This Study Material has been prepared by the faculty of the Board of Studies. The objective of the Study Material is to provide teaching material to the students to enable them to obtain knowledge and skills in the subject. Students should also supplement their study by reference to the recommended text books. In case students need any clarifications or have any suggestions to make for further improvement of the material contained herein, they may write to the Director of Studies.

All care has been taken to provide interpretations and discussions in a manner useful for the students. However, the Study Material has not been specifically discussed by the Council of the Institute or any of its Committees and the views expressed herein may not be taken to necessarily represent the views of the Council or any of its Committees.

Permission of the Institute is essential for reproduction of any portion of this material.

© THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

All rights reserved. No part of this book may be reproduced, stored in retrieval system, or transmitted, in any form, or by any means, Electronic, Mechanical, photocopying, recording, or otherwise, without prior permission in writing from the publisher.

Revised Edition : January, 2016

Website : www.icai.org

Department/ Committee : Board of Studies

E-mail : bosnoida@icai.in

ISBN No. : 978-81-8441-077-8

Price : ₹ 200/-

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, India.

Typeset and designed at Board of Studies.

Printed by : Repro India Ltd.

December/2015/P1869 (Revised)
Level of Knowledge: Advanced Knowledge

Objective:
“To develop competencies and skill-sets in evaluation of controls and relevant evidence gathering in an IT environment using IT tools and techniques for effective and efficient performance of accounting, assurance and compliance services provided by a Chartered Accountant”.

Contents:

   Role of information technology and IS Strategy in business strategy, operations and control, business value from use of IT, business impact of IS risks different types of Information Systems Risks, IS Risk management overview, IT Compliance overview – Role and responsibilities of top management as regards IT-GRC. Role of Information Systems Assurance. Overview of Governance of Enterprise IT and COBIT.


5. Acquisition, Development and Implementation of Information Systems (SDLC): Business process design (integrated systems, automated, and manual interfaces), Software procurement, RFP process, evaluation of IT proposals, computing ROI,
Computing Cost of IT implementation and cost benefit analysis, systematic approach to SDLC and review of SDLC controls at different stages.

6. **Auditing of Information Systems**: Different types of IS audit and assurance engagements. Evaluating IT dependencies for audit planning. Overview of continuous auditing. Auditing Information Systems- Approach methodology, and standards for auditing information systems. IS Audit planning, performing an IS audit, rules of digital evidence, best practices and standards for IS audit. Reviewing General Controls, Application Controls, Application control reviews: Review of controls at various levels/layers such as: Parameters, user creation, granting of access rights, input, processing and output controls.

7. **Information Technology Regulatory Issues**: Overview of Specific section of IT Act 2008 & Rules as relevant for assurance: Electronic Contracting, digital signatures, cyber offences, etc. Need for systems audit as per various regulations such as: SEBI Clause 49 listing requirements and internal controls, systems control & audit requirements as per RBI, SEBI, IRDA. Concepts of Cyber forensics/Cyber Fraud investigation, Overview of Information Security Standards ISO 27001, ISAE 3402/SA 402, ITIL.

A Word about Study Material

In today’s business world, accounting professionals have to interact with computer-based Information systems on a regular basis. As primary users of information systems in organizations, accountants participate in their design and understand their operations. Accounting managers must measure and evaluate the performance of Information Systems. Internal and external auditors must assess the quality of Information Systems and evaluate the accuracy of information input and output. The major share of the work of accounting consultants is in the design, implementation, evaluation and control of information systems.

In this fast changing world of Information and Communication Technologies, the Institute recognized the importance of Information Technology (IT), and thus included it as a part of the course curriculum both at Intermediate (IPC) and Final levels of the Chartered Accountancy course. A paper on Information Systems Control and Audit forming a part of the final course helps the students to develop competencies and skill-sets in evaluation of controls and relevant evidence gathering in an IT environment using IT tools and techniques for effective and efficient performance of accounting, assurance and compliance services provided by a Chartered Accountant. The basic knowledge about IT gained at Intermediate (IPC) level is sought to be built up further through this paper.

The Study Material of this paper covering the theoretical framework in detail has been revised. However, it is also noteworthy to mention here that in addition to the Study Material, students may also refer the recommended reading books available on this paper to enrich their knowledge levels. In addition, they are also advised to update themselves with the latest changes in the IT sector. For this, they may refer the monthly journal ‘The Chartered Accountant’ and the Students’ Journal published by the Institute and also other IT Journals/Magazines. Chapter-wise coverage of this Study material is given as follows:

Chapter 1 of the study material is devoted to the discussion on concept of Governance and management of Information Systems. In addition, the role of IT in businesses, operations and controls, business impact of IS risks, role and responsibilities of top management as regards IT-GRC etc. have also been covered.

Chapter 2 deals with the basic concepts of Information System and its various types like MIS, DSS, TPS, EIS etc.

Chapter 3 discusses the protection of Information Systems. It highlights the importance of Information Security in today’s vulnerable IT world, its policies, related standards/guidelines and also provides a detailed discussion on IS Controls, their objectives and functions with reference to Information Systems. Understanding of these controls is essential to the Chartered Accountants to strengthen their ability for conducting IS Audit in any organization.
Chapter 4 outlines Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) along with its related concepts.

Chapter 5 deals with systems development process for an information system. Various stages of systems development life cycle are also discussed. In this chapter, students will also get an idea ‘how computerized business applications are conceived and designed’. Various tools and techniques of systems analysis and design and programming are also briefly covered in this Chapter.

Chapter 6 is devoted to the auditing of Information Systems. It highlights the IS Audit planning, performing an IS audit, rules of digital evidence, best practices and standards for IS audit etc. In addition, the chapter also emphasizes on the reviewing of General and Application Controls.

Chapter 7 extensively deals with IT Regulatory issues. Along with a wide coverage of the relevant sections of IT Act 2000, other related regulatory issues e.g. need for system audit as per Clause 49 of SEBI listing requirements and audit requirements as per RBI, IRDA have also been discussed in the chapter.

Chapter 8 is devoted to the emerging technologies. Major evolving technologies/concepts like Cloud Computing, Mobile Computing, BYOD, Web 2.0 & Social Media and Green IT etc. have been covered in this chapter to make the students familiar with such technological developments.

Students are advised to refer to corresponding Practice Manual to further Case study based questions

The significant additions in the revised edition are highlighted in bold and Italics and have also been consolidated in the form of table “Significant additions in the Edition” in subsequent page.

In case you need any further clarification/guidance, please send your queries at bosnoida@icai.in/ sukriti.arora@icai.in.

Happy Reading and Best Wishes!
<table>
<thead>
<tr>
<th>Chapter No.</th>
<th>Chapter Name</th>
<th>Sections/Sub Sections wherein major additions/ updations have been done</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>3.7.3 Programming Management Controls</td>
<td>3.42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.7.4 Data Resource Management Controls</td>
<td>3.43</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.7.5 Quality Assurance Management Controls</td>
<td>3.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.7.6 Security Management Controls</td>
<td>3.44 – 3.46</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.7.7 Operations Management Controls</td>
<td>3.46 – 3.47</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.9 Information Technology General Controls (ITGC)</td>
<td>3.61 – 3.62</td>
</tr>
<tr>
<td>4.</td>
<td>Business Continuity Planning and Disaster Recovery Planning</td>
<td>4.8.2 Classification of Critical Activities</td>
<td>4.15 – 4.16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.14 Types of Back-ups</td>
<td>4.23 – 4.26</td>
</tr>
<tr>
<td>6.</td>
<td>Auditing of Information Systems</td>
<td>6.7 Managerial Controls and their Audit Trails</td>
<td>6.26 – 6.27</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.7.1 Top Management and Information Systems Management Controls</td>
<td>6.27 – 6.28</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.7.2 System Development Management Controls</td>
<td>6.28</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.7.3 Programming Management Controls</td>
<td>6.28 – 6.30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.7.4 Data Resource Management Controls</td>
<td>6.30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.7.5 Quality Assurance Management Controls</td>
<td>6.30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.7.6 Security Management Controls</td>
<td>6.30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.7.7 Operations Management Controls</td>
<td>6.30</td>
</tr>
<tr>
<td>8.</td>
<td>Emerging Technologies</td>
<td>8.2 Grid Computing</td>
<td>8.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.3.4 Cloud Computing Environment</td>
<td>8.6 – 8.12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.3.5 Cloud Computing Service Models</td>
<td>8.12 – 8.19</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.4.1 Limitations of Mobile Computing</td>
<td>8.26 – 8.27</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.4.2 How Mobile Computing Works?</td>
<td>8.27</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page Range</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>8.4.5</td>
<td>Limitations of Mobile Computing</td>
<td>8.28</td>
<td></td>
</tr>
<tr>
<td>8.4.6</td>
<td>Issues in Mobile Computing</td>
<td>8.28 – 8.30</td>
<td></td>
</tr>
<tr>
<td>8.5.2</td>
<td>Green Computing Best Practices</td>
<td>8.31 – 8.32</td>
<td></td>
</tr>
<tr>
<td>8.6.1</td>
<td>Advantages of BYOD</td>
<td>8.33 – 8.34</td>
<td></td>
</tr>
<tr>
<td>8.7.2</td>
<td>Web 2.0</td>
<td>8.36</td>
<td></td>
</tr>
<tr>
<td>8.7.3</td>
<td>Components of Web 2.0 for Social Networks</td>
<td>8.36 – 8.37</td>
<td></td>
</tr>
<tr>
<td>8.7.6</td>
<td>Applications of Web 2.0</td>
<td>8.40 – 8.41</td>
<td></td>
</tr>
<tr>
<td>8.7.8</td>
<td>Web 3.0</td>
<td>8.41 – 8.42</td>
<td></td>
</tr>
</tbody>
</table>
STUDY PLAN – KEY TO EFFECTIVE LEARNING

Introduction
The primary objective for the inclusion of the ‘Information Systems Control and Audit’ paper at the Final Level of the Chartered Accountancy course is to provide conceptual understanding of different aspects of IT risks, security, controls and auditing various aspects of IT processes. This paper enables to understand the enterprise level aspects of governance, risk, compliance, assurance as applicable to enterprises. While updating this paper, the primary rationale has been to ensure the coverage of the latest concepts of Governance, Risk and Compliance (GRC), which has been a regulatory requirement not only for listed enterprises but also for all types of enterprises. Further, implementing GRC in an IT environment requires updated knowledge and skills based on the latest developments and best practices and this is sought to be provided through this paper. Students are advised to read these topics not only from examination point of view but keeping in mind the fact that these topics are highly relevant to their work as articles and in their careers whether they seek to be employed in enterprises or self-employed.

The topics have been given so as to link all the topics together from the macro perspective of Governance, risk, compliance and assurance to the micro perspective and implementation level so that a blend of both concepts as well as the practical aspects could be provided. This knowledge will equip CA students with holistic approach to IT assurance rather than function oriented IS control and audit perspective. This will provide the required competency to meet the challenges of IT environment, which they face in their work area.

Before going to the chapter-wise specific tips, it is important to understand the detailed learning objectives that are given below:

- To understand the key concepts of Governance, Risk and Compliance aspects in enterprises as relevant to IT;
- To identify and review IT risks, security, controls and risk management approach;
- To assess impact on controls and organisation structure on account of integration of technological applications and resources into operational processes;
- To assess Business Continuity Plans of enterprises for adequacy from perspective of going concern;
- To assess information systems acquisition, development and implementation strategy including review of Systems Development Life Cycle (SDLC) process;
- To understand how to perform auditing including collecting and evaluating evidence in an IT environment;
- To understand the relevant regulatory procedures, guidelines and standards; and
To have an overview of IT best practices and impact of emerging technologies on enterprises.

Chapter-wise Tips for Preparation

While studying ISCA paper, students should try to understand the linkages between the chapters at macro-level. This will help them in recollecting the concepts during examination. Chapter-wise suggestions are given as follows:

1. First of all, students should understand the key points covered in the first chapter. The usage of IT is rapidly increasing in most of the large enterprises and also to a great extent even in small and medium enterprises. There is no doubt to say that IT is at the core of most of the key business operations. Further, there is an increasing thrust on corporate governance by regulators encompassing governance, risk management and controls. The use of IT covering all key aspects of business processes of an enterprise impacts not only 'how information is processed' but also 'how computerized information systems are used for strategic and competitive advantage'. Internal controls are integral part of information systems of an enterprise. Hence, it is important to understand 'how information systems are organized' and 'how controls are integrated'. In this chapter, students should understand the relevance of IT in Governance and other related concepts. Further, they should cover the topic IT Governance and Governance on Enterprise IT (GEIT).

Afterwards, students should also understand that successful design and deployment of information systems using IT, determines the success of an enterprise. Hence, it is critical to ensure that the required controls are implemented not only from IT perspective but also from management and regulatory perspective. This requires that the controls are implemented from Governance perspective using a holistic approach and has involvement of the senior management as required. Implementing IT Governance as subset of enterprise governance ensures that implementation of IT meets all the stakeholder requirements including regulators and management. Regulatory requirements mandate not only implementation of governance but also its independent evaluation. Hence, auditors are required to evaluate these aspects in their roles as internal or external auditors. As IT proliferates, there is increasing demands for pro-active objective assessments of governance, risk, compliance and controls of information systems. Accordingly, students should understand the Enterprise Risk Management, internal controls and related concepts. They should also cover various concepts relating to risk namely, vulnerabilities, attacks, threats etc. Once conceptual clarity has been acquired, students should have an idea about Risk assessment/management process. Finally, students should thoroughly study COBIT 5, which is a well-known GEIT Framework used by the enterprises worldwide.

2. As the name of the paper is 'Information Systems Control and Audit'; it is essential that students should understand about the information systems and its related concepts. Accordingly, second chapter of ISCA is on “Information Systems Concepts”, which provides an overview of different information systems. In this chapter, students should clearly understand the general concepts of the systems, and their types. In addition, they should also understand the practical aspects of application of information systems in various processes of an enterprise. Further, they should realize that information is a key business asset and
accordingly, they should thoroughly study the topic ‘information’ and its various attributes. Afterwards, students should understand the relative importance of information systems from strategic and operational perspective along with different types of information systems such as MIS, DSS, EIS, and ES etc. For each type of information systems, its features, attributes, advantages, and limitations must be clearly understood. Students should thoroughly understand the key points given in the material; however, they may write the description of these points in their own language with full coverage of related concepts. Finally, they should also have an overview of underlying IT technologies.

3. Information security plays a vital role in today's highly connected world. Any information system must have three fundamental aspects: resist, tolerate and recover. Hence, the third chapter is dedicated to protection of Information Systems and its related concepts. Students should clearly understand the need for information security and its importance to enterprises, its detailed concepts, various information security policies and their hierarchy. In addition, they should also focus on different categories of information that may be considered sensitive and how the same needs to be protected.

A control is a system that prevents, detects, or corrects unlawful events. In an information system, necessary controls must be incorporated at the appropriate places starting from the development itself. Keeping in mind the aforementioned fact, the chapter provides a detailed discussion on the controls. Accordingly, students should understand the need for the controls and related topics. They should also understand responsibility for controls from the perspective of Management, IT, Personnel, Auditors, and cost effectiveness of control procedures. Then, they should try to understand various IS Control Techniques and particularly User Controls. Afterwards, they should clearly understand the controls over data integrity and security, which are very essential towards protection of information systems. In addition, they should also cover Logical & Physical Access Controls and Environmental Controls along with their related concepts. Understanding of these controls is essential to the Chartered Accountants to strengthen their ability for conducting IS Audit in any organization. Students should also have an in-depth knowledge of Cyber Frauds following by major cyber-attacks as reported by different monitoring agencies like CERT-IN in India. They should also have an overview of the techniques to commit cyber frauds and finally, the students should assess the impact of these cyber frauds on business enterprises.

4. Information systems should continue without fail at any circumstances. 'What strategies should be followed to achieve this goal' is discussed in the fourth chapter on Business Continuity Planning and Disaster Recovery Planning. First of all, students should realize the need for Business Continuity Management (BCM) in enterprises, and understand BCM Policy, Business Continuity Planning (BCP) and its objectives/goals in depth. Moreover, students should know that how Business Continuity Plan is actually developed, covering all the eight phases. Students should also focus on various backup techniques and disaster recovery plans. Further, various audit tools and techniques must be understood by the students and finally, audit of Disaster Recovery and Business Continuity Plan must be covered in detail, which focuses on various important checkpoints relating to auditing.
5. As the paper is basically dedicated to Information Systems Controls; only the generalized knowledge of information systems is not sufficient rather various concepts of the Software Development Life Cycle (SDLC) are also needed. Accordingly, the fifth chapter is on SDLC in which all the relevant concepts of SDLC for a Chartered Accountant perspective are introduced. In this chapter, students should grasp the key issues for the system development process. They should understand the Request For Proposal (RFP) process and its evaluation along with the concepts of Return on Investment (RoI) in terms of investments made in systems. Afterwards, concepts relating to all the development models namely Waterfall, Spiral etc. used for developing the software should be clearly understood. Normally, the weaknesses of the previous model are addressed by the next model, and these weaknesses become the strengths of the current model. In this way, students may remember the concepts of various models. Further, it also establishes a link between the need for businesses and the method adopted to develop the suitable information system for them.

Further, all the phases of SDLC namely Preliminary Investigation, Requirements Analysis, Designing, Coding, Testing, Implementation, and Maintenance should be studied with the coverage of all the major activities in each of the phases in detail. Here, it is also noteworthy to mention that students must have the knowledge of appropriate controls required for various stages of SDLC starting from Preliminary Investigation till Maintenance. Finally, a checklist relating to SDLC is also included at the end of this chapter, which should be clearly understood by the students.

6. Sixth Chapter is on auditing of information systems. In the chapter, first of all, students should understand Information System Audit and the method of performing the same. Further, they should also know that an organization may face losses; incase, it does not get it audited. Afterwards, students should assess the impact of computers on audit and audit procedures adapted. Then, they should understand the detail steps to perform an Information System Audit. The idea of pre-audit survey and planning of an audit, for effective execution of an audit should also be understood by them in-depth.

Afterwards, students should also gain the knowledge of various auditing standards that an auditor can use for performing a systems audit. In addition, they should understand the auditing and evaluation techniques of general, physical and environmental controls including specialized security arrangements like firewalls. Concept of continuous auditing along with its advantages and disadvantages must be understood by the students. Finally, students should go through application controls covering input, processing and output controls along with their audit in detail. In addition, they must have the knowledge of operational, tactical and strategic layers of Application Security Controls and related audit issues.

7. In the current IT driven environment, there was a tremendous need for introducing laws to facilitate e-commerce and give legal recognition to electronic records and digital signatures. Realizing this need, Govt. of India introduced Information Technology Act in the year 2000. However, due to various transformations in technology, it was felt necessary to carry out certain amendments to make the Act more relevant and accordingly, Govt. of India passed these amendments through a bill in 2008. Students should understand various definitions covered under this act, and clearly understand the important provisions of this Act.
Afterwards, students should also know the requirements regarding system audit/disclosure by other governing bodies like RBI, SEBI and IRDA etc. Recognizing the importance of Information Security, Government of India has also introduced National Cyber Security Policy 2013 in July, 2013, which should also be understood by the students. In addition, they should also go through other related standards like ISO 27001 and ITIL in detail with emphasis on the key points of each standard in depth. Here, it is noteworthy to mention that Students must keep themselves updated with the latest developments in the standards.

8. Emerging technologies are seen to be having enormous potential to meet the global challenges of enterprises and accordingly, the eighth and last chapter is dedicated to the emerging technologies. In this chapter, students should start from the cloud computing, which simply means the use of computing resources as a service over a network typically the internet. They should study the pertinent issues and goals of cloud computing. Further, they should understand the cloud computing architecture and environment covering public, private and hybrid clouds. In addition, students must have an overview of different cloud computing models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Network as a Service (NaaS) and Communication as a Service (CaaS). Afterwards, they should also learn numerous advantages that can be achieved by implementing cloud architecture in an enterprise. Like any other technology, in spite of its various advantages, cloud computing also has certain major challenges, which requires proper attention from research community. These challenges must be clearly understood by the students.

Afterwards, students should have an overview of Mobile Computing and BYOD (Bring Your Own Device). While going through BYOD, they must know the emerging threats arising due to the same. Then, they should read the Web 2.0 and Social Media along with other related concepts. Finally, students should study the topic of Green IT and its associated sub topics like Green IT Security Services and Challenges. The main objective of this chapter is to make the students familiar with the latest technological developments in the related areas.

Examination related tips

1. In the paper of ISCA, first question may be based on a case study. These case studies may be from the practical oriented topics such as GRC, SDLC, Protection of Information Systems, BCP/DRP, and IS Audit Guidelines/Standards etc. The case study may also be based on the concepts taken from 3-4 chapters of the study material. Hence, students should read the case study carefully and identify the relevant concept/s based on which, the questions are to be answered.

2. It is observed that sometimes students write the answers in brief while attempting long answer type questions and accordingly, they do not get good marks. Hence, before writing the answer, students should clearly understand the weightage assigned to that particular question.

3. Wherever possible, students should try to include relevant diagrams, tables, rough sketch etc.

4. At the Final level, sometimes, questions are also framed on generalized topics of IT, which may not be adequately discussed in the study material. To answer such questions, students should not feel any psychological pressure; rather they should write the answer based on their general understanding of the topic/s with reference to IT.
CONTENTS

CHAPTER 1 – CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

1.1 Introduction .......................................................................................................... 1.2
1.2 Key Concepts of Governance ................................................................................ 1.3
1.3 Information Technology and Governance .............................................................. 1.5
1.4 Corporate Governance and IT Governance ........................................................... 1.6
1.5 IT Governance and Governance of Enterprise IT (GEIT) ........................................ 1.7
1.6 Corporate Governance, Enterprise Risk Management and Internal Controls ........... 1.9
1.7 Role of IT in Enterprises ..................................................................................... 1.13
1.8 IT Strategy Planning ........................................................................................... 1.15
1.9 Risk Management ............................................................................................... 1.20
1.10 COBIT 5 Business Framework – Governance and Management of Enterprise IT… 1.27
1.11 IT Compliance Review ........................................................................................ 1.36
1.12 Information System Assurance ............................................................................ 1.38
1.13 Summary ............................................................................................................ 1.44

CHAPTER 2 – INFORMATION SYSTEMS CONCEPTS

2.1 Introduction .......................................................................................................... 2.2
2.2 Overview of Information Systems and Practical Aspects of their Applications in Enterprise Processes ............................................................ 2.3
2.3 Relative Importance of Information Systems from Strategic and Operational Perspectives ...................................................................................................... 2.34
2.4 Information as a Key Business Asset and its Relation to Business Objectives and Processes .................................................................................................. 2.36
2.5 Various types of Business Applications .................................................................. 2.38
2.6 Overview of Underlying IT Technologies .............................................................. 2.40
2.7 Summary ............................................................................................................ 2.42

CHAPTER 3 – PROTECTION OF INFORMATION SYSTEMS

3.1 Introduction .......................................................................................................... 3.1
3.2 Need for Protection of Information Systems ........................................................... 3.2
3.3 Information System Security .................................................................................. 3.3
# Information Security Policy

- 3.4 Information Security Policy .............................................................. 3.4
- 3.5 Information Systems Controls ............................................................. 3.8
- 3.6 Classification of Information Systems Control ...................................... 3.12
- 3.7 Managerial Controls and their Categories ............................................ 3.37
- 3.8 Application Controls and their Categories ........................................... 3.47
- 3.9 Information Technology General Controls .......................................... 3.61
- 3.10 Controls over Data Integrity and Security ........................................... 3.62
- 3.11 Financial Controls ............................................................................ 3.66
- 3.12 Personal Computer Controls ............................................................. 3.67
- 3.13 Cyber Frauds .................................................................................... 3.67
- 3.14 Summary .......................................................................................... 3.71

## CHAPTER 4 – BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

- 4.1 Introduction ...................................................................................... 4.1
- 4.2 Need of Business Continuity Management (BCM) .............................. 4.2
- 4.3 BCM Policy ..................................................................................... 4.4
- 4.4 Business Continuity Planning ............................................................ 4.5
- 4.5 Developing a Business Continuity Plan ............................................. 4.6
- 4.6 Components of BCM Process ............................................................ 4.10
- 4.7 Business Continuity Management Process ....................................... 4.11
- 4.8 BCM Information Collection Process ............................................. 4.13
- 4.9 BCM Strategy Process .................................................................... 4.17
- 4.10 BCM Development and Implementation Process ............................ 4.17
- 4.11 BCM Testing and Maintenance Process .......................................... 4.18
- 4.12 BCM Training Process ................................................................... 4.21
- 4.13 Types of Plans ................................................................................. 4.22
- 4.14 Types of Back-ups ......................................................................... 4.23
- 4.15 Alternate Processing Facility Arrangements ..................................... 4.26
- 4.16 Disaster Recovery Procedural Plan .................................................. 4.27
- 4.17 Audit of the BCP/DRP .................................................................... 4.28
- 4.18 Summary ........................................................................................ 4.31

© The Institute of Chartered Accountants of India