INTERNAL AUDIT AND IT AUDIT SERIES

The Complete Guide for CISA Examination Preparation

Richard E. Cascarino

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

The Complete Guide for CISA Examination Preparation

Internal Audit and IT Audit

Series Editor

Dan Swanson, Dan Swanson and Associates, Ltd.,
Winnipeg, Manitoba, Canada.

The Internal Audit and IT Audit series publishes leading-edge books on critical subjects facing audit executives as well as internal and IT audit practitioners. Key topics include Audit Leadership, Cybersecurity, Strategic Risk Management, Auditing Various IT Activities and Processes, Audit Management, and Operational Auditing.

The Complete Guide for CISA Examination Preparation
Richard E. Cascarino

Blockchain for Cybersecurity and Privacy: ***Architectures, Challenges, and Applications***
Yassine Maleh, Mohammad Shojafar, Mamoun Alazab, Imed Romdhani

The Cybersecurity Body of Knowledge: ***The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity***
Daniel Shoemaker, Anne Kohnke, Ken Sigler

Corporate Governance: ***A Pragmatic Guide for Auditors, Directors, Investors, and Accountants***
Vasant Raval

The Audit Value Factor
Daniel Samson

Managing IoT Systems for Institutions and Cities
Chuck Benson

Fraud Auditing Using CAATT: ***A Manual for Auditors and Forensic Accountants to Detect Organizational Fraud***
Shaun Aghili

How to Build a Cyber-Resilient Organization
Dan Shoemaker, Anne Kohnke, Ken Sigler

Auditor Essentials: ***100 Concepts, Tips, Tools, and Techniques for Success***
Hernan Murdock

Project Management Capability Assessment: ***Performing ISO 33000-Based Capability Assessments of Project Management***
Peter T. Davis, Barry D. Lewis

For more information about this series please visit: https://www.routledge.com/Internal-Audit-and-IT-Audit/book-series/CRCINTAUDITA

The Complete Guide for CISA Examination Preparation

Richard E. Cascarino

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

First edition published 2021
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

ISBN: 9781138308763 (hbk)
ISBN: 9780367551742 (pbk)
ISBN: 9780429030000 (ebk)

Typeset in Caslon Pro
by Deanta Global Publishing Services, Chennai, India

Contents

THE COMPLETE GUIDE FOR CISA EXAMINATION PREPARATION xi

CHAPTER 1 INTRODUCTION TO THE CISA EXAMINATION 1
The Examination Itself 1
Becoming Certified 1
Experience Requirements 2
Educational Waivers 2
Passing the Examination 3
CISA Job Practice Domains and Task and Knowledge Statements 4
ISACA's Code of Professional Ethics 5
The ISACA Standards 6
Continuous Professional Education (CPE) 7

CHAPTER 2 DOMAIN 1 – THE PROCESS OF AUDITING INFORMATION SYSTEMS 9
The First Task 9
The Second Task 10
The Third Task 11
The Fourth Task 11
The Final Stage 12
Knowledge Statements 12
Knowledge of ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics, and Other Applicable Standards 12
Understanding the Fundamental Business Processes 19
Control Principles Related to Controls in Information Systems 22

Reliability and Integrity of Information 22
Compliance with Policies, Plans, Procedures, Laws, and Regulations 22
Safeguarding of Assets 23
Effectiveness and Efficiency of Operations 23
Risk-Based Audit Planning and Audit Project Management Techniques 24
Inherent Risk 25
Control Risk 25
Audit Risk 25
Planning the Audit Project 25
Quality of the Internal Control Framework 27
Competence of Management 28
Complexity of Transactions 28
Liquidity of Assets 28
Ethical Climate and Employee Morale 28
Auditor Understanding of the Applicable Laws and Regulations That Affect the Scope, Evidence Collection and Preservation, and Frequency of Audits 29
Evidence Collection Techniques 30
Audit Techniques 32
Automated Audit Tools 33
Domain 1 – Examination Tips 35
Domain 1 – Practice Questions 37
Domain One – Review Questions and Hands-On Exercise 42
Domain 1 – Answers to Practice Questions 43
Exercise 1 Sample Answer 46

CHAPTER 3 DOMAIN 2 – GOVERNANCE AND MANAGEMENT OF IT 47
Governance in General 47
IT Architecture 51
IT Policies and Standards 52
Project Management 54
Role of the Project Management Office (PMO) 55
Resource Management 56
Project Planning 57
Function Point Analysis 58
Project Tracking and Oversight 59
Project Management Tools 59
GANTT or Bar Charts 60
Program Evaluation Review Techniques (Also Known as a Network Diagram) 60
Critical Path Method 61
Timebox Management 61
Management of Resource Usage 62
Auditor's Role in the Project Management Process 62
Audit Risk Assessment 63

Audit Planning 65
Domain 2 – Practice Questions 67
Domain 2 – Review Questions and Hands-on Exercise 72
Exercise 2 – Audit of Customer Receivables 72
You are required to: 73
Exercise 2 Sample Answer 73
Domain 2 – Answers to Practice Questions 74

CHAPTER 4 DOMAIN 3 – INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND IMPLEMENTATION 77
Systems Acquisition 77
Cloud-Based Systems Acquisition 79
Systems Development 80
The SDLC 81
The Iterative Model 85
Prototyping and Rapid Application Development (RAD) 85
Agile Methodologies 85
Lean Methodology 87
Systems Implementation 87
Systems Maintenance Review 88
Domain 3 – Practice Questions 90
Domain 3 – Review Questions and Hands-On Exercise 94
Exercise 3 95
Required 96
Exercise 3 Sample Answer 96
Domain 3 – Answers to Practice Questions 98

CHAPTER 5 DOMAIN 4 – INFORMATION SYSTEMS OPERATIONS, MAINTENANCE, AND SERVICE MANAGEMENT 101
Hardware 102
CPU 102
Peripherals 102
Memory 102
Computer Types 103
Networks 103
Storage 104
Communications 105
Input 105
Output 106
Control 107
Systems Software 107
Auditing Operating Systems 107
People 109
Job Scheduling 110
System Interfaces 110
Frameworks 110

ITIL 112
Change Management 113
Change Management in the Use of Cloud-Based Applications 115
Problem Management 116
Auditing Change Control 116
Service Management 116
Disaster Recovery Planning 117
Auditing Service Delivery 119
Domain 4 – Practice Questions 122
Domain 4 – Review Questions and Hands-On Exercise 125
Exercise 4 127
Exercise 4 Sample Answer 127
Domain 4 – Answers to Practice Questions 128

CHAPTER 6 DOMAIN 5 – PROTECTION OF INFORMATION ASSETS 131
Protection of Information Assets 132
Privacy Principles 133
Design, Implementation, Maintenance, Monitoring, and Reporting of Security Controls 134
- Physical and Environmental Controls and Supporting Practices for the Protection of Information Assets 134
- Physical Access Controls for the Identification, Authentication, and Restriction of Users 135
- Environmental Controls 138
- Logical Access Controls for the Identification, Authentication, and Restriction of Users 139
- Risk and Controls Associated with Virtualization of Systems 139
- Risks and Controls Associated with the Use of Mobile and Wireless Devices 142
- Voice Communications Security 143

Network and Internet Security Devices, Protocols, and Techniques 143
Configuration, Implementation, Operation, and Maintenance of Network Security Controls 144
Encryption-Related Techniques and Their Uses 144
Public Key Infrastructure (PKI) Components and Digital Signature Techniques 145
Peer-to-Peer Computing, Instant Messaging, and Web-Based Technologies 146
Data Classification Standards Related to the Protection of Information Assets 147
Storage, Retrieval, Transportation, and Disposal of Confidential Information Assets 148
Data Leakage 148
Risks in End-User Computing 149

Implementing a Security Awareness Program 149
Information System Attack Methods and Techniques 150
Prevention and Detection Tools and Control Techniques 151
Malware 151
Phishing 151
Pharming 151
Password Attacks 152
Denial of Service (DoS) Attacks 152
'Man in the Middle' (MITM) attacks 153
Drive-By Downloads 153
Rogue Software 153
Ransomware 154
Spyware and Adware 154
Social Engineering 155
Security Testing Techniques 155
Penetration Testing and Vulnerability Scanning 155
Monitoring and Responding to Security Incidents 156
Forensic Investigation and Procedures in Collection and Preservation of the Data and Evidence 156
Domain 5 – Practice Questions 157
Domain 5 – Review Questions and Hands-On Exercise 165
Exercise 5 166
Exercise 5 Sample Answer 166
Domain 5 – Answers to Practice Questions 167

CHAPTER 7 PREPARING FOR THE EXAMINATION 173

APPENDIX A: GLOSSARY OF TERMS 177
APPENDIX B: CISA SAMPLE EXAMINATION – CHOOSE ANY 150 QUESTIONS 211
APPENDIX C: SAMPLE EXAMINATION ANSWERS 243
INDEX 245

The Complete Guide for CISA Examination Preparation

Introduction

For any organization to survive and compete successfully in today's environment, successful implementation of appropriate Computer Systems is essential. Such implementation involves not only the development of appropriate systems, but also their usage, maintenance, and reliability. Protection of information assets, systems availability, data integrity, confidentiality, and robustness have become non-negotiables in the competitive world we face today.

In response to this, ISACA has updated its Certified Information Systems Auditor (CISA) certification as of June 2019 to reflect the changing priorities and industry trend in order to ensure the alignment of the Information Systems Auditor's knowledge base with the needs of tomorrow's digital age.

In order for organizations to utilize the leverage achievable with the effective use of IT, it is important that the systems can be relied upon and they require that the auditors confirm that this is indeed the case. The modern auditors therefore require significantly more knowledge of IT, IT risk, and IT control than did their predecessors.

Today's IT systems process data in high volumes and at high speed with limited or no manual interventions and control opportunities. As a result, the control opportunities previously monitored by management have migrated within the IT environment itself. Fundamental business controls previously relied upon by the auditor, such as segregation of duties and management authorization are no longer carried out external to the IT environment and must be audited in a different manner.

The concentration of risk resulting from the shift and control implementation means that the balance between preventative, detective, and corrective controls has also had to move into alignment while technology such as cloud-based systems has moved the basis of legal constraints and burdens of proof in the event of dispute into a whole new arena.

While this may sound negative, these changes can greatly increase opportunities for auditors to deliver quality service because a concentration of risk facilitates the auditors focusing their efforts and utilizing the computer itself to assist in the audit of the IT environment and application systems usage. In addition, built-in program procedures allow the auditor to adopt a systems approach to auditing because the computer encourages consistent execution of controls as opposed to the older manual controls where execution was, to a large extent, at the mercy of the individual supervisor or manager.

The effect on the audit is that the focus can be on the control environment, its design and implementation and the substantive testing of the results of individual transactions can be significantly reduced.

Controls with IT systems may be generally classified into two main subdivisions, namely:

- **General controls** – that is, controls governing the environment within which the computer system is developed, maintained, and operated and within which the application controls operate. These controls include the implementation of appropriate systems development standards, controls over the operation of the computer installation and those governing the functioning and maintenance of System Software. As such, they have a pervasive effect on all application systems.

- **Application controls** – these are the controls which operate within the business application to ensure that data is processed completely, accurately, and in a timely manner.

Ultimately, the auditors' job is to determine if the application systems function as intended and evaluate management controls to ensure the integrity, accuracy, and completeness of all information processing.

Not only must management rely upon the work done by the auditors, whether internal or external, but they need assurance that the work is carried out to internationally accepted standards and the audit processes themselves can be relied upon. As such, management seeks independent proof that the work carried out by the auditors meets this standard.

The international standard by which IT auditors are judged is the possession of the qualification of Certified Information Systems Auditor (CISA). This designation is awarded by the Information Systems Audit and Control Association (ISACA) based upon demonstrable work experience as well as success in the CISA examination. ISACA, itself, can trace its roots to the EDP Auditors Association (EDPAA) which was founded in 1969. In 1994 it changed its name to the Information Systems Audit and Control Association and in 2008 rebranded itself as simply ISACA. Today, ISACA consists of more than 145,000 members of whom 140,000 have achieved the CISA qualification since its inception in 1978. This examination evaluates the auditors' knowledge, skills, and expertise in assessing the risks inherent within the specific IT environment and the adequacy and effectiveness of the controls implemented by management.

This book is intended as a study guide for the Certified Information Systems Auditor (CISA) examination and will consist of in-depth explanations of each topic covered within this examination as well as practice questions and tips to highlight key examination information. Each chapter will contain a summary which will serve as a quick review guide, combined with end-of-chapter questions and hands-on exercises. An examination simulation is included to get candidates familiar with the examination structures.

CISA is the most recognized certification in the world for information systems auditors and is recognized by all members of the

World Trade Organization including more than 150 governments worldwide.

The qualification is intended to affirm:

- The auditors' experience and knowledge
- The level of knowledge and competency which may be expected of the qualification holder
- The currency of the holder's knowledge due to the requirements for continuing education

From an employer's perspective it demonstrates that their IT auditor may be relied upon as a proficient and experienced professional with competencies in all five of the domains covered including:

- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition Development and Implementation
- Information Systems Operations, Maintenance, and Service Management
- Protection of Information Assets

while at the same time maintaining an up-to-date level of knowledge which can be relied upon as an indicator of the anticipated job performance level.

From an individual auditor's perspective, the CISA is internationally recognized as a gold standard of IT auditing professionalism. It enhances the acceptability of opinions expressed in the eyes of management and, in general, makes the auditor more marketable for future career opportunities. The auditor can also gain respect from their peers and other technical specialists. For non-specialist auditors who wish to enter the IT auditing specialization, either within the organization or as external consultants, CISA provides a recognized entrance into the booming market of IT auditing. For auditors who wish simply to understand the increasing complexities and risk elements of today's business environment, understanding the CISA dimensions will assist in the demystification of current and future control complexities.

The book is comprised of seven chapters.

- **Chapter 1** covers the CISA examination itself

- **Chapter 2** covers Domain 1 – The Process of Auditing Information Systems
- **Chapter 3** covers Domain 2 – Governance and Management of IT
- **Chapter 4** covers Domain 3 – Information Systems Acquisition, Development, and Implementation
- **Chapter 5** covers Domain 4 – Information Systems Operations, Maintenance, and Service Management
- **Chapter 6** covers Domain 5 – Protection of Information Assets
- **Chapter 7** covers preparing for the examination
- **Appendix A** contains a glossary of commonly used computer terms
- **Appendix B** contains 175 CISA-type questions from which the candidate can construct multiple simulated examinations
- **Appendix C** contains multiple choice answers to the Appendix B questions

1

Introduction to the CISA Examination

By the end of this chapter, readers will understand:

- The structure of the CISA examination
- The process of becoming certified
- Requirements for examination participation
- The CISA Domains
- The role of ISACA's Code of Professional Ethics
- The use and implementation ISACA Standards
- The need for maintaining continuing professional competency

The Examination Itself

The examination was revised in 2019 and consists of 150 multiple-choice questions to be answered over a four-hour period.

The examinations themselves are administered at CBT (Computer Based Testing) locations. The worldwide list of examination sites may be found at https://isacaavailability.psiexams.com/. Due to the variability of examination sites, all prospective candidates should check this list prior to registering and submitting payment for the examination since registration fees are non-refundable.

Becoming Certified

There is a four-stage process involved in becoming CISA certified.

1. **Check the Examination Schedule**

   Before candidates register and pay their fee, it is critical that they verify there is a test site available in a location the candidate can easily access. Candidates may search by location and date on the ISACA website to ensure that they can take their examination as planned.

2. **Register for the Examination**
   Once candidates have verified that there is a suitable testing site available where and when they need it, the candidate can register for their examination. Scheduling for the examination is Step 4.
3. **Pay for the Examination**
   Payment is required before a candidate can schedule their examination, however it is not required that payment is made at the time of registration. Candidates may pay on registering for CISA, or choose to register, study at their own pace, and pay at a later stage, prior to examination scheduling.
4. **Schedule the Examination**
   Once site availability has been assured, registration and payment made, candidates can schedule their examination. The actual scheduling is managed on the testing partner's website, not on ISACA.org.

Experience Requirements

It is not an essential to have sufficient experience to undertake the CISA examination but in order to be classified as a full CISA, candidates are required to have five (5) or more years of experience in professional information systems auditing, control, or security work experience. In addition, there is a time limit on application. Starting from the date of initially passing the examination (not the date of original registration for the examination), a completed CISA application must be submitted to ISACA. If this is not submitted within five years from the passing date of the examination, the individual will be required to re-take and re-pass the examination.

Individual experience claimed is required to have been gained within the ten-year period preceding the application date for certification or within five years of passing the examination and must be verified independently by employers.

Educational Waivers

Individuals registering as CISAs may request waivers for a maximum of three (3) years substitution for actual IT audit experience. Educational waivers may, at ISACA's discretion, be permitted to substitute for up to two years of experience. At the time of writing, these educational substitutions may be credited.

- One year of information systems OR one year of non-IS auditing experience can be substituted for one year of experience.
- 60 to 120 credit hours (two-year or four-year degree) from university – one or two years credit respectively.
- A master's degree in information security or information technology from an accredited university – one-year credit.
- A bachelor's or master's degree from a university that enforces the ISACA-sponsored Model Curricula – one-year credit, although only where the three years of educational waiver and experience substitution have not already been claimed.
- A candidate who has obtained other degrees, qualifications, and credentials with significant IS auditing, control, assurance, or security components may submit the case to the CISA Certification Committee for consideration.

Passing the Examination

It is not uncommon for highly skilled IS auditors to fail the CISA examination at the first attempt. Generally, this is not due to a lack of knowledge, but the wrong approach to the examination as a whole and the questions in particular, which cause these problems.

CISA candidates are expected to have a broad knowledge of the overall concepts and practice of information technology within an organization as well as:

- IS risks.
- The use of controls to mitigate risks.
- The use of the appropriate security features and controls within IS components.
- The roles of the auditor in conducting IS audits, including:
  - Developing an understanding of the risks inherent within the systems as implemented.
  - Understanding the security risks within the specific architecture utilized by the organization.
  - Identification and evaluation of the controls implemented to mitigate these risks.
  - Quantify weaknesses uncovered and make appropriate recommendations to mitigate these weaknesses and improve the overall control effectiveness.

CISA Job Practice Domains and Task and Knowledge Statements

Job Practice serves as the basis for the CISA exam and indicates the knowledge requirements which are expected to be at the fingertips of all professional IS auditors to earn the certification. The CISA examination covers five Domains which encompass knowledge of:

- Domain 1 – The Process of Auditing Information Systems.
  - This domain defines the procedures and methodology that an IS auditor should follow when conducting an information systems audit.
- Domain 2 – Governance and Management of IT.
  - This domain is focused on both the leadership and organizational processes which ensure that IT operates effectively with the auditor ensuring that the organization is following its own processes and procedures.
- Domain 3 – Information Systems Acquisition, Development, and Implementation.
  - The main focus is on the auditor's role in review and validation of the acquisition and testing methods of hardware acquisition to ensure that they are both adequate and follow industry best practice, and ensuring that systems promulgated by IT are both reliable and achieve the organizational objectives.
- Domain 4 – Information Systems Operations, Maintenance, and Service Management.
  - This domain encompasses the day-to-day operations of the application systems utilized within the organization as well as the maintenance of such systems. Operations include continuity planning as well as disaster recovery planning.
- Domain 5 – Protection of Information Assets.
  - This domain has gained increasing importance over recent years and involves the review and evaluation of the internal controls intended to ensure that information systems are adequately protected against a variety of threats. From

time to time the percentage of the examination allocated to each domain may be varied by ISACA but at the time of writing are:

- Domain 1 – 21%
- Domain 2 – 16%
- Domain 3 – 18%
- Domain 4 – 20%
- Domain 5 – 25%

Additional questions may appear as IS knowledge requirements develop.

For each of these Domains, ISACA provides the CISA candidate with a list of *Task Statements* indicating the tasks a professional IS auditor may be expected to undertake and *Knowledge Statements* indicating the knowledge a CISA is expected to have available in order to professionally undertake the Domain's task list. These are covered in more detail under each Domain while, at any time, the latest list of these may be downloaded from the ISACA website at http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Job-Practice-Areas/Pages/CISA-Job-Practice-Areas.aspx.

ISACA's Code of Professional Ethics

All CISA and ISACA members are required to comply with the ISACA Code of Professional Ethics. This code is intended to guide both the professional and the personal conduct of members of ISACA as well as holders of the CISA designation. The Code states that

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security, and risk management.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.

3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.
4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge, and competence.
6. Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including audit, control, security, and risk management.*

Failure to comply with this Code of Professional Ethics can result in disciplinary measures being instituted against the CISA or member should an investigation into a member's or CISA's conduct deem that an infringement has taken place.

The ISACA Standards

As with all Professional Associations, ISACA has promulgated its *Standards for IS Audit and Assurance* to contain statements of mandatory requirements for IS audit and assurance.

The Standards cover:

1001 Audit Charter
1002 Organizational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency

* https://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx

1007 Assertions
1008 Criteria
1201 Engagement Planning
1202 Risk Assessment in Planning
1203 Performance and Supervision
1204 Materiality
1205 Evidence
1206 Using the Work of Other Experts
1207 Irregularity and Illegal Acts
1401 Reporting
1402 Follow-Up Activities.

The latest Standards may be found at*:* http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/Standards-for-IT-Audit-and-Assurance.aspx.

Overall, the Standards are intended to indicate to IS audit and assurance professionals the minimum acceptable level of performance required to ensure the professional responsibilities set out in the ISACA are met. They indicate to management the profession's expectations concerning the work of IS audit practitioners and therefore the degree of professionalism management may expect. These Standards are mandatory for all holders of the CISA designation.

Continuous Professional Education (CPE)

In order to ensure that all CISAs maintain an adequate level of current knowledge and proficiency in their professional field of information systems audit, control, and security, ISACA requires that, over an annual and three-year certification period, CISAs must comply with the following CPE requirements in order to retain validity of their certification. CISAs must:

- Attain and report an annual minimum of twenty (20) CPE hours. These hours must be appropriate to the currency or advancement of the CISA's knowledge or ability to perform CISA-related tasks. The use of these hours towards meeting the CPE requirements for multiple ISACA certifications is permissible when the professional activity is applicable to satisfying the job-related knowledge of each certification.

- Submit annual CPE maintenance fees to ISACA international headquarters in full.
- Attain and report a minimum of one hundred and twenty (120) CPE hours for a three-year reporting period.
- Respond and submit required documentation of CPE activities if selected for the annual audit.
- Comply with ISACA's Code of Professional Ethics.
- Abide by ISACA's IT auditing standards.*

* https://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/Maintain-Your-CISA.aspx

2

Domain 1 – The Process of Auditing Information Systems

This chapter covers the processes involved in the auditing of Information Systems and the areas covered within the CISA examination. As has been noted, this domain currently approximates 21% of the examination, that is some 32 questions. Five task statements and 11 knowledge statements are included within this domain.

By the end of this chapter, readers will be able to:

- Demonstrate a knowledge of ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics, and other applicable standards.
- Understand the concepts requiring a knowledge of fundamental business processes (e.g. purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes.
- Comprehend the control principles related to controls in information systems.
- Explain the concepts of risk-based audit planning and audit project management techniques, including follow-up.
- Explain the role of auditor understanding of the applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits.
- Describe the evidence collection techniques (e.g. observation, inquiry, inspection, interview, data analysis, forensic investigation techniques, computer-assisted audit.

The First Task

The first task involves the execution of an appropriate IS audit risk-based strategy in order to ensure that areas of primary risk are fully audited.

Those risk areas would be the ones with the highest impact or exposure to the organization. Such areas are typically to be found around mission-critical activities of the organization. The IS auditor must always bear in mind that not everything needs to be audited nor, indeed, can be audited and therefore areas of higher interest must be prioritized. In achieving this, the IS auditor must be cognizant of the audit strategies and standards in effect. From a CISA perspective, perhaps the best source is the Professional Practices Framework for IS Audit and Assurance (ITAF) which is downloadable from http://www.isaca.org. Although examination questions are not directly drawn from ITAF, nevertheless it covers all of the standards and guidelines incorporated within the CISA examination.

The Second Task

> The second task incorporated within this domain is that of formulating the audit plans for specific audits to determine whether information systems are protected, controlled, and provide value to the organization.

The plan incorporates the scope of the audit, i.e. what is included and what is excluded from this particular audit with the selection of systems to be audited being derived from the audit risk evaluation. The typical audit plan will include identification of system risks, internal controls designed to mitigate against those risks including both general controls, and the systems environment as well as systems-specific controls were designed to address risks within a given business application area. Having identified the governing controls, the auditor would typically identify those key controls which govern the majority of the risk and design the appropriate tests in order to evaluate the effectiveness and efficiency of these controls in mitigating the risk. The first step in designing the audit program is to identify the source of evidence which the auditor will rely on in the control evaluation. Once the evidence has been located, the auditor can select the appropriate audit technique to obtain the evidence and, if necessary, select the appropriate audit tool. The selection of such tools and techniques should be in line with the Professional Standards which, as previously indicated, may be found on the ISACA website together with guidelines, tools, and techniques for the assistance of the auditor in implementing the plan.

The Third Task

> The third task involves the execution of the audit to ensure they are conducted in accordance with IS audit standards to achieve planned audit objectives.

If the audit program designed addresses the major significant risks and the audit tests have been designed appropriately to obtain the desired evidence, all the auditor needs to do is follow the audit program, obtain the evidence, and evaluate the results. The evaluation should result in a conclusion that control is being maintained at an adequate level to mitigate the corporate risk or that it is not at an adequate level and recommendations to improve control effectiveness will be required. Such recommendations could involve improving the effectiveness of existing controls or, where a gap exists in the control structure, implementation of a new control may be required.

The Fourth Task

> Once the audit fieldwork has been completed and the results evaluated, the fourth task involves the communication of the audit results and recommendations to key stakeholders and decision makers through meetings and the production of audit reports to promote change to control structures when necessary.

The value the organization derives from an audit depends on the effectiveness of the communication of the results of the audit.

Typically, this will involve a presentation to executive management of the major risks, control objectives, control effectiveness, possible weaknesses, and recommendations for improvements. This presentation will normally be accompanied by the written audit report which will contain an executive summary as well as detailed findings and recommendations for implementation by middle management, together with the degree of acceptance of the recommendations and the timescale for implementation. The report should include (at a minimum) the audit scope and objectives, a description of the audit subject, a narrative of the audit work activity performed, conclusions,