various other enablers.

Corporates across the world for SOX compliance have used COSO (www.coso.org) and COBIT (www.isaca.org/cobit) as the primary framework and best practices for implementing governance, risk management and internal controls. The objective of COSO is to improve the quality of financial reporting through business ethics, effective internal control and corporate governance. The COSO 2013 framework outlines 17 principles of internal controls and highlights the need for management to implement a system of risk management at the enterprise level. COBIT is a comprehensive framework for the governance and management of enterprise IT, comprising five domains, 37 IT processes and over 200 management practices and activities divided into governance and management processes. COBIT has been used as the business framework for implementing Governance of enterprise IT. Together COSO and COBIT can be used for implementing a system of enterprise risk management integrated with technology ensuring both conformance and performance. Although, there is need for implementing Governance, risk management and controls from regulatory perspective, stakeholders would be looking at performance perspective also in such implementation. The objective of the Governance of Enterprise IT is to ensure that organisations can ensure business value from their investment in IT, while managing risk.

Good corporate governance is vital for all types of enterprises big or small in view of the benefits which accrues due to its implementation. Governance helps in ensuring that control failures are mitigated appropriately. However, good corporate governance on its own cannot make an organisation successful. There is a danger that insufficient attention is paid to the need for organisations to create wealth or stakeholder value. Strategy and performance are also important. The key message of enterprise governance is that an organisation must balance the two dimensions of conformance and performance needs to ensure long-term compliance and success. This requires that governance is ideally implemented with the right balance of conformance and performance dimensions. These two dimensions are briefly outlined here.

1.4.1 Conformance or Corporate Governance Dimension

The conformance dimension of governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: roles of the chairman and CEO, role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance. Regulatory requirements and standards generally address this dimension with compliance being subject to assurance and/or audit. There are established oversight mechanisms for the board to ensure that good corporate governance processes are effective. These might include committees composed mainly or wholly of independent non-executive directors, particularly the audit committee or its equivalent in countries where the two tier board system is the norm. Other committees are usually the nominations committee and the remuneration committee. The Sarbanes Oxley Act of US and the Clause 49 listing requirements of SEBI are examples of providing for such compliances from conformance perspective.

1.4.2 Performance or Business Governance Dimension

The performance dimension of governance is pro-active in its approach. It is business oriented and takes a forward looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required. The conformance dimension is monitored by the audit committee. However, the performance dimension in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee. Remuneration and financial reporting are scrutinised by a specialist board committee of independent non-executive directors and referred back to the full board. In contrast, the critical area of strategy does not get the same dedicated attention. There is thus an oversight gap in respect of strategy. One of the ways of dealing with this lacunae is to establish a strategy committee of similar status to the other board committees which will report to the board. The performance dimension in terms of how to implement performance management system is covered in more detail in chapter 5 of this module.

1.5 Enterprise governance framework

Fundamentally, enterprise governance is the entire accountability framework of the organisation, with the twin dimensions of conformance and performance of processes, with more emphasis on the latter. In implementing enterprise governance, it is important to use best practices developed by various professional associations and also use relevant guidelines issued by regulatory bodies. Enterprise governance in general is broader and encapsulates corporate governance, performance management, internal control and enterprise risk management. In implementing controls, it is important to adapt a holistic and comprehensive approach. Hence, ideally it should consider the overall business objectives, processes, organisation structure, technology deployed and the risk appetite. Based on this, overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner. The objective of implementing enterprise governance is to ensure that the governance objectives of benefits realisation, risk optimisation and resource optimisation are achieved considering the stakeholder needs and which leads to value creation for the enterprise. This is depicted in the figure 1.2 given here.

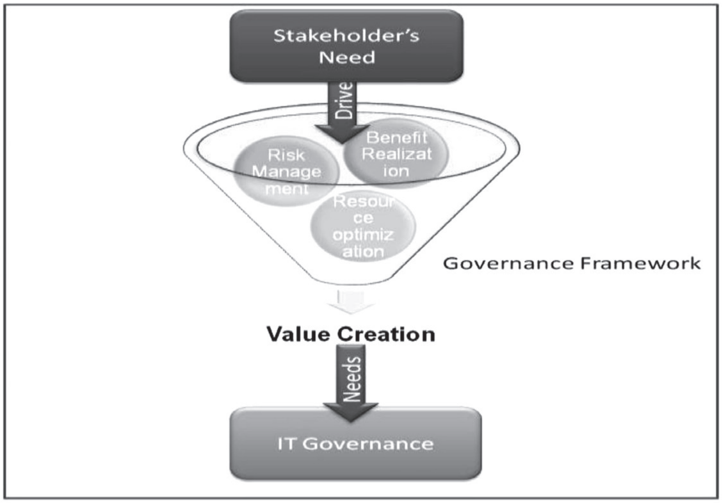


Figure 1.2: Governance framework and Drivers

Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise. Hence, the type of controls implemented in information systems in an enterprise would depend on this risk management strategy. There are multiple frameworks for implementing risk management. The next chapter covers details of some of the key concepts and approaches for implementing risk management in enterprises.

1.6 Enterprise Risk Management

Enterprise risk management deals with risks and opportunities affecting value creation or preservation and is defined by the Institute of Internal Auditors as: “Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." The management to ensure that the enterprise risk management strategy considers information and its associated risks while formulating IT security and controls as relevant. IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise

1.7 Governance of Enterprise IT (GEIT)

Governance of Enterprise IT is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, establish and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives. The key benefits of using GEIT is that it provides a consistent approach integrated and aligned with the enterprise governance approach. It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives and the IT-related processes are overseen effectively and transparently.

Implementing a GEIT framework helps in better compliance with legal and regulatory requirements and ensures that the governance requirements for board members are met. A few decades back, IT was one of the wagons but now IT is the engine propelling enterprise growth. IT interfaces all aspects of the enterprise and not just transaction processing. It can be said that IT has become inseparable from the business. Hence, in a modern enterprise, IT has moved from being a mere service provider to a strategic partner which helps enterprises in achieving both competitive and strategic advantage. Considering this huge dependence on IT and the fact that internal controls are embedded in IT and effective risk management can be achieved by using IT, implementing Governance of Enterprise IT has become imperative for a modern enterprise. Regulatory agencies, professional bodies and associates issue guidelines on use of generic and specific best practices. For example, the Reserve Bank of India issues guidelines covering various aspects of secure technology deployment. These guidelines are prepared based on various global best practices such as COBIT and ISO 27001. The Information Technology Rules outlines the need for maintaining secrecy of personal and sensitive information and identifies ISO 27001 as best practices framework for implementing best practices.

1.7.1 Governance Objectives

It is important to identify specific governance objective in implementing GEIT. Generally, the focus area of implementing GEIT as specified in COBIT 5 are these three governance objectives:

- **Benefit realisation:** Creating new value for the enterprise through IT, maintaining and increasing value derived from existing IT investments, and eliminating IT initiatives and assets that are not creating sufficient value for the enterprise. The basic principles of IT value are delivery of fit-for-purpose services and solutions on time and within budget, and generating the financial and non-financial benefits that were intended. The value that IT delivers should be aligned directly with the values on which the business is focused and measured in a way that transparently shows the impacts and contribution of the IT-enabled investments in the value creation process of the enterprise.

- **Risk optimisation:** Addressing the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT-related business risk consists of IT-related events that could potentially impact the business. While value delivery focuses on the creation of value, risk management focuses on the preservation of value. The management of IT-related risks should be integrated within the enterprise risk management approach to ensure a focus on IT by the enterprise and be measured in a way that transparently shows the impacts and contribution of IT-related business risk optimisation in preserving value.
- **Resource optimisation:** Ensuring that the right capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Resource optimisation ensures that an integrated, economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolete systems are updated or replaced. It recognises the importance of people, in addition to hardware and software, and, therefore, focuses on providing training, promoting retention and ensuring competence of key IT personnel.

1.7.2 Internal Controls

Regulatory requirements and best practices framework require internal control system to be an integral part of enterprise risk management and governance system. Hence, it is important to understand how internal control requirements are generally implemented through management systems. “An effective internal control system is an essential part of the efficient management of a company” established through the governance system. Such systems should establish an adequate system of internal control to “support business requirements foe effective and efficiency of operations, reliability of information and compliance with laws and regulations.” While appropriate internal control is a required outcome of sound governance and a necessary supporting element of effective governance, it does not in itself represent governance.

Any audit whether it is compliance or IS oriented would require understanding of internal control system implemented within the enterprise. Internal control is an element of the management system rather than an aspect of the governance system. Internal control must be supported by effective risk management process with internal control arrangements determined by the enterprises level of risks. Risk management requires establishing a sound system of risk oversight and management and internal control. The Securities and Exchange Commission (SEC) of USA rules define “internal control over financial reporting” as a “process designed by, or under the supervision of, the company’s principal executive and principal financial officers, or persons performing similar functions, and effected by the company’s board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the company;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorisations of management and directors of the company;

- Provide reasonable assurance regarding prevention or timely detection of unauthorised acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

COSO 2013 can be used as the over-arching framework for implementing risk management and internal controls and COBIT 5 framework can be used under COSO as umbrella framework for implementing Governance of Enterprise IT. Other frameworks and management policies can be implemented under these two frameworks to ensure both conformance and performance. Implementing internal controls systems is imperative for effective governance both from regulatory and management perspective. As auditors are primarily control experts, they can review the availability, adequacy and appropriateness of implemented controls and provide appropriate recommendations for mitigating control weaknesses. IS Auditors may be required to review and evaluate the system of governance, risk management and controls as embedded in IT and information systems and provide assurance on the effectiveness to meet established objectives.

1.7.3 Implementing GEIT

Governance of Enterprise IT is built on the principles of Governance but applied to IT. Hence, implementing GEIT in organisations requires understanding concepts of Governance, IT deployment and how IT can be used to implement Governance. GEIT is a blend of these concepts. Implementing GEIT requires establishing the right structures with defined roles and responsibilities, implementing relevant processes using best practices as required and establishing the relational mechanisms by active participation of relevant stakeholders as required in a collaborative effort to achieve enterprise goals.

The improvement of governance of enterprise IT is increasingly recognised by top management as an essential part of enterprise governance. Effective GEIT will result in improved business performance as well as compliance to external requirements, yet successful implementation remains elusive for many enterprises. Effective GEIT requires a range of enablers with carefully prescribed roles, responsibilities and accountabilities that fit the style and operational norms specific to the enterprise. Implementing GEIT from conformance (corporate) perspective would require viewing the enterprise at macro level and consider not only the business but also the external linkages. In case of performance (business) the enterprise has to be viewed at internal level and the focus on the processes and activities within the enterprise.

The key areas of focus in implementing GEIT are summarised in the table here.

Table 3.1: Implementing Governance from Conformance or performance perspective

Area	Conformance (Corporate)	Performance (Business)
Scope	• Board Structure, Roles and Remuneration	• Strategic decision making and value creation
Addressed via	• Standards and Codes	• Best practices, tools and techniques
Auditability	• Can be audited for compliances	• Not easily auditable
Oversight Mechanism	• Audit Committee	• Balance score cards

The COBIT framework can be used for implementing GEIT from any/both the above perspectives. The seven key enablers of GEIT which are required for effective implementation are described in next chapter. Overall, GEIT requires structures, processes and relational mechanisms.

The components and relationship of IT Governance framework are outlined in figure given below.

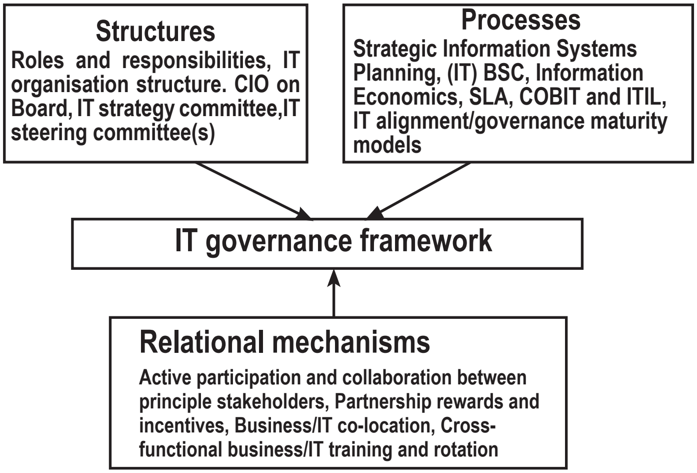

Structures
Roles and responsibilities, IT organisation structure. CIO on Board, IT strategy committee,IT steering committee(s)
Processes
Strategic Information Systems Planning, (IT) BSC, Information Economics, SLA, COBIT and ITIL, IT alignment/governance maturity models
IT governance framework
Relational mechanisms
Active participation and collaboration between principle stakeholders, Partnership rewards and incentives, Business/IT co-location, Cross-functional business/IT training and rotation

Figure 1.3: Components of Governance framework

The structures involve the organisation, and location of the IT function, the existence of clearly defined roles and responsibilities and a diversity of IT/ business committees. The processes refer to strategic decision making, strategic information systems planning (SISP) and monitoring, control, and process frameworks. The relational mechanisms finally complete the governance framework and are critical for attaining and sustaining business-IT alignment, even when the appropriate structures and processes are in place. These mechanisms include business/IT participation, strategic dialogue, training, shared learning, and proper communication. COBIT 5 which is the business framework for implementing GEIT can be used by enterprises of all sizes and types and regardless of technology deployment.

1.7.4 Guidelines for implementing GEIT

The primary objective of implementing GEIT is to ensure IT delivers value to the business and helps in mitigation of IT-related risk. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals. The COBIT 5 implementation guide provides a systematic approach with defines phases and specific roles and responsibilities for implementing GEIT. This approach can be customised and used by any organisation regardless of size, nature of business, sector or technology used.

1.7.5 Systemic approach to implementing GEIT

Research studies have established that effective implementation of GEIT maximises the contribution made by IT to organisational success. There can be multiple approaches to implementing GEIT as this varies with the needs of the enterprise and the specific framework used. It is advisable to adapt a systematic and well-proven approach as outlined in some of the best practices and frameworks. IT solution providers and regulators also provide their own approaches for implementing GEIT. It is important to remember that the focus should be first on implementing the systems and processes first and then automating rather than expecting that automation will implement systems and processes as required. As explained earlier, frameworks such as COSO and COBIT 5 also provide a systematic approach for implementing the relevant frameworks. The technology and business frameworks can be easily integrated under these frameworks. We are giving below some general guidelines on implementing GET which can be adapted as required.

1. Aligning IT Goals with Business Goals

Achieving better governance starts with the business, and more specifically with understanding its strategy and goals. IT management should be involved early in the business strategy definition process, especially in those companies that are highly dependent on IT. The IT goals should be aligned to the business goals. The IT strategy should be an IT blueprint of the business strategy plan. The IT goals, set out in the IT strategy plan should clearly support the achievement of one or more business goals. It is the responsibility of the board and senior management to ensure that the IT strategy is aligned with the business strategy. This could be achieved through:

- Clear business goals, communicated to the entire organisation
- Early involvement of IT in business strategy process
- Align IT goals to business goals
- Derive IT strategy from business strategy

2. Formalise and implement right IT Governance Processes

After aligning the IT goals with the business goals, it is important to implement required set of efficient and effective IT governance and management processes. Using best practices such as COSO and COBIT will facilitate such implementation. It is important to select the most critical process based on business priorities, assign process owners, develop metrics and monitor the achievement of process as per set objectives.

3. Establish required IT Organisation and decision structure

Effective Governance of enterprise IT is determined by the way the IT department is organised and where the IT decision-making authority is located within the organisation. The responsibility for governance rests with the board of directors as they are responsible for evaluating, directing and monitoring the governance processes as per stakeholder requirements. They have to establish the right management structure with the C suite to ensure there is proper collaboration between business and IT department.

4. Involve Board of Directors/Executive Management in IT related matters

Governance initiatives may be initiated by IT or internal auditors but the overall responsibility vests with the board who assign specific responsibility to senior management from both business and IT. The executive management has to be aware and actively participating in the existing governance activities. IT topics and decisions should regularly appear and be discussed in executive committees or on board level, especially in organisations where IT plays a crucial role in keeping the business running. Even when the CIO is not a part of the executive committees, he should be represented by another executive member or he/she could be invited whenever an IT related topic is handled.

5. Govern and manage roles and responsibilities

The board should ensure that governance and management structures are established involving the organisation, the location of the IT function, the existence of clearly defined roles and responsibilities and a diversity of IT/business committees. The organisation structure should specify clear responsibilities defined towards the business they work for, and this throughout all levels, including the CIO and IT management. To make sure individuals adopt and execute upon their roles and responsibilities, a process of 'formal' evaluation and regular process of review has to be implemented as part of performance management system.

6. Establish IT Strategy and IT Steering Committee

Effective committees created at the right level with clearly defined roles and responsibilities play an important role in establishing ensuring alignment of IT with business which is key to successful implementation of GEIT. IT strategy committee has to operate at the board level and the IT steering committee has to operate at executive level with each committee having specific responsibility, authority and membership. The roles and responsibilities of these two key committees are explained in later chapter of this module.

7. Plan, align and manage IT enabled Investment as a Portfolio

Successful implementation of GEIT requires organisation to effectively their IT enabled investments throughout the economic life cycle of the projects using best practices of project management as required. Clear responsibility has to be allocated between IT who would be responsible for execution of IT enabled projects but business has to be responsible for analysing the anticipated benefits and making decisions.

8. Implement Performance Measurement system integrated with regular process

Measuring and monitoring the different IT processes at different levels is very important to review whether the set required service levels are met as set by the functional management. Goals have to be set at each of the levels starting from activity to process and linked to IT goals which are in turn linked to business goals. Metrics have to be set and monitored to ensure implementation and corrective action has to be taken as required. The performance management system could be integrated using the balanced scorecard technique with the complete set of metrics which is consolidated for different levels and areas as required. This is explained in detail in chapter 5.

9. Establish Sustainability through support, monitoring and regular communication

IT is most important support function to business activities as most of the service now a days are delivered through IT. Aligning business goals with IT goals requires ongoing and constant interaction between IT and business function. There has to be effective collaboration and interaction between business and IT. This requires a constant communication channel and mechanism to encourage the relationship between business and IT.

1.8 Summary

This chapter has provided an overview of concepts and practice of various aspects of Governance such as enterprise governance, corporate governance and GEIT. The interfaces between the different levels at which governance is implemented have also been highlighted. As IT is a key enabler of organisation processes, it is critical to implement GEIT as an integral part of governance. The regulatory and management requirements for implementing governance start with clearly established objectives and require using a systematic approach and use of relevant best practices frameworks as required. Corporate Governance and GEIT are closely inter-linked with enterprise risk management and internal controls. Regulatory requirement mandate the implementation of governance, enterprise risk management and internal controls. Organisations are established with the objective of value creation. Hence, they will implement governance not only from conformance perspective but also to provide value to the organisation. Hence, the two dimensions of conformance and performance have to be balanced in implementing governance in enterprises. Guidelines for implementing GEIT have been explained through generic guidelines starting from aligning IT strategy with enterprise strategy and ending with ensuring sustainability of GEIT implementation and thus making it an integral part of day-to-day process.

1.9 Questions

1. Who is responsible for establishing right structure of decision-making accountabilities?
   - A. Senior management
   - B. Operational management
   - C. Chief information officer
   - D. IT steering committee
2. The MOST important benefit of implementing Governance of Enterprise IT is:
   - A. Monitor and measure enterprise performance
   - B. Provide guidance to IT to achieve business objectives
   - C. Run the companies to meet shareholders’ interest
   - D. Ensure strategic alignment of IT with business
3. The primary objective of Corporate Governance is:
   - A. Reduce IT cost in line with enterprise objectives and performance.
   - B. Optimise implementation of IT Controls in line with business needs
   - C. Implement security policies and procedures using best practices.
   - D. Increase shareholder value by enhancing economic performance.
4. The ultimate objective Governance of Enterprise IT is to ensure that IT activities in an enterprise are directed and controlled to achieve business objectives for meeting the needs of:

A. Shareholders
B. Stakeholders
C. Investors
D. Regulators

5. Which of the following is a key component of Corporate Governance?
A. Employee rights
B. Security policy
C. Transparency
D. Risk assessment

6. Enterprise governance and Governance of Enterprise IT governance requires a balance between:
A. Compliance and return on investment expected by shareholders
B. Profit maximization and wealth maximization as decided by board
C. IT risks and cost of implementing IT controls as set by IT
D. Conformance and performance goals as directed by the board.

7. Business Governance helps the Board by enabling them to understand:
A. Enterprise functions
B. Risk assessment
C. Key performance drivers
D. Key controls

8. The effectiveness of the IT governance structure and processes are directly dependent upon level of involvement of
A. Heads of Business units
B. Internal auditor department
C. Technology management
D. Board/senior management

9. Which of the following is one of the key benefits of GEIT?
A. Identification of relevant laws, regulations and policies requiring compliance.
B. Improved transparency and understanding of IT's contribution to business
C. Better utilisation of human resources by using automation
D. Increased revenues and higher Return on investments.

10. Which of the following is the primary objective for implementing ERM?
A. Implement right level of controls.
B. Better availability of information.
C. Tighter security at lower cost.
D. Implement IT best practices.

1.10 Answers and Explanations

1. A. The senior management is responsible for ensuring right structure of decision-making accountabilities. The operational management is responsible for ensuring that operations of the enterprise are run as per enterprise policy. The chief information officer is responsible for ensuring IT enabled investments provide business value and the IT steering committee is responsible for steering IT enabled projects toward successful completion of objectives.

2. D. The MOST important benefit of implementing Governance of Enterprise IT is that it helps in ensuring strategic alignment of IT with business. Alignment of IT strategy in tune with enterprise strategy ensures value delivery from IT enabled investments. The monitoring and measuring of enterprise performance is one of the key processes of GEIT. GEIT does not provide guidance to IT to achieve business objectives but provides overall framework and setting for IT to achieve business objectives. Although GEIT is often implemented from a regulatory perspective and enables enterprises to meet corporate governance requirements, it does not directly focus on running the enterprises based on shareholders' interest. Shareholders are one of the key stakeholders whose objectives are considered while formulating enterprise goals.

3. D. The primary objective of Corporate Governance is to implement security policies and procedures using best practices. Corporate governance requirements are best met by using best practices which are globally accepted. The focus of implementing corporate governance is on ensuring regulatory compliance and this does not look at cost aspects. Hence, reducing IT cost in line with enterprise objectives and performance is not an objective. Further, optimised implementation of IT Controls in line with business needs has to be considered as part of GEIT and is not directly objective of corporate governance. There are multiple stakeholders whose interests are sought to be protected by regulations of corporate governance. One of the stakeholders are shareholders. However, the regulations do not consider how to increase shareholder value by enhancing economic performance but to protect their interests.

4. B. The ultimate objective Governance of Enterprise IT (GEIT) is to ensure that IT activities in an enterprise are directed and controlled to achieve business objectives for meeting the needs of the stakeholders. There are multiple stakeholders and GEIT requires balancing the needs of these stakeholders. Shareholders, Investors and Regulators are some of the stakeholders.

5. C. One of the key components of Corporate Governance is ensuring transparency. This promotes effective governance through establishing, communication and monitoring of performance. Employee rights are not the focus of corporate governance. Security policy as prepared by the IT as applicable for the enterprise is approved by the board. Corporate governance requirements do not provide any specific details of risk assessment but only outline need for implementing risk management as appropriate for the enterprise.

6. D. Enterprise governance and Governance of Enterprise IT governance requires a balance between IT risks and cost of implementing IT controls as set by IT. Risk appetite and Risk tolerance is set by the Board and this is based on risks which are acceptable and limit to which these are acceptable. The compliance and return on investment expected by shareholders is not relevant as shareholders do not have a stake in deciding this. The

last two options about profit maximisation and wealth maximisation as decided by board and conformance and performance goals directed by the board are translated through the overall enterprise strategy which is then translated into business and IT strategy.

7. C The primary objective of Business Governance is to ensure performance and hence the focus by Board is to understand and implement key performance drivers. The other options are related to operational areas which are dealt by management at their level as required.

8. D. The Board/senior management play the most critical role in ensuring the effectiveness of the IT governance structure and processes. Hence, the effectiveness of Governance is directly dependent upon their level of involvement. The head of business units work on implementing the directions of the board and are focused on management. The internal auditor department plays an important role in evaluating how well IT governance is implemented but their role is providing guidance. The technology management is responsible for aligning IT strategy in line with the enterprise strategy and implementing IT solutions which help meet enterprise objectives.

9. B. Implementing GEIT requires active collaboration between the board/senior management in directing IT towards enterprise objectives and putting a governance framework in place. Hence, the key benefit of GEIT is the improved transparency and understanding of IT's contribution to business which is reflected in the performance management system. Although identification of relevant laws, regulations and policies requiring compliance is important in implementing GEIT, this is not the primary benefit. Directly, the focus of GEIT is neither on better utilisation of human resources by using automation or on increased revenues and higher return on investments although they are considered as required.

10. A. The primary objective for implementing ERM is it helps in deciding and implementing the right level of controls. The other 3 options are indirect benefits of implementing ERM.

CHAPTER 2: GRC FRAMEWORKS AND RISK MANAGEMENT PRACTICES

Learning Objectives

As IT increasingly becomes a key enabler in enterprises of all types and sizes and there is transformation of enterprises from “Technology Oriented” to “Business and Technology oriented”, governance and risk management become imperative to ensure value creation and compliance. In the first chapter, we have understood how GEIT implementation can help in balancing performance with conformance. Use best practices framework helps in balancing risk vs return by implementing the right level of security. Implementing GEIT principles is critical to strive and thrive in the highly intensive IT era. Governance frameworks provide the structure within which the management can effectively operate to deliver results as per set objectives. A governance framework typically set in motion by the board of directors defines the rules under which the management system operates to translate the board strategy into specific actions. Governance is about ensuring that the required authority and responsibility is allocated appropriately within the organisation. It defines the boundaries of decision making together with mechanism that ensures that performance is monitored and risks are identified and escalated so they are managed at the appropriate level. Risk management at enterprise level encompassing all levels and all areas is critical for successful implementation of governance. Governance, Risk and Compliance is a regulatory requirement and this can be effectively implemented using well established frameworks. There are a plethora of frameworks for implementing GRC and GEIT. This chapter provides overview of some of the key GRC frameworks and also elaborates key concepts of risk management from strategy to operations.

2.1 Introduction

IT is key enabler of enterprises and forms the edifice on which the information and information systems are built. Implementing Governance, risk management and internal controls is not only a management requirement but is also mandated by law. In India, Clause 49 listing requirements seek *inter alia* certification of governance, risks and control by auditors. In an IT environment embedding the right level of controls within the information systems to ensure that users can access required information securely and safely and as per business requirements is critical for survival. This not only ensures business success but is also a key requirement for the continued growth of the enterprise. In implementing internal controls in an IT environment, the legacy approach of considering IT and its contents as boxes to be secured by the IT department is fraught with extreme risk as the traditional methods of securing IT from perimeter perspective is no longer relevant. Users of IT need to access and use information from anywhere, anytime. There is need to adapt a macro level and architecture perspective for securing information and information systems. Hence, both from regulatory as well as enterprise perspective, senior management have to be involved in providing direction on how governance, risk and control are implemented using a holistic approach encompassing all levels from strategy to execution. The Board of directors have to evaluate, direct and monitor effective use of IT to achieve enterprise objectives. This governance approach will ensure harnessing the power of information and information technology for achieving business objectives in addition to meeting regulatory requirements. Best practices framework provide management with distilled knowledge of experts and this can be customised to meet stakeholder requirements which include *inter alia* management and regulators. Management has to choose the right mix of frameworks for implementing governance, risk, security and controls. IS Auditors can assist management in implementing these frameworks in an advisory capacity or provide assurance on how well the GRC frameworks have been implemented to meet stakeholder requirements and provide recommendations for improvement. From regulatory perspective, management have to certify whether Risk management and internal controls have been implemented as per organisation needs and auditors have to certify whether this implementation is appropriate and adequate.

2.2 GRC frameworks

2.2.1 COSO

COSO is an Enterprise Risk Management-Integrated Framework which was first published by the Committee of Sponsoring Organisations (COSO) established by Treadway commission in 1992 to define the internal control framework for business organisations, particularly listed companies where the stakeholders are common people who invest in securities. The latest update of COSO is the COSO Framework 2013. COSO has developed the framework for internal controls focusing on designing of controls based on risk assessment. According to COSO framework internal control is defined as “a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”. The Executive Summary of Internal Control: Integrated Framework provides a high-level overview of the 2013 Framework and is intended for the CEO and other senior management, boards of directors, and regulators.

The COSO framework 2013 formalises the principles embedded in the original more explicitly, incorporates business and operating environment changes over the past two decades, and improves the Framework’s ease of use and application. The 2013 Framework also makes it easier for management to see what’s covered and where gaps may exist in their current SOX 404 compliance program. The Framework set out in detail, defining internal control, describing the components of internal control and underlying principles, and providing direction for all levels of management in designing and implementing internal control and assessing its effectiveness.

The 2013 Framework has three categories of objectives: operations, reporting, and compliance and consists of five integrated components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities. The Framework is adaptable to a given organisation’s structure, allowing customisation to consider internal controls from an entity, divisional, operating unit, and/or functional level, such as for a shared services centre. The key role of management judgment in designing, implementing, and maintaining internal control, as well as assessing its effectiveness, is retained. A visual representation of COSO’s Internal Control: Integrated Framework (i.e., the updated COSO Cube) is given here.

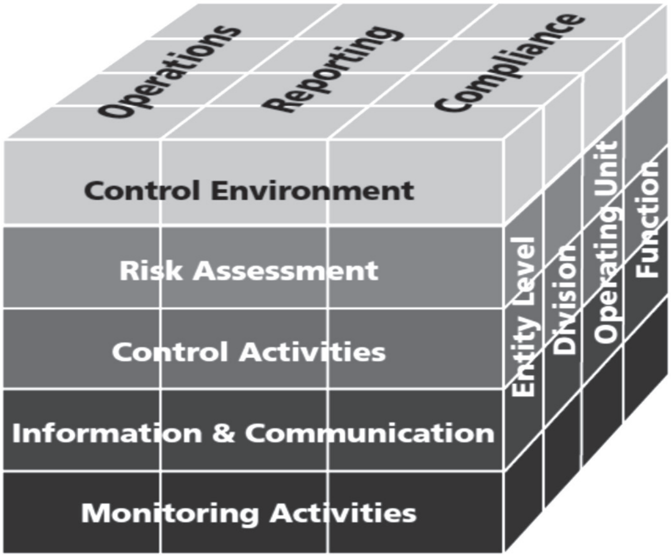


Figure 2.1: COSO 2013 Framework Cube

The COSO cube has 3 dimensions. The first dimension depicts internal controls and the 5 interrelated components. The second dimension depicts control objectives and third dimension provides controls at different levels of the enterprise. The titles of the 17 internal control principles organised by the five internal control component are given below:

Control Environment: For each business process, an organisation needs to develop and maintain a control environment including categorising the criticality and materiality of each business process, plus the owners of the business process.

- Demonstrates commitment to integrity and ethical Values
- Exercises oversight responsibility
- Establishes structure, authority, and responsibility
- Demonstrates commitment to competence
- Enforces accountability

Risk Assessment: Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.

- Specifies suitable objectives
- Identifies and analyses risk
- Assesses fraud risk
- Identifies and analyses significant change

Control Activities: Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

- Selects and develops control activities
- Selects and develops general controls over technology
- Deploys thourgh policies and procedures

Information and Communication: Associated with control activities are information and communication systems. These enable an organisation to capture and exchange the information needed to conduct, manage, and control its business processes.

- Uses relevant information
- Communicates internally
- Communicates externally

Monitoring: The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

- Conducts ongoing and/or separate evaluations
- Evaluates and communicates deficiencies

The three main categories of Control objectives of COSO are:

1. **Operations objectives:** Relate to the achievement of the organisation's mission and are based on management's choices relating to structure, industry considerations and the performance of the entity.
2. **Reporting objectives:** These are further divided into:
   a. **External financial reporting objectives:** Relate to the organization's obligations for its financial statements.
   b. **External non-financial reporting required objectives:** Include reporting on its internal control effectiveness and operational processes.
3. **Compliance objectives:** Relate to the laws and regulations that apply to the entity considering any foreign entities that are relevant.

Enterprises planning to implement COSO have to consider the five inter-related components and principles of internal control apply to the enterprise and adapt this as per specific requirements of the enterprise. The principles are generic and have to be customised as per stakeholder needs and as decided by the management. The involvement starts with the senior management setting the risk appetite and risk tolerance limits for the enterprise as whole.

Requirements for effective internal control

COSO 2013 clarifies requirements for effective internal control as follows:

- Effective internal control provides reasonable assurance regarding the achievement of objectives and requires that:
  - Each component and each relevant principle is present and functioning
  - The five components are operating together in an integrated manner
- Each principle is suitable to all entities; all principles are presumed relevant except in rare situations where management determines that a principle is not relevant to a component (e.g., governance, technology)

- Components operate together when all components are present and functioning and internal control deficiencies aggregated across components do not result in one or more major deficiencies
- A major deficiency represents an internal control deficiency or combination thereof that severely reduces the likelihood that an entity can achieve its objectives

COSO 2013 framework describes the role of controls to effect principles. The Framework does not prescribe controls to be selected, developed, and deployed for effective internal control. An organization's selection of controls to effect relevant principles and associated components is a function of management judgment based on factors unique to the entity. A major deficiency in a component or principle cannot be mitigated to an acceptable level by the presence and functioning of other components and principles. However, understanding and considering how controls effect multiple principles can provide persuasive evidence supporting management's assessment of whether components and relevant principles are present and functioning.

COSO is primarily a framework for implementing internal controls that IS auditor reviews for effectiveness. Identification of controls is based on level of risk mitigated by that controls, hence COSO focuses on Risk management as major area of the framework. However it does not provide how organizations should approach the risk assessment and control identification. Hence it is a high-level framework. Please visit www.coso.org for latest updates of COSO framework.

Clause 49 of the listing agreements issued by SEBI in India is on similar lines of SOX regulation and mandates inter alia the implementation of enterprise risk management and internal controls and holds the senior management legally responsible for such implementation. Further, it also provides for certification of these aspects by the external auditors. It may be noted that COSO and COBIT together have been internationally used as best practices framework for complying with SOX. The details of how IT compliance can be best implemented or reviewed by using best frameworks such as COSO and COBIT 5 is explained further in the following sections.

2.2.2 COBIT 5

COBIT 5 issued by ISACA (www.isaca.org) is the Business Framework of Governance and Management of Enterprise IT. As per COBIT 5, Information is the currency of the 21st century enterprise. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues. COBIT 5 provides the approach and latest thinking based on global best practices. It is an umbrella framework for implementing Governance and management of information systems.

COBIT 5 can be used as a benchmark for reviewing and implementing governance and management of enterprise IT. It has a set of 5 principles and 7 enablers which are the building block of the framework. This principles and enablers make COBIT 5 an effective tool for implementing GEIT and helps enterprises in various ways such as: simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities. As COBIT 5 is a comprehensive framework and has best practices covering all key process, it's implementation can enable enterprises to adapt it as required to achieving enterprise objectives for the governance and management of enterprise IT. The best practices of COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.

COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders. COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy. COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction. The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

Need for Enterprises to Use COBIT 5

Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance and management to address these critical business issues. COBIT 5 is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies. It helps enterprises to create optimal value from their information and technology. COBIT 5 provides the tools necessary to understand, utilise, implement and direct important IT related activities, and make more informed decisions through simplified navigation and use. COBIT 5 is intended for enterprises of all types and sizes, including non-profit and public sector and is designed to deliver business benefits to enterprises, including:

- Increased value creation from use of IT;
- User satisfaction with IT engagement and services;
- Reduced IT related risks and compliance with laws and regulations.
- Development of more business-focused IT solutions and services; and
- Increased enterprise wide involvement in IT-related activities.

Integrating COBIT 5 with other frameworks

There is no single framework which provides all the requirements for all types of enterprises. Hence, enterprises have to select the right blend of frameworks and best practices. The main advantage of using COBIT 5 is that it is provides an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance. COBIT 5 also provides a basis to integrate effectively other frameworks, standards and practices used such as ITIL, TOGAF and ISO 27001. It is also aligned with The GEIT standard ISO/IEC 38500:2008, which sets out high-level principles for the governance of IT, covering responsibility, strategy, acquisition, performance, compliance and human behaviour that the governing body (e.g., board) should evaluate, direct and monitor. Thus, COBIT 5 acts as the single overarching framework, which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language. The COBIT 5 Framework provides an overview of specific related frameworks in terms of breadth, depth and level of coverage. This helps in understanding and integrating different frameworks as required. The integration of framework and resulting enablers should be aligned with and in harmony with (amongst others) the:

- Enterprise policies, strategies, governance and business plans, and audit approaches;
- Enterprise risk management framework; and
- Existing enterprise governance organisation, structures and processes.

Customising COBIT 5 as per requirement

COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Enterprises can select required guidance and best practices from specific publications and processes of COBIT 5 and implement these in specific areas based on their areas of need. Because of its open design, it can be applied to meet needs related to Information security, Risk management, GEIT, Assurance activities, legislative and regulatory compliance, etc.

Five Principles of COBIT 5

COBIT 5 simplifies governance challenges with just five principles. The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimises information and technology investment and use for the benefit of stakeholders. These principles are shown in Fig. 2.2 and each of the principles are explained as their understanding is critical for implementation.

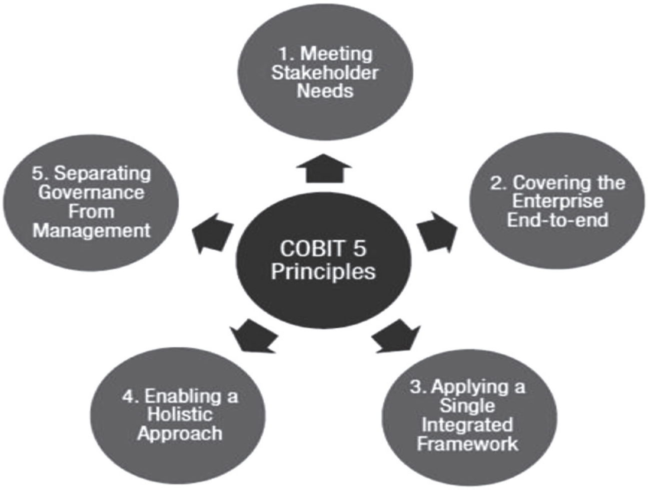

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Figure 2.2: Five Principles of COBIT 5

Principle 1: Meeting Stakeholder Needs

Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes and practices.

Every enterprise operates in a different context; this context is determined by external factors (the market, the industry, geopolitics, etc.) and internal factors (the culture, organisation, risk appetite, etc.), and requires a customised governance and management system. Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customised enterprise goals, IT related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

Principle 2: Covering the Enterprise End-to-End

COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. It considers all IT related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone: internal and external that is relevant to governance and management of enterprise information and related IT. The end –to-end governance approach is the foundation of COBIT 5 and covers all the key components of a governance system.

Principle 3: Applying a Single Integrated Framework

There are many IT related standards and best practices, each providing guidance on a sub set of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.

Principle 4: Enabling a Holistic Approach

Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.

Principle 5: Separating Governance from Management

The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organisational structures and serve different purposes. The interface between governance and management processes and activities at different levels is depicted here.

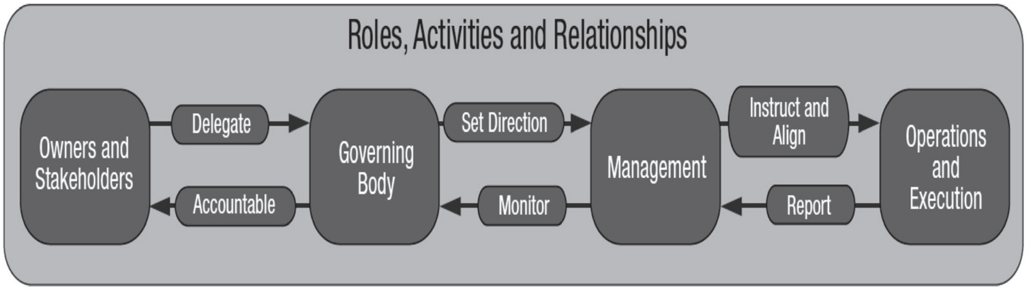


Figure 2.3: Roles, activities and relationships of Governance and management

Governance: It ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

In most of the enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in larger, complex enterprises.

Management: It plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

In most of the enterprises, management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO). From the definitions of governance and management, it is clear that they comprise different types of activities, with different responsibilities. The role of governance is to evaluate, direct and monitor. There is need for a set of interactions between governance and management to result in an efficient and effective governance system. The specific interfaces between Governance and management are established through governance mechanisms. These interfaces include:

- Principles and policies that define objectives, agreed plans, responsibilities, boundaries, authority, exception arrangements and reporting arrangements;
- Structure for decision making based on agreed principles and policies;
- Processes and Practices to ensure implementation; and
- Relationship Mechanism aimed at improving communication between business and IT.

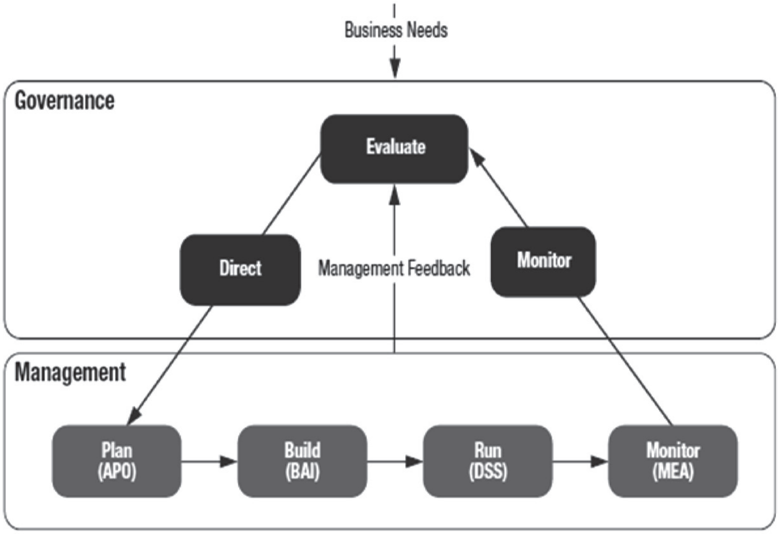


Figure 2.4: Key Areas of Governance and Management

Seven Enablers of COBIT 5

Enablers are factors that, individually and collectively, influence whether something will work; in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. The COBIT 5 framework describes seven categories of enablers which are to be implemented as required for meeting stakeholder requirements. The seven enablers are briefly discussed here and are depicted in in Fig. 2.5.

- **Principles, Policies and Frameworks:** The vehicle to translate the desired behaviour into practical guidance for day-to-day management.
- **Processes:** Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organisational structures:** The key decision-making entities in an enterprise.
- **Culture, Ethics and Behaviour:** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
- **Information:** is pervasive throughout any organisation and includes all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications:** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies:** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

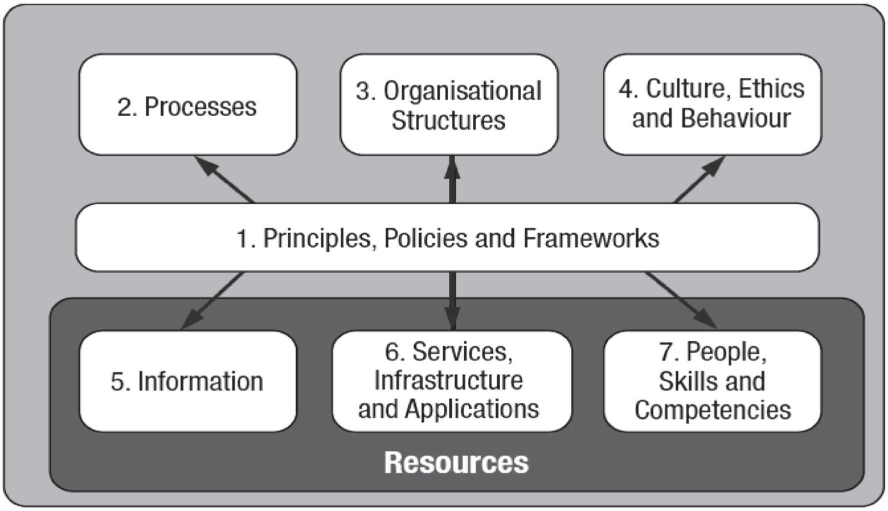

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Figure 2.5: Seven Enablers of Governance

2.2.3 ISO 38500

ISO 38500 is the ISO standard for corporate governance of IT. The standard is focused at high level and states that the board of directors should govern IT by:

1. **Evaluating** the current and future use of IT.
2. **Directing** preparation and implementation of plans and policies to ensure that the use of IT meets business objectives.
3. **Monitoring** conformance to policies and performance against the plans.

The objective of ISO 38500 is to provide a structure of principles for directors and other stake holders to use when evaluating, directing and monitoring the use of IT in their organisations. It provides a structure for effective governance of IT to assist those at the highest level of organisations to understand and fulfil their legal, regulatory and ethical obligations regarding their organisations' use of IT. The scope of the standard is to provide guiding principles for directors of organisations on the effective, efficient and acceptable use of IT within their organisations. It is applicable for all organisations, from the smallest to the largest, regardless of purpose, design or ownership structure. The standard is more of a high level expectation from management as to what should be the outcome from IT governance, however it does not provide direction or guidelines as to how it should be achieved. COBIT 5 ensures that these guidelines are available and organization implementing COBIT can be ISO 38500 compliant.

2.2.4 ISO 31000

ISO has developed a new standard for IT risk management. The standard primarily adopts AS/ NZS 4360 for risk management. The modification it has made is that ISO has added processes for IT risk governance by defining IT risk committee. More details of ISO standards are provided in Chapter 3 of Module 2.

2.2.5 RIMS ERM

Standard developed by Risk and Insurance Management Society of Standards and Technology, primarily for insurance sector. RISM primarily focuses on enterprise risk management and provides all-encompassing process for risk management within organisation.

- **ERM-based approach**
  - o Executive support covering all processes, functions, business lines, roles and geographies.
  - o Integration, communication and co-ordination of internal audit, information technology, compliance, control and risk management.
- **ERM process management**
  - o Embedding the ERM Process into business processes
  - o To identify, assess, evaluate, mitigate and monitor.
  - o Using qualitative methods supported by quantitative methods, analysis, tools.
- **Risk appetite management**
  - o Understanding the risk-reward trade-offs.
  - o Accountability within leadership
  - o Policy to guide decision-making
  - o Attack gaps between perceived and actual risk.
  - o Define Risk appetite boundaries for acceptable risk and risk tolerance
- **Root cause discipline:**
  - o Measuring a problem's root cause
  - o Binding events with their process sources to drive the reduction of uncertainty

  - Collection of information and measurement of the controls' effectiveness.
  - Measure risk from people, external environment, systems, processes and relationships

- **Uncovering risks**
  - Documenting risks and opportunities.
  - Collecting knowledge from employee expertise, databases and other electronic files
  - Uncover dependencies and correlation across the enterprise.
- **Performance management**
  - Executing vision and strategy, working from financial, customer, business process and learning and growth perspectives using tools like BSC.
  - Exposure to uncertainty, or potential deviations from plans or expectations.
- **Business resiliency and sustainability**
  - Extent of ERM Process's sustainability integrated into operational planning.
  - Evaluating how planning supports resiliency and value.
  - Ownership and planning beyond recovering technology platforms.

2.2.6 RiskIT: Risk Management framework by ITGI and ISACA

RiskIT framework is created by ISACA and ITGI. The framework is based on COBIT framework and can be mapped to most global standards. This framework is process driven framework and covers three major areas:

1. Risk Governance
2. Risk Evaluation
3. Risk Response

IT risk management as suggested by ISO 27001. It is a method based on identifying risks and vulnerabilities within IT assets and implement controls to mitigate them. However, considering the shortcomings of this method, the revised ISO 27001:2013 has recommended using ISO 31000 for IT risk management. ISACA has recently released COBIT 5 for Risk which integrates the principles of Risk IT, Val IT and COBIT 5. COBIT 5 for Risk which is built on the principles of COBIT 5 can be used for implementation of risk management from governance perspective.

2.3 Enterprise risk management and IT risk management

2.3.1 Risk Management

Enterprise Risk Management and IT Risk Management are key components of an effective IT governance structure of any enterprise. Effective IT governance helps to ensure close linkage to the enterprise risk management activities, including Enterprise Risk Management (ERM) and IT Risk Management. IT governance has to be an integral part of overall corporate risk management efforts so that appropriate risk mitigation strategies are implemented based on the enterprise risk appetite. The risk assessment approach adapted has to consider business impact of IS risk and different types of risks. There has to be timely and regular communication of status of residual risks to key stakeholders so that appropriate action is taken to manage the IT risk profile. This section will provide an overview of related terms like threats, vulnerabilities etc., IS Risks and exposures and risk mitigation strategies, which can be adapted by the organisations.

Risk management process is a crux of any business today and it is a day-to-day activity. Risk management processes primarily focuses on three major areas viz. Market Risk, Credit Risk and Operational Risk. Most organisation addresses first two risks i.e. market risk and credit risks since these are part and partial of business activities. Whereas operational risks addresses the issues and concerns related to operations of a business. Today's organisations depend heavily on information and related technology and majority operations have been automated. Hence, it is important to consider IT risks as these by themselves are very critical but in terms of impact on other risks, they can impact all areas of enterprise operations. Hence, it is important to understand how the use of technology has introduced various new types of risks and their impact specifically in organisations which are heavily dependent on technology. The Figure below describes the relationship on technology risks in overall risk scenario.

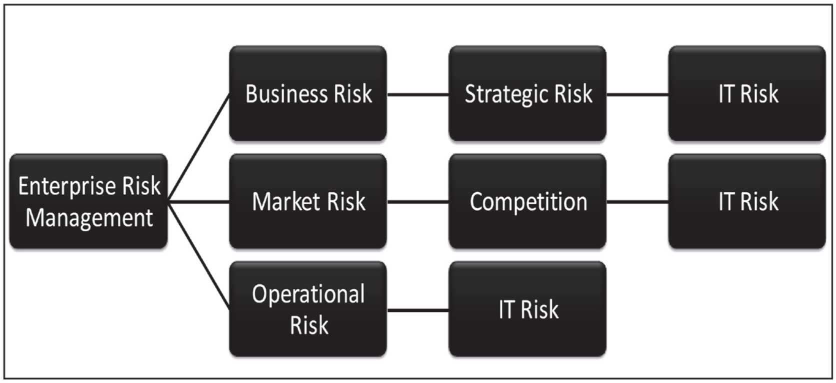


Figure 2.6: Relation of IT Risks

2.3.2 Risk Management in COBIT 5

IT Risks have to be managed from holistic perspective and this approach is called risk optimisation. The COBIT framework provides excellent guidance on risk management strategy and practices from governance and management perspective. The Governance domain contains five governance processes and one of the Governance process: "EDM03: Ensure risk optimization" primarily focuses on stakeholder risk-related objectives. The objective of this process is to ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated and that risk of IT is identified and managed. The key benefits of implementing appropriate risk optimisation process is that it ensures that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures are minimised.

The COBIT framework has management domain of "Align, Plan and Organise", which contains a risk-related process: "APO12: Manage Risk". This process requires continually identifying, assessing and reducing IT-related risk within levels of tolerance set by enterprise executive management. The primary purpose of this process is to integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk. All enterprise activities have associated risk exposures resulting from environmental threats that exploit enabler vulnerabilities.

The combination of Governance practices of “EDM 03: Ensure risk optimization” (which ensures that the enterprise stakeholders approach to risk is articulated to direct how risks facing the enterprise will be treated) and the management practices of “APO12 Manage risk” (which provides the enterprise risk management (ERM) arrangements that ensure that the stakeholder direction is followed by the enterprise) together ensured that Risk management covers the entire life cycle and covers both governance and management perspective. Further, detailed guidance is available in the form of specific practices and activities that are designed to treat related risk (avoid, educe/ mitigate/control, share/transfer/accept). In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process including risk-related roles at each level of management as appropriate.

Key Governance Practices of Risk Management

Implementing governance requires that governance practices covering all the aspects of governance of risk management are covered. There are three broad areas:

- **Evaluate Risk Management:** Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;
- **Direct Risk Management:** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board’s risk appetite; and
- **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

Key Management Practices of Risk Management

Implementing Risk Management requires that the risk management practices are embedded in all the key organisational processes as required and are performed as part of the day to day tasks and activities. A process oriented approach has to be followed for implementing risk management. The key management practices of effective risk management are:

- **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.
- **Analyse Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.
- **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.

- **Articulate Risk:** Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.
- **Respond to Risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

Metrics of Risk Management

Enterprises have to monitor the processes and practices of IT risk management by using specific metrics. Some of the key metrics are:

- Percentage of critical business processes, IT services and IT-enabled business programmes covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk Assessment;
- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

2.3.3 Risk Factors

There are unique risks for each organisation, given the nature of operations, although generally organisations within the same sector will have common risk elements. The appropriate risk response will be different from organisation to organisation, depending on how management views the risk in terms of magnitude. Risks are represented in the external environment in which the organisation chooses to operate, as well as those in the internal environment. Risk factors in the external environment and generally outside of the organisation's direct control. External risk factors include political situations, the economy, regulations, natural disasters, competition. Internal risk factors includes Organisation's culture, Internal environment affecting employees moral, policies, ethics and values projected by senior management, process environment, control environment and so on.

2.3.4 Categories of Risks

The risk management process begins with the identification of risk categories. An organisation will have several risk categories to analyse and identify risks that are specific to the organisation. Some examples of risk categories are:

- **Business Risks:** Also sometimes referred as inherent risks. These are risk associated with nature of business. E.g. loss of finished product for food industry
- **Market Risks:** Risks associated with fluctuations on market affecting the customer base of organization. E.g. Customer preferring smart phones over traditional phones affecting Nokia products.
- **Financial Risks:** Risk associated with financial decisions and environment in which business operates. E.g. Non-availability of funds, excess expenditure etc.
- **Operational Risks:** Risks associated with failure of operations of organisation. E.g. failure of assembly-line for car manufacturer, non-availability of IT for banking services etc.

- **Strategic Risks:** Associated with incorrect and inappropriate strategy selection and implemention. E.g. Planning for implementing IT application that is outdated, selecting application for automation that may not satisfy future growth expectations. Not-considering effect of smart phones by Nokia management.
- **IT Risks:** How the company's IT infrastructure relates to business operations and their impact on business in case risk materialises. E.g. failure of networks affecting communications, failure of applications impacting operations and service delivery.
- **Compliance Risks:** Risk when an organisation does not comply with legal, regulatory, contractual or internal compliance requirements E.g. failure of complying with privacy laws, labour laws, software license agreement.

2.3.5 Elements of Risk Management

Before establishing a strategy for information risk management, the following elements must be in place to permit effective risk management:

- **Top Management Support:** The need for risk management must start and be supported at the highest level within the company. This includes the governance level and the CEO.
- **Proactive Approach:** Risk management efforts must be proactive. This involves the active identification, measurement and management of the risks, scanning of changes in the risk profile and reports on managing the risk profile.
- **No Ambiguity:** There needs to be a clear definition of the risks, and these must be understood across the organization.
- **Accountability:** Responsibility for responding to and managing the risks must be clearly understood and individuals held accountable for fulfilling the roles.
- **Resource Allocation:** Appropriate resources including people and tools need to be deployed and available to help managers, executive and the governance level conduct their obligations within the risk management framework.
- **Cultural Change:** The organisation’s culture must provide for the active management of risk.

2.4 Risk Management strategies

When risks are identified and analysed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is illustrated below in Figure 2.7:

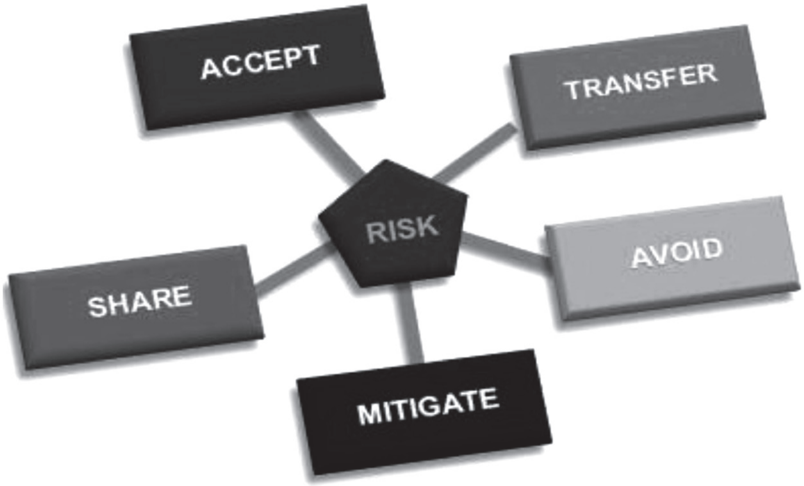


Figure 2.7: Risk Mitigation strategies

The risk mitigation strategy is explained for each of the options.

- **Tolerate/Accept the Risk.** One of the primary functions of management is managing risks. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the Risk.** It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the Risk.** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organisation. Risk also may be mitigated by transferring the cost of realised risk to an insurance provider.
- **Treat/mitigate the Risk.** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimise its effects.
- **Turn Back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

2.4.1 Developing Strategies for Information Risk Management

Some organisations have adopted a centralised model for risk management, while others are using a decentralised model. The approach depends on:

a. An organisation's particular operations

b. The significant risks

c. The culture of the organisation

d. The management style and

e. The control environment i.e. the degree of centralisation or the delegation of authority and the infrastructure of the business.

In a centralised model it is the Information Risk Management team that develops policies for the board to consider. Other organizations have decentralized model requiring the involvement of front line staff in managing the inherent risks of the company, of the business unit or of the process.

2.4.2 Risk Register and control catalogue

It is a collective record of all identified and evaluated risks along with risk owner and risk response. The structure of risk register may vary from organisation to organization, however it must:

1. Contain risk scenario, likelihood, assets impacted, overall impact on business (assessment), owner, risk response decision, reference to control catalogue, review date.
2. It must be maintained based on updating process.
3. Generally it is used to develop risk profile for reporting to management and approval.

IS auditor should use this risk register to review and audit the risk management process and also ensure that appropriate controls are identified, designed and implemented. Control catalogue is collective register of all controls designed and implemented within organisation with reference to risk register.

2.5 Risk management process

The Objective of risk management process is to ensure that the organisation can manage risks with acceptable limits. These acceptable limits are decided by Risk Appetite ad Risk tolerance.

Risk Appetite: It is ability of organisation to sustain losses due to materialisation of risk. It also represents the ability of organisation to take risk while considering new business initiatives.

Risk Tolerance: It is the limit up to which organization can tolerate to sustain loss of business in case risk materialises. In other words, in case any risk materializes the organisation must recover from it within specified time decided by risk materialization.

Information Risk Management process involves a continuous cycle to identify, assess, measure, decide response, assign responsibility and monitor information risk. Organisation may adopt any standard or framework discussed earlier for implementing Information risk management. Although different framework describe different processes for managing IT risks, typically IT risk management process follows following steps:

1. Risk Identification
2. Risk Evaluation
3. Risk Prioritisation
4. Risk Response

5. Risk Mitigation
6. Risk Monitoring

2.5.1. Risk Identification

As name suggest it is process to identify risks for organisation. Organisation may deploy one or more methods to identify risks. Some methods are:

1. Workshop and brainstorming sessions with stakeholders and process owners: In this method the process owners and risk practitioners (IS Auditors) meet and discuss the possible causes for process failures affecting desired outcome. This workshops typically covers risk identification, risk evaluation, control definition steps. In case process owners does not agree a method called Delphi technique we used to assess the risks.
2. Use of generic risk scenarios based on industry experience and historical data: Generic scenarios are the list of possible incidents affecting desired outcome of business process objectives.
3. Review and audit of processes and technology. This includes vulnerability assessment: Audit findings, lessons learned from Incident response, vulnerability assessments helps organization in identifying possible threats that can impact the normal functioning of business processes.

Organisations may adopt various methods for identifying and recording risks some of them are discussed here.

Threat profile/ Inventory

It is a list of all possible threats that might have impact on organisation. Organisation may prefer to categorize them based on nature.

- **Physical and Environmental** for example fire, theft, humidity, temperature
- **External** threats that are not in control of organisation like hackers, Denial of service, virus, sabotage, targeted attacks
- **Internal** threats are those are initiated within organisation for example disgruntled employee, unauthorised access by authorised users, confidential data leakage by employee, misuse of management override. Majority breaches are due to internal threats
- **Natural** threats like earthquake, floods, and tsunami

Organisation may prepare a list of threats and try to evaluate how they affect organisation.

Vulnerability Assessment

A vulnerability assessment is one of the proceses of identifying, the vulnerabilities in a system. Vulnerability assessment is a one process in risk identification. The Vulnerability Assessment is an evaluation to identify gaps and vulnerabilities in your network, servers, etc. help you validate your configuration and patch management, and identify steps you can take to improve your information security. The assessment helps you meet your minimum compliance mandates and security assessment needs. Assessments are typically performed according to the following steps:

a. Cataloguing assets and resources in a system.

b. Assigning quantifiable value or rank and importance to those resources

c. Identifying the vulnerabilities or potential threats to each resource

Vulnerabilities that may exist across your systems and applications can create an easy path for hackers to gain access to and exploit your environment. With dozens and even hundreds of applications and systems across your environment with access to the Internet, maintaining and updating system operating systems and applications to eliminate vulnerabilities is paramount – especially when those applications and systems are tied to sensitive customer, patient or cardholder information.

Asset Inventory

Risks when materialise affect the functioning of organisation. The impact of a risk can be different for different business function depending upon the various factors like time of incident, functions affected etc. For example in case on a Bank failure of connectivity might affect ATM network as well as branch network, however if the failure happens after business hours impact of non-availability of ATM could be higher. In other words providing protection for connectivity to ATM shall be different as compared to branch networks. In order to provide appropriate security organisations may focus on implementing controls over assets that supports business processes. ISO27001:2005 also recommends to implement controls around assets by prioritizing them based on results of risk evaluation. (ISO27001:2013 recommend ISO31000 for Risk management and also states that risk management need not be asset based.)

Risk components

Risk to be managed effectively have to be understood in totality. Hence, it is important to understand all the specific components of all identified risks and these are:

- **Risk Scenario :** A possible event due to materializing of one or more risks for example Failure of connectivity might be caused due to one or more reasons like physical damage to cables / devices, malfunction of devices, virus/malware attack, Denial of service attack, failure of service provider
- **Threat :** Reason for risk materialization for example theft of equipment, fire, natural disaster, non-availability of human resources, Virus
- **Vulnerability:** Weakness that gets exploited due to threat. For example absence of antivirus is a vulnerability that will enable a virus to infect the system or improper physical security leading to theft
- **Likelihood/Probability:** Judgment of possibility that threat shall exploit vulnerability. For example there is always a possibility of earthquake, however it may not take place every day. The possibility can be worked out based on historical data and seismic zone in which facility is located. Or possibility of virus attacking systems can happen multiple times in a day
- **Impact/Consequences:** When threat materialises, it will affect normal functioning which might result in loss of business, interruption of services. A calculation of possible loss expressed in monetary terms.

- **Response:** Action Plan designed by organisation to minimize impact or likelihood of risk materializing. There are four types of responses and organisation may choose one or more for each risk. The four types are: Accept, Transfer, Avoid and Mitigate. For example Management may have process to monitor virus by maintaining antivirus tool updated and also run a schedule scan. In case cost of process and tool is higher than impact organisation may decide to do nothing and accept the risk
- **Controls/Mitigation:** In order to mitigate risk management implements controls. For example Access controls reduces the likelihood of unauthorised access, Fire suppression system reduces the impact due to fire
- **Inherent Risk:** Total risk without any controls is inherent risk
- **Residual Risk:** Controls cannot mitigate the risk completely. It may reduce likelihood and/ or impact. There is a small portion of risk still remains that is known as residual risk. It also includes accepted risk
- **Risk Aggregation:** A risk faced by organisation may have different impact on different business function/ locations. However from organisation's perspective it is necessary to present them as total risk for organisation. For example a location on seashore may have higher risk of flooding as compared to another location away from seashore.
- **Risk Profile:** Collective view of all risks an organisation likely to face
- **Heat Map:** Graphical representation of risk profile
- **Risk Register:** A document that is maintained to provide information on identified risks and contents details of components
- **Risk Owner:** Person or entity that is responsible for evaluation and decision of response for identified risk

2.5.2. Risk Evaluation

Also called risk assessment. It is a process for assessing likelihood and impact of identified risk. There are two methods used for risk evaluation

1. **Quantitative Risk Analysis** refers to expressing total risk in monetary terms
2. **Qualitative Risk Analysis** refers to expressing total risk with qualification like high, medium, low etc. However the challenge is perception of these terms differs from person to person, hence it is necessary to define the meaning of terms high, medium and low so that there are interpreted uniformly across organisation.

Determine likelihood of risk

Once risks are identified, the next step is to determine the likelihood that the potential vulnerability can be exploited. Several factors need to be considered when determining this likelihood.

a. Consider source of the threat, motivation behind the threat, and capability of the source.

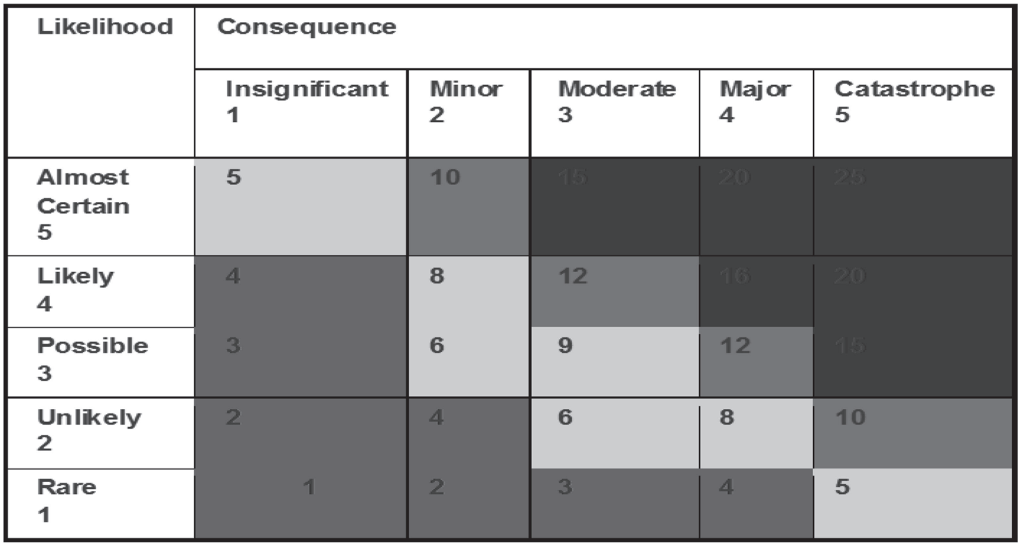
b. Determine the nature of the vulnerability and,

c. The existence and effectiveness of current controls to deter or mitigate the vulnerability. The likelihood that a potential vulnerability could be exploited can be described as high, medium, or low.

Most of the time the likelihood is judgment of analysts hence it is best estimated by risk owners who are the business process owners as they are likely to be affected due to risk materialization. This helps in arriving at likelihood.

2.5.3. Risk prioritisation

Based on evaluation of risks, have to be prioritised into high, medium or low or ranked on scale of 1 to 5. This risk ranking will help enterprises to decide the priority in which the risks will be mitigated. Based on the decisions taken in this process/stage, the next step of risk response is implemented. The organisations generally use Risk profile and Heat map to prioritise evaluated risks based on criticality of risks and priorities of business objectives.



Likelihood	Consequence				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophe 5
Almost Certain 5	5	10	15	20	25
Likely 4	4	8	12	16	20
Possible 3	3	6	9	12	15
Unlikely 2	2	4	6	8	10
Rare 1	1	2	3	4	5

Figure 2.8: Risk prioritisation

2.5.4. Risk Response

With the potential impact assessment in hand, the next step is to determine what the appropriate response is to prudently manage the risk. The risk responses are given here:

Response	Description
Avoid	Eliminate the risk by eliminating the cause e.g. where feasible, do not implement processes that would incur risk
Accept	This response is to accept the level of risk and monitor
Transfer/Share	This response is to transfer the risk to someone else, e.g. purchase insurance or share with outsourcing service provider
Mitigate	Refers to define controls to reduce the likelihood or impact or both so as to bring the residual risk within the acceptable limits defined by risk appetite and risk tolerance

For each risk identified, the risk response can be articulated the objective is to bring the estimated risk below the Risk appetite and Risk tolerance of the organisation. For example, where the risk response is to accept the risk, this becomes part of the organisation's risk tolerance, means the business must recover from impact before tolerance limits.

2.5.5. Risk Mitigation

Defining controls to reduce likelihood and/or impact of risk is referred as risk mitigation. The controls are designed based on the nature and type of process after considering process objectives. Controls are selected based on the cost benefit analysis. The cost of control covers cost for tools, impact on process efficiency, resource requirements, training requirements and cost associated with monitoring of control. Total cost is compared against the total impact reduced due to controls i.e. difference between evaluation of inherent risk and residual risk. In case of positive difference controls are implemented. In case of negative results organisation may select another response like accept or avoid the risk.

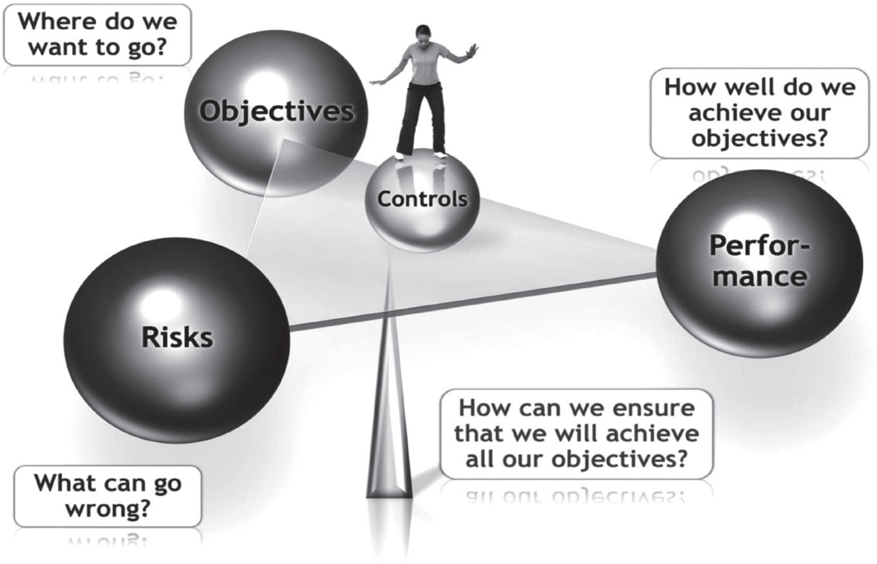

Where do we want to go?
Objectives
How well do we achieve our objectives?
Controls
Perfor-mance
Risks
How can we ensure that we will achieve all our objectives?
What can go wrong?

Figure 2.9: Relationship of Risks and Controls

2.5.6. Risk Monitoring

Once the controls are implemented what remains is residual risk i.e. risk remaining after implementing controls and risk accepted. For example organisation may implement fire resistant material to reduce the likelihood of risk. They also implement policies regarding use of inflammable material and safe electrical design using circuit breakers. Still if the fire breaks out smoke detectors are implemented to get early warning so that the incident can be responded to contain damage. Depending upon the level of impact organisation may install fire suppression system that will automatically activated based on temperature levels and response time and hence damage is further reduced. However there still remains risk of fire and hence it needs to be monitored by including processes for testing control equipment, processes etc. Risk monitoring is process consists of following activities:

1. Periodic review identified and evaluated risks to confirm that the evaluation is appropriate. This might change due to various factors like changes in environment, business strategy and focus, Market changes and so on.
2. Review of risks associated with changes in infrastructure, processes and IT. Change might have effect on risks, for example organisation has implemented uninterruptible power supply system. Subsequently it might have added more equipment and hence the capacity of UPS may not be sufficient in future. Identifying evaluating this risk in time shall reduce impact of failure.
3. Incident response and lessons learned is another area that prompts for review of risks that materialised.
4. Audit findings also requires review of risks since non-effective controls might provide false comfort of compliance to management.

2.6 IS Risks and Risk Management

There are numerous changes in IT and its operating environment that emphasises the need to better manage IT related risks. Dependency on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. Increasing disclosures of information system disasters and increasing electronic fraud, in turn, drive this. The management of IT related risks is now being understood as a key part of enterprise governance.

Risk is the possibility of something adverse happening, resulting in potential loss/exposure. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources. Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security. This security has to be implemented as per required control system envisaged by the management of the enterprise. The risks in IT environment are mitigated by providing appropriate and adequate IS Security. IS security is defined as "procedures and practices to assure that computer facilities are available at all required times, that data is processed completely and efficiently and that access to data in computer systems is restricted to authorized people".

IS Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate the risks. If controls are unavailable or inadequate or inappropriate, then there would be a control weakness, which has to be reported to auditee management with appropriate recommendations to mitigate them.

2.7 Summary

This chapter has provided an overview of various types of Governance and risk management frameworks which can be used by organisations for implementing. There is no single framework which meets all requirements. Hence, it is important to understand the scope and coverage of each of these frameworks so that they can be adapted as required for implementation. Risk management is an integral aspect of governance and management. Risks have both positive and negative attributes. Risks provide challenges but they also provide opportunities. Risk management requires effective mitigation of risks by adapting the risk management process strategy thereby balancing risk versus benefits.

2.8 Questions

1. The most important requirement for IT governance function to be effective is:
   - A. Monitoring
   - B. Evaluation
   - C. Directing
   - D. Managing
2. The primary objective of implementing principles, policies and framework within an organization is to:
   - A. Communicate stakeholder's intent
   - B. Benchmark performance against competitors
   - C. Confirm with regulatory compliance
   - D. Implement corporate governance
3. The MOST important benefit of implementing IT risk management process is that it helps in:
   - A. Optimizing internal control framework
   - B. Ensuring residual risk is at acceptable level
   - C. Prioritizing business functions for audit planning
   - D. Complying with regulatory requirements
4. Which of the following is a major risk factor?
   - A. Existence of inflationary trends
   - B. Vendor launches new software
   - C. Board of directors elects new chairman
   - D. Change in government post elections
5. The level to which an enterprise can accept financial loss from a new initiative is:
   - A. Risk tolerance
   - B. Risk management
   - C. Risk appetite
   - D. Risk acceptance
6. Designing and implementing a control to reduce the likelihood and/or impact of risk materializing is a:
   - A. Risk acceptance
   - B. Risk transfer

C. Risk treatment

D. Risk transfer

7. Which of the following is a valid risk statement?

A. Network service provider is unable to meet bandwidth

B. Hacker attempts to launch attack on web site

C. Application server crash due to power failure

D. Delay in servicing customers due to network congestion

8. Which of the following is primary reason for periodic review of risk? The changes in:

A. Risk factors

B. Risk appetite

C. Budget

D. Risk strategy

9. Which of the following is a strategic IT risk?

A. IS audit may not identify critical non-compliance.

B. Non-availability of networks impacting services to customers.

C. New application may not achieve expected benefits.

D. Defer replacement of obsolete hardware.

10. Which of the following is the most essential action after evaluation of inherent risks?

A. Evaluate implemented controls.

B. Update risk register.

C. Prepare heat map.

D. Prioritized evaluated risk.

2.9 Answers and Explanations

1. **C.** Directing is the most critical of the Governance function which can be performed by the Board. A**lthough, g**overnance has three critical functions: Evaluate, direct and monitor, evaluation and monitoring can be performed against directions.

2. **A.** Principles, policies and framework have to be implemented within organisations primarily to communicate the intent of management (Stakeholders) so that management can implement or translate this into specific action.

3. **B.** The primary function of IT risk management process is to support value creation by reducing the risk to an acceptable level. The other options are secondary benefits of IT risk management.

4. **D.** Risk factors are conditions that affect the risk profile of a organisation. Change in government is one of major risk factors szas compared with other options.

5. **C.** Risk appetite denotes the level of risk acceptable by management. Risk tolerance is the time up to which an organisation can afford to accept the risk. Risk management is a process of risk mitigation and risk acceptance is decision of the management and is considered as risk response.

6. **C.** Implementing control is a risk treatment.

7. **D.** Options A, B and C are threats and not risks.

8. **A.** Changes in risk factors is the primary reason for reviewing changes in risk levels for an organisation. The other options are secondary reasons.

9. **D.** Deferring replacement of obsolete hardware is strategic decision and hence it is a strategic IT risk. Others are operational IT risks.

10. **A.** Once risks are evaluated it is necessary to find out the current state of risk mitigation (gaps in controls) by evaluating the existing controls. This help in identifying gaps and implementing controls so as to reduce the total exposure within acceptable limits. Other activities are required but not as essential as identifying gaps in controls.

CHAPTER 3: GEIT AND GRC

Learning Objectives

Governance, Risk and Compliance (GRC) has been at the fore front of corporate world due to the increasing emphasis on implementing this to meet regulatory requirements of Corporate Governance. Failures of some large enterprises in the last two decades due to lack of adequate level of Enterprise Risk Management (ERM) has compelled regulators to mandate its enforcement thus necessitating GRC implementation. Effective implementation of ERM requires consideration of multiple factors such as using a: holistic approach which encompasses enterprise from end-to-end, top down approach, best practices framework, technology deployment, related regulatory requirements and business needs. As IT is a key enabler for most enterprises, it makes good economic sense to implement IT GRC as a sub-set of overall GRC under the regulatory umbrella of corporate governance. This chapter provides an overview of the need for GEIT and how GRC requirements of compliance can be implemented using GEIT framework such as COBIT 5 and other related best practices.

3.1 Introduction

Modern enterprises are required to comply with a plethora of regulations covering not only business and regulatory aspects but also social and environment aspects. Most of the enterprises today are increasingly dependent on IT extensively for providing business services. The pervasiveness of technology in the current era can be gauged from the fact that the cost of Technology in a modern car is significantly higher than the cost of steel and the car can be considered as a mobile data centre as it has multiple processors which work together to provide safer and comfortable experience to the user. Technology provides the capability to deliver products and services at speeds hitherto unknown and also in a uniform and structured manner which is dynamically scalable. Enterprises using IT recognise that value is not derived miraculously from technology but is only realised when the capability of technology is applied and managed for enabling the required changes in delivering services of core business processes. This technology enablement process has its own inherent risks which coupled with compliance requirements make it imperative to implement an effective system of risk management encompassing both business and IT. There is a growing need to balance risk vs. value, benefits vs. cost and convenience vs. controls by implementing the right level of controls from the holistic perspective of enterprise risk management (ERM). As business processes and related controls get embedded into technology it is critical to implement IT risk management as strategic and integral part of ERM.

This ERM-enabled technology deployment provides a robust platform for enterprises to service customers empowering them to not only survive but also thrive in a dynamic competing environment. The principles of GRC can be used even in Small and Medium Enterprises (SME) as they provide the benefit of a safe and secure environment. However, the scope and level of ERM would be lesser for SMEs. This has led to an increasing demand for GRC related services which is being provided by vendors and solution providers ranging from consulting firms to large IT vendors. This chapter provides overview of regulatory need for GRC and how a GRC programme can be implemented or reviewed using COBIT 5.

3.2 What is GRC?

GRC has been given multiple interpretations by different vendors who have varied solutions to offer. GRC in general is the umbrella term which encompasses corporate governance, enterprise risk management (ERM) and compliance with applicable laws and regulations. GRC gained prominence globally after enactment of Sarbanes Oxley Act (SOX) in the US and similar legislations across the world. In India, Clause 49 of the Listing agreements applicable for listed companies *inter alia* includes all the key aspects of SOX and covers corporate governance requirements which include GRC. Some key definitions of GRC which need to be understood while implementing/reviewing GRC are:

- **Corporate Governance:** The systems and processes, by which enterprises are directed, controlled and monitored.
- **Compliance:** The systems and processes that ensure conformity with business rules, policy and regulations.
- **Governance:** Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in larger, complex enterprises.
- **Management:** Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).
- **Governance of Enterprise IT (GEIT):** Concerned with IT value delivery to the business and the mitigation of IT-related risks. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals.
- **Risk Management:** The culture, processes and structures that are directed to the effective management of potential opportunities and adverse effects
- **Risk:** The potential for an event to occur that could have an effect on the Enterprise objectives or operations
- **Framework:** Set of controls and/or guidance organized in categories, focused on a particular topic. It is a structure upon which to build strategy, achieve objectives and monitor performance.
- **Control:** Refers to the policies, procedures, practices and organisation structure which are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.

3.2.1 GRC from Corporate Governance perspective (Clause 49)

Specific provisions highlighting the regulatory requirements for implementing GRC in enterprises as per Clause 49 Listing requirements are:

Risk Management

Section 49(C) outlines the need for Board Disclosures relating to Risk management and states: "The Company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework.

CEO/CFO Certification

Section 49(V) deals with CEO/CFO certification and states that the CEO, i.e. the Managing Director or Manager appointed in terms of the Companies Act, 1956 and the CFO i.e. the whole-time Finance Director or any other person heading the finance function discharging that function shall certify to the Board and includes *inter alia* the following:

(c) **They accept responsibility for establishing and maintaining internal controls and that they have evaluated the effectiveness of the internal control systems of the company** and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies.

(d) They have indicated to the auditors and the Audit committee

    (i) **Significant changes in internal control during the year;**

    (ii) Significant changes in accounting policies during the year and that the same have been disclosed in the notes to the financial statements; and

    (iii) **Instances of significant fraud** of which they have become aware and the involvement therein, if any, of the management or an employee having a significant role in the company's internal control system

Internal Control

Internal control is a formal system of safeguards established by top management to provide a feedback on the way a financial institution, industrial organisation, or any other entity observes the board's and senior management's policies, plans, directives, and rules as well as the law of the land and regulatory requirements. It should be seen as a process:

- Promoting transparency,
- Enhancing communications, and
- Affecting all levels of personnel.

The competitive advantage of internal control is that it enables board members to supervise, and senior executives to manage, by tracking exposure to deviations from guidelines, programmes, established courses of action, and regulations. Such deviations may increase in credit risk, market risk, operations risk, settlement risk, legal risk, or other exposures relating to transactions, assets, and liabilities as well as to fraud and other events due to breaches of security. Beyond risks, internal control goals include the preservation of assets, account reconciliation, and compliance. Without any doubt, laws and regulations impact on IC, whose able management requires policies, organisation, technology, open communications channels, reliable information, access to all transactions, quality control, experimentation, and corrective action. The major objectives of implementing internal control are:

- Promote personnel accountability and
- Keep open the arteries of corporate communications.

The development, implementation, and proper functioning of an internal control system require the existence of clearly stated internal bylaws and directives; a rigorous sense of supervisory activity; compliance with government regulations; and an organisation that is flexible, dynamic, and appreciative of the need for management control

Auditor Certification

Section 49(VII) deals with compliance aspects and states that the company shall obtain a certificate from either the auditors or practicing company secretaries regarding compliance of conditions of corporate governance as stipulated in this clause and annex the certificate with the director's report, which is sent annually to all the shareholders of the company. The same certificate shall also be sent to the stock exchanges along with the annual report filed by the company. Based on the above, it is clear that implementing GRC requires implementing enterprise risk management and internal control system as required to meet the compliance requirements.

3.2.2 GRC programme implementation

Although a GRC programme (project) can be implemented primarily from a compliance perspective, it is advisable to consider business requirements also so as to optimise the investments made in implementing relevant processes, control structures and systems. GRC programme Implementation requires:

- Defining clearly what GRC requirements are applicable
- Identifying the regulatory and compliance landscape
- Reviewing the current GRC status
- Determining the most optimal approach
- Setting out key parameters on which success will be measured
- Using a process oriented approach
- Adapting global best practices as applicable
- Using uniform and structured approach which is auditable

Successful implementation of GRC in enterprise can be measured in general by the assurance provided to the senior management on the adequacy of controls implemented. However, specific success of a GRC programme can be measured by using the following goals and metrics:

1. Reduction of redundant controls and related time to execute (audit, test and remediate)
2. The reduction in control failures in all key areas
3. The reduction of expenditure relating to legal, regulatory and review areas
4. Reduction in overall time required for audit for key business areas
5. Improvement through streamlining of processes and reduction in time through automation of control and compliance measures
6. Improvement in timely reporting of regular compliance issues and remediation measures

7. Dashboard of overall compliance status and key issues to senior management on a real-time basis as required

3.2.3 Using COBIT 5 for effective GRC programme

GRC is about compliances. However, the focus of GEIT is on benefit realisation, risk optimisation and resource optimisation. Hence, implementing GEIT will help in implementing GRC. Benefit realisation focusses on creating new value for the enterprise through IT, maintaining and increasing value derived from existing IT investments, and eliminating IT initiatives and assets that are not creating sufficient value for the enterprise. Risk optimization addresses the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT-related business risk consists of IT-related events that could potentially impact the business. Resource optimization focuses on ensuring that the right capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Implementing a GRC programme using GEIT framework will help in ensuring that GRC not only facilitates conformance but also helps in ensuring performance.

3.2.4 Responsibility of Senior Management in GRC

The responsibility of senior management in implementing and monitoring functioning of requisite GRC measures is not only a regulatory requirement but it also makes business sense as effective GRC implementation helps in meeting not only compliance but business requirements as well. Using best practices frameworks such as COBIT 5 can help in discharging this responsibility by ensuring that all aspects of GRC are implemented. It is advisable that the board should mandate adoption of a GEIT framework such as COBIT 5, as an integral part of enterprise governance development. COBIT 5 framework would provide the overall approach and based on this, relevant guidance can be selected from specific standards and good practices for designing specific policies, processes, practices and procedures. This ensures that appropriate governance processes and other enablers are developed and optimised so that GEIT operates effectively as part of normal business practice and becomes a supporting culture as demonstrated by top management. Alignment with COBIT 5 best practices would also result in faster and more efficient external audits since COBIT is widely accepted as a basis for IT audit procedures.

3.3 IT Compliance Review

Failures of some large enterprises in the last decade due to lack of adequate level of ERM has compelled regulators to mandate its enforcement thus necessitating compliance with Governance, Risk Management and Compliance (GRC). Effective implementation of ERM requires consideration of multiple factors such as using a holistic approach, which encompasses enterprise from end-to-end, top down approach, best practices framework, technology deployment, related regulatory requirements and business needs. As IT is a key enabler for most enterprises, it makes good economic sense to implement IT GRC as a sub-set of overall GRC under the regulatory umbrella of corporate governance.

3.3.1 SOX requirements

As discussed earlier, In the US, Sarbanes Oxley Act has been passed to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. In India, Clause 49 of listing agreement issued by SEBI mandates similar implementation of enterprise risk management and internal controls as appropriate for the enterprise. Further, the Information Technology Act, which was passed in 2000 and amended in 2008 provides legal recognition for electronic records and also mandates responsibilities for protecting information. The Act also identifies various types of cyber-crimes and has imposed specific responsibilities on corporates. Hence, it can be rightly said that implementing Governance, Risk, security and controls is not only a management requirement but is mandated by law, too. Hence, it is important for enterprises to be aware of and be well conversant of IT compliances and accordingly implement processes and practices to manage these compliances both from conformance and performance perspective.

3.3.2 Clause 49 Requirements

All listed Companies in India have to enter into an agreement with the stock exchange and this agreement is called the Listing Agreement. This agreement is more or less defined by SEBI and all stock exchanges have similar wordings. Apart from other clauses in the agreement some of the clauses in the listing agreement require additional disclosures from the listed companies and compliance with corporate governance and other requirements. One such clause is Clause 49 of the Listing Agreement that prescribes certain additional disclosure requirements and also corporate governance requirements. This requirement is similar to the requirement of the Sarbanes Oxley Act of the USA and there are similar legislations in Australia, Japan and other countries. In USA, the PCAOB has come out with detailed guidelines on Compliance by Auditors and Companies under the Act. In India, no such guidance is available for Companies and Auditors other than limited guidance from the ICAI to its members, which focuses primarily on audit requirements.

3.3.3 Risk management

Every enterprise should have a risk management function and process to meet both management and regulatory requirements. The scope of process of "Manage Risk" is to continually identify, assess and reduce IT-related risks within levels of tolerance set by enterprise executive management. This helps in integrating the management of IT-related enterprise risk with overall ERIM, and balance the costs and benefits of managing IT-related enterprise risk.

3.3.4 Internal control requirements and Clause 49

The Internal control requirements of Clause 49 are similar to SOX requirements. Section 302 of the SOX requires CEOs and CFOs to certify the dependability of their firms' financial statements, including whether their entities have:

(a) Effective systems of internal control related to external financial disclosures and

(b) Procedures capable of notifying both external auditors and their audit committees when significant control deficiencies are detected in these systems.

Section 404 of SOX demands that a firm's external auditor must report on the reliability of management's assessment of internal controls. Similar to SOX, under section F.I.6, the clause 49 Listing Agreement requires the Directors to cover their internal controls systems and their adequacy in the Management Analysis and Discussion. Under section V(c), the agreement requires the CEO/CFO to accept responsibility for establishing and maintaining internal controls for financial reporting and that they have evaluated the effectiveness of internal control systems of the company pertaining to financial reporting and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of such internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies.

Reporting on Internal control requirements are also mandated by the Indian Companies Act, 1956 for all companies and a separate annexure to the audit report has to be provided by auditors as per Companies (Auditor's Report) Order, 2003 (CARO). Hence, implementing internal controls is mandated by law not only for listed companies but for all companies. The recently passed Companies Act 2013 also similar audit reporting requirements in addition to reporting of fraud by auditors. This reinforces the need for implementing internal control system and risk management to meet regulatory requirements as well as stakeholder needs.

3.3.5 Compliance in COBIT 5

As discussed in earlier chapters, COSO and COBIT are two most popular frameworks which have been used for ensuring compliance. In this section, we will discuss how compliance is facilitated in COBIT 5 and the specific processes which provide the best practices for implementing compliance process in the organisation. The Management domain of "Monitor, Evaluate and Assess" has a compliance focused process titled: "MEA03 Monitor, Evaluate and Assess Compliance with External Requirements". This process is designed to evaluate that IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements. This requires that the enterprise has processes in place to obtain assurance and that these requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance. The primary purpose of this process is to ensure that the enterprise is compliant with all applicable external requirements.

Legal and regulatory compliance is a key part of the effective governance of an enterprise. Hence, its inclusion in the GRC term and in the COBIT 5 Enterprise Goals and supporting enabler process structure (MEA03). In addition to MEA03, all enterprise activities include control activities that are designed to ensure compliance not only with externally imposed legislative or regulatory requirements but also with enterprise governance-determined principles, policies and procedures. In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process, which also include a compliance-related role.

The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities. The Governance activities related to GEIT are covered in the five processes of the Governance domain. The risk management process and supporting guidance for risk management spread across the GEIT space meet the compliance need of regulations such as SOX and other similar regulations across the world. COBIT has a specific focus on compliance activities within the framework and explains how they fit within the complete enterprise picture. Inclusion of GRC arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements as silos of activity but instead provides a comprehensive and holistic approach for ensuring compliance.

3.4 Key Management Practices of IT Compliance

COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. These practices can be adapted as required:

- **Identify External Compliance Requirements:** On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.
- **Optimise Response to External Requirements:** Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and best practice guidance for adoption and adaptation
- **Confirm External Compliance:** Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements
- **Obtain Assurance of External Compliance:** Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

3.4.1 Key Metrics for Assessing Compliance Process

Implementing compliance practices requires monitoring of metrics. A list of sample metrics for reviewing the process of evaluating and assessing compliance are given here for both areas of compliance with external laws and regulations and IT compliances with internal policies:

Compliance with External Laws and Regulations

- Cost of IT non-compliance, including settlements and fines;
- No. of IT related non-compliance issues reported to board or causing public comment or embarrassment;
- No. of non-compliance issues relating to contractual agreements with IT service providers;
- Coverage of compliance assessments.

IT Compliance with Internal Policies

- Number of incidents related to non-compliance to policy;
- Percentage of stakeholders who understand policies;
- Percentage of policies supported by effective standards and working practices; and
- Frequency of policies review and updates.

3.5 Using COBIT 5 Best Practices for GRC

Although a GRC programme (project) can be implemented primarily from a compliance perspective, it is advisable to consider business requirements also in such a project so as to optimise the investments made in implementing relevant processes, control structures and systems. Implementing GRC requires:

- Defining clearly what GRC requirements are applicable;
- Identifying the regulatory and compliance landscape;
- Reviewing the current GRC status;
- Determining the most optimal approach;
- Setting out key parameters on which success will be measured;
- Using a process oriented approach;
- Adapting global best practices as applicable; and
- Using uniform and structured approach which is auditable.

The responsibility of senior management in implementing and monitoring functioning of requisite GRC measures is a regulatory requirement. However, it also makes business sense to focus not only on compliance but business requirements as well. Using best practices frameworks such as COBIT 5 can help in discharging this responsibility by ensuring that all aspects of GRC are implemented covering both conformance and performance perspectives as required. It is advisable that the board should mandate adoption of a GEIT framework such as COBIT 5, as an integral part of enterprise governance development.

COBIT 5 framework provides the overall approach and based on this, relevant guidance can be selected from specific standards and good practices for designing specific policies, processes, practices and procedures. This ensures that appropriate governance processes and other enablers are developed and optimised so that GEIT operates effectively as part of normal business practice and becomes a supporting culture as demonstrated by top management. Alignment with COBIT 5 best practices would also result in faster and more efficient external audits since COBIT is widely accepted as a basis for IT audit procedures.

Successful implementation of GRC in enterprise can be measured in general by the assurance provided to the senior management on the adequacy of controls implemented. However, specific success of a GRC programme can be measured by using the following goals and metrics:

- The reduction of redundant controls and related time to execute (audit, test and remediate);
- The reduction in control failures in all key areas;
- The reduction of expenditure relating to legal, regulatory and review areas;
- Reduction in overall time required for audit for key business areas;
- Improvement through streamlining of processes and reduction in time through automation of control and compliance measures;
- Improvement in timely reporting of regular compliance issues and remediation measures;
- Dashboard of overall compliance status and key issues to senior management on a real-time basis as required.

3.6 Summary

Implementing GRC is mandatory requirement as per law and using the right type of GEIT framework helps in meeting regulatory and management requirements. COBIT 5 is a globally accepted GEIT framework and includes the necessary guidance to support enterprise GRC objectives and supporting activities. The Governance activities related to GEIT are covered in the 5 processes of the Governance domain. The Risk management process and supporting guidance for risk management cut across the GEIT space. Compliance is a specific focus on compliance activities within the GEIT framework and they fit in well to provide the complete enterprise GRC perspective. There is a specific process in COBIT 5 on ensuring compliance. Further, there are specific best practices provided in COBIT 5 which facilitate in meeting compliance requirements. The inclusion of GRC arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements which is silos of activity which are not integrated. Implementing GRC using GEIT framework will help in meeting both conformance and performance requirements. Implementing compliance is considered as project of GRC implementation. Outline of steps to be followed for such implementation have been outlined in this chapter.

The COBIT 5 framework is available to all as a free download from ISACA at www.isaca.org/cobit.

3.7 Questions

1. Which of the following scenarios has the highest impact?
   - A. Absence of business continuity plan
   - B. Absence of Security operations centre
   - C. Absence of monitoring of SLA
   - D. Absence of risk management process
2. Which of the following is the best strategy to address the risk of non-compliance?
   - A. Maintain inventory compliance requirements
   - B. Embedding risk of non-compliance in operations
   - C. Appointing chief compliance officer
   - D. Implement IT governance framework
3. Implementing IT risk management process is essential for implementing IT governance because IT risk management primarily helps enterprise in:
   - A. Protecting and securing IT resources
   - B. Arriving at likelihood and impact of risk
   - C. Optimising cost of control based on risk
   - D. Monitoring performance of resources
4. Which of the following is most important requirement of compliance with governance?
   - A. Monitoring performance
   - B. Whistle blower policy
   - C. Independent directors
   - D. Assurance on controls

5. Which of the following is main benefit of implementing GRC framework with organization?

   A. Reduction in compliance expenditure

   B. Assurance on compliance and controls

   C. Reduction in internal audit cycles over year

   D. Availability of compliance status dashboard

6. Which type of non-compliance does situation of an organisation using evaluation version of software provided by vendor beyond specified number of days without paying for it?

   A. Regulatory

   B. Legal

   C. Contractual

   D. Internal

7. Overall reduction in regulatory non-compliances within the organisation over a period of time indicates that:

   A. Governance practices implemented are effective

   B. The risk response policy adopted is to avoid risk

   C. Legal framework provides for heavy penalties

   D. Increase in number of internal audits performed

8. Which of the following is first step in implementing GRC framework with organisation?

   A. Perform IT risk assessment

   B. Identify internal policy requirements

   C. Determining critical success factors

   D. Perform control gap analysis

9. Primary objective of implementing legal and regulatory requirement framework like SOX or clause 49 is to:

   A. Make management accountable

   B. Protect stakeholder's interest

   C. Get assurance on internal controls

   D. Facilitate trading on stock exchanges

10. GRC compliances were made mandatory because of:

   A. Management override of controls

   B. Frauds committed by staff members

   C. Reduction in market value of shares

   D. Adoption of open economic policy

3.8 Answers and Explanations

1. **A.** Of the options absence of BCP shall have highest impact when incident results in disaster.
2. **B.** Embedding compliance requirements in operations controls in best strategy to mitigate the risks related to on-compliance.
3. **C.** Risk management helps in selecting cost beneficial controls based on exposure. This in turn helps in value creation for organisation.
4. **D.** Most important requirement of Governance compliance is assurance on internal controls implemented within organisation. Other requirements are important but secondary.
5. **B.** Main benefit of implementing GRC framework is to provide assurance to stakeholders on compliance and internal controls. Others are secondary and subjective.
6. **C.** It is a breach of contract between vendor and organisation. Depending on provisions it can be regulatory and internal non-compliance also. It will be legal non-compliance if the software is used without paying and informing to vendor.
7. **A.** Reduction in non-compliances indicates that the governance framework is effective. Others may or may not be concluded.
8. **D.** The first step in implementing GRC framework is to perform control gap analysis in order to achieve the desired state. Identifying policy requirements is performed based on gap analysis. Performing risk assessment also uses the input from control gaps. Deciding critical success factors is done after plan is defined.
9. **B.** Protecting stakeholder's interest has been primary objective of compliance requirements.
10. **A.** Management of some organisation's committed financial frauds jeopardising existence of organisations and hence stakeholder's investments.

CHAPTER 4: KEY ENABLERS OF GEIT

Learning Objectives

An enabler can be defined as capabilities, forces, and resources that contribute to the success of an entity, programme, or project. An enabler has a positive impact on the initiative and supports the achievement of the goals and objectives. Enablers represent the heart and lifeblood of any initiative. A key enabler has a significant positive impact on the initiative and compensates to some extent for other factors that may be less positively ranked. Key enablers can also be called as the critical success factors that provide the vision, direction, energy and resources to initiate, sustain and realize their promised benefits. COBIT 5 which is based on seven key enablers can be used for implementing Governance of Enterprise IT (GEIT). This chapter discusses the key enablers of GEIT which facilitate the successful achievement of enterprise goals and IT enabled goals.

4.1 Introduction

Organisations which wish to implement GEIT for achieving enterprise objectives have to consider various key aspects such as goals, objectives, benefit and value for the organisation. However to ensure these are achieved, an appropriate GEIT framework must be implemented. Implementing GEIT does not occur in a vacuum but has to consider the specific environment applicable to the enterprise. We have discussed in earlier chapters how implementation of GEIT can be focused both on conformance and performance. GEIT implementation has to be taken as a project with an empowered project champion vested with responsibility for results. Selecting and implementing the right type of enablers as required is the key to successful implementation of a GEIT framework. This implementation takes place in different conditions and circumstances determined by numerous factors impacting both internal and external environment and these could be pertain to:

- Ethics and culture of the organisation
- Laws, regulations and policies
- Applicable standards
- Industry practices
- Competitive environment

Implementing GEIT requires consideration of specific aspects applicable to the enterprise and these could pertain to:

- Mission, vision, goals and values
- Governance policies and practices
- Culture and management style
- Models for roles and responsibilities
- Business plans and strategic intentions
- Operating model and level of maturity

4.2 Overview of Seven Enablers of COBIT 5

The best approach to implement GEIT is to build on and enhance the existing approaches so as to be inclusive of IT rather than developing a new approach just for GEIT. Implementing any new initiative requires implementation of required enablers to the required extent as applicable. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise. They are also the factors that, individually and collectively, influence whether something will work for example: implementing GEIT. In COBIT 5, enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. There are seven enablers of COBIT 5 which have been described briefly earlier in chapter 2. In this chapter, we will discuss the key characteristics of each of these seven enablers. The step-to-step approach to implementing Governance and management practices including specific aspects of performance management system using seven enablers are explained in next two chapters.

4.2.1 Principles, policies and framework

The first enabler of COBIT 5 is: "Principles, policies and framework". It may be noted that these enablers although provided in COBIT 5 from a GEIT perspective can be equally applicable and adaptable for any new project or initiative.

The purpose of principles policy and framework is to convey the governing body's and management's direction and instructions. They are instruments to communicate the rules of the enterprise, in support of the governance objectives and enterprise values as defined by the board and executive management. The primary reason for implementing principles, policies and frameworks is to translate the desired strategy into practical guidance for day-to-day management. The key difference between principles and policies are that principles need to be limited in number. The characteristics of good policies are that they should:

- **Be effective:** Achieve their purpose
- **Be efficient:** Especially when implementing them
- **Non-intrusive:** Should make sense and be logical to those who have to comply with them.

Policies should have a mechanism (framework) in place where they can be effectively managed and users know where to go. Specifically they should be:

- Comprehensive, covering all required areas
- Open and flexible allowing for easy adaptation and change
- Current and up-to-date

The purpose of a policy life cycle is that it must support a policy framework in order to achieve defined goals and express clearly as possible the core values of the enterprise. Policies are more detailed guidance on how to put principles into practice. The good practice requirements for policies and frameworks have to be approved by the Board and senior management. These are important and should specifically cover the following:

- Scope and applicability
- Consequences of failing to comply with the policy
- Means of handling exceptions

- How they will be monitored.

The links and relationships between principles, policies and frameworks and other enablers are:

- Principles, policies and frameworks reflect the cultures, ethics and values of the enterprise.
- Processes are the most important vehicle for executing policies.
- Organisational structures can define and implement policies.
- Policies are part of information which has to documented and communicated.

4.2.2 Processes

The second enabler of COBIT 5 is “Processes”. COBIT 5 has a specific publication titled: “COBIT 5: Enabling process” which provides specific guidance for the governance and management domains. Let us look at some of the key components and what they cover:

- ***A process is defined*** as ‘a collection of practices influenced by the enterprises policies, and procedures that takes inputs from a number of sources (including other processes) manipulates the inputs and produces outputs (e.g. products and services).
- ***Process practices*** are defined as the ‘guidance’ necessary to achieve process goals.
- ***Process activities*** are defined as the ‘guidance’ to achieve management practices for successful governance and management of enterprise IT.
- ***Inputs and Outputs*** are the process work products/artefacts considered necessary to support operation of the process.

Process model of COBIT 5 focuses on generic processes required by organisation to implement within organisation. It clearly distinguishes between Governance processes and management processes. The Governance domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined. The four management domains are in line with responsibility areas of plan, build, run and monitor (PBRM). The four management domains are: “Align, Plan and Organise (APO)”, “Build, Acquire and Implement (BAI)”, “Deliver, Support and Service (DSS)” and “Monitor, Evaluate and Assess (MEA)”. There are 32 processes covering the management domain. Each process provides:

- Process description
- Process purpose statement
- IT-related Goals
- Each IT-related goal is associated with a set of generic related metrics
- Process Goals (also from the goals cascade mechanism and is referred to as Enabler Goals).
- Each process goal is associated or related with a set of generic metrics.
- Each Process contains a set of Management Practices.
- These are associated with a generic RACI chart (Responsible, Accountable, Consulted, Informed)
- Each management practice contains a set of inputs and outputs (called work products)
- Each management Practice is associated with a set of activities.

In addition COBIT 5 identifies the goals for each process and also defines the metrics to measure the performance of each process.

4.2.3 Organisation Structures

The third enabler of COBIT 5 is "Organisation structure". Establishing accountability mechanisms through appropriate organisation structure is the corner-stone of governance implementation. Deployment of IT requires involvement not only from management (management processes) but also from the Board of directors (governance processes). Hence, the organisation structure has to include establishing specific responsibility for both governance and management. The key role and responsibilities for most of the typical functions in an organisation from governance and management perspective is identified for each of the 200+ management practices covering all the 37 COBIT processes. This is provided in the RACI chart which will help in defining roles, responsibilities covering risks and controls for all critical areas as per COBIT processes and practices. Using these practices will help organisations to establish a number of good practices of organizational structure such as:

- **Operating principles:** The practical arrangements regarding how the structure will operate, such as meeting frequency documentation and other rules
- **Span of control:** The boundaries of the organisation structure's decision rights.
- **Level of authority:** The decisions that the structure is authorized to take.
- **Delegation of responsibility:** The structure can delegate a subset of its decision rights to other structures reporting to it.
- **Escalation procedures:** The escalation path for a structure describes the required actions in case of problems in making decisions.

Implementing right organisation structure from governance perspective requires creation of the right accountability mechanisms and decision-making system. This requires establishing committees at different levels covering all areas right from strategy to execution. Two important committees which are required for implementing effective GEIT are the IT Strategy Committee and the IT Steering Committee. The roles and responsibilities of each of these committees is explained in this chapter. Further, clear job definitions have to be provided for all key IT positions so as to ensure that the required IT organisation structure is established. It is also important to understand the roles, responsibilities and risks of key IT personnel. Hence, roles, risks and controls for some of the key IT roles are outlined in this chapter. Understanding of the roles and responsibilities and customizing these as per requirements of the organisation is critical for implementing GEIT. In establishing the right organisation structure for GEIT, it is important to get the distinction between governance and management. This is summarised in the table here.

Table 3.1: Distinction between Governance and Management

Governance	Management
• **Evaluate: Stakeholder needs, conditions and options**	• Plan, build, run and monitor activities
• **Determine: Agreed on enterprise objectives**	• Align with: direction set by the governance body

Governance	Management
• **Set direction: Prioritisation and decision making**	• Achieve: Enterprise objectives
• **Monitor: Performance and compliance**	• Monitor and Report: Performance and conformance
• **Responsibility: Board of directors**	• Responsibility: Management at all levels

IT Strategy Committee

Governance of enterprise IT should be an integral part of corporate governance, and in this way a primary concern of the board of directors. Boards may carry out their governance duties through committees and they can consider the criticality of IT through an IT strategy committee. The IT strategy committee is composed of board and non-board members. They should assist the board in governing and overseeing the enterprise's IT-related matters. This committee should ensure that IT is a regular item on the board's agenda, where it must be addressed in a structured way. The IT strategy committee should work in close relationship with the other board committees and with management in order to provide input to, and to review and amend the aligned enterprise and IT strategies. The implementation of the IT strategy must be the responsibility of executive management assisted by one or more IT steering committees. Typically, such a steering committee has the responsibility for overseeing major projects and managing IT priorities, IT costs, and IT resource allocation. While the IT strategy committee operates at the board level, the IT steering committee is situated at executive level, which implies that they have different responsibility, authority and membership

IT Steering Committee

Planning is essential for determining and monitoring the direction and achievement of the enterprise goals and objectives. As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the steering committee. Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management. As the members comprise of function heads of departments, they would be responsible for taking decisions relating to their departments as required. The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises. The key functions of the committee would include:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and set priorities within the scope;

- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

Appointment: The IS Steering Committee is appointed by the Board in order to oversee the IS Department's processes, and it operates at the executive level.

Responsibilities: The duties, responsibilities, authority and accountability of the Steering Committee should be defined in a formal charter, which should be approved by the Board. Members should know IS department policies, practices and procedures. Each member should have the authority to make decisions within the group for his or her respective areas.

Objective: The primary objective of the Steering Committee is to ensure that the IS department is aligned with the organization's mission and objectives. It provides planning and control for the organization's IS function.

Chairman: It should preferably be chaired by a member of the board of directors who understands information technology risks and issues.

Representation: The membership of the committee should be broad-based and should include a cross-section of senior business managers including legal and finance, senior management, user management and IS department.

4.2.4 Roles, Responsibilities and Risks of IT department

Implementing Governance of Enterprise IT requires establishing the right organisation structure with proper accountability mechanism. COBIT 5 provides the RACI chart for each of the process for each of the management practices. In implementing specific processes or management practices, these can be used as a model and adapted as required. Implementing internal control and risk management requires implementing appropriate segregation of duties through job definition of each of the key roles and designations for all key functions in the IT department. The risks and controls of the various roles performed by personnel in the IS Department are briefly outlined here.

Chief Information Officer (CIO)

The CIO reports to the Chief Operating Officer or the Board of Directors and is the overseer of all IT activities in most organisations. He is responsible for the alignment of strategic business goals with the IT processes. Instead of routine day-to-day functions, he focuses on business, IT planning and strategy. The IT processes cover delivery and support of:

- Traditional computer data processing services

- Internet technology
- Telecommunications
- Network services
- User support etc.

Risks

- Inadequate interface with the top management may result in loss of alignment with business and IT processes.
- This position may give him unrestricted access to the system.
- Inadequate background checking and performance review may bring in uncontrollable risks

Controls

In view of the importance of this function the following internal controls may be employed:

- Regular interface with the board of directors.
- Training and other appropriate HR controls in order to ensure competency and trustworthiness.
- Work should be documented and subject to regular reviews.
- Access should be granted on a “need to know”, “need to do” basis.

Application Systems Development Manager (ASDM)

The main role of the ASDM is to oversee the work of

a) Application systems analysts and

b) Application programmers, who design, develop and maintain new or existing application programmes.

Risks

- Inadequate communication with the CIO may result in loss of effectiveness and efficiency of this important function.
- Work may not be documented and subject to regular reviews.
- Access may have been granted without reference to his job needs.

Controls

- Employ a competent and trusted person by using HR controls.
- Regular interface with the CIO.
- Work should be documented and subject to regular reviews.
- Access should be granted on a “need to know”, “need to do” basis.

Application Systems Analysts

Such persons are responsible for designing application systems based on user specifications, resulting in the development of functional specifications and other high level systems design documents required by the application programmers.

Risks

- Inadequate HR controls may introduce an undesirable person in the company.
- Work may not have been documented and subject to regular reviews.
- Access may have been granted without reference to his job needs.

Controls

- Employ a competent and trusted person by using HR controls.
- Work should be documented and subject to regular reviews.
- Access should be granted on a “need to know”, “need to do” basis.

Application Systems Programmers (ASP)

The main role of the ASP is to develop new application systems and maintain the existing production systems based on the design made by the application systems analyst.

Risks

The main risks are manipulation of live programmes and data in order to perpetrate a fraud.

Controls

- Employ a competent and trusted person by using HR controls.
- Should not have access to live programmes and data.
- Should work in a test–only environment.
- Should not be allowed to have any change control duties that would enable him to say, modify a programme and launch it in the live environment without going through change controls like quality control, security and end user signoff.

Data Administrator (DA)

This role may only be found in large IT environments only, while in smaller IT environments, the functions of the DA may be merged with those of the database administrator. The DA is responsible for the long term planning of the data architecture and management of data. It is basically a policy making and administrative role.

- Undertake strategic data planning, determining user needs
- Specifying validation criteria for data
- Specifying new conceptual and external schema definitions
- Specifying retirement policies for data
- Determining end-user requirements for database tools; testing and evaluating end-user database tools

Database Administrator (DBA)

The DBA performs a technical role, and is responsible for short term planning, design, definition, maintenance and integrity of the database systems in an organisation.

- Define, manage, create and retire data
- Specify and change the physical data definition
- Make the database available to users
- Service the users' needs
- Maintain database integrity
- Monitor database operations
- Set up new installation, perform upgrades and migrations
- Select and implement database optimization tools
- Test and evaluate programmer and optimisation tools
- Implement database definition controls, access controls, update controls and concurrency controls
- Monitor database usage, collect performance statistics and tune the database
- Define and initiate backup and recovery processes and procedures
- Ensure security of data

Quality management

Quality management is the means by which IS department based processes are controlled, measured and improved. Processes in this context are defined as a set of tasks that when properly performed, produce the desired results. These processes may be split between assurance and control functions. These processes which impact all IT related functions, also follow the PDCA cycle, namely:

- Formulate quality goals
- Implement standards
- Monitor processes, report and train users
- Suggest programmes for obtaining improvement in the processes

Quality Assurance Manager

This function deals with assuring adherence to prescribed quality processes in all IT related functions like programming, data entry etc., e.g. ensuring that programmes and allied documentation adhere to the prescribed standards and computer naming conventions adopted by the organisation.

Quality Control Manager

This function deals with applying quality control procedures, e.g. conducting tests in order to verify and ensure that the software and other allied processes are free from defects before they are transferred to live operations and that it meets the needs and expectations of the end users.

Risks

There will be impairment in quality processes if:

- A person is allowed to carry out a quality review of his own work.
- Incompetent persons are recruited due to inadequate HR controls.
- Quality management do not have independence in their reporting function

Controls

- Employ a competent and trusted person by using HR controls.
- Should be given appropriate training in the latest quality management systems.
- Should not have any application programming responsibilities because QC manager is the “checker” not the “maker” of a system.
- Should report to the CIO to maintain independence.

Security management

Top management should demonstrate their commitment to security by developing an information security management policy considering the nature of business, its assets, technology and the organization structure. This includes the development of business continuity and disaster recovery plans related to IS functions. The approved policy should state the:

- Framework for setting objectives that gives a sense of direction to information security
- Business, legal, regulatory and contractual requirements that apply
- Alignment of the policy with the organisation’s strategic risk management process
- Criteria for determining how risk will be evaluated

Security Manager

- Maintains the access rules for data and other IS resources
- Ensures security and confidentiality for the issuance and maintenance of authorised user IDs and passwords.
- Monitors activities for security breaches and take appropriate corrective actions.
- Reviews the security policy and suggest necessary changes.
- Provides appropriate training and awareness programmes to users.
- Tests the security processes in order to determine their strengths and weaknesses and detect possible threats.
- Implements new or better security software.

Risks

There will be impairment in the security management processes if:

- Allowed to carry out conflicting work like application programming.
- Incompetent or dishonest persons may be recruited due to inadequate HR controls.
- The security manager may not have independence due to the reporting structure.

Controls

- Should report directly to the CIO in order to maintain independence. In small organisations where this is not possible, the security manager may report to the operations manager, in which case some compensating controls like monitoring and awareness have to be implemented.
- Employ a competent and trusted person by using HR controls.
- Should be given appropriate training in the latest security management systems.
- Should not have any conflicting duties like application programming responsibilities because security manager is the “checker” not the “maker” of a system.

Technical support manager

This function is responsible for overseeing the following technical support functions:

- Systems Analyst
- Systems Programmer
- Systems Administrator
- Network Administrator
- End User Support Manager

Risks

- Incompetent or dishonest persons may be recruited due to inadequate HR controls.

Controls

- Employ a competent and trusted person by using the HR controls

Systems Analyst

Systems Analyst is responsible for designing systems software and therefore may have complete access to the system libraries. They interpret the user needs and develop requirements and functional specifications, as well as high-level design documents; which enable programmers to create the particular application.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer logs are not enabled, any breach of security will remain undetected.

Controls

- Employ competent and trusted persons by deploying the HR controls.
- Activities should be recorded in the computer logs in order to detect access breaches.
- Access to the system libraries should be granted on a “need to know”, “need to do” basis.

Systems Administrator

This is generally applicable where a network of computers are used. The responsibilities of this function include:

- Creation and deletion of user accounts.
- Installation and maintenance of systems software e.g. the operating system.
- Taking proactive virus prevention measures.
- Allocating storage space for data and programmes.
- The addition and configuration of client machines.
- Maintenance of major multi-user computer systems, including local area networks as well as mainframe systems.
- Initiating backups at the end of or during the day.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer logs are not enabled, any breach of security will remain undetected.

Controls

- Employ competent and trusted persons by using HR controls.
- Activities should be recorded in the computer logs in order to detect access breaches.
- Access to the system libraries should be granted on a “need to know”, “need to do” basis.
- Should not have any application programming duties.

Network Administrator

They are responsible for the entire network of the organisation which may include LANs, WANs and wireless communication and voice networks. The infrastructure of the network may include routers, hubs, switches, firewalls, network segmentation through e.g. VLANs etc. They are also responsible for network performance management, network maintenance, remote access etc. This position is responsible for technical and administrative control over the LAN. This includes ensuring that transmission links are functioning correctly, backups of the system are occurring, and software/hardware purchases are authorised and installed properly.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- Breach confidentiality, integrity and availability of data by eavesdropping on communication between two nodes on the network or by launching denial-of-service attack.

Controls

- Employ competent and trusted persons by using HR controls.
- Should not have any application programming responsibilities.
- Activities should be recorded in the computer logs in order to detect access breaches.

End User Support Manager

This function is responsible for liaison between the end users and the IS department, including the management of the help desk. The function of the help desk is to resolve the users' hardware and software technical problems through e-mail, telephone or the fax machine. All the reported problems are recorded and the user is given a reference number for his complaint. The help desk will send this complaint to the appropriate engineers who will resolve the problem by telephone, fax, e-mail or by personal visit to the user. The help desk may also acquire hardware or software and train users in order to enable the user to function effectively and efficiently. In very large organizations this function is becoming more and more important. The function may be performed in-house or outsourced.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer complaint logs are not enabled, the resolution, frequency and nature of complaints will remain undetected.

Controls

- All user complaints should be logged and allotted a complaint number.
- Depending on the severity of the complaint, the complaint should be forwarded to the appropriate engineer.
- All unresolved problems should be followed up and closed by an independent person.
- Competent and trusted staff should be employed.
- Complaints should be periodically summarised and reviewed for the nature and frequency of the complaints.

Operations Manager

The operations manager's functions include responsibility for computer operations personnel including computer operators, librarians, data entry personnel and maintenance operators. They are also responsible for physical and data security of the department.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- Unauthorised access to the operations centre may result in breach of security.

Controls

- A competent and trusted person should be employed based on the HR controls.
- Only operations personnel should have access to the operations department, based on the "need to know", "need to do" access principle.
- All operations and programming functions should always be separated.

4.2.5 Culture, Ethics and Behaviour

The fourth enabler of COBIT 5 is “Culture, Ethics and Behaviour”. The principles of this enabler are inbuilt in the processes and other guidance. Organisational Ethics determine the values by which the enterprise want to live (its code). Individual ethics determined by each person’s personal values and dependent to some extent on external factors not always under the enterprise’s control. Individual behaviours which collectively determine the culture of the enterprise and is dependent on both organizational and individual ethics. In governance terms, culture is significantly influenced but what is referred to as “The Tone from the Top”. In other words, the spoken and unspoken messages sent from the IT executive leadership, which in turn influences managerial behaviour and directly influences company plans, policies, and organisational direction. In short, culture is shaped and transformed by consistent patterns of senior management action. Some examples are:

- Behaviour towards risk taking
- Behaviour towards the enterprise’s principles and policies
- Behaviour towards negative outcomes, e.g. loss events

Good practices for creating, encouraging and maintaining desired behaviour throughout the enterprise include:

- Communication throughout the enterprise of desired behaviours and corporate values. (This can be done via a code of ethics)
- Awareness of desired behaviour, strengthened by senior management example. This is one of the keys to a good governance environment when senior management and the executives ‘walk the talk’ so to speak. It is sometimes a difficult area and one that causes many enterprises to fail because it leads to poor governance. (Typically this will be part of a training and awareness sessions based around a code of ethics)
- Incentives to encourage and deterrents to enforce desired behaviour. There is a clear link to HR payment and reward schemes
- Rules and norms which provide more guidance will typically be found in a Code of Ethics

4.2.6 Information

Information is the fifth important most enabler of COBIT 5. Information is processed using information technology. The success of an enterprise in the digital world depends on how well information is harnessed for achieving enterprise objectives. Information is the most valuable asset and success of an enterprise is determined by how well information is processed and made available to all the stakeholders with the requisite level of security. Ensuring the right type of information using information systems in safe and secure environment is the most critical aspects of technology deployment. As per COBIT 5, Information is currency of the 21st century. Process requires information and management at all levels require information for decision making and monitoring performance. IT maintains information and hence the attributes of information are most important for business and management. IT supports business process by generating and processing data. The information is then transformed into knowledge that creates value for management and helps in decision which affects the business process. There is a specific publication titled: “COBIT: information” which is designed on the principles of COBIT 5 and provides additional guidance on implementing this most important enabler. The attributes required to assess the context and quality of information to the user which need to be considered, specifically are:

- **Relevancy:** The extent to which information is applicable and helpful for the task at hand
- **Completeness:** The extent to which information is not missing and is of sufficient depth and breath for the task at hand
- **Appropriateness:** The extent to which the volume of information is appropriate for the task at hand.
- **Conciseness:** The extent to which the information is compactly represented.
- **Consistency:** The extent to which the information is presented in the same format.
- **Understandability:** The extent to which the information is easily understandable
- **Ease of Manipulation:** The extent to which information is easy to manipulate and apply to different tasks.

4.2.7 Services, Infrastructure and Applications

The sixth enabler of COBIT 5 is: “Services, infrastructure and Applications”. This refers to the services provided by IT to business and stakeholders to meet internal as well as external requirements. Application helps in providing services by processing information. Application is hosted using IT infrastructure. Application software are at the heart of processing of transaction processing and encompass all mission critical processes. In a modern enterprise where services are provided an on-line, real-time basis, services, infrastructure and applications provide the most critical foundation for providing services to customers. Hence all these three aspects: services, infrastructure and applications must be considered together. Modern applications are complex and interacts with various technologies, for example core banking application is hosted on server that processes and provide data in real time to various delivery channels likes ATM, Mobile banking, Internet banking, Branch banking. All delivery channels are set of applications focusing on providing services to customers. Hence a bank must consider all these three objects together. COBIT 5 does not have specific publication for this enabler but this is integrated in all the best practices provided by COBIT for all the processes. Further, ITIL framework which is focused on service management can be integrated with COBIT 5.

There are five architecture principles that govern the implementation and use of IT-Related resources. This is part of the good practices of this enabler. Architecture principles are overall guidelines that govern the implementation and use of IT-related resources within the enterprise. Examples of such principles are:

- **Reuse:** Common components of the architecture should be used when designing and implementing solutions as part of the target or transition architectures.
- **Buy vs. build:** Solutions should be purchased unless there is an approved rationale for developing them internally.
- **Simplicity:** The enterprise architecture should be designed and maintained to be simple as possible while still meeting enterprise requirements.
- **Agility:** The enterprise architecture should incorporate agility to meet changing business needs in an effective and efficient manner.
- **Openness:** The enterprise architecture should leverage open industry standards.

The services, infrastructure and applications as an enabler is also designed and built based on the IT strategic plan which in turn is derived from the enterprise strategic plan. For most enterprises, the investment and cost of this enabler would be the highest and hence needs to be managed both as a one-time projects and as on-going maintenance projects as relevant. Any new business initiative would require IT enabled change which has to be supported by required services, infrastructure and applications and once deployed, there is a need for on-going maintenance to ensure that the required level of services are provided.

4.2.8 People, Skills and Competencies

People, Skills and competencies are the most valuable asset of an enterprise. In an increasingly digital world where most of the routine transaction processing is automated. It is the people with the required skills and competencies who are the key differentiator. IT is only enabler and by itself provide value. Value is derived by how IT is harnessed through right blend of people, process and technology. It is the employees of an enterprise who as knowledge workers use the power of IT to provide services to customers. In the service industry, the human resources are the most valuable asset. Technology can be bought but effective implementation requires people to be trained with the requisite skills and competencies to provide services. Nothing can move unless supported and managed by people who use their intrinsic capacity to analyse information and take decisions. Without people organizations will not exist. People, however possess different skills and organisations need people with different skills. In order to ensure appropriate skills organisations follow various people management practices like training, motivational programmes, career progressions, job rotation.

While defining organization structure organizations also define job description, roles and responsibilities along with competencies required to perform the job. For example IT related activities likes business analysis, system design, development and coding, testing. Organisations also consider outsourcing to ensure appropriate skill and competencies are available to achieve performance and service delivery objectives. For implementing GEIT, organizations require skills for developing and executing IT Policy formulation, IT strategy, enterprise architecture, innovation, financial management, portfolio management and many such related processes as relevant.

The seven enablers of COBIT 5 have to be implemented in enterprises of all sizes regardless of nature of business or sector or technology deployment. However, the relevance of each these enablers would vary across enterprises. For example, in a software company, the enabler: people, skills and competencies is extremely important whereas in the case of highly regulated industry, the enabler: culture, ethics and behaviour is most important. For successful implementation of GEIT, selecting the right blend of these enablers customised as required is most critical. The enablers also have the openness of integrating across various frameworks.

4.3 Summary

The seven key enablers for implementing GEIT are the building blocks for any technology deployment. This chapter has provided details of key characteristics of each of the seven enablers. These seven enablers are: Principles, policies and framework, Processes, Information, Organisation structure, Services, infrastructure and applications, People, skills and competencies and Culture, ethics and behavior. Each of these enablers is critical. However, information is most valuable for most of the enterprises. Each of these enables have their own characteristics that have to be considered while implementing GEIT. Organisation need to ensure that these enablers are implemented as appropriate depending on the requirements of the organisation.

In implementing GEIT, it is most important to note that Governance and management are different concepts. Governance is providing direction and monitoring performance, whereas management is about implementing, executing and monitoring activities as per the strategy to ensure that enterprise objectives are achieved. How well these enablers are effective would also depend on the involvement of senior management with the governance perspective of providing direction and channelising use of technology from strategic perspective. COBIT 5 provides generic guidance for each of these enablers and in case of processes and information, there are specific publications which provide detailed guidance. However, implementation of these seven enablers requires integration and use of detailed guidance from other relevant frameworks as required. However, considering that COBIT 5 is an umbrella framework, it provides the overall framework for integration of best practice guidance from all frameworks.

4.4 Questions

1. Which of the following is most important resource of the organisation?
   - A. Policies and procedures
   - B. IT infrastructure and applications
   - C. Information and data
   - D. Culture, ethics and behaviour
2. Which of the following is most important characteristic of policies?
   - A. Must be limited in number.
   - B. Requires framework to implement.
   - C. Reviewed periodically.
   - D. Non-intrusive and logical.
3. Primary function of a process is to:
   - A. Act on input and generate output.
   - B. Define activities to be performed.
   - C. Focus on achieving business goals.
   - D. Comply with adopted standards.
4. Effective organization structure focuses on:
   - A. Defining designations.
   - B. Delegating responsibility.
   - C. Defining escalation path.
   - D. Deciding span of control.

5. Implementing GEIT is a primary responsibility of which of the following?
   A. IT steering committee
   B. IT strategy committee
   C. IT risk committee
   D. IT portfolio management
6. Prioritisation of IT initiatives within organisation is primarily based on:
   A. Results of risk assessments
   B. Expected benefit realization
   C. Recommendations of CIO
   D. Rate of obsolescence of IT
7. Primary objective of IT steering committee is to:
   A. Align IT initiatives with business
   B. Approve and manage IT projects
   C. Supervise IT and business operations
   D. Decide IT strategy for organisation
8. A data administrator is primarily a:
   A. Data base administrator
   B. Data owner
   C. Data custodian
   D. Data integrator
9. Which of the following is a function of information security manager?
   A. Implement firewalls in organization
   B. Perform IT risk assessment
   C. Approve information security policy
   D. Define rules for implementing ID
10. Which of the following is best control for building requisite skills and competencies within organisation?
   A. Hiring only highly qualified people
   B. Outsourcing the critical operations
   C. Conducting skill enhancement training
   D. Defining skill requirements in job description

4.5 Answers and Explanations

1. **C.** Entire GEIT implementation focuses on Information and data. Policies are defined based on nature of information and data, culture and behaviour. IT infrastructure and applications stores, process and communicates information.

2. **D.** Policies are vehicle to communicate intent of management and hence must be clear and easy to implement that will make them effective. B and D are requirements to maintain policies and A is characteristic of principles.

3. **A.** Primary function of process is to process received inputs and generate output to achieve process goals. Process is a set of activities but it is not primary function to define activities. Although processes are defined to achieve business goals, these are broken down to arrive at process goals. Compliance with standards may need certain processes but the primary function is to process input.

4. **B.** Effectiveness of organisation structure depends on right level of delegation of responsibilities. Defining designation is only naming of specific role which is not directly relevant. Other options depend upon level of delegation.

5. **B.** IT strategy committee is appointed at board level and they are responsible for implementing GEIT. Other committees are more tactical and operational in nature.

6. **B.** Although the IT steering committee considers all inputs, the primary consideration is expected benefits to the organisation.

7. **A.** The primary objective of appointing IT steering committee is to ensure that IT initiatives are in line with business objectives. D is objective of IT strategy committee. B and C are secondary objectives derived from A.

8. **C.** Data administrator is primarily a data custodian.

9. **D.** Information security manager does not perform A, B and C. A is performed by network manager, B is performed by department heads, security manager is facilitator, information security policy is defined by security manager and approved by management.

10. **C.** The best control for building requisite skills and competencies within organisation is to ensure skill enhancement training is provided.

CHAPTER 5: PERFORMANCE MANAGEMENT SYSTEMS

Learning Objectives

The Governance processes of ISO 38500 and COBIT 5 primarily focus on "Evaluate, Direct and Monitor". Governance is an oversight function and evaluates the business environment in terms of the business strategy and objectives, the technology environment, market conditions, competitive environment, regulatory requirements and emerging innovations that could significantly impact and influence the business strategic and operating models of the organisation.

The governance function thus provides the direction that the IT operation should integrate to maximise the support and involvement to the business. The governance function also monitors the performance of the IT operation in terms of its direction and the goals achieved. The 'direct' function provides what is expected from management, whereas 'monitor' function focuses on whether what was expected has been achieved or not. The challenge is to 'evaluate' what is actually achieved and validate whether it is as per set objectives. This evaluation should help enterprise to make a realistic assessment of what was achieved, what are the gaps and how to monitor the performance not only on reactive but proactive basis. This chapter provides an overview of key concepts and models of performance management system.

5.1 Introduction

An effective performance management system is the corner-stone for meeting this challenge and implementing effective governance. This requires setting goals and metrics which are integrated across all the key areas and are measured and monitored. The system of performance measurement can be implemented by use of relevant governance and performance frameworks such as balanced scorecards, maturity models, and quality systems. This chapter provides an overview of performance management systems with specific details of goals cascade from COBIT 5 and also explains the principles of Balanced Scorecard and Strategic Scorecard.

5.2 Performance Measurement

Performance measurement is the process of collecting, analysing and/or reporting information regarding the performance of an individual, group, organisation, system or component. It can involve studying the processes and strategies within organisations or studying enterprise processes, parameters and phenomena, to evaluate whether the results are in line with what was intended or should have been achieved. An important principle of good governance is that management should provide direction using clearly defined and communicated objectives, and then manage adherence to objectives by applying appropriate practices. Monitoring of performance using metrics enables management to ensure that goals are achieved. In developing a performance management system, it is important to identify the enterprise goals and then obtain understanding of the connection between the entity's mission, vision and strategies and its operating environment.

The board phases of performance measurement system are:

- Establishing and updating performance measures
- Establishing accountability for performance measures
- Gathering and analysing performance data
- Reporting and using performance information

5.3 Performance measurement system

As per COBIT 5: Enterprises exist to create value for their stakeholders. Consequently, any enterprise whether commercial or not, will have value creation as a governance objective. Value creation means realising benefits at an optimal resource cost while optimising risk. Benefits can take many forms, e.g., financial for commercial enterprises or public service for government entities. To assess performance against set objectives, it is important to implement a performance management system which assessese's performance against goals by setting right key goals indicators (KGI) and also implementing key process indicators (KPI) to monitor performance of process. Performance measurement system is one of the ways of monitoring and evaluating the business achievements. Getting business value from IT and measuring that value are, therefore, important governance domains. They are responsibilities of both the business and IT and should take both tangible and intangible costs and benefits into account. In this way, good IT performance management should enable both the business and IT to fully understand how IT is contributing to the achievement of business goals, in the past and in the future. IT performance management is aimed at identifying and quantifying IT costs and IT benefits. There are different monitoring instruments available, depending on the features of the costs and benefits.

The ability of enterprise to manage organisational performance is based on how well they the design governance processes that address short-term and long-term management information needs, decisions and control frameworks. Further, enterprise has to identify specific roles, responsibilities, expectations, policies and procedures to be followed for decision-making and accountability. The performance management system has to consider various reward and recognition systems that are implemented and how they might impact performance. Performance is evaluated at various levels such as: at organisation level against goals and objectives, resource level against set performance goals by defining key performance indicators (KPI), risk level based on key risk indicators (KRI). There are two approaches for performance measurements:

1. Proactive approach where management implements measure to provide assurance on achieving goals by implementing best practices and using lead indicators.
2. Reactive approach were achievements are compared with goals using lag indicators.

5.4 Goal Setting

Goal setting is the first pre-requisite of performance management. This could be done at different levels of enterprise and each of these need to be integrated and linked together at all levels of the enterprise. At a macro level, the Board of directors set the enterprise direction and goals to be achieved. These are the overall enterprise goals and are derived from the enterprise strategy. The enterprise goals could be set from a top-down or bottom-up or combination of these two approaches. Typically, the top management sets the goal considering the views of the business units. Once the goals are set, the top level goals need to be allocated to function/business units and specific goals set for each of them. From a governance perspective, the enterprise goals will have to be shared by the IT department which will prepare the IT strategy in alignment with the enterprise strategy. Based on the enterprise, the IT department will prepare the IT strategic plan and IT related goals. These IT goals facilitate achievement of enterprise goals. There are various models or frameworks which could be used for implementing performance management system. For example: COBIT 5 goals cascade which is based on the Balanced Scorecard principles. In a manufacturing industry, six sigma or quality management system may be implemented and in a software development company, the Capability Maturity model may be used.

A performance measurement system will broadly have two types of goals. These are:

- **Outcome:** These are called as goals and are evaluated through KGI (key goal indicators). The focus is on achieving the set results. These are also called lag indicators as the measurement of achievement is after the event or period.
- **Performance:** These refer to performance and are evaluated through KPI (key performance indicators). These are also called lead indicators as they measure the performance.

There are many approaches to performance management. In this chapter, we will understand some of the performance management practices based on COBIT 5, Balanced Scorecard and Quality management.

5.5 Performance measurement in COBIT 5

Enterprises exist to create value for their stakeholders. Consequently, any enterprise: commercial or not will have value creation as a governance objective. Value creation means realising benefits at an optimal resource cost while optimising risk. Benefits can take many forms, e.g., financial for commercial enterprises or public service for government entities. COBIT 5 provides an effective way to understand business and governance priorities and requirements and then use this knowledge when implementing improved governance and management enablers. This approach also enhances the preparation of business cases for governance improvements, obtaining the support of stakeholders, and the realisation and monitoring of the expected benefits. The relationship can be summarised in this top-down flow. COBIT 5 helps ensure strategic alignment and drive what to do, supported by the selected enterprise goals mapped to relevant IT related goals to identified IT processes and cascaded further into prioritised governance or management practices and activities. COBIT 5 framework provides multiple approaches to setting goals. These could start from identifying stakeholder needs or the governance objectives or directly selecting relevant processes as required.

Enterprises have many stakeholders, and 'creating value' means different and sometimes conflicting things to each of them. Governance is about negotiating and deciding amongst different stakeholders' value interests. By consequence, the governance system should consider all stakeholders when making benefit, risk and resource assessment decisions. For each decision, the following questions can and should be asked:

- For whom are the benefits?
- Who bears the risk?
- What resources are required?

Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customised enterprise goals, IT-related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements.

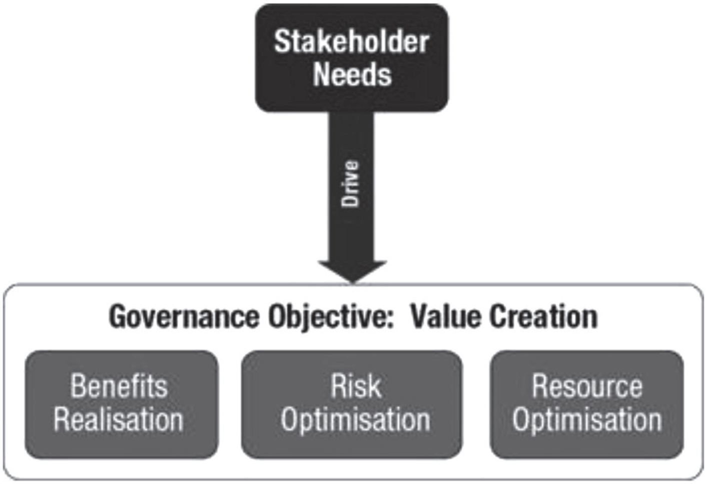


Figure 5.1: The Governance Objective: Value Creation

5.5.1 Goal setting and stakeholder needs

Understanding of current stakeholder needs relating to GEIT and current enterprise goals and how they impact *GEIT* is very helpful for three reasons:

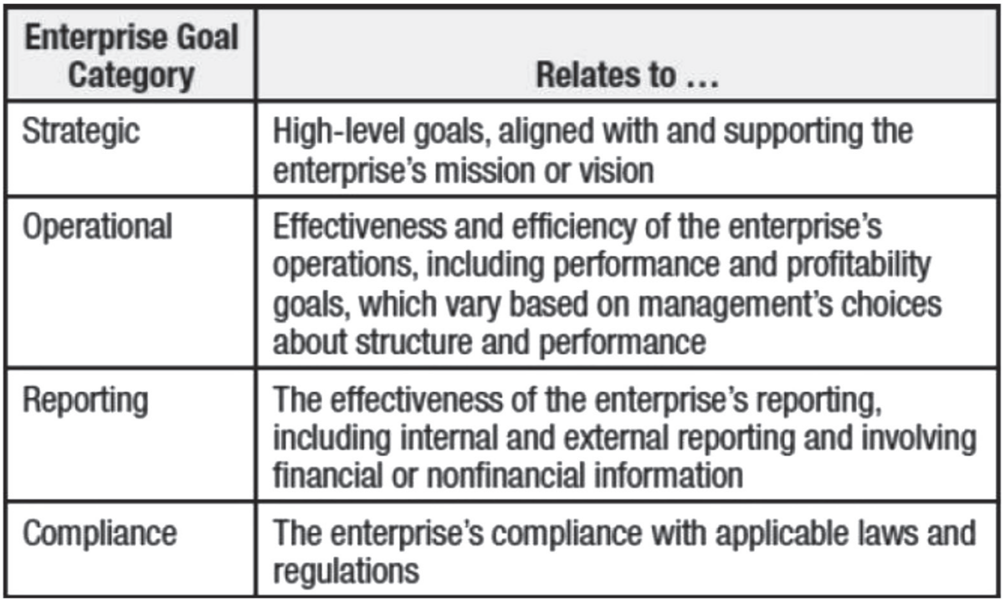
- The stakeholder needs and enterprise objectives influence the requirements and priorities of *GEIT.* For example, there could be a focus on cost reduction, compliance or launching a new business product, each of which could put a different emphasis on current governance priorities.
- The stakeholder needs and enterprise objectives help to focus where attention should be given when improving GEIT and
- It assists the business and IT functions to do better forward planning of opportunities to add value to the enterprise.

COBIT 5 provides useful guidance and examples for defining enterprise and IT related objectives and how they relate to each other. A generic set of 17 enterprise goals and 17 IT related goals is presented as a cascade in the COBIT 5 Framework and Process Reference Guide. These sample goals are provided with relevant metrics. Further, there are mapping tables for stakeholder needs to enterprise goals, enterprise goals to IT goals and IT goals to IT processes which help in easy selection and customisation of the goals as required. This enables users to relate their enterprise's current business and IT environment to specific objectives, and then map them onto the processes that are likely to be relevant in successfully achieving these goals.

5.5.2 Category of Enterprise Goals

Goals to be effective need to be covering all levels of operations of the enterprise. They also need to be linked and automated and used as a measure of evaluating how well the department or employees have performed. Enterprise goals could be categorised as per the table given below.

Table 5.1: Categories of Enterprise goals



Enterprise Goal Category	Relates to ...
Strategic	High-level goals, aligned with and supporting the enterprise's mission or vision
Operational	Effectiveness and efficiency of the enterprise's operations, including performance and profitability goals, which vary based on management's choices about structure and performance
Reporting	The effectiveness of the enterprise's reporting, including internal and external reporting and involving financial or nonfinancial information
Compliance	The enterprise's compliance with applicable laws and regulations

5.5.3 COBIT 5 enterprise and IT relates goals

The COBIT 5 enterprise and IT related goals are used as the basis for setting IT objectives and for establishing a performance measurement framework. IT objectives are expressed as goals and need to be aligned with enterprise goals. COBIT 5 provide structures for defining goals at three levels: for the enterprise, for IT overall, for IT processes. These goals are supported by metrics known as outcome measures because they measure the outcome of a desired goal. The metrics at a specific level also act as performance drivers for achieving higher-level goals. These goals and metrics can be used to set objectives and monitor performance by establishing scorecards and performance reports as well as for driving improvements. COBIT 5 provides guidance on how to define and break down business objectives and create monitoring metrics based on the balanced scorecard.

5.5.4 Requirements for Measures

Measures and performance information need to be linked to strategic management processes. An effective performance management system produces information that provides following benefits:

- It is an early warning indicator of problemmes and the effectiveness of corrective action.
- It provides input to resource allocation and planning. It can help enterprises prepare for future conditions that are likely to impact program and support function operations and the

demands for products and services, such as decreasing personnel or financial resources or changes in work load. Use of measures can give organizations lead times for needed resource adjustments, if these conditions are known in advance.

- It provides periodic feedback to employees, customers and stakeholders about the quality, quantity, cost and timeliness of products and services.

The most important benefit of setting measures is that it builds a common results language among all decision makers. Selected measures define what is important to an enterprise, what it holds itself accountable for, how it defines success and how it structures its improvement efforts.

5.5.5 Performance Measurement processes/indicators

This is considered to be an important part of the IT governance processes. They say that what cannot be measured cannot be improved on. Therefore metrics should be generated for example all products and processes, financial measurement, benchmarking and external party evaluation, satisfaction of customers, internal staff and stakeholders, in order to ensure that they are achieving the desired results. Performance measurement is used to:

- Measure and manage products and services
- Assure accountability
- Make budgeting decisions and
- Optimise performance i.e. improve the productivity of IS to its highest possible level without making unnecessary added investments in the IS infrastructure.

Phases of performance measurement

Performance measurement typically has the following phases:

- Plan, establish and update performance measures
- Plan and establish the accountability of persons for the performance measures
- Collect and analyse data on performance
- Report on performance information and
- Take corrective action

Performance indicators or metrics will determine how well the process is performing in enabling the goals to be achieved. They are also indicators of capabilities and skills of IS personnel.

Examples of performance measures

- Better use of communications bandwidth and computing power
- Lower number of non-compliance with prescribed processes reported
- Better cost and efficiency of the process
- Lower numbers of complaints made by stakeholders
- Better quality and increased innovation etc.
- Lower number of errors and rework
- Improved staff productivity

5.5.6 Measures defined in COBIT

In the context of GEIT, goals and metrics are defined by the COBIT framework at three levels:

1. **Enterprise goals as metrics:** Define the organisational context and objectives and how to measure them
2. **IT-related goals and metrics:** Define what the business expects from IT and how to measure it
3. **Process goals and metrics:** Define what the IT-related process must deliver to support IT's objectives and how to measure it

In these three levels, it is important to make a distinction between outcome measures and performance drivers. Outcome measures indicate whether goals have been met. These can be measured only after the fact and, therefore, are sometimes called lag indicators. Using the COBIT framework, outcome measures inform management whether an IT function, process or activity has achieved its goals.

5.5.7 Enterprise Goals

Enterprise goals are set by the board of directors based on the strategy and objectives. The list of enterprise goals from COBIT 5 are given here. These need to be customised by selecting by what is relevant for the enterprise and adding specific dates, values and number to the identified goals:

1. Stakeholder value of business investments
2. Portfolio of competitive products and services
3. Managed business risk (safeguarding of assets)
4. Compliance with external laws and regulations
5. Financial transparency
6. Customer-oriented service culture
7. Business service continuity and availability
8. Agile responses to a changing business environment
9. Information-based strategic decision making
10. Optimisation of service delivery costs
11. Optimisation of business process functionality
12. Optimisation of business process costs
13. Managed business change programmes
14. Operational and staff productivity
15. Compliance with internal policies
16. Skilled and motivated people
17. Product and business innovation culture

Sample metrics for enterprise goal

1. Stakeholder value of business investments	• Percent of investments where value delivered meets stakeholder expectations • Percent of products and services where expected benefits are realised • Percent of investments where claimed benefits are met or exceeded

5.5.8 IT related Goals

COBIT 5 provides IT related goals which are mapped to the enterprise goals. As discussed earlier, the selected IT goals need to be customised as required by adding values, number and dates to make them practically relevant. It may be noted that the IT related goals are closely linked to the enterprise goals and as per the goals cascade an identified list of IT related goals would be required to achieve enterprise goals. Please refer to COBIT Framework for more details.

1. Alignment of IT and business strategy
2. IT compliance and support for business compliance with external laws and regulations
3. Commitment of executive management for making IT-related decisions
4. Managed IT-related business risk
5. Realised benefits from IT-enabled investments and services portfolio
6. Transparency of IT costs, benefits and risk
7. Delivery of IT services in line with business requirements
8. Adequate use of applications, information and technology solutions
9. IT agility
10. Security of information, processing infrastructure and applications
11. Optimisation of IT assets, resources and capabilities
12. Enablement and support of business processes by integrating applications and technology into business processes
13. Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
14. Availability of reliable and useful information for decision making
15. IT compliance with internal policies
16. Competent and motivated business and IT personnel
17. Knowledge, expertise and initiatives for business innovation

Sample metrics for IT related is given below:

01 Alignment of IT and business strategy	• Per cent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Per cent of IT value drivers mapped to business value drivers

5.5.9 Sample goals and metrics for Resource optimisation

We have discussed earlier that COBIT 5: enabling process publication provides specific guidance for each of the processes. We are giving below an extract for one process to highlight how COBIT 5 specifically provides guidance on performance measures for each process in terms of IT related goals with metrics and process goals with metrics. This demonstrates how goals and metrics can be set in an integrated manner by using and adapting best practices as required.

Process: EDM04 Ensure Resource Optimisation	**Area:** Governance Domain: Evaluate, Direct and Monitor
Process Description: Ensure that adequate and sufficient IT-related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost.	
Process Purpose Statement: Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities

Process: EDM04 Ensure Resource Optimisation	**Area:** Governance Domain: Evaluate, Direct and Monitor
16 Competent and motivated business and IT personnel	• Per cent of staff whose IT-related skills are sufficient for the competency required for their role • Per cent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The resource needs of the enterprise are met with optimal capabilities	• Level of stakeholder feedback on resource optimisation • Number of benefits (e.g., cost savings) achieved through optimal utilisation of resources • Number of deviations from the resource plan and enterprise architecture strategies
2. Resources are allocated to best meet enterprise priorities within budget constraints	• Number of deviations from, and exceptions to, resource management principles • Per cent of projects with appropriate resource allocations
3. Optimal use of resources is achieved throughout their full economic life cycles	• Per cent of re-use of architecture components • Per cent of projects and programmes with a medium- or high-risk status due to resource management issues • Number of resource management performance targets realised

5.6 Balanced scorecard (BSC)

A Balanced Scorecard, as defined by Robert S. Kaplan and David P. Norton, groups objectives, measures, targets, and initiatives into four perspectives: financial, customer, learning and growth, and internal processes. However, some organizations create their own perspectives that align more closely with the way they run their business. Most executives quickly discover that the BSC methodology is more than a performance measurement system. It is also a strategic management system that they can be used to execute strategy and manage organisational performance. BSC is described as a tool to create a "strategy-focused organisation" - in which strategy becomes the driving force of organsational activity and communication. The BSC focuses the energy of an organisation into achieving strategic goals and objectives that are represented by key performance indicators (KPIs) customised to every group or business unit of the organisation. BSC is a methodology to solve challenges in balancing the theories of a strategy with its execution. BSC has the following characteristics:

- The methodology is suitable for managing business strategy.
- Uses a common language at all levels of the organisation.

- Uses a common set of principles to manage day-to-day operations as well as to framework the organisation's strategy.
- Designed to identify and manage business purposes.
- Provides a balance between certain relatively opposing forces in strategy:
  - o Internal and external influences
  - o Leading and lagging indicators and measures
  - o Financial and non-financial goals
  - o Organisational silos focused on their own goals and an over-arching framework of goals
  - o Finance priorities and operations
- Aligns strategic goals with objectives, targets, and metrics.

5.6.1 BSC perspectives

The four perspectives of BSC with examples are explained here.

Financial Perspective. The Financial perspective contains measures that indicate whether a strategy is achieving bottom-line results. Financial metrics are classic lagging indicators. The more common ones are:

- Profitability
- Revenue growth
- Economic value added

Customer Perspective. The Customer perspective defines the organisation's target customers and the value proposition it offers them, whether it is efficiency (low price, high quality), innovation, or exquisite service. Most customer metrics are lagging indicators of performance, as follows:

- Customer satisfaction
- Customer loyalty
- Market share, "share of wallet"

Internal Process Perspective. Delivering value to customers involves mastering numerous internal processes, including product development, production, manufacturing, delivery, and service. Organisations may need to create brand new processes to meet goals outlined in the Customer perspective. Common metrics are:

- Patents pending, ratio of new products to total products
- Inventory turnover, stock-outs
- Zero defects, on-time deliveries

Learning and Growth Perspective. This perspective measures the internal resources needed to drive the other three perspectives. These include employee skills and information technology. Typical metrics are:

- Employee satisfaction, turnover rate, absenteeism

- Training hours, leadership development programmes
- Number of cross-trained employees, average years of service

5.6.2 BSC as a Management tool

The BSC is an invaluable management tool to translate strategy into action and to bring non-financial performance indicators into better focus. BSC is considered to be less effective where uncertain and complex decisions are required to formulate the strategy during times of transformational change. The BSC is used to solve a “measurement problem” but it is also a management system. Traditional financial measurements do not capture the value creating activities in an organisation like skills, competencies, IT etc. It provides a prescription as to what enterprises should measure in order to ‘balance’ the financial perspective. If something cannot be measured, it cannot be improved upon. Metrics allow managers to view their enterprise from many perspectives and therefore, make better decisions. BSC attempts to move businesses from monitoring to measurement; from measurement to management and from management to direction setting:

- **Monitoring:** The art and science of observing employee behaviour and coaching.
- **Measurement:** The art and science of gauging, using numbers and metrics, performance to a task.
- **Management:** The art and science of motivating, coaching, and enabling individuals and teams in the achievement of an objective.
- **Direction setting:** Discovering strategic directions that are unique and differentiating in the marketplace, communicating this to all levels in the organisation in the form that they can identify and co-relate their day-to-day actions to the goals.

Successful organisations who are goal-oriented can get a complete perspective of where they are compared to where they want to be. This requires that they have to measure “where we are and how far we have to go”. This assessment helps in identifying the gaps and designing and implementing the roadmap to bridge the gaps. The basis for any action plan is knowledge. Knowledge, using BSC is purposeful and focused on strategic action and this helps in translating strategy into day-to-day action plans and initiatives.

As BSC provides a view of organisation from four perspectives, it is important to develop metrics, collect data and analyse it in relation to these perspectives. BSC has been used in some enterprises to translate strategy into action while others have used it to measure non-financial performance indicators. The BSC is useful in making strategy actionable. BSC is also designed to ensure that performance metrics and strategic themes are balanced with financial and non-financial, operational and financial, leading and lagging indicators. A diagrammatic representation of the four perspectives of BSC is given in figure 5.1 here. This clearly highlights how the overall vision and strategy are linked to each of the perspectives with specific objectives, measures, targets and initiatives for each of the four perspectives.

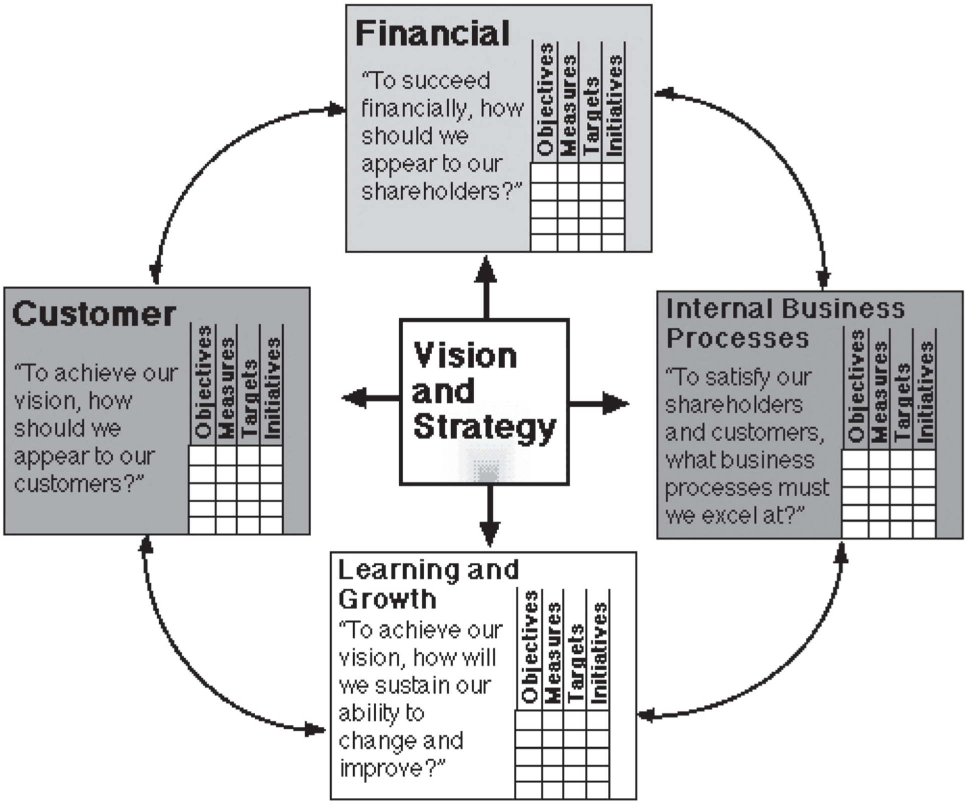

Financial
"To succeed financially, how should we appear to our shareholders?"
Objectives
Measures
Targets
Initiatives
Customer
"To achieve our vision, how should we appear to our customers?"
Objectives
Measures
Targets
Initiatives
Vision and Strategy
Internal Business Processes
"To satisfy our shareholders and customers, what business processes must we excel at?"
Objectives
Measures
Targets
Initiatives
Learning and Growth
"To achieve our vision, how will we sustain our ability to change and improve?"
Objectives
Measures
Targets
Initiatives

Figure 5.1: The Balanced Scorecard

5.6.3 IT Balanced Scorecard

BSC cascades to all levels of the organisation and can be linked with IT. Use of an IT BSC is one of the most effective means to aid the board and management to achieve IT and business alignment. The IT BSC provides a balanced view of the total value delivery of IT to the business. It provides a snapshot of where the IT organisation is at a certain point in time. The user orientation perspective represents the user evaluation of IT. The operational excellence perspective represents the IT processes employed to develop and deliver the applications. The future orientation perspective represents the human and technology resources needed by IT to deliver its services over time. The business contribution perspective captures the business value created from the IT investments. Each of these perspectives must be translated into corresponding metrics and measures that assess the current situation. As noted previously, the cause-and-effect relationships between measures are essential components of the IT BSC, and these relationships are articulated by two types of measures: Outcome measures and performance drivers

Outcome measures: Such as programmers' productivity (e.g., number of function points per person per month), need performance drivers, such as IT staff education (e.g., number of education days per person per year) communicate how the outcomes are to be achieved.

Performance drivers: Need outcome measures to ensure a way to determine whether the chosen strategy is effective, especially important in cases where a significant investment is made. These cause-and-effect relationships must be defined throughout the entire scorecard: more and better education of IT staff (future orientation) is an enabler (performance driver) for a better quality of developed systems (operational excellence perspective) that in turn is an enabler for increased user satisfaction (user perspective) that eventually will lead to higher business value of IT (business contribution). The starting point is the vision which leads to the mission and based on the mission, specific strategies are formulated. The chosen strategies should be implemented through appropriate initiatives which have their own milestones and deliverables. The table below illustrates how to implement BSC covering mission and strategies.

Table 5.2: Implementing BSC covering mission and strategies

User Orientation *How do the users view the IT department?*	**Corporate Contribution** *How does management view the IT department?*
Mission To be the preferred supplier of information systems	**Mission** To obtain a reasonable business contribution of IT investments
Strategies • Preferred supplier of application • Preferred supplier of operations • Partnership with users • User-satisfaction	**Strategies** • Control of IT expenses • Provide new business capabilities • Business value of new IT projects
Operational excellence *How effective and efficient are the IT processes?*	**Future orientation** *How well is IT positioned to answer future challenges?*
Mission To deliver effective and efficient deliver IT applications and services	***Mission*** To develop opportunities to answer future challenges
Strategies • Efficient an effective software development • Efficient an effective operations	***Strategies*** • Training and education of IT staff • Expertise of IT staff • Age of the application portfolio • Research into emerging IT

5.7 Strategic Scorecard

The CIMA (Chartered Institute of Management Accountants) Strategic Scorecard was developed in response to the key findings that emerged from a project led by the International Federation of Accountants (IFAC) and CIMA to develop the framework of enterprise governance. By providing a continuous process with standard progress reporting with which directors become familiar, the CIMA Strategic Scorecard can address all three issues and thus makes for a more effective board. The scorecard approach forms a key element of what has been termed the enterprise governance framework.

The scorecard is a pragmatic and flexible tool that is designed to help boards to fulfil their responsibilities to contribute to and oversee strategy effectively. It is the responsibility of the management team to develop and propose the strategy. However, it is not for the board to undertake the detailed strategic planning. The board's focus should be to challenge the strategy constructively, endorse it and monitor its implementation. The implementation of the scorecard assumes that the organisation has already determined its broad strategic direction and has a strategic plan in place. The scorecard represents a process for developing and moving this strategy forward in a dynamic way.

The enterprise governance framework helps understand the importance of both conformance and performance to the organisation's long-term success. What the scorecard does is to give the board a simple, but effective process that helps it to focus on the key strategic issues and – most importantly – to ask the right questions. This means that the board can work constructively with management to promote the future success of the organisation. The uniqueness of the scorecard lies in the fact that it:

- Summarises the key aspects of the environment in which an organisation is operating to ensure that the board is aware of changing competitor, economic and other factors.
- Identifies the (key) strategic options that could have a material impact on the strategic direction of the organisation and helps the board to determine which options will be developed further and implemented.

Enterprise governance encapsulates two dimensions of corporate governance processes i.e. conformance and performance that need to be kept in balance. This has been discussed earlier in detail in the first chapter: Governance and Management of information systems.

- **Conformance dimension:** Covers issues such as board structures and roles as well as executive remuneration. Codes and/or standards can generally address this dimension with compliance being subject to assurance/audit.
- **Performance dimension:** Focuses on strategy and value creation. The focus is on helping the board to make strategic decisions, understand its appetite for risk and the key drivers of performance. This dimension does not lend itself easily to a regime of standards and audit.

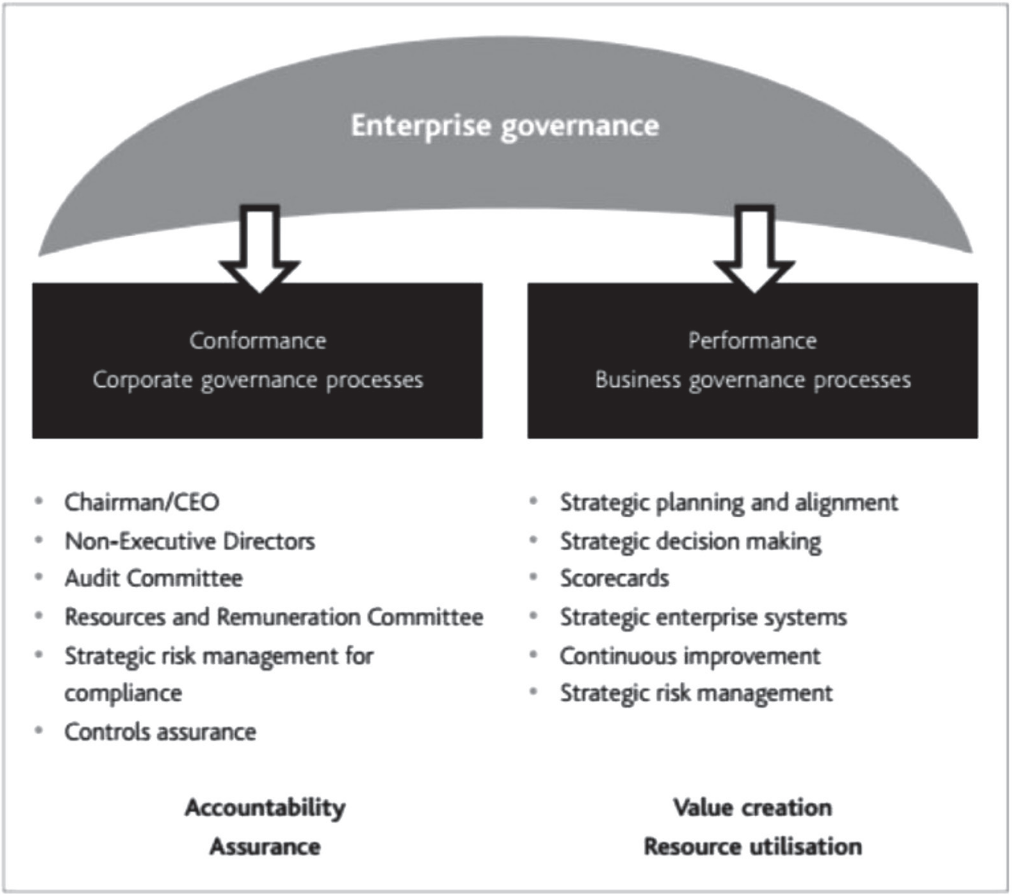

Enterprise governance
Conformance
Corporate governance processes
Performance
Business governance processes
Chairman/CEO
Non-Executive Directors
Audit Committee
Resources and Remuneration Committee
Strategic risk management for compliance
Controls assurance
Strategic planning and alignment
Strategic decision making
Scorecards
Strategic enterprise systems
Continuous improvement
Strategic risk management
Accountability
Assurance
Value creation
Resource utilisation

Figure 5.2: Enterprise Governance framework

The enterprise governance framework given above outlines clearly the focus, scope and responsibilities of each of these dimensions. Management has to balance these dimensions.

The primary objectives of using the strategic scorecard are:

- Assist the board in the oversight of a strategic process
- Deal with the strategic choice and transformational change
- Give a true and fair view of the company's strategic position and progress
- Track the actions into and out from the strategic process
- At the heart of the framework is the argument that good corporate governance can help to prevent failure, but it does not guarantee good business performance.

The Strategic Scorecard has four basic elements (Figure 5.3) aimed at helping the board to ensure that all strategic aspects are covered by making the board aware of what work is being done.

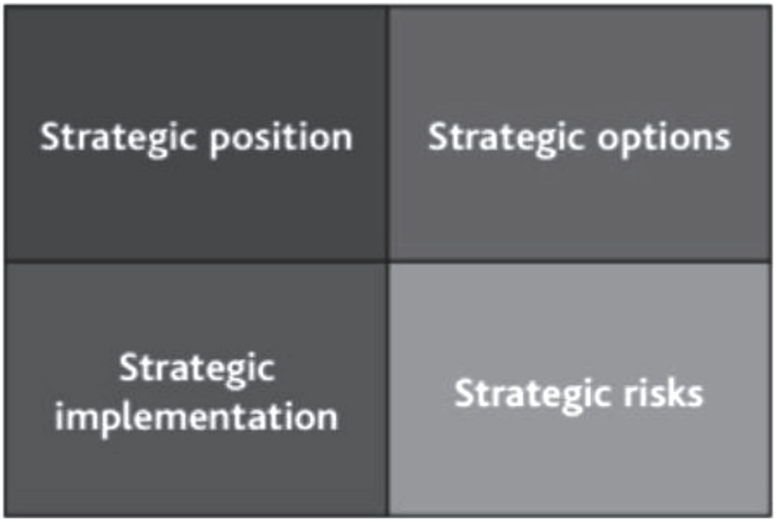


Figure 5.3: Strategic Scorecard

1. **Strategic Position** deals with information on:
   - The micro environment e.g. market, competition and customers
   - The macro environment e.g. political, economic and regulatory factors
   - Threats from changes e.g. strategic inflexion points
   - Business position e.g. market share, pricing, quality, service
   - Capabilities e.g. core competencies and SWOT analysis which deals with Strengths, Weaknesses, Opportunities and Threats
   - Stakeholders e.g. vendors, employees, shareholders
2. **Strategic Options** deals with what options are available with respect to:
   - Scope change e.g. area, product, market sector
   - Direction change e.g. high or low growth, price and quality offers
3. **Strategic Implementation** deals with:
   - Project milestones and timelines
   - Pursue or abandon the plan etc.
4. **Strategic Risks** deals with what can go wrong and what must go right with respect to:
   - Informing the board on risks and how they are being managed
   - Measurement of risks
   - Internal controls

Goal Accomplishment processes / indicators: These are used in order to determine the effectiveness of a system by comparing actual performance with predefined business and IT goals. This can be done by using manual or automated logs in order to issue early warnings, for various processes such as:

- Productivity improvements like lower data entry time taken and errors
- Meeting customer requirements for quality
- Lower hardware or software errors
- Lower IS risks
- Standardised processes
- Lower security violations etc.

These goal indicators will determine whether the targets are being met for the processes.

5.8 Methods to report on IT resource performance

In any modern enterprise using IT extensively, the Investment in IT projects is a major investment and the expenditure on IT operations is one of the major revenue items. Hence, it is important to ensure that the metrics are set for this not only at the operational level but at strategic level.

5.8.1 Strategic Metrics for IT Projects

For IT projects, there should be metrics in place to measure IT project effectiveness in terms of timeliness of delivery, budget vs. actual spending, and whether the solutions delivered contributed to the achievement of organisational objectives as noted in their cost benefit analysis. Cost benefit analysis for each potential IT investment should include ROI analysis, transformation costs, and benefits. It also is important to note the distinction between output and outcome and measure each. While output metrics might be useful and possibly the only means of measurement, the internal auditor should analyse these in relation to actual outcomes. In addition, performance-based agreements and incentives should be reviewed to ensure the organisation is exercising intended governance. Post-implementation reviews are a useful tool for learning and increasing knowledge of what works and what does not.

5.8.2 Strategic Metrics for IT Operations

Metrics should be in place to measure the effectiveness of the day-to-day operational aspects of the IT function. From an internal perspective, IT management will require more technical metrics such as system uptime/ downtime, helpdesk ticket open-to-closed ratio, peak usage time periods, capacity, and utilisation. To enable easier measurement of IT's impact on the achievement of strategic organisation goals, it could be helpful to break down these goals into lower level operational component objectives and use various metrics such as SLAs and operations level agreements (OLAs).

5.9 Maturity Model

Capability Maturity Model Integration (CMMI) is a process improvement approach that provides enterprise with the essential elements of effective processes. It can be used to guide process improvement across a project, division or entire organisational CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes and a point of reference for appraising current processes.

The COBIT 5 product set includes a process capability model, based on the internationally recognised ISO/IEC 15504 Software Engineering: Process Assessment standard. This model provides a means to measure the performance of any of the governance (Evaluate, Direct and Monitor [EDM]-based) processes or management (Plan, Build, Run and Monitor [PBRM]-based) processes and will allow areas for improvement to be identified.

The ISO/IEC 15504 standard specifies that process capability assessments can be performed for various purposes and with varying degrees of rigour. Purposes can be internal, with a focus on comparisons between enterprise areas and/or process improvement for internal benefit, or they can be external, with a focus on formal assessment, reporting and certification.

5.10 Total Quality Management

Total quality management (TQM) is a management strategy aimed at embedding awareness of quality in all organizational processes. It is a set of systematic activities carried out by the entire enterprise to effectively and efficiently achieve company objectives and provide products and services with a level of quality that satisfies customers at the appropriate time and price. At the core of TQM is a management approach to long-term success through customer satisfaction. In a TQM effort, all members of an enterprise participate in improving processes, products, services and the culture in which they work. Quality management for IT services is a systematic way of ensuring that all the activities necessary to design, develop and implement IT services that satisfy the requirements of the organization and of users take place as planned and that the activities are carried out in a cost-effective manner.

5.11 Quality Management

The scope of the process of "Manage Quality" is to define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring and the use of proven practices and standards in continuous improvement and efficiency efforts. This helps in ensuring the consistent delivery of solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.

The development and maintenance of defined and documented processes by the IS department is evidence of effective governance of information resources. Observance of documented processes and use of related process management techniques is key to the effectiveness and efficiency of the IS organisation. Various standards have emerged to assist IS organisations in achieving these results. Quality standards are increasingly being used to assist IS organisations in achieving an operational environment that is predictable, measurable, repeatable and certified for their IT resources. Quality has to be monitored by setting of appropriate goals and metrics both at strategic and operational level.

Quality management is the means by which IS department-based processes are controlled, measured and improved. Processes in this context are defined as set of tasks that, when properly performed, produce the desired results. Areas of control for quality management may include the following:

- Software development, maintenance and implementation
- Acquisition of hardware and software
- Day-to-day operations
- Service management
- Security
- HR management
- General administration

5.12 Summary

The purpose of performance measurement is to uncover, communicate and evolve organisational performance drivers. The choice of measures communicates to stakeholders what is important, and this affects what gets done. Choosing measures that answer critical management questions improves management's visibility into key processes. This chapter has provided an overview of performance management system with specific details from COBIT 5 using enterprise goals, IT related goals with examples of specific process with IT related goals with related metrics and process goals with related metrics. Further, the key concepts of Balanced scored card with the four perspectives with example of IT BSC have been illustrated. Other examples of performance measurement such as strategic scorecard, maturity model, TQM and total Quality management have been covered in brief.

The key to success is setting goals and monitoring them to ensure success with corrective steps to be taken as required. Use of frameworks helps in setting the right goals with the metrics to measure and monitor successful achievement of the goals. Performance measurement is critical for successful implementation of Governance or GEIT. Performance management helps management in keeping on track towards meeting stakeholder requirements and also in complying with regulatory requirements on time. IS Auditors with knowledge of performance management system can provide assurance or advisory services on the performance management system in place and provide recommendations for improving the effectiveness.

5.13 Questions

1. Which of the following is best approach for monitoring the performance of IT resources?
   - A. Compare lag indicators against expected thresholds
   - B. Monitor lead indicators with industry best practices
   - C. Define thresholds for lag indicators based on long term plan
   - D. Lead indicators have corresponding lag indicator.
2. Performance monitoring using balance score card is most useful since it primarily focuses on:
   - A. Management perspective
   - B. Product and services
   - C. Customer perspectives
   - D. Service delivery processes
3. Which of the following is considered as an example of a lead indicator?
   - A. Number of gaps with respect to industry standard
   - B. Comparative market position of organisation
   - C. Percentage of growth achieved over three years
   - D. Improvement in customer satisfaction survey

4. The **PRIMARY** objective of base lining IT resource performance with business process owners is to:

   A. Define and implement lead and lag indicators

   B. Ensure resource planning is aligned with industry

   C. Assess cost effectiveness of outsourcing contracts

   D. Benchmark expected performance measurement

5. Which of the following is **BEST** measure to optimize performance of skilled IT human resources?

   A. Include personal development plan in job description

   B. Document personal expectations during exit interviews

   C. Implement 'Bring Your Own Device (BYOD)' policy

   D. Monitor performance measure against baseline

6. IT resource optimisation plan should primarily focus on

   A. Reducing cost of resources

   B. Ensuring availability

   C. Conducting training programs

   D. Information security issues

7. The **PRIMARY** objective of implementing performance measurement metrics for information assets is to:

   A. Decide appropriate controls to be implemented to protect IT assets

   B. Compare performance of IT assets with industry best practices

   C. Determine contribution of assets to achievement of process goals

   D. Determine span of control during life cycle of IT assets

8. Which of the following is the **PRIMARY** purpose of optimising the use of IT resources within an enterprise?

   A. To increase likelihood of benefit realization

   B. To ensure readiness for future change

   C. To reduce cost of IT investments

   D. To address dependency on IT capabilities

9. While monitoring the performance of IT resources the **PRIMARY** focus of senior management is to ensure that:

   A. IT sourcing strategies focus on using third party services

   B. IT resource replacements are approved as per IT strategic plan

   C. Key goals and metrics for all IT resources are identified

   D. Resources are allocated in accordance with expected performance

10. Organisation considering deploying application using cloud computing services provided by third party service provider. The MAIN advantage of this arrangement is that it will

    A. Minimize risks associated with IT

    B. Help in optimizing resource utilization

    C. Ensure availability of skilled resources

    D. Reduce investment in IT infrastructure

5.13 Answers and Explanations

1. **B.** Lead indicators are proactive approach for ensuring performance shall be as expected and hence are defined using industry best practices. Lag indicators are useful after the fact (A), Thresholds based on long term plane may not provide input on performance during execution. (C). All lead indicators may not have lag indicator.
2. **C.** The Balance Score card (BSC) focuses on Financial, Customer, internal and learning perspective.
3. **A.** Lead indicators are proactive in nature and helps management in planning. Identification of gaps with respect to industry standard is beginning of process of implementing best practices. Other indicators are result of past performance.
4. **D.** In order to plan resources performance of resource must be determined and compared with business expectation from IT. This will help management in implementing performance measures against expected performance. Other options uses baselines.
5. **A.** Motivation helps human resources in performing better. Career progression planning including in job description along with performance norms shall help in motivating human resources.
6. **B.** Resource optimisation plan primarily focus on availability of right resources at right time. Other requirements are secondary.
7. **C.** Resource performance is essential to measure the performance of business and IT processes so as to monitor the level of contribution in achieving process goals and hence business objectives. Performance measurement is performed to measure this contribution.
8. **A.** IT resource optimisation within an enterprise must primarily focus on increasing benefit realization from IT so as to deliver value to business. B. Ensuring readiness for future change is essential to meet the growing IT service delivery and is part of resource optimisation requirements, but not the primary purpose. C. Resource optimisation may or may not reduce IT costs, however it will help in increasing return on IT investment. D. Business dependency on IT depends on capabilities of IT to deliver services to business. Resource optimization is one of the processes to address this dependency not objective.
9. **D.** Management must monitor the performance of IT resources to ensure that the expected benefits from IT are being realised as per planned performance. This is done by allocating IT resources in accordance to the planned performance of business process cascaded down to IT resources supporting business processes.
10. **B.** Outsourcing shall help organisation in optimizing use of existing IT resources by outsourcing, which in turn shall help in focusing on more critical business requirements and hence improving benefit realisation. However outsourcing may or may not minimize risks associated with IT. i.e. it may minimise risks associated with own investment but may introduce risks associated with outsourcing. Although outsourcing helps in ensuring availability of skilled resources, it is not main advantage. Outsourcing may or may not reduce investment in IT, i.e. it may reduce need for acquisition of IT infrastructure, but there is cost associated with outsourcing and there is additional cost for SLA monitoring.

CHAPTER 6: IMPLEMENTING GOVERNANCE AND MANAGEMENT PRACTICES

Learning Objectives

Implementing Governance is about implementing key Governance practices with responsibility set right at the top with Board and executive management involved in all key areas of IT and evaluating, directing and monitoring the use of technology to achieve enterprise goals. COBIT 5 clarifies the distinction between governance and management practices with the addition of a new Governance domain. The design of specific processes and procedures based on COBIT 5 should always fit the needs of the enterprise's culture, management style and IT environment. The guidance in COBIT 5 must be tailored appropriately. It is important to select and adopt the best practices that are recommended but adapt them so that they will be practical and appropriate to each specific enterprise's objectives and needs. The activities provide guidance on what needs to be implemented to achieve a specific management practice. The COBIT 5 practices and activities are based on current relevant standards and best practices which should be used and integrated to obtain more detailed and specific guidance. This chapter briefly describes systematic approach to implementing GEIT and illustrates how to implement GEIT practices in specific areas. It also provides methodology for scoping IS assurance and consulting assignments using COBIT 5 processes.

6.1 Introduction

One of the primary reasons for implementing GEIT is to alleviate pain points. Another reason could be trigger events. Some examples of trigger events could be acquisition/merger, new market conditions or new regulations. Some examples of the pain points faced by enterprises could be:

- Complicated IT assurance efforts due to entrepreneurial nature of many of the organisations.
- Complex IT operating models due to the internet service based business models in use.
- Geographically dispersed entities, made up of diverse cultures and languages.
- The Federated and largely autonomous business control model employed within the group.
- Implementing reasonable levels of IT management, given a highly technical, and at times, volatile IT workforce.
- IT's balancing of the enterprise's drive for innovation capabilities and business agility, with the need to manage risks and have adequate control.
- The setting of risk and tolerance levels for each business unit.
- Increasing need to focus on meeting regulatory (Privacy) and contractual (PCI), compliance requirements.
- Regular audit findings about poor IT controls and reported IT quality of service problems.
- Delivering new and innovative services in a highly competitive market successfully on time.

6.2 Stakeholders in implementing GEIT

There are many stakeholders who need to collaborate to achieve the overall objective of improved IT performance. COBIT 5 is based on stakeholder needs and the approach provided in this guide will help to develop an agreed-upon and common understanding of what needs to be achieved to satisfy specific stakeholder concerns in a coordinated and harmonised way. The most important stakeholders and their specific role and responsibilities are outlined here:

- **Board and executive management:** How do we set and define enterprise direction for the use of IT and monitor that relevant and required *GEIT* enablers are established so that business value is delivered and IT-related risks are mitigated?
- **Business management and business process owners:** How do we enable the enterprise to define/align IT-related goals to ensure that business value is delivered from the use of IT and IT-related risks are mitigated?
- **Chief Information Officer (CIO), IT management and IT process owners:** How do we plan, build, deliver and monitor information and IT solutions and service capabilities as required by the business and directed by the board?
- **Risk, compliance and legal experts:** How do we ensure that we are in compliance with policies, regulations, laws and contracts, and risks are identified, assessed and mitigated?
- **Internal audit:** How do we provide independent assurance on value delivery and risk mitigation?

6.3 Critical Success factors of GEIT implementation

There are many factors which help in successful implementation of GEIT in an enterprise and these vary across enterprises. However, in generally, the critical success factors for a successful GEIT implementation are:

- Top management provides the direction and mandate
- All stakeholders understand the enterprise and IT-related objectives
- Effective communication mechanism and channels are established
- Enablement of the necessary organisational and process changes.
- Frameworks and good practices to fit the purpose and design of the organisation are identified, adapted and used.
- The initial focus is on quick wins and the prioritisation of the most beneficial improvements that are easiest to implement to demonstrate benefit and build confidence for further improvement.
- Benefits of implementation are communicated regularly to all stakeholders.
- Implementation of GEIT is taken as a project with a project champion who is empowered with the requisite responsibility and authority for execution.
- The project implementation is monitored with specific milestones and deliverables.
- On closure of the project, the processes are integrated as part of day-to-day activities to ensure sustainability.

6.4 Using systematic approach for implementing GEIT

COBIT 5: Implementation provides a systematic approach for implementing GEIT project within an enterprise with specific phases, tasks and activities and roles and responsibilities and deliverables of each of these phases. One of the key enablers of GEIT implementation is “Culture, ethics and behaviour”. This is set by the tone at the top with the senior management establishing and enforcing the right culture. In implementing GEIT, this is most critical. The COSO framework also highlights this. The overall enterprise environment should be analysed to determine the most appropriate change enablement approach. This will include aspects such as the management style, culture (ways of working), formal and informal relationships, and attitudes. It is also important to understand other IT or enterprise initiatives that are ongoing or planned, to ensure that dependencies and impacts are considered. It should be ensured from the start that the required change enablement skills, competencies and experience are available and utilised: for example, by involving resources from the HR function or by obtaining external assistance. As an outcome of this phase, the appropriate balance of directive and inclusive change enablement activities required to deliver sustainable benefits can be designed. A systematic approach for implementing GEIT is provided in the publication: “COBIT 5: Implementation”. This is based on the Kotter model. Brief overview of each of the phases of a GEIT implementation is provided. This approach has to be adapted as per requirements of the project.

6.4.1 Phase 1: Establish the desire to change

The purpose of this phase is to understand the breadth and depth of the envisioned change, the various stakeholders that are impacted, the nature of the impact on and involvement required from each stakeholder group, as well as the current readiness and ability to adopt the change. Current pain points and trigger events can provide a good foundation for establishing the desire to change. The ‘wake-up call’, an initial communication on the programme, can be related to real-world issues that the enterprise may be experiencing. Also, initial benefits can be linked to areas that are highly visible to the enterprise, which creates a platform for further changes and more widespread commitment and buy-in. While communication is a common thread throughout the implementation or improvement initiative, the initial communication or wake-up call is one of the most important and should demonstrate the commitment of senior management - therefore, it should ideally be communicated by the Executive Committee or CEO.

6.4.2 Phase 2: Form an effective implementation team

Dimensions to consider in assembling the right core implementation team include involving the appropriate areas from business and IT as well as the knowledge and expertise, experience, credibility, and authority of team members. Obtaining an independent, objective view as provided by external parties, such as consultants and change agent, could also be highly beneficial and aid the implementation process or could address skill gaps that may exist within the enterprise. Therefore, another dimension to consider is the appropriate mix of internal and external resources. The essence of the team should be a commitment to:

- A clear vision of success and ambitious goals
- Engaging the best in all team members, all the time
- Clarity and transparency of team processes, accountabilities and communications

- Integrity, mutual support and commitment to each other's success
- Mutual accountability and collective responsibility
- Ongoing measurement of its own performance and the way it behaves as a team
- Living out of its comfort zone, always looking for ways to improve, uncovering new possibilities and embracing change

It is important to identify potential change agents within different parts of the business that the core team can work with to support the vision and cascade changes down.

6.4.3 Phase 3: Communicate desired vision

A high-level change enablement plan should be developed in conjunction with the overall programme plan. A key component of the change enablement plan is the communication strategy, which should address who the core audience groups are, their behavioural profiles and information requirements, communication channels, and principles. The desired vision for the implementation or improvement programme should be communicated in the language of those affected by it. The communication should include the rationale for and benefits of the change, as well as the impacts of not making the change (purpose), the vision (picture), the road map to achieving the vision (plan) and the involvement required of the various stakeholders (part). Senior management should deliver key messages (such as the desired vision). It should be noted in the communication that both behavioural/cultural and logical aspects should be addressed, and that the emphasis is on two-way communication. Reactions, suggestions and other feedback should be captured and acted upon.

6.4.4 Phase 4: Empower role players and identify quick wins

As core improvements are designed and built, change response plans are developed to empower various role players. The scope of these may include:

- Organisational design changes such as job content or team structures
- Operational changes such as process flows or logistics
- People management changes such as required training and/or changes to performance management and reward systems

Any quick wins that can be realised are important from a change enablement perspective. These could be related to the pain points and trigger events discussed in Chapter 2. Visible and unambiguous quick wins can build momentum and credibility for the programme and help to address any scepticism that may exist. It is imperative to use a participative approach in the design and building of the core improvements. By engaging those impacted by the change in the actual design, e.g., through workshops and review sessions, buy-in can be increased.

6.4.5 Phase 5: Enable operation and use

As initiatives are implemented within the core implementation life cycle, the change response plans are implemented. Quick wins that may have been realised are built on and the behavioural and cultural aspects of the broader transition are addressed (issues such as dealing with fears of loss of responsibility, new expectations and unknown tasks). It is important to balance group and individual interventions to increase buy-in and engagement and to ensure that all stakeholders obtain a holistic view of the change.

Solutions will be rolled out and during this process, mentoring and coaching will be critical to ensure uptake in the user environment. The change requirements and objectives that had been set during the start of the initiative should be revisited to ensure that they were adequately addressed. Success measures should be defined and should include both hard business measures and perception measures that track how people feel about a change.

6.4.6 Phase 6: Embed new approaches

As concrete results are achieved, new ways of working should become part of the enterprise's culture and rooted in its norms and values ('the way we do things around here') – for example, implementing policies, standards and procedures. The implemented changes should be tracked, the effectiveness of the change response plans should be assessed and corrective measures taken as appropriate. This might include enforcing compliance where still required. The communication strategy should be maintained to sustain ongoing awareness.

6.4.7 Phase 7: Sustain

Changes are sustained through conscious reinforcement and an ongoing communication campaign, and they are maintained and demonstrated by continued top management commitment. Corrective action plans are implemented, lessons learned are captured and knowledge is shared with the broader enterprise

6.5 Implementing Governance and Management practices

Implementing Governance and management practices is essential for every enterprise to meet management and regulatory requirements. However, the specific practices which need to be implemented vary depending on various factors such as requirements, current maturity level, management style, regulatory environment, etc. One of the guiding principles in COBIT is the distinction made between governance and management. In line with this principle, every enterprise would be expected to implement a number of governance processes and a number of management processes to provide comprehensive governance and management of enterprise IT. When considering processes for Governance and management in the context of the enterprise, the difference between types of processes lies within the objectives of the processes.

6.5.1 Governance Processes and Practices

Governance processes

Governance processes deal with the stakeholder governance objectives—value delivery, risk optimisation and resource optimisation—and include practices and activities aimed at evaluating strategic options, providing direction to IT and monitoring the outcome (Evaluate, direct and monitor [EDM] - in line with the ISO/IEC 38500 standard concepts). The relationship between Governance and management is clearly established with Governance being based on the principles of "Evaluate, Direct and Monitor". COBIT 5 has five Governance processes.

Governance practices

The generic governance practices provided in COBIT 5 to implement Governance are:

- **Evaluate the Governance System:** Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;
- **Direct the Governance System:** Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making; and
- **Monitor the Governance System:** Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

6.5.2 Key Management Processes and Practices

Management processes

In line with the definition of management, practices and activities in management processes cover the responsibility areas of PBRM enterprise IT, and they have to provide end-to-end coverage of IT. Although the outcome of both types of processes is different and intended for a different audience, internally, from the context of the process itself, all processes require 'planning', 'building or implementation', 'execution' and 'monitoring' activities within the process. The guidance for implementing processes and practices has structure and contents provided in a consistent manner which can be applied across the enterprises. The processes also have inbuilt PDCA (Plan, Do, Check, Act) cycle for ensuring continuous quality improvement.

Management practices

COBIT 5 has four domains covering all areas of management. There are 32 processes in the four domains of: Align, Plan and Organise (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS) and Monitor, Evaluate and Assess (MEA). Each of these process has set of management practices and there are more than 200 management practices covering all the processes. Further, each of the management practices has set of activities which can be implemented to achieve the management practices and thus ensure that the required process structure is in place. Please refer to COBIT 5: Process for more details of the process.

6.6 Implementing GEIT in specific areas

Chapter 1 provides generic guidelines on implementing GEIT. Further, in first section of this chapter we have reviewed the systematic approach with specific phases for implementing GEIT. The most critical factors in implementing GEIT is to identifying the scope and objectives of such implementation and based on this prioritise which of the 37 processes the organisation has to select and focus on for making implementation achieve the objectives. The ideal implementation approach would be to take a top-down perspective and obtain understanding of the business' strategic goals through discussions with business-unit management and executives. This will help in understanding of pain points and identifying relevant best practice guidance to adapt and implement. Another critical aspects of implementing GEIT is identifying and setting the outcomes and performance measures for specific goals and activities by using the pragmatic approach of adopt and adapt so as to make these relevant for the organisation. Some specific examples of implementing GEIT in specific areas are explained in the next section of this chapter. These cover key areas such as: Strategic alignment, value optimisation, resource optimisation, outsourcing and capacity management.

6.6.1 Strategic alignment of IT with business

Strategic alignment and performance measurement are important and apply overall to all the Governance and management activities to ensure that IT goals are aligned with the enterprise goals and there are process goals are set for the IT goals and metrics are designed for these. IT is a key enabler of corporate business strategy. Chief Executive Officers (CEO), Chief Financial Officers (CFO) and Chief Information Officers (CIO) agree that strategic alignment between IT and business objectives are a critical success factor for the achievement of business objectives. Corporate governance drives the corporate information needs to meet business objectives. IT has to provide critical inputs to meet the information needs of all the required stakeholders or it can be said that enterprise activities require information from IT activities in order to meet enterprise objectives. Hence, corporate governance drives and sets IT governance.

Management Strategy determines at the macro level the path and methodology of rendering services by the enterprise. Strategy outlines the approach of the enterprise and is formulated by the senior management. Based on the strategy adapted, relevant policies and procedures are formulated. From business strategy perspective, IT is affecting the way in which enterprises are structured, managed and operated. One of the most dramatic developments affecting enterprises is the fusion of IT with business strategy. Enterprises can no longer develop business strategy separate from IT strategy and vice versa. Accordingly, there is a need for the integration of sound IT planning with business planning and the incorporation of effective financial and management controls within new systems. Management primarily is focused on harnessing the enterprise resources towards achievement of business objectives. This would involve the managerial processes of planning, organising, staffing, directing, co-ordinating, reporting and budgeting.

Objective of IT Strategy

The primary objective of IT strategy is to provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment by leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives. Alignment of the strategic IT plans with the business objectives is done by clearly communicating the objectives and associated accountabilities so they are understood by all and all the IT strategic options are identified, structured and integrated with the business plans as required.

IT organisations should define their strategies and tactics to support the organisation by ensuring that day-to-day IT operations are delivered efficiently and without compromise. Metrics and goals are established to help IT perform on a tactical basis and also to guide the efforts of personnel to improve maturity of practices. The results will enable the IT function to execute its strategy and achieve its objectives established with the approval of enterprise leaders. Internal audit can determine whether the linkage of IT metrics and objectives aligns with the organisation's goals, adequately measure progress being made on approved initiatives, and express an opinion on whether the metrics are relevant and useful. Additionally, auditors can validate that metrics are being measured correctly and represent realistic views of IT operations and governance on a tactical and strategic basis.

IT Strategy Planning

IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation. Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise. Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

IT Strategic Planning Process

The strategic planning process has to be dynamic in nature and IT management and business process owners should ensure a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the enterprise's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long and short-range plan are developed and maintained. IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

Aligning IT Strategy with Enterprise Strategy

The key management practices, which are required for aligning IT strategy with enterprise strategy, are highlighted here:

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.
- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT

environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.

- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT-related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritise the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

The success of alignment of IT and business strategy can be measured by reviewing the percentage of enterprise strategic goals and requirements supported by IT strategic goals, extent of stakeholder satisfaction with scope of the planned portfolio of programmes and services and the percentage of IT value drivers, which are mapped to business value drivers.

Role of IS Auditors

IS auditors could be involved in providing assurance requiring review of Information Systems as implemented from control perspective. However, auditors may also be required to provide consulting before, during or after implementation of information systems strategy. It becomes imperative for the auditor to understand the concepts of the enterprise strategy as relevant. Hence, auditors must have good understanding of management aspects as relevant to deployment of IT and IT strategy. This would include understanding of the IS Strategy, policies, procedures, practices and enterprise structure, segregation of duties, etc.

6.6.2 Value optimisation

Business value from use of IT is achieved by ensuring optimisation of the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost. The benefit of implementing this process will ensure that enterprise is able to secure optimal value from IT-enabled initiatives services and assets, cost-efficient delivery of solutions and services, and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.

Key Governance practices

The key management practices, which need to be implemented for evaluating 'whether business value is derived from IT', are highlighted as under:

- **Evaluate Value Optimisation:** Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimise value creation.
- **Direct Value Optimisation:** Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.
- **Monitor Value Optimisation:** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.

The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realised from IT enabled investments and services portfolio and the how transparency of IT costs, benefits and risk is implemented.

Metrics for value optimisation

Some of the key metrics, which can be used for such evaluation, are:

- Percentage of IT enabled investments where benefit realisation monitored through full economic life cycle;
- Percentage of IT services where expected benefits realised;
- Percentage of IT enabled investments where claimed benefits met or exceeded;
- Percentage of investment business cases with clearly defined and approved expected IT-related costs and benefits;
- Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

6.6.3 Resource Optimisation

The process of Resource optimisation has to be implemented to ensure that adequate and sufficient IT related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost. The primary objectives of implementing this process is to ensure that the resource needs of the enterprise are met in the most optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change. A key to successful IT performance is the optimal investment, use and allocation of IT resources (people, applications, technology, facilities, data) in servicing the needs of the enterprise. Most enterprises fail to maximise the efficiency of their IT assets and optimise the costs relating to these assets. *GEIT* is concerned with IT value delivery to the business and the mitigation of IT-related risks. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals. ISACA's COBIT 5 introduces a "resource governance" process to "Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised and there is an increased likelihood of benefit realisation and readiness for future change".

Key Governance practices

The key Governance practices of this process are defined as follows:

- **EDM04.01 Evaluate resource management:** Continuously examine and make judgment on the current and future need for IT-related resources, options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.
- **EDM04.02 Direct resource management:** Ensure the adoption of resource management principles to enable optimal use of IT resources throughout their full economic life cycle.
- **EDM04.03 Monitor resource management:** Monitor the key goals and metrics of the resource management processes and establish how deviations or problems will be defined, tracked and reported for remediation.

6.6.4 Sourcing processes

Sourcing is managed through suppliers and appropriate service agreements. COBIT 5 has specific processes: Manage Services and Manage Suppliers which provide specific guidance. The scope of the process of “Manage service agreements” is to align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators. This helps in ensuring that IT services and service levels meet current and future enterprise needs.

The scope of process of "Manage Supplier" is to ensure that IT-related services provided by all types of suppliers meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance. This helps in minimising the risk associated with non-performing suppliers and ensure competitive pricing.

Sourcing processes refer to the procurement practices of an organisation in order to find, evaluate and engage vendors of goods and services are called sourcing processes. The purchasing processes should ensure that the processes are defined and capable of meeting organisational needs. This involves several activities like:

- Timely identification of needs.
- Evaluation of product cost, performance and delivery and installation logistics.
- Method of evaluating that quality needs have been met.
- Contract administration, guarantee replacement or warranty, access to the vendors premises, vendor development and
- Reduction of vendor related risks.

6.6.5 Outsourcing

Outsourcing is a strategic decision for management in order to achieve long-term improvement in business performance, by utilising the vendor’s core competencies. Outsourcing is the order of the day for many organisations today. IT is one of the key areas which is outsourced in part or in totality depending on the criticality of the processes. There are many service providers who provide a range of outsourcing services. Although IT outsourcing has many benefits, it has inherent risks which need to be mitigated. The risks are much more when IT outsourcing covers strategic use of IT. Hence, mitigating these risks require all the service provider are managed through an appropriate structure. This vendor management process should not only monitor performance but also include specific functional heads who have the appropriate level of authority to hold the service providers accountable. Some of the important tools which are used to manage and monitor IT service providers are performance targets, service level agreements (SLAs), and scorecards. It is critical to note that senior management cannot abdicate its ultimate responsibility for IT service delivery just because it has been outsourced as the responsibility for compliance and ensuring performance vests with the enterprise. The key principles and guidelines as explained earlier relating to sourcing are applicable to outsourcing as this is also a form of sourcing.

6.6.6 Capacity Management & Growth Planning processes

Capacity management is the process of planning, sizing and continuously optimising IS capacity in order to meet long and short-term business goals in a cost effective and timely manner. Its primary goal is to ensure that IT capacity meets current and future business requirements in a cost-effective manner. Capacity management is covered in COBIT in the process of "Manage Configuration." The scope of this process is to define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository. This helps in providing sufficient information about service assets to enable the service to be effectively managed, assess the impact of changes and deal with service incidents.

Capacity management to be effective has to be supported by an effective process of monitoring and evaluating Performance and Conformance. The scope of this process is to collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed performance and conformance goals and metrics and provide reporting that is systematic and timely. This helps in providing transparency of performance and conformance and drive achievement of goals. Capacity management or configuration management process is used in order to assess the effectiveness and efficiency of the IS operations. Capacity includes:

- Storage space
- Network throughput
- Human resources
- Electronic messaging
- Customer Relationship Management
- Quantum of data processed, etc.

The ITIL framework provides a set of best practices in service delivery and views capacity management from three dimensions:

1. Business Capacity Management
2. Service Capacity Management and
3. Component or resource Capacity Management

The success of capacity management depends on factors like:

- The availability of precise and timely business forecasts
- Having a thorough understanding of present and future technologies
- Proper communication with service management processes
- Planning and acquiring appropriate levels of resources in order to meet business needs

The benefits of good capacity management are:

- Enhanced customer satisfaction
- Better justification of spending on IS resources
- Avoiding incorrect capacity sizing which may lead to inappropriate utilisation of IS resources and insufficient capacity to process the production workloads
- A reduction in capacity failures
- Better alignment of business needs and IS resources
- Better service level management

6.6.7 Capex and Opex

Outsourcing and capacity management requires effective utilisation of resources thereby resulting in business value from investments. There are various options for procuring IT assets. In the current era, IT is being regarded increasingly as a utility and there are vendors providing all types of IT outsourcing services. Use of IT through outside vendors reduces capital expenditure but increases revenue expenditure or it can be said that Capex is converted to Opex. It is important for management to understand the key concepts of Capex and Opex as they impact the funds outflow and ROI on usage of such IT resources. These concepts are briefly explained here.

Capex stands for Capital Expenditures and is the money spent of generating physical assets. Opex stands for Operating Expenditures and refers to day-to-day expenses required to maintain physical assts. Capex and Opex are necessary to be measured to arrive at the valuation of any organization. Capex is a business expense incurred to create future benefit i.e. acquisition of assets that will have a useful life beyond the tax year. For example expenditure on assets like building, machinery, equipment or upgrading existing facilities so their value as an asset increases. Since capital expenses acquire assets that have a useful life beyond the tax year, these expenses cannot be fully deducted in the year in which they are incurred. Instead, they are capitalized and either amortized or depreciated over the life of the asset. Intangible assets like intellectual property (e.g. patents) are amortised and tangible assets like equipment are depreciated over their lifespan.

Capex refers to all assets, whether tangible or intangible, that is made use of, to generate more business and thus, revenues. Capex is an investment in the business. It adds to shareholders value. These are expenditures made keeping in mind the future benefits. These investments could be on machinery, equipment, property or upgrade of apparatus. It is usually shown in the financial statement as cash flow or investment in plant, machinery or similar head. Depreciation of such assets takes place every year until it becomes zero. Opex refers to expenses that are incurred on maintenance and running of assets generated through Capex. Day-to-day running expenses for sales and administration and R&D are taken as Opex. Thus Opex are expenses that are necessary to maintain capital assets. On the other hand, those expenditures required for the day-to-day functioning of the business, like salaries, administrative expenses, maintenance, repairs, etc. These fall under the category of Opex. Opex is the money the business spends in order to turn inventory into throughput. Operating expenses also include depreciation of plants and machinery which are used in the production process or official work. Operating expenditure, on the other hand, can be fully deducted. "Deducted" means subtracted from the revenue when calculating the profit/loss of the business. Most companies are taxed on the profit that they make; so what expenses you deduct impacts your tax bill.

In general, Capex is what needs to be avoided, while Opex is something to be kept under tight control. Opex can be considered to be (in) efficiency of any business. It has a direct relation with the value of the business. If you can reduce Opex without hurting day to day operations, you eventually increase valuation of any business. The concept of Capex and Opex is critical to consider in making IT enabled investment decisions. The distinction between Capex and Opex has become important as most of the organisations now look at outsourcing as the preferred option for all non-core activities. Further, in cloud computing environment, critical activities are outsourced by organisations considering the benefits of converting Capex into Opex. IS Auditors who are required to evaluate such alternatives have to consider not only the cost benefit analysis but also the associated risks and how these risks have been mitigated through implementation of appropriate controls.

6.7 Auditing Governance and Management Practices

Technology will keep on evolving on a regular basis. We have seen IT moving from main frame to desktops to laptops to tablets. Similarly, the networking has moved from wired/cabled to wireless and computing is moving from fixed location to cloud computing to mobile computing. Each phase of technology evolution brings with its own benefits and inherent risks. The risks need to be mitigated by implementing appropriate controls and independent assurance is required by management. CA firms with the right Technology skills can exploit this opportunity to provide assurance and consulting services to clients. There are no ready-made solutions/training courses which can meet all the requirements of CA firms. CA firms have to perform their own SWOT analysis and chalk out the strategy for updating skills to remain relevant with the times. IT strategic planning and IT planning could enable CA firms to successfully ride the technology wave and become thought leaders in the dynamic IT arena.

Auditors whether internal or external, whether general or specialists, have to understand business processes and assess how controls are implemented for any assurance engagement. However, understanding of business process and assessment of controls in an IT environment requires understanding technology and how controls are implemented using technology to mitigate risks. The old approach of putting “ticks” by using checklists is no longer relevant; auditors need to learn how to “click”. It is said auditing was and always will be a thinking person's profession and no software will ever replace that but building relevant IT competencies and skill-sets to harness the power of technology is a must.

Using global best practices can help in developing standard approach for providing IT enabled services. For example, a good understanding of the COBIT 5 Concepts and COBIT 5 Enabling process documents (available at www.isaca.org/cobit) will enable auditors to provide different types of IT enabled services by using a combination relevant processes from the list of 37 processes. These processes have detailed management practices, input-output matrix, RACI chart and activities which can be used as a benchmark and customised for scoping assignments as required. By reading the contents of each of the process, one can get good idea of what is covered in each of these processes. The contents from each of these processes or a combination of selected processes as relevant can be made for preparing the proposal which becomes starting point from discussion regarding scope and objective of the assurance/consulting assignment. Once the scope is agreed upon, the extracted contents from these processes can be customised and used as a benchmark for providing the required services. This annexure provides a list of IT enabled services with title of the assignment, sample scope and objectives of the assignment. This list can be used as the starting point for identifying current competencies and building capabilities to provide services in identified areas of services which can be provided by CAs.

6.8 Summary

Successful implementation of GEIT requires use of systematic approach. This chapter has provided outline of approach for implementing GEIT with specific phases, milestones and deliverables. GEIT implementation requires differentiating governance and management so that senior management has the responsibility with the Board and executive management involved in all key areas of IT and evaluating, directing and monitoring the use of technology to achieve enterprise goals. Management has to understand the governance setting and accordingly work on operationalising these into specific actionable items for implementation.

The definition of Governance and Management from COBIT 5 have been provided. The key principles of Governance and management with detailed list of practices under each of them have been outlined. Further, specific examples on how to implement governance and management practices in key areas such as strategic alignment, value optimisation, resource optimisation, outsourcing and capacity management have been explained. Finally, IS Auditors have an important role to play in implementing and evaluating GEIT. An overview of the specific role of IS Auditors with examples of how to scope such assignments using COBIT processes have been provided in the appendix.

6.9 Questions

1. Which of the following is MOST critical for implementing GEIT?
   - A. Obtaining financial budget for IT
   - B. Building business case for implementation
   - C. Creating the right environment
   - D. Documenting the enterprise architecture
2. Which of the following principles are MOST relevant for Governance domain?
   - A. Plan, Do, Check and Act
   - B. Evaluate, Direct and Monitor
   - C. Plan, Build, Run and Monitor
   - D. Four dimensions of Balanced Scorecard

3. The primary objectives of implementing Resource optimisation process is to ensure:

   A. resource needs of the enterprise are minimised

   B. return on IT investments is ensured

   C. increased monitoring of benefit realization

   D. making enterprise IT infrastructure resilient

4. Which of the following is MOST critical for ensuring sustained alignment of IT strategic plans? The IT strategic plans provide:

   A. direction to IT department on deployment of information systems

   B. key functionaries are involved in development and implementation

   C. IT long and short-range plans are communicated to stakeholders

   D. feedback is captured, reported and evaluated for inclusion in future IT planning

5. The primary objective of value optimisation process is to ensure:

   A. IT-enabled investments are made at the lowest cost

   B. appropriate IT-enabled initiatives are selected

   C. cost-efficient delivery of solutions and services

   D. Quantification of IT costs and likely benefits

6. Which of the following is the key benefit of capacity management?

   A. Meet long-term business goals in a cost effective and timely manner

   B. Meets current and future business requirements in a cost-effective manner

   C. Define and maintain relationships between key resources and capabilities

   D. Assess the impact of changes and deal with service incidents.

7. In order to ensure that IT strategic plan is successful, the organization first ensure that the plan:

   A. focuses on optimization of cost

   B. is aligned with business strategy

   C. provides direction for IT deployment

   D. consists of long and short term goals

8. Which of the following indicators assurance that IT strategy is focuses on benefit realization?

   A. Low percentage of IT enabled investments where claimed benefits met or exceeded;

   B. High percentage of IT services approved based on reduction in operational costs

   C. High percentage of business cases approved based on costs and benefits

   D. Satisfaction survey of key stakeholders is neutral on IT service delivery.

9. Which of the following is most important to be included in SLA, while considering the outsourcing of IT operation to cloud service provider?

   A. Ownership of information

   B. Periodic audit reports

   C. Logical access controls

   D. Reduction in operational costs

10. Which of the following is primary input for IT resource capacity management planning?

   A. Annual financial budget for IT

   B. IT resource acquisition plan

   C. Number of databases in use

   D. Expected growth of business

6.10 Answers and Explanations

1. C. Creating the right environment is the most critical for implementing GEIT. Obtaining financial budget for IT is an operational activity. Building business case for implementation is done for all projects and not just for GEIT. Documenting the enterprise architecture may help to some extent in implementing GEIT but is not a critical factor.

2. B. Governance domain is built on the three principles of Evaluate, Direct and Monitor. PDCA is pertaining to continuous improvement initiatives. PBRM is pertaining to management domain. The four dimensions of Balanced Scorecard are useful in translating strategy into action. They are useful aid in implementing Governance as measure of performance management but they are not principles of Governance.

3. C. The primary objectives of implementing Resource optimisation process is to ensure increased monitoring of benefit realization. The resource needs of the enterprise are to be optimised and not minimised. Implementing resource optimisation process does not ensure return on IT investments. In implementing resource optimisation the focus is on utilisation considering the investments and benefits. Resilience of IT infrastructure is considered in the process of maintaining business continuity.

4. D. Capturing, reporting and evaluating feedback for inclusion in future IT planning is MOST critical for ensuring sustained alignment of IT strategic plans as this provides metrics for monitoring and also ensuring that the performance is maintained not only for the current but also for the future. Top management shares the enterprise strategy based on which IT strategy is prepared by the IT department. There is no direction to IT department on deployment of information systems provided as part of IT strategic planning. The involvement of key functionaries in development and implementation is critical to ensure success but it is required in the initial stages. However, this does not guarantee the sustainability of the initiative. The communication of IT long and short-range plans is important to get buy-in and to keep all stakeholders informed but this is only a reporting process.

5. B. The primary objective of value optimisation process is to ensure cost-efficient delivery of solutions and services. The focus of value optimisation process is not on ensuring lowest cost but optimal cost of all IT-enabled investments. Selection of appropriate IT-enabled initiatives is one of the operational activities of value optimisation. Although it is critical but it is not the primary objective. All IT investments benefits cannot be quantified. Hence, the option of quantification of IT costs and likely benefits is not correct. Further, this is not the objective but a mechanism of performance monitoring

6. B. The key benefit of capacity management is to ensure that not just the current but the future business requirements are met in a cost-effective manner. Capacity management looks at both long-term as well as short-term business goals in a cost effective and timely manner. Defining, describing and maintaining relationships between key resources and capabilities is a primary requirement of capacity management and not a benefit. Assessing the impact of changes and deal with service incidents is one of the benefits of capacity management but compared to option A, this is not a key benefit

7. B. IT strategic plan must be aligned with business strategic plan in order to maximize benefit realization, optimize cost, provide direction to management and consist of long term and short term goals

8. C. Most IT initiatives are approved based on cost and benefits indicates that the IT strategy is focused on benefit realization. B Indicated focus in on cost reduction. A indicates that IT initiatives does not achieve expected benefits and D indicates that IT services are just enough

9. A. Establishing ownership of assets deployed on infrastructure owned by third party is most essential. Other aspects are required and must be addressed in SLA

10. D. Expected growth of business is primary input for capacity planning of IT resources. IT resources must fulfil the business requirements. Other options depends on expected business growth

6.11 References

www.icai.org

www.cit.icai.org

www.isaca.org/cobit

www.ifac.org

www.aicpa.org

www.sox.org

www.theiia.org

https://cloudsecurityalliance.org/

http://www.cag.gov.in/

http://deity.gov.in/

www.coso.org

www.rbi.org.in

SECTION 2: APPENDIX

IT enabled Services in Governance, Management, Assurance and Control using COBIT 5

P.No	Area	Details
1	***Process***	**Ensure Governance Framework Setting and Maintenance**
1	***Scope***	Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.
1	***Objectives***	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements are confirmed, and the governance requirements for board members are met.
2	***Process***	**Ensure Benefits Delivery**
2	***Scope***	Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost.
2	***Objectives***	Secure optimal value from IT-enabled initiatives services and assets, cost-efficient delivery of solutions and services, and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
3	***Process***	**Ensure Risk Optimisation**
3	***Scope***	Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and risks to enterprise value related to the use of IT are identified and managed
3	***Objectives***	Ensure that IT-related enterprise risks do not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
4	***Process***	**Ensure Resource Optimisation**
4	***Scope***	Ensure that adequate and sufficient IT-related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost.

P.No	Area	Details
4	***Objectives***	Ensure that the resource needs of the enterprise are met in the most optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change
5	***Process***	**Ensure Stakeholder Transparency**
5	***Scope***	Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions
5	***Objectives***	Make sure that the communication to stakeholders is effective and timely and the basis for reporting is established in order to increase performance, identify areas for improvement, and confirm that IT-related objectives and strategies are in line with the enterprise's strategy
6	***Process***	**Manage the IT Management Framework**
6	***Scope***	Clarify and maintain the governance of enterprise IT mission and vision. Implement and maintain mechanisms and authorities to manage information and the use of IT in the enterprise in support of governance objectives in line with guiding principles and policies.
6	***Objectives***	Provide a consistent management approach to enable the enterprise governance requirements to be met, covering management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies
7	***Process***	**Manage Strategy**
7	***Scope***	Provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment, leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives.
7	***Objectives***	Align strategic IT plans with business objectives. Clearly communicate the objectives and associated accountabilities so they are understood by all, with the IT strategic options identified, structured and integrated with the business plans.
8	***Process***	**Manage Enterprise Architecture**
8	***Scope***	Establish a common architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realising enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. Define requirements for taxonomy, standards,

P.No	Area	Details
.		guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components
8	***Objectives***	Represent the different building blocks that make up the enterprise and their inter relationships as well as the principles guiding their design and evolution over time, enabling a standard, responsive and efficient delivery of operational and strategic objectives.
9	***Process***	**Manage Innovation**
9	***Scope***	Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to business needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions
9	***Objectives***	Achieve competitive advantage, business innovation, and improved operational effectiveness and efficiency by exploiting information technology developments.
10	***Process***	**Manage Portfolio**
10	***Scope***	Execute the strategic direction set for investments in line with the enterprise architecture vision, and the desired characteristics of the investment and related services portfolio, and consider the different categories of investments and the resources and funding constraints. Evaluate, prioritise and balance programmes within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programmes into the active services portfolio for execution. Monitor the performance of the overall portfolio, of services and programmes, proposing adjustments to it as necessary in response to programme performance or changing enterprise priorities.
10	***Objectives***	Optimise the performance of the overall portfolio of programmes in response to programmer performance and service performance and changing enterprise priorities and demands.
11	***Process***	**Manage Budget and Costs**
11	***Scope***	Manage the IT related financial activities in both the business and IT functions, covering budgeting, cost and benefit management, and prioritisation of spending through the use of formal budgeting practices and a fair and equitable system of

P.No	Area	Details
		allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed.
11	***Objectives***	Foster partnership between IT and enterprise stakeholders to enable the effective and efficient use of IT related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of IT solutions and services
	Process	**Manage Human Resources**
12	***Scope***	Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people.
12	***Objectives***	Optimise the human resource capabilities to meet enterprise objectives.
	Process	**Manage Relationships**
13	***Scope***	Manage the relationship between the business and IT in a formalised and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance. Base the relationship be based on mutual trust, using open and understandable terms and common language and a willingness to take ownership and accountability for key decisions.
13	***Objectives***	Create improved outcomes, increased confidence, and trust in IT and effective use of resources.
	Process	**Manage Service Agreements**
14	***Scope***	Align IT enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators
14	***Objectives***	Ensure that IT services and service levels meet current and future enterprise needs.
15	***Process***	**Manage Supplier**
15	***Scope***	Ensure that IT related services provided by all types of suppliers meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.

P.No	Area	Details
15	***Objectives***	Minimize the risk associated with non performing suppliers and ensure competitive pricing.
16	***Process***	Manage Quality
16	***Scope***	Define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring and the use of proven practices and standards in continuous improvement and efficiency efforts.
16	***Objectives***	Ensure the consistent delivery of solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs
17	***Process***	Manage Risk
17	***Scope***	Continually identify, assess and reduce IT related risks within levels of tolerance set by enterprise executive management
17	***Objectives***	Integrate the management of IT-¬▯related enterprise risk with overall ERIM, and balance the costs and benefits of managing IT-related enterprise risk.
18	***Process***	Manage Security
18	***Scope***	Define, operate and monitor a system for information security management.
18	***Objectives***	Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels
19	***Process***	**Manage Programmes and Projects**
19	***Scope***	Manage all programmes and projects from the investment portfolio in alignment with enterprise strategy and in a co-ordinated way. Initiate, plan, control, and execute programmes and projects, and close with a post implementation review.
19	***Objectives***	Realise business benefits and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users, ensuring the value and quality of project deliverables, and maximizing their contribution to the investment and services portfolio
20	***Process***	**Manage Requirements Definition**
20	***Scope***	Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with enterprise requirements covering business processes, applications, information/data, infrastructure and services. Co-ordinates with affected stakeholders the review feasible options including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.

P.No	Area	Details
20	***Objectives***	Create feasible optimal solutions that meet enterprise needs while minimising risks.
21	***Process***	**Manage Solutions Identification and Build**
21	***Scope***	Establish and maintain identified solutions in line with enterprise requirements covering design, development, procurement/ sourcing, configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.
21	***Objectives***	Establish timely and cost effective solutions capable of supporting enterprise strategic and operational objectives.
22	***Process***	**Manage Availability and Capacity**
22	***Scope***	Balance current and future needs for availability, performance and capacity with cost effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.
22	***Objectives***	Maintain service availability, efficient management of resources and optimisation of system performance through prediction of future performance and capacity requirements
23	***Process***	**Manage Organisational Change Enablement**
23	***Scope***	Maximise the likelihood of successfully implementing sustainable enterprise wide organisational change quickly and with reduced risk covering the complete life cycle of the change and all affected stakeholders in the business and IT
23	***Objectives***	Prepare and commit stakeholders for business change and reduce the risk of failure.
24	***Process***	**Manage Changes**
24	***Scope***	Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation
24	***Objectives***	Enable fast and reliable delivery of change to the business and mitigation of the risks of negatively impacting the stability or integrity of the changed environment.

P.No	Area	Details
25	***Process***	**Manage Change Acceptance and Transitioning**
25	***Scope***	Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post implementation review.
25	***Objectives***	Implement solutions safely and in line with the agreed upon expectations and outcomes
26	***Process***	**Manage Knowledge**
26	***Scope***	Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making, and plan for the identification, gathering, organising, maintaining, use and retirement of knowledge
26	***Objectives***	Provide the knowledge required to support all staff in their work activities and for informed decision making and enhanced productivity
27	***Process***	**Manage Assets**
27	***Scope***	Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for Objectives), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licences to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements.
27	***Objectives***	Account for all IT assets and optimise the value provided by these assets.
28	***Process***	**Manage Configuration**
28	***Scope***	Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.
28	***Objectives***	Provide sufficient information about service assets to enable the service to be effectively managed, assess the impact of changes and deal with service incidents.

P.No	Area	Details
29	***Process***	Manage Operations
29	***Scope***	Co-¬ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of pre defined standard operating procedures and the required monitoring activities
29	***Objectives***	Deliver IT operational service outcomes as planned.
30	***Process***	**Manage Service Requests and Incidents**
30	***Scope***	Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.
30	***Objectives***	Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.
31	***Process***	**Manage Problems**
31	***Scope***	Identify and classify problems and their root causes and ensure timely resolution to prevent recurring incidents providing recommendations for improvements
31	***Objectives***	Increase availability, improve service levels, reduce costs, and improve customer convenience and satisfaction, by reducing the number of operational problems.
32	***Process***	Manage Continuity
32	***Scope***	Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise
32	***Objectives***	Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption
33	***Process***	Manage Security Services
33	***Scope***	Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring.
33	***Objectives***	Minimise the business impact of operational information security vulnerabilities and incidents

P.No	Area	Details
34	***Process***	Manage Business Process Controls
34	***Scope***	Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements
34	***Objectives***	Maintain information integrity and the security of information assets handled within business processes in the enterprise or outsourced
35	***Process***	Monitor and Evaluate Performance and Conformance
35	***Scope***	Collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed performance and conformance goals and metrics and provide reporting that is systematic and timely.
35	***Objectives***	Provide transparency of performance and conformance and drive achievement of goals.
36	***Process***	Monitor, Evaluate and Assess the System of Internal Control
36	***Scope***	Continuously monitor and evaluate the control environment, including self assessments and independent assurance reviews. Enable management to identify management deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities
36	***Objectives***	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risks.
37	***Process***	Monitor, Evaluate and Assess Compliance with External Requirements
37	***Scope***	Evaluate that IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with and integrate IT compliance with overall enterprise compliance.
37	***Objectives***	Ensure that the enterprise is compliant with all applicable external requirements.