CISA – Certified Information Systems Auditor Study Guide

Aligned with the CISA Review Manual 2019 to help you audit, monitor, and assess information systems

Hemang Doshi

Packt
www.packt.com

CISA – Certified Information Systems Auditor Study Guide

Aligned with the CISA Review Manual 2019 to help you audit, monitor, and assess information systems

Hemang Doshi

BIRMINGHAM - MUMBAI

CISA – Certified Information Systems Auditor Study Guide

Acquisition Editor: Karan Gupta
Content Development Editor: Kinnari Chohan
Senior Editor: Rohit Singh
Technical Editor: Pradeep Sahu
Copy Editor: Safis Editing
Project Coordinator: Deeksha Thakkar
Proofreader: Safis Editing
Indexer: Manju Arasan
Production Designer: Aparna Bhagat

First published: August 2020

Production reference: 1210820

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-83898-958-3

www.packt.com

To my mother, Jyoti Doshi, and to the memory of my father, Hasmukh Doshi,
for their sacrifices and for exemplifying the power of determination.
To my wife, Namrata Doshi, for being my loving partner throughout our life journey together, and to my 6 year-old daughter, Jia Doshi, for allowing me to write this book.
To my sister, Pooja Shah, my brother-in-law, Hiren Shah, and my nephew, Phenil Shah,
for their love, support, and inspiration.
To my in-laws, Chandrakant Shah, Bharti Shah, and Ravish Shah,
for their love and motivation.
To my mentor and guide, Dipak Mazumder, for showing me how talent and creativity evolve.

– Hemang Doshi

Packt.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.packt.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at customercare@packtpub.com for more details.

At www.packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Contributors

About the author

Hemang Doshi is a chartered accountant and a Certified Information System Auditor with more than 15 years' experience in the field of IS auditing/risk-based auditing/compliance auditing/vendor risk management/due diligence/system risk and control. He is the founder of www.cisaexamstudy.com and www.criscexamstudy.com, dedicated platforms for CISA and CRISC study, respectively. He has also authored other books on auditing.

I wish to thank those people who have been close to me and supported me, especially my wife, Namrata, and my parents.

About the reviewer

Gokhan Polat works in the consulting department of EY Turkey and, in addition to implementing business development activities for technology services, he has also managed projects on cybersecurity assessments and data privacy consultancy. Previously, he created an internal audit department at Bakirkoy Municipality and headed up this department for 3 years. He also has 14 years' experience in the Turkish Armed Forces as an

officer involved in various assignments with multinational teams.

As a risk management professional, he has CISSP, CISA, CRISC, CDPSE, CIA, and CRMA qualifications, which bear testimony to his dedication to the profession. He has authored articles that have been published in the internal auditing magazine of IIA Turkey and the ISACA journal of ISACA Global. Currently, he is a member of the ISACA Istanbul Chapter and sits on the board of CSA Turkey.

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to

help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Table of Contents

2. Section 2: Governance and Management of IT

3. IT Governance

- IT enterprise governance (EGIT)
  - EGIT processes
  - Difference between governance and management
  - EGIT good practices
  - Effective information security governance
  - EGIT – success factors
  - Key aspects from the CISA exam perspective
  - Self-assessment questions
- IT-related frameworks
- IT standards, policies, and procedures
  - Standard
  - Policies
  - Procedures
  - Guidelines
  - Information security policy
    - Content of the information security policy
    - Information security policy users
    - Information security policy audit
    - Information security policy review
  - Key aspects from CISA exam perspective
  - Self-assessment questions
- Organizational structure
  - Relationship between the IT strategy committee and the
  - IT steering committee

- Laws, regulations, and industry standards affecting the organization

4. IT Management

- IT resource management
  - Human resource management
    - Hiring
    - Training
    - Scheduling and time reporting
    - During employment
    - Termination policies
  - IT management practices
  - Financial management practices
  - Key aspects from CISA exam perspective
  - Self-assessment questions
- IT service provider acquisition and management
  - Evaluation criteria for outsourcing
  - Steps for outsourcing
  - Outsourcing – risk reduction options
  - Provisions for outsourcing contracts
  - Role of IS auditors in monitoring outsourced activities
  - Globalization of IT functions
  - Outsourcing and third-party audit reports
  - Monitoring and review of third-party services
  - Key aspects from CISA exam perspective
  - Self-evaluation questions

Preface

Certified Information System Auditor (**CISA**) is one of the most sought-after courses in field of auditing, control, and information security. CISA is a globally recognized certification that validates your expertise and gives you the leverage you need in order to advance in your career. CISA certification is key to a successful career in IT.

CISA certification can showcase your expertise and assert your ability to apply a risk-based approach to planning, executing, and reporting on projects and engagements. It helps to gain instant credibility as regards your interactions with internal stakeholders, regulators, external auditors, and customers.

As per ISACA's official website (`www.isaca.org`), the average salary of a CISA holder is USD110,000 +.

Who this book is for

If you are a passionate auditor, risk practitioner, IT professional, or security professional, and are planning to enhance your career by obtaining a CISA certificate, this book is for you.

What this book covers

`Chapter 1`, *Audit Planning*, deals with the audit processes, standards, guidelines, practices, and techniques that an IS auditor is expected to use during audit assignments. An IS auditor must have a detailed knowledge of IS processes, business processes, and risk management processes in order to protect an organization's assets.

`Chapter 2`, *Audit Execution*, covers project management techniques, sampling methodology, and audit evidence collection techniques. It provides details regarding data analysis techniques, reporting and communication techniques, and quality assurance processes.

`Chapter 3`, *IT Governance*, provides an introduction to IT governance and aspects related to IT enterprise governance. Enterprise governance includes the active involvement of management in IT management. Effective IT governance and management involves an organization's structure as well as IT standards, policies, and procedures.

`Chapter 4`, *IT Management*, walks you through various aspects of designing and approving IT management policy and effective information security governance. It will also teach you to audit and evaluate IT resource management, along with services

provided by third-party service providers, while also covering IT performance monitoring and reporting.

Chapter 5, *Information Systems Acquisition and Development*, provides information about project governance and management techniques. This chapter discusses how an organization evaluates, develops, implements, maintains, and disposes of its information systems and related components.

Chapter 6, *Information Systems Implementation*, covers various aspects of information systems implementation. The implementation process comprises a variety of stages, including system migration, infrastructure deployment, data conversion or migration, user training, post-implementation review, and user acceptance testing.

Chapter 7, *Information Systems Operations*, explains how to identify risk related to technology components and how to audit and evaluate IT service management practices, systems performance management, problem and incident management policies and practices, change, configuration, release and patch management processes, and database management processes.

Chapter 8, *Business Resilience*, covers all aspects of the business impact analysis, system resiliency, data backup, storage and restoration, the business continuity plan, and disaster recovery plans.

Chapter 9, *Information Asset Security and Control*, provides information about the information security management framework, privacy principles, physical access and environmental controls, and identity and access management.

Chapter 10, *Network Security and Control*, provides an introduction to various components of networks, network-related risks and controls, types of firewalls, and wireless security.

Chapter 11, *Public Key Cryptography and Other Emerging Technologies*, details various aspects of public key cryptography, cloud computing, virtualization, mobile computing, and the Internet of Things.

Chapter 12, *Security Event Management*, looks in depth at how to evaluate an organization's information security and privacy policies and practices. It also discusses various types of information system attack methods and techniques, and covers different security monitoring tools and techniques as well as evidence collection and forensics methodology.

To get the most out of this book

This book is aligned with ISACA's CISA Review Manual and covers all the topics that a CISA aspirant needs to understand in order to pass the CISA exam successfully. The key aspect of

this book is its use of simple language, which makes this book ideal for candidates with non-technical backgrounds. At the end of each topic, key pointers from the CISA exam perspective are presented in table format. This is the unique feature of this book. It also contains 850 plus exam-oriented practice questions. The questions are designed in consideration of the language and testing methodology used in an actual CISA exam. This will help any CISA aspirant to face the CISA exam with increased confidence. For more practice questions along these lines, please refer to `www.cisaexamstudy.com`.

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here:

`https://static.packt-cdn.com/downloads/9781838989583_ColorImages.pdf`

Conventions used

There are a number of text conventions used throughout this book.

Bold: Indicates a new term, an important word, or words that you see on screen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "**Electromagnetic Interference (EMI)**: EMI generally

results from electric storms or noisy electrical equipment. EMI may result in system corruption or damage."

> *Warnings or important notes appear like this.*
>
> *Tips and tricks appear like this.*

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packtpub.com/support/errata`, selecting your book, clicking on the Errata Submission Form link, and entering the details.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions, we at Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit `packt.com`.

Section 1: Information System Auditing Process

This part contains 21 percent of the CISA exam, approximately 32 questions.

This part contains the following chapters:

- `Chapter 1`, *Audit Planning*
- `Chapter 2`, *Audit Execution*

Audit Planning

An audit plan is a step-wise approach to be followed to conduct an audit. It helps to establish the overall audit process in an effective and efficient manner. An audit plan should be aligned with the audit charter of the organization. To plan an audit, the IS auditor is required to have a thorough understanding of business processes, business applications, and relevant controls. Audit planning includes both short- and long-term planning.

The following topics will be covered in this chapter:

- The content of an audit charter
- Audit planning
- Business process applications and controls
- Types of controls
- Risk-based audit planning
- Types of audit and assessment

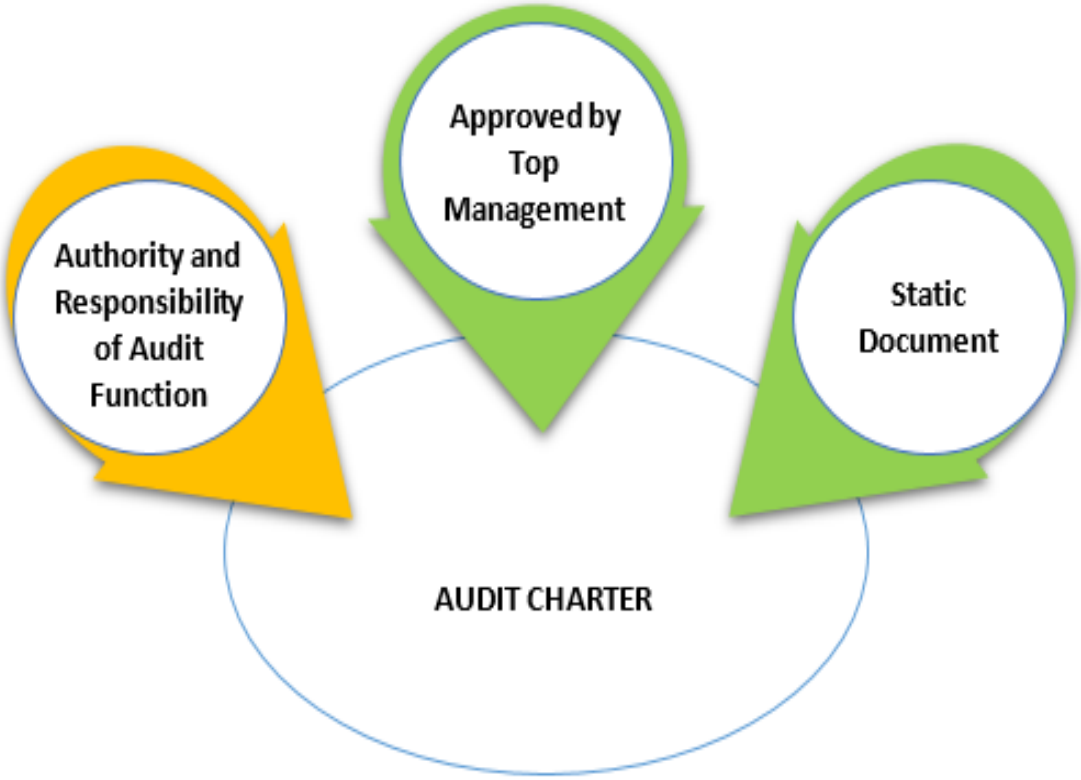
The content of an audit charter

An internal audit is an independent activity and it should ideally be reported to a board-level committee. In most

organizations, the internal audit function reports to the audit committee of the board. This helps to protect the independence of the audit function.

The independence of the audit function is ensured through a management-approved audit charter.

The following figure shows the features of an audit charter:



The CISA candidate should note the following features of the audit charter:

- An audit charter is a formal document defining the internal audit's objective, authority, and responsibility.

The audit charter covers the entire scope of audit activities.

- An audit charter must be approved by top management.
- An audit charter should not be changed too often and hence procedural aspects should not be included in it. Also, it is recommended to not include a detailed annual audit calendar including things such as planning, the allocation of resources, and other details such as audit fees, other expenses for the audit, and so on in an audit charter.
- An audit charter should be reviewed annually to ensure that it is aligned with business objectives.

Essentially, an auditor's activities are impacted by the charter of audit department, which authorizes the accountability and responsibility of the audit department.

An audit charter includes the following:

- The mission, purpose, and objective of the audit function
- The scope of the audit function
- The responsibilities of management
- The responsibilities of internal auditors
- The authorised personnel of the internal audit work

If an audit is outsourced to an audit firm, the objective of the audit, along with its detailed scope, should be incorporated in an audit engagement letter.

An audit charter forms the basis of structured audit planning. Activities relevant to audit planning are discussed in the next topic.

Key aspects from CISA exam perspective

The following table covers important aspects from the CISA exam perspective:

CISA questions	Possible answers
Who should approve the audit charter of an organization?	Senior management
What should the content of an audit charter be?	The scope, authority, and responsibilities of the audit function

What is the prime reason for review of an organization chart?	To understand the authority and responsibility of individuals
The actions of an IS auditor are primarily influenced by	Audit charter
Which document provides the overall authority for an auditor to perform an audit?	Audit charter
What is the primary reason for the audit function directly reporting to the audit committee?	The audit function must be independent of the business function and should have direct access to the audit committee of the board

Self-evaluation questions

1. **An audit charter should be approved by:**

    1. Higher management
    2. The head of audit
    3. The Information Security department
    4. The project steering committee

2. **The audit charter should**:

    1. Be frequently upgraded as per changes in technology and the audit profession
    2. Incorporate yearly audit planning
    3. Incorporate business continuity requirements
    4. Incorporate the scope, authority, and responsibility of the audit department

3. **The prime objective of an audit charter is to**:

    1. Document the procedural aspect of an audit
    2. Document system and staff requirements to conduct the audit
    3. Document the ethics and code of conduct for the audit department
    4. Document the responsibility and authority of the audit department

4. **The document that delegates authority to the audit department is:**

    1. The audit planner
    2. The audit charter
    3. The IT policy
    4. The risk assessment and treatment document

5. **The prime reason for the review of an organization chart is to:**

    1. Get details related to the flow of data
    2. Analyze the department-wise employee ratio
    3. Understand the authority and responsibility of individuals
    4. Analyze department-wise IT assets

6. **An IS auditor would be primarily influenced by**:

    1. The charter of the audit department
    2. The representation by management
    3. The structure of the organization
    4. The number of outsourcing arrangements

7. **Which of the following is the result of a risk management process?**

1. A corporate strategic plan
2. A charter incorporating the audit policy
3. Decisions regarding the security policy
4. Outsourcing arrangements

8. **Which of the following should be included in an audit charter?**

    1. Annual audit planning
    2. The audit function's reporting structure
    3. Guidelines for drafting audit reports
    4. An annual audit calendar

9. **The scope, authority, and responsibility of the IS audit function is defined by:**

    1. The approved audit charter
    2. The head of the IT department
    3. The operational head of the department
    4. The head of audit

10. **Which of the following functions is governed by the audit charter?**

    1. The information technology function
    2. The external audit function
    3. The internal audit function

4. The information security function

11. **Which of the following covers the overall authority to perform an IS audit?**

    1. The audit scope with goals and objectives
    2. Management's request to perform an audit
    3. The approved audit charter
    4. The approved audit schedule

12. **The audit function should be reported to the audit committee of the board because**:

    1. The audit function has few resources
    2. The audit function must be independent of the business function and should have direct access to the audit committee of the board
    3. No other function should use the resources of the audit function
    4. The audit function can use their own authority to complete the audit on a priority basis.

13. **The best objective for the creation of an audit charter is to:**

    1. Determine the audit resource requirements

2. Document the mission and long-term strategy of the audit department
3. Determine the code of conduct for the audit team
4. Provide the authority and responsibility of the audit function

Audit planning

CISA aspirants should understand the following important terms before reading about the different aspects of audit planning:

- **Audit universe**: An inventory of all the functions/processes/units under the organization.
- **Qualitative risk assessment**: In a qualitative risk assessment, risk is assessed using qualitative parameters such as high, medium, and low.
- **Quantitative risk assessment**: In a quantitative risk assessment, risk is assessed using numerical parameters and is quantified.
- **Risk factors**: Factors that have an impact on risk. The presence of those factors increases the risk, whereas the absence of those factors decreases the risk.

All of the preceding elements are important prerequisites for the design of a structured audit plan. Next, let's discuss the benefits of a structured and well-designed audit plan.

Benefits of audit planning

Audit planning is the initial stage of the audit process. It helps to establish the overall audit strategy and the technique to complete the audit. Audit planning aids in making the audit process more structured and objective oriented.

An audit plan helps to identify and determine the following aspects:

- The objectives of the audit
- The scope of the audit
- The periodicity of the audit
- The members of the audit team
- The method of audit

The following are some of the benefits of audit planning:

- It helps the auditor to focus on high-risk areas
- It helps in the identification of resource requirements to conduct the audit

- It helps to estimate the budget for the audit
- It helps to carry out audit work in a defined structure, which ultimately benefits the auditor as well as the auditee units

Selection criteria

An IS auditor should have a sufficient understanding about the various criteria for the selection of audit processes.

One of the criteria for audit planning is to have an audit universe. All of the significant processes of the enterprise's business should be included in the audit universe.

Each business process may undergo a qualitative or quantitative risk assessment by evaluating the risk in respect to relevant risk factors. Risk factors influence the frequency of the audit. After the risk is evaluated for each relevant factor, criteria may be defined to determine the risk of each process. The audit plan can then be designed to consider all the high-risk areas.

Reviewing audit planning

This audit plan should be reviewed and approved by top management. Generally, approval is obtained from the audit committee of the board.

The audit plan should be flexible enough to address the change in risk environment (that is, new regulatory requirements, changes in the market condition, and other risk factors).

The approved audit plan should be communicated promptly to the following groups:

- Senior management
- Business functions and other stakeholders
- The internal audit team

Individual audit assignments

The next step after doing the overall annual planning is to plan individual audit assignments. The IS auditor must understand the overall environment under review. While planning an individual audit assignment, an IS auditor should consider the following:

- Prior audit reports
- Risk assessment reports
- Regulatory requirements
- Standard operating processes
- Technological requirements

Like every other process, the audit process will also have some input and output. The following diagram will help you to understand input and output elements of the audit process:

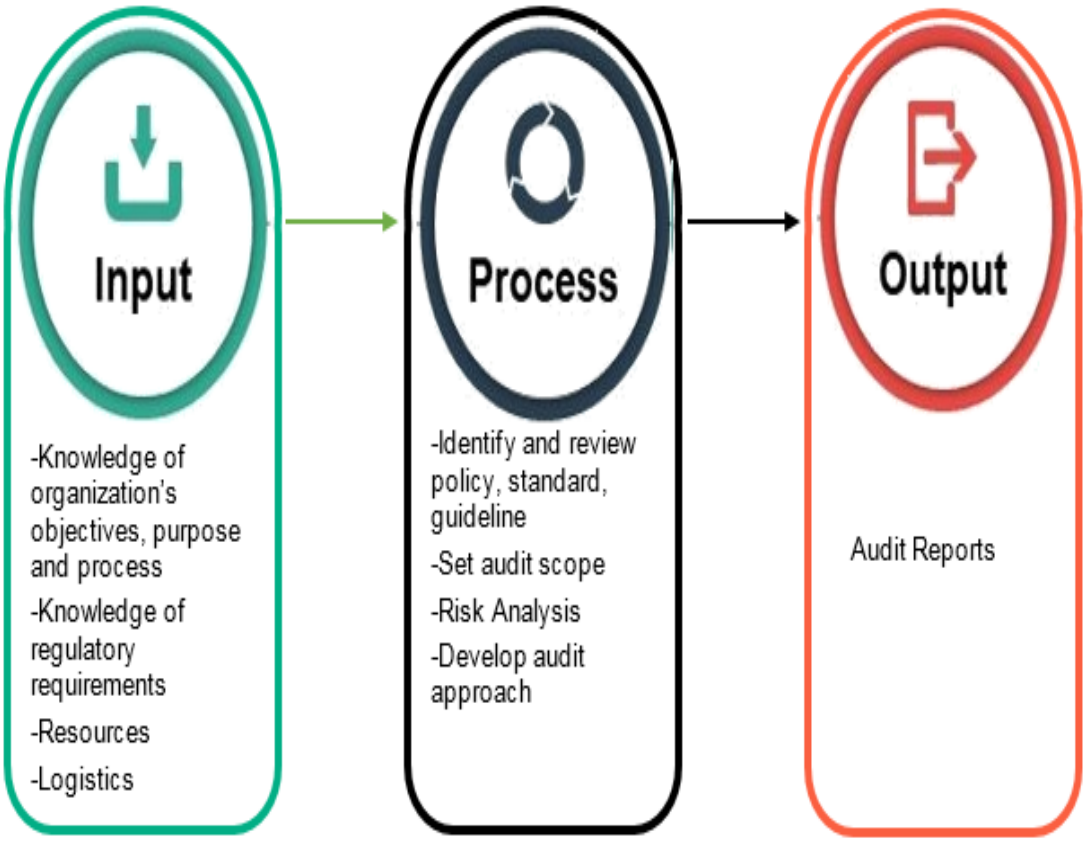


Figure 1.3 – Audit process flow

For effective audit planning, it is of utmost importance that the IS auditor has a thorough understanding of business process applications and controls. The basic architecture of some of the commonly used applications and their associated risks are discussed in the next topic.

Key aspects from CISA exam perspective

The following figure covers important aspects from the CISA exam perspective:

CISA questions	Possible answers
What is the first step in risk-based audit planning?	To identify areas of high risk
What is a major benefit of risk-based audit planning?	The utilization of resources for high-risk areas
What is the first step to conduct a data center review?	What is the first step to conduct a data center review?

Self-evaluation questions

1. **Which of the following is the first step in risk-based audit planning?**

1. To identify the requirements of relevant stakeholders
2. To identify high-risk processes in the company
3. To identify the budget
4. To identify the profit function

2. **Which of the following is a major advantage of a risk-based approach to audit planning?**

    1. Advance communication of the audit plan
    2. Completion of the audit exercise within the allotted time and budget
    3. The collection of audit fees in advance
    4. Optimum use of audit resources for high-risk processes

3. **Which of the following should be the first exercise while reviewing data center security?**

    1. The evaluation of the physical security arrangement
    2. The evaluation of vulnerabilities and threats to the data center location
    3. The evaluation of the business continuity arrangement for the data center
    4. The evaluation of the logical security arrangement

4. **Which of the following is the most important aspect of planning an audit?**

    1. Identifying high-risk processes
    2. Identifying the experience and capabilities of audit staff
    3. Identifying control testing procedures of the audit
    4. Determining the audit schedule

Business process applications and controls

Working knowledge of the business environment and business objectives is required to plan a risk-based audit. The IS auditor should have a sufficient understanding of the overall architecture and technological specifications of the various applications used by the organization and the risks associated with those applications.

In understanding the issues and current risks facing the business, the IS auditor should focus on the areas that are most meaningful to management. To effectively audit business application systems, an IS auditor is required to gain a thorough understanding of the system under the scope of the audit.

The following are some of the widely used applications in business processes. The CISA candidate should be aware of the risks associated with each of them.

E-commerce

Let's start with understanding how e-commerce works:

- Single-tier architecture runs on a single computer, that is, a client-based application
- Two-tier architecture includes a client and server
- Three-tier architecture consists of the following:
    - A presentation tier (for interaction with the user)
    - An application tier (for processing)
    - A data tier (for the database)

The risks are as follows:

- A compromise of confidential user data
- Data integrity issues due to unauthorized alterations
- The system being unavailable may impact business continuity

- The repudiation of transactions by either party

The IS auditor's roles are as follows:

- To review the overall security architecture related to firewalls, encryption, networks, PKI to ensure confidentiality, integrity, availability, and the non-repudiation of e-commerce transactions
- To review the process of log capturing and monitoring for e-commerce transactions
- To review the incident management process
- To review the effectiveness of the controls implemented for privacy laws
- To review anti-malware controls
- To review business continuity arrangements

Electronic Data Interchange (EDI)

Let's start with understanding how EDI works:

- EDI is the online transfer of data or information between two enterprises.
- EDI ensures an effective and efficient transfer platform without the use of paper.

- The traditional exchange of paper documents between organizations has been replaced with EDI platforms.
- EDI applications contain processing features such as transmission, translation, and the storage of transactions flowing between two enterprises.
- An EDI setup can be either traditional EDI (batch transmission within each trading partner's computers) or web-based EDI (accessed through an internet service provider).

The risks are as follows:

- One of the biggest risks applicable to EDI is transaction authorization.
- Due to electronic interactions, no inherent authentication occurs.
- There could be related uncertainty with a specific legal liability when we don't have a trading partner agreement.
- Any performance-related issues with EDI applications could have a negative impact on both parties.
- Other EDI-related risks include unauthorized access, data integrity and confidentiality, and the loss or duplication of EDI transactions.

The IS auditor's roles are as follows:

- To determine the data's confidentiality, integrity, and authenticity, as well as the non-repudiation of transactions
- To determine invalid transactions and data before they are uploaded to the system
- To determine the accuracy, validity, and reasonableness of data
- To validate and ensure the reconciliation of totals between the EDI system and the trading partner's system

The IS auditor should determine the use of some controls to validate the sender, as follows:

1. The use of control fields within an EDI message
2. The use of VAN sequential control numbers or reports
3. Acknowledgment transactions with the sender

The auditor should also determine the availability of the following controls:

Control requirements for inbound transactions:

- A log of each inbound transaction on receipt

- Segment count totals built into the transaction set trailer
- Checking digits to detect transposition and transcription errors

Control requirements for outbound transactions:

- Transactions to be compared with the trading partner's profile
- Proper segregation of duties for high-risk transactions
- A log to be maintained for outbound transactions

EDI audits also involve the use of audit monitors (to capture EDI transactions) and expert systems (to evaluate transactions).

Point of Sale (POS)

Let's start with understanding how POS works:

- Debit and credit card transactions are the most common examples of POS.
- Data is captured at the time and place of sale.

The risks of this are as follows: