Certified Information Security Manager Exam Prep Guide

Aligned with the latest edition of the CISM Review Manual to help you pass the exam with confidence

Hemang Doshi

Certified Information Security Manager Exam Prep Guide

Aligned with the latest edition of the CISM Review Manual to help you pass the exam with confidence

Hemang Doshi

Packt

BIRMINGHAM—MUMBAI

Certified Information Security Manager Exam Prep Guide

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Vijin Boricha
Publishing Product Manager: Preet Ahuja
Senior Editor: Shazeen Iqbal
Content Development Editor: Romy Dias
Technical Editor: Nithik Cheruvakodan
Copy Editor: Safis Editing
Project Coordinator: Shagun Saini
Proofreader: Safis Editing
Indexer: Manju Arasan
Production Designer: Joshua Misquitta

First published: November 2021

Production reference: 1241121

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

ISBN 978-1-80107-410-0

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.

To the extremely talented editorial team at Packt, including Preet Ahuja, Neil D'mello, Shazeen Iqbal, and Romy Dias, for their wonderful support throughout the journey of writing this book.

– Hemang Doshi

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 information system auditing/risk-based auditing/compliance auditing/vendor risk management/due diligence/system risk and control. He is the founder of CISA Exam Study and CRISC Exam Study, dedicated platforms for those studying for the CISA and CRISC certifications, respectively. He has also authored a few books on information security.

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

About the reviewers

When **George McPherson** was pulled through the ranks and pinned as a 21-year-old Sergeant in the U.S. Army over 20 years ago, he learned two things about himself. He could accomplish anything he put his mind to, and he would always pull others up if he was in a position to do so. George prides himself on integrity, an insane work ethic, attention to detail and (his greatest super-power) outside-the-box creativity. With 25 years in the technology industry, the first 18 in telecoms and the last 7 in cybersecurity, George has had the opportunity to work in industries such as the military, telecoms, local government, healthcare, and electric utilities.

George has over 20 professional certifications, including the CISM certification.

I would like to thank my beautiful wife, Audrey, whose constant support and sacrifice fuel my success.

Upen Patel is an IT professional with 20 years' experience, holding numerous professional IT certifications including CISM, CISA, CDPSE, CRISC, CCSP, CISSP, and Splunk Certified Architect. Upen attained a B.Sc. in geology from York College (CUNY), an M.Sc. in environment engineering from NYU Polytechnic Institute, and an M.Sc. in security and information assurance from Pace. Upen has held several positions, including cloud architect and security engineer, risk assessment expert, CyberArk consultant, and Splunk architecture consultant. He has worked on the implementation of many large public cloud projects on Azure and AWS and developed an automated DevRiskOps process in public. He has also implemented a large Splunk SIEM solution.

I would like to thank my family for their motivation and support.

Table of Contents

Preface

Section 1: Information Security Governance

1

Information Security Governance

Introducing information security governance 4

The responsibility of information security governance 4

Governance framework 5

Key aspects from the CISM exam perspective 6

Questions 7

Understanding governance, risk management, and compliance 14

Key aspects from the CISM exam perspective 14

Questions 15

Discovering the maturity model 15

Key aspects from the CISM exam perspective 16

Questions 16

Getting to know the information security roles and responsibilities 18

Board of directors 18

Senior management 19

Business process owners 19

Steering committee 19

Chief information security officer 20

Chief operating officer 20

Data custodian 20

Communication channel 20

Indicators of a security culture 21

Key aspects from the CISM exam perspective 21

Questions 22

Finding out about the governance of third-party relationships 36

The culture of an organization 37

Compliance with laws and regulations 37

Key aspects from the CISM exam perspective 38

Questions 38

Obtaining commitment from senior management 46

Information security investment 47
Strategic alignment 47
Key aspects from the CISM exam perspective 48
Questions 48

Introducing the business case and the feasibility study 56
Feasibility analysis 57
Key aspects from the CISM exam perspective 57
Questions 57

Understanding information security governance metrics 63
The objective of metrics 63
Technical metrics vis-à-vis governance-level metrics 63
Characteristics of effective metrics 63
Key aspects from the CISM exam perspective 64
Questions 64

Summary 67

2

Practical Aspects of Information Security Governance

Information security strategy and plan 70
Information security policies 70
Key aspects from the CISM exam perspective 71
Practice questions 72

Information security program 87
Key aspects from the CISM exam perspective 88
Practice questions 88

Enterprise information security architecture 91
Challenges in designing security architectures 91
Benefits of security architectures 92
Key aspects from the CISM exam perspective 92
Practice questions 92

Organizational structure 93
Board of directors 93
Security steering committee 93
Reporting of the security function 93
Centralized vis-à-vis decentralized security functioning 94
Key aspects from the CISM exam perspective 95
Practice questions 95

Record retention 97
Electronic discovery 97
Key aspects from the CISM exam perspective 97
Practice questions 98

Awareness and education 99
Increasing the effectiveness of security training 99
Key aspects from the CISM exam perspective 99

Summary 99

Section 2: Information Risk Management

3

Overview of Information Risk Management

Risk management overview **104**
Phases of risk management 104
The outcome of the risk management program 105
Key aspects from the CISM exam's perspective 105
Questions 105

Risk management strategy **107**
Risk capacity, appetite, and tolerance 107
Risk communication 108
Risk awareness 109
Tailored awareness program 109
Training effectiveness 109
Awareness training for senior management 109
Key aspects from the CISM exam's perspective 110
Questions 110

Implementing risk management **113**
Risk management process 113
Integrating risk management in business processes 114
Prioritization of risk response 114
Defining a risk management framework 114
Defining the external and internal environment 115
Determining the risk management context 115
Gap analysis 115
Cost-benefit analysis 116
Other kinds of organizational support 116
Key aspects from the CISM exam's perspective 117
Questions 119

Risk assessment and analysis methodologies **139**
Phases of risk assessment 139

Risk assessment **140**
Asset identification 140
Asset valuation 140
Aggregated and cascading risk 141
Identifying risk 141
Threats and vulnerabilities 143
Risk, likelihood, and impact 144
Risk register 145
Risk analysis 145
Annual loss expectancy 148
Value at Risk (VaR) 148
OCTAVE 148
Other risk analysis methods 149
Evaluating risk 150
Risk ranking 151
Risk ownership and accountability 151
Risk treatment options 151
Understanding inherent risk and residual risk 152
Security baseline 153
Key aspects from the CISM exam's perspective 154
Questions 155

Summary **177**

4

Practical Aspects of Information Risk Management

Information asset classification 180

Benefits of classification 180

Understanding the steps involved in classification 180

Success factors for effective classification 181

Criticality, sensitivity, and impact assessment 182

Business dependency assessment 182

Risk analysis 182

Business interruptions 182

Key aspects from the CISM exam's perspective 183

Questions 184

Asset valuation 194

Determining the criticality of assets 194

Key aspects from the CISM exam's perspective 194

Questions 195

Operational risk management 200

Recovery time objective (RTO) 200

Recovery Point Objective (RPO) 200

Difference between RTO and RPO 200

Service delivery objective (SDO) 202

Maximum tolerable outage (MTO) 203

Allowable interruption window (AIW) 203

Questions 203

Outsourcing and third-party service providers 203

Evaluation criteria for outsourcing 204

Steps for outsourcing 205

Outsourcing – risk reduction options 205

Provisions for outsourcing contracts 206

The role of the security manager in monitoring outsourced activities 206

Service-level agreement 206

Right to audit clause 207

Impact of privacy laws on outsourcing 207

Sub-contracting/fourth party 207

Compliance responsibility 208

Key aspects from the CISM exam's perspective 208

Questions 209

Risk management integration with the process life cycle 221

System development life cycle 221

Key aspects from the CISM exam's perspective 222

Questions 222

Summary 223

5

Procedural Aspects of Information Risk Management

Change management 226

The objective of change management 226

Approval from the system owner 226

Regression testing 226

Involvement of the security team 226

Preventive control 226

Key aspects from a CISM exam perspective 227

Questions 227

Patch management 232

Key aspects from a CISM exam perspective 233

Questions 233

Security baseline controls 236

Benefits of a security baseline 236

Developing a security baseline 236

Key aspects from a CISM exam perspective 236

Questions 237

Risk monitoring and communication 239

Risk reporting 239

Key risk indicators 240

Reporting significant changes in risk 240

Key aspects from a CISM exam perspective 241

Questions 241

Security awareness training and education 252

Key aspects from a CISM exam perspective 254

Questions 254

Documentation 263

Summary 264

Preface

ISACA's **Certified Information Security Manager** (**CISM**) certification indicates expertise in information security governance, program development and management, incident management, and risk management. Whether you are seeking a new career opportunity or striving to grow within your current organization, a CISM certification proves your expertise in these work-related domains:

- Information security governance
- Information risk management
- Information security program development and management
- Information security incident management

Who this book is for

This book is ideal for IT risk professionals, IT auditors, CISOs, information security managers, and risk management professionals.

What this book covers

Chapter 1, *Information Security Governance*, is an overview of information security governance.

Chapter 2, *Practical Aspects of Information Security Governance*, discusses information security strategies.

Chapter 3, *Overview of Information Risk Management*, covers basic elements of risk management.

Chapter 4, *Practical Aspects of Information Risk Management*, covers tools and techniques for risk management programs.

Chapter 5, *Procedural Aspects of Information Risk Management*, covers risk communication and security training awareness.

Chapter 6, *Overview of Information Security Program Development Management*, discusses basic elements of information security program development and management.

Chapter 7, *Information Security Infrastructure and Architecture*, discusses information security infrastructure and architecture.

Chapter 8, *Practical Aspects of Information Security Program Development Management*, discusses various controls and countermeasures.

Chapter 9, Information Security Monitoring Tools and Techniques, emphasizes the importance of monitoring tools and techniques.

Chapter 10, *Overview of Information Security Incident Manager*, discusses basic elements of information security incident management.

Chapter 11, *Practical Aspects of Information Security Incident Management*, covers business continuity and disaster recovery processes.

To get the most out of this book

This book is completely aligned with the CISM Review Manual of ISACA. It is advisable to follow these steps during your CISM studies:

1. Read this book.
2. Complete ISACA's QAE book or database.
3. Refer to ISACA's CISM Review Manual.

CISM aspirants will gain a lot of confidence if they approach their CISM preparation by following these steps.

Download the color images

We also provide a PDF file that has color images of the screenshots and diagrams used in this book. You can download it here: `https://static.packt-cdn.com/downloads/9781801074100_ColorImages.pdf`.

Get in touch

Feedback from our readers is always welcome.

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

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` and fill in the form.

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`.

Share your thoughts

Once you've read *Certified Information Security Manager Exam Guide*, we'd love to hear your thoughts! Please click here to go straight to the Amazon review page for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Section 1: Information Security Governance

This part is about the management and governance of information security. It covers 24% of the CISM certification exam.

This section contains the following chapters:

- *Chapter 1, Information Security Governance*
- *Chapter 2, Practical Aspects of Information Security Governance*

1
Information Security Governance

Governance is an important aspect of the **certified information security manager** (**CISM**) exam.

In this chapter, we will cover an overview of **information security governance** and aim to understand the impact of good governance on the effectiveness of information security projects.

You will learn about assurance functions such as **governance**, **risk**, and **compliance** (**GRC**), and details about the various roles and responsibilities of the security function. You will also be introduced to the best practices for obtaining the commitment from the senior management of an organization toward information security.

The following topics will be covered in this chapter:

- Introducing information security governance
- Understanding GRC
- Discovering the maturity model
- Getting to know the information security roles and responsibilities
- Finding out about the governance of third-party relationships

- Obtaining commitment from senior management
- Introducing the business case and the feasibility study
- Understanding information security governance metrics

Let's dive in and discuss each one of these topics in detail.

Introducing information security governance

In simple terms, **governance** can be defined as *a set of rules to direct, monitor, and control an organization's activities*. Governance can be implemented by way of policies, standards, and procedures.

The information security governance model is primarily impacted by the complexity of an organization's structure. An organization's structure includes objectives, its vision and mission, different function units, different product lines, hierarchy structure, leadership structure, and other relevant factors. A review of organizational structure will help the security manager to understand the roles and responsibilities of information security governance, as discussed in our next topic.

The responsibility of information security governance

The responsibility for information security governance primarily resides with the **board of directors** and **senior management**. Information security governance is a subset of the overall enterprise governance. The board of directors is required to make security an important part of governance by way of monitoring key aspects of security. Senior management holds the responsibility to ensure that security aspects are integrated with business processes.

The involvement of senior management and the steering committee in discussions and in the approval of security projects indicates that the management is committed to aspects relating to security. Generally, a steering committee consists of senior officials from different departments. The role of an information security steering committee is to provide oversight on the security environment of the organization.

It is very important for a CISM aspirant to understand the steps for establishing the governance, as we will discuss in the next section.

Steps for establishing the governance

For effective governance, it should be established in a structured manner. A CISM aspirant should understand the following steps for establishing governance:

1. First, determine the **objectives** of an information security program. Most often, these objectives are derived from risk management and the acceptable level of risk that you are willing to take. One example of an objective for a bank may be that the system should always be available for customers – that is, there should be *zero* downtime. Information security objectives must also align with and be guided by the organization's business objectives.
2. The next step is that the information security manager develops a **strategy** and **requirements** based on these objectives. The security manager is required to conduct a gap analysis and identify the strategy to move to the desired state of security from its current state of security. The desired state of security is also termed as the **security objectives**. This gap analysis becomes the basis for the strategy.
3. The final step is to create the road map and identify specific actionable steps to achieve the security objectives. The security manager needs to consider various factors such as time limits, resource availability, the security budget, laws and regulations, and other relevant factors.

These specific actions are implemented by way of security policies, standards, and procedures.

Governance framework

The **governance framework** is a structure or outline that supports the implementation of the information security strategy. They provide the best practices for a structured security program. Frameworks are a flexible structure that any organization can adopt as per their environment and its requirements. Governance frameworks such as **COBIT** and **ISO 27000** are both examples of widely accepted and implemented frameworks for security governance.

Let's look a bit closer at an example of information security governance in the next section.

The aim of information security governance

Information security governance is a subset of the overall **enterprise governance** of an organization. The same framework should be used for both enterprise governance and information security governance for better integration between the two.

The following are the objectives of information security governance:

- To ensure that security initiatives are aligned with the business's strategy and support organizational objectives.
- To optimize security investments and ensure the high-value delivery of business processes.
- To monitor the security processes to ensure that security objectives are achieved.
- To integrate and align the activities of all assurance functions for effective and efficient security measures.
- To ensure that residual risks are well within acceptable limits. This gives comfort to the management.

We will now go through the key aspects from the perspective of the CISM exam, and in our next topic, we will discuss important aspects of GRC. A CISM aspirant should understand why it is important to integrate all GRC functions.

Key aspects from the CISM exam perspective

The following are some of the key aspects from the CISM exam perspective:

Question	**Possible answer**
Which approach (that is, top-down or bottom-up) is more effective for governance?	In a top-down approach, policies, procedures, and goals are finalized by senior management, and hence policies and procedures are directly aligned with business objectives. A bottom-up approach may not directly address management priorities. The effectiveness of governance is best ensured by a top-down approach.
What is the important aspect from a senior management perspective in an information security strategy?	Business priorities, objectives, and goals.
What is a governance framework?	A governance framework is a structure that provides the outline to support the processes and methods.

Table 1.1 – Key aspects from the CISM exam perspective

Questions

1. The effectiveness of information security governance is best indicated by which of the following?

   A. Security projects are discussed and approved by a steering committee.

   B. Security training is mandatory for all executive-level employees.

   C. A security training module is available on the intranet for all employees.

   D. Patches are tested before deployment.

   Answer: A. Security projects are discussed and approved by a steering committee.

   Explanation: The involvement of a steering committee in the discussion and approval of security projects indicates that the management is committed to security governance. The other options are not as significant as option *A*.

2. An information security governance model is most likely to be impacted by which of the following?

   A. The number of workstations.

   B. The geographical spread of business units.

   C. The complexity of the organizational structure.

   D. The information security budget.

   Answer: C. The complexity of the organizational structure.

   Explanation: The information security governance model is primarily impacted by the complexity of the organizational structure. The organizational structure includes the organization's objectives, vision and mission, hierarchy structure, leadership structure, different function units, different product lines, and other relevant factors. The other options are not as significant as option *C*.

3. Which of the following is the first step in implementing information security governance?

   A. Employee training.

   B. The development of security policies.

   C. The development of security architecture.

   D. The availability of an incident management team.

   Answer: B. The development of security policies.

   Explanation: Security policies indicate the intent of the management. Based on these policies, the security architecture and various procedures are designed.

4. Which of the following factors primarily drives information security governance?

   A. Technology requirements.

   B. Compliance requirements.

   C. The business strategy.

   D. Financial constraints.

   Answer: C. The business strategy.

   Explanation: Information security governance should support the business strategy. Security must be aligned with business objectives. The other options are not a primary driver of information security governance.

5. Which of the following is the responsibility of the information security governance steering committee?

   A. To manage the information security team.

   B. To design content for security training.

   C. To prioritize the information security projects.

   D. To provide access to critical systems.

   Answer: C. To prioritize the information security projects.

   Explanation: One of the important responsibilities of a steering committee is to discuss, approve, and prioritize information security projects and to ensure that they are aligned with the goals and objectives of the enterprise.

6. Which of the following is the first step of information security governance?

   A. To design security procedures and guidelines.

   B. To develop a security baseline.

   C. To define the security strategy.

   D. To develop security policies.

   Answer: C. To define the security strategy.

   Explanation: The first step is to adopt the security strategy. The next step is to develop security policies based on this strategy. The step after this is to develop security procedures and guidelines based on the security policies.

7. Which of the following is the most important factor for an information security governance program?

   A. To align with the organization's business strategy.

   B. To be derived from a globally accepted risk management framework.

   C. To be able to address regulatory compliance.

   D. To promote a risk-aware culture.

   Answer: A. To align with the organization's business strategy.

   Explanation. The most important objective of an information security governance program is to ensure that the information security strategy is in alignment with the strategic goals and objectives of the enterprise. The other options are secondary factors.

8. Which of the following is effective governance best indicated by?

   A. An approved security architecture.

   B. A certification from an international body.

   C. Frequent audits.

   D. An established risk management program.

   Answer: D. An established risk management program.

   Explanation: An effective and efficient risk management program is a key element of effective governance. The other options are not as significant as an established risk management program.

9. Which of the following is the effectiveness of governance best ensured by?

   A. The use of a bottom-up approach.

   B. Initiatives by the IT department.

   C. A compliance-oriented approach.

   D. The use of a top-down approach.

   Answer: D. The use of a top-down approach.

   Explanation: In a top-down approach, policies, procedures, and goals are set by senior management, and as a result, the policies and procedures are directly aligned with the business objectives. A bottom-up approach may not directly address management priorities. Initiatives by the IT department and a compliance-oriented approach are not as significant as the use of a top-down approach.

10. What is the prime responsibility of the information security manager in the implementation of security governance?

    A. To design and develop the security strategy.

    B. To allocate a budget for the security strategy.

    C. To review and approve the security strategy.

    D. To train the end users.

    Answer: A. To design and develop the security strategy.

    Explanation: The prime responsibility of the information security manager is to develop the security strategy based on the business objectives in coordination with the business process owner. The review and approval of the security strategy is the responsibility of the steering committee and senior management. The security manager is not directly required to train the end users. The budget allocation is the responsibility of senior management.

11. What is the most important factor when developing information security governance?

    A. To comply with industry benchmarks.

    B. To comply with the security budget.

    C. To obtain a consensus from the business functions.

    D. To align with organizational goals.

    Answer: D. To align with organizational goals.

    Explanation: The objective of the security governance is to support the objectives of the business. The most important factor is to align with organizational objectives and goals. The other options are secondary factors.

12. What is the prime objective of GRC:

    A. To synchronize and align the organization's assurance functions.

    B. To address the requirements of the information security policy.

    C. To address the requirements of regulations.

    D. To design low-cost a security strategy.

    Answer: A. To synchronize and align the organization's assurance functions.

    Explanation: The concept of GRC is an effort to synchronize and align the assurance activities across the organization for greater efficiency and effectiveness. The other options can be considered secondary objectives.

13. What organizational areas are the main focus for GRC?

    A. Marketing and risk management.

    B. IT, finance, and legal.

    C. Risk and audit.

    D. Compliance and information security.

    Answer: B. IT, finance, and legal.

    Explanation: Though a GRC program can be applied in any function of the organization, it is mostly focused on IT, finance, and legal areas. Financial GRC focuses on effective risk management and compliance for finance processes. IT GRC focuses on IT processes. Legal GRC focuses on the overall enterprise-level regulatory compliance. GRC is majorly focused on IT, finance, and legal processes to ensure that regulatory requirements are adhered to and risks are appropriately addressed.

14. What is the most effective way to build an information security governance program?

    A. To align the requirements of the business with an information security framework.

    B. To understand the objectives of the business units.

    C. To address regulatory requirements.

    D. To arrange security training for all managers.

    Answer: B. To understand the objectives of the business units.

    Explanation: The information security governance program will not be effective if it is not able to address the requirements of the business units. The objective of the business units can be best understood by reviewing their processes and functions. Option *A* is not correct, as security requirements should be aligned with the business and not the other way round. Options *C* and *D* are not as significant as option *B*.

15. What is the main objective of information security governance?

    A. To ensure the adequate protection of information assets.

    B. To provide assurance to the management about information security.

    C. To support complex IT infrastructure.

    D. To optimize the security strategy to support the business objectives.

Answer: D. To optimize the security strategy to support the business objectives.

Explanation: The objective of security governance is to set the direction to ensure that the business objectives are achieved. Unless the information security strategy is aligned with the business objectives, the other options will not offer any value.

16. The security manager noticed inconsistencies in the system configuration. What is the most likely reason for this?

    A. Documented procedures are not available.

    B. Ineffective governance.

    C. Inadequate training.

    D. Inappropriate standards.

    Answer: B. Ineffective governance.

    Explanation: Governance is the process of oversight to ensure the availability of effective and efficient processes. A lack of procedures, training, and standards is a sign of ineffective governance.

17. What is an information security framework best described as?

    A. A framework that provides detailed processes and methods.

    B. A framework that provides required outputs.

    C. A framework that provides structure and guidance.

    D. A framework that provides programming inputs.

    Answer: C. A framework that provides structure and guidance.

    Explanation: A framework is a structure intended to support the processes and methods. They provide outlines and basic structure rather than detailed processes and methods. Frameworks are generally not intended to provide programming inputs.

18. What is the main reason for integrating information security governance into business activities?

    A. To allow the optimum utilization of security resources.

    B. To standardize the processes.

    C. To support operational processes.

    D. To address operational risks.

    Answer: D. To address operational risks.

Explanation: The main objective of integrating the security aspect in business processes is to address operational risks. The other options may be considered secondary benefits.

19. Which of the following is the most important attribute of an effective information security governance framework?

A. A well-defined organizational structure with necessary resources and defined responsibilities.

B. The availability of the organization's policies and guidelines.

C. The business objectives support the information security strategy.

D. Security guidelines supporting regulatory requirements.

Answer: A. A well-defined organizational structure with necessary resources and defined responsibilities.

Explanation: The most important attribute is a well-defined organizational structure that minimizes any conflicts of interest. This ensures better governance. Options *B* and *D* are important aspects, but option *A* is more critical. Option *C* is not correct, as the security strategy supports the business objectives, and not the other way round.

20. What is the most effective method to use to develop an information security program?

A. A standard.

B. A framework.

C. A process.

D. A model.

Answer: B. A framework.

Explanation: A framework is the most suitable method for developing an information security program as they are more flexible in adoption. Some of the common frameworks include ISO 27001 and COBIT. Standards, processes, and models are not as flexible as frameworks.

Understanding governance, risk management, and compliance

GRC is a term used to align and integrate the processes of governance, risk management, and compliance. GRC emphasizes that governance should be in place for effective risk management and the enforcement of compliance.

Governance, risk management, and compliance are three related aspects that help to achieve the organization's objectives. GRC aims to lay down operations for more effective organizational processes and avoiding wasteful overlaps. Each of these three disciplines impacts the organizational technologies, people, processes, and information. If governance, risk management, and compliance activities are handled independently of each other, it may result in a considerable amount of duplication and a waste of resources. The integration of these three functions helps to streamline the assurance activities of an organization by addressing the overlapping and duplicated GRC activities.

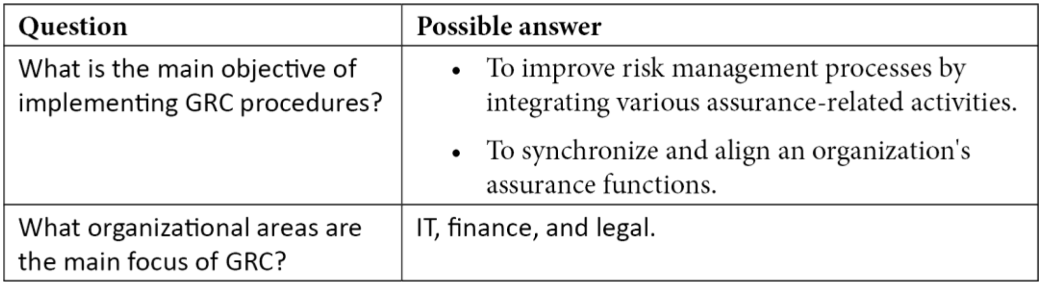
Though a GRC program can be applied in any function of the organization, it is mostly focused on the financial, IT, and legal areas.

Financial GRC focuses on effective risk management and compliance for finance processes. **IT GRC** focuses on information technology processes. **Legal GRC** focuses on the overall enterprise-level regulatory compliance.

GRC is an ever-evolving concept, and a security manager should understand the current state of GRC in their organization and determine how to ensure its continuous improvement.

Key aspects from the CISM exam perspective

The following are some of the key aspects from a CISM exam perspective:



Question	**Possible answer**
What is the main objective of implementing GRC procedures?	• To improve risk management processes by integrating various assurance-related activities. • To synchronize and align an organization's assurance functions.
What organizational areas are the main focus of GRC?	IT, finance, and legal.

Table 1.2 – Key aspects from the CISM exam perspective

Questions

1. Which of the following is the main objective of implementing GRC procedures?

   A. To minimize the governance cost.

   B. To improve risk management.

   C. To synchronize security initiatives.

   D. To ensure regulatory compliance.

   Answer: B. To improve risk management.

   Explanation: GRC is implemented by integrating interrelated control activities across the organization for improving risk management activities. The other options are secondary objectives.

2. What is the prime objective of GRC?

   A. To synchronize and align the organization's assurance functions.

   B. To address the requirements of the information security policy.

   C. To address the requirements of regulations.

   D. To design a low-cost security strategy.

   Answer: A. To synchronize and align the organization's assurance functions.

   Explanation: The concept of GRC is an effort to synchronize and align the assurance activities across the organization for greater efficiency and effectiveness. The other options can be considered secondary objectives.

Discovering the maturity model

CISM aspirants are expected to understand the basic details of a **maturity model**. A maturity model is a tool that helps the organization to assess the current effectiveness of a process and to determine what capabilities they need to improve their performance.

Capability maturity models (**CMM**s) are useful to determine the maturity level of governance processes. The following list defines the different maturity levels of an organization:

- **Level 0: Incomplete**: On this level, the process is not implemented or does not achieve its intended purpose.
- **Level 1: Performed**: On this level, the process can achieve its intended purpose.
- **Level 2: Managed**: On this level, the process can achieve its intended purpose. Also, the process is appropriately planned, monitored, and controlled.

- **Level 3: Established**: Apart from the Level 2 process, there is a well-defined, documented, and established process to manage the process.
- **Level 4: Predictable**: On this level, the process is predictable and operates within defined parameters and limits to achieve its intended purpose.
- **Level 5: Optimized**: This is the level at which the process is continuously improved to meet the current as well as projected goals.

The CMM indicates a scale of *0* to *5* based on process maturity level, and it is the most common method applied by organizations to measure their existing state and then to determine the desired one.

Maturity models identify the gaps between the current state of the governance process and the desired state to help the organization to determine the necessary remediation steps for improvement. A maturity model requires continuous improvement in the governance framework. It requires continuous evaluation, monitoring, and improvement to move towards the desired state from the current state.

Key aspects from the CISM exam perspective

The following are some of the key aspects from an exam perspective:

Question	**Possible answer**
Which models are used to determine the extent and level of processes?	• The maturity model • Process performance and capability models
What is the best way to determine the continuous improvement of the risk management process?	The adoption of the maturity model.

Table 1.3 – Key aspects from the CISM exam perspective

Questions

1. What is the most important factor for the development of a maturity model-based information security governance framework?

   A. Continuous evaluation, monitoring, and improvement.

   B. The return on technology investment.

   C. Continuous risk mitigation.

   D. Continuous **key risk indicator** (**KRI**) monitoring.

Answer: A. Continuous evaluation, monitoring, and improvement.

Explanation: The maturity model requires continuous improvement in the governance framework. It requires continuous evaluation, monitoring, and improvement to move towards the desired state from the current state. The other options are not as significant as option *A*.

2. What best indicates the level of information security governance?

A. A defined maturity model.

B. The size of the security team.

C. The availability of policies and procedures.

D. The number of security incidents.

Answer: A. A defined maturity model.

Explanation: A defined maturity model will be the best indicator to determine the level of security governance. The maturity model indicates the maturity of the governance processes on a scale of *0* to *5*, where *Level 0* indicates incomplete processes, and *Level 5* indicates optimized processes. The other options may not be as useful as the maturity model in determining the level of security.

3. What is the most effective indicator of the level of security governance?

A. The annual loss expectancy.

B. The maturity level.

C. A risk assessment.

D. An external audit.

Answer: B. The maturity level.

Explanation: A defined maturity model will be the best indicator to determine the level of security governance. The maturity model indicates the maturity of the governance processes on a scale of *0* to *5*, where *Level 0* indicates incomplete processes, and *Level 5* indicates optimized processes. The other options may not be as useful as the maturity model in determining the level of security.

Getting to know the information security roles and responsibilities

It is very important to ensure that security-related *roles* and *responsibilities* are clearly defined, documented, and communicated throughout the organization. Each employee of the organization should be aware of their respective roles and responsibilities. Clearly defined roles also facilitate effective access rights management, as access is provided based on the respective job functions and job profiles of employees – that is, on a *need-to-know* basis only.

One of the simplest ways of defining roles and responsibilities in a business or organization is to form a matrix known as a **RACI chart**. This stands for **responsible**, **accountable**, **consulted**, and **informed**.

This chart indicates who is *responsible* for a particular function, who is *accountable* with regard to the function, who should be *consulted* about the function, and who should be *informed* about the particular function. Clearly defined RACI charts make the information security program more effective.

Let's look at the definitions of RACI in more detail:

- **Responsible**: This is the person who is required to execute a particular job function.
- **Accountable**: This is the person who is required to supervise a job function.
- **Consulted**: This is the person who gives suggestions and recommendations for executing a job function.
- **Informed**: This is the person who should be kept updated about the progress of the job function.

In the next section, I will take you through the various roles that are integral to information security.

Board of directors

The role of board members in information security is of utmost importance. Board members need to be aware of security-related **KRIs** that can impact the business objectives. The intent and objectives of information security governance must be communicated from the board level down.

The current status of key security risks should be tabled and discussed at board meetings. This helps the board to determine the effectiveness of the current security governance.

Another essential reason for the board of directors to be involved in security governance is **liability**. Most of the organization obtains specific insurance to make good on the financial liability of the organization in the event of a security incident. This type of insurance requires those bound by it to exercise due care in the discharge of their duties. Any negligence from the board in addressing the information security risk may make the insurance void.

Senior management

The role of **senior management** is to ensure that the intent and requirements of the board are implemented in an effective and efficient manner. Senior management is required to provide ongoing support to information security projects in terms of budgets, resources, and other infrastructure. In some instances, there may be disagreement between IT and security. In such cases, senior management can take a balanced view after considering performance, cost, and security. The role of senior management is to map and align the security objectives with the overall business objectives.

Business process owners

The role of a **business process owner** is to own the security-related risks impacting their business processes. They need to ensure that information security activities are aligned and support their respective business objectives. They need to monitor the effectiveness of security measures on an ongoing basis.

Steering committee

A **steering committee** comprises the senior management of an organization. The role of a steering committee is as follows:

- To ensure that security programs support the business objectives
- To evaluate and prioritize the security programs
- To evaluate emerging risk, security practices, and compliance-related issues

The roles, responsibilities, and scope of a steering committee should be clearly defined.

Chief information security officer

The **chief information security officer** (**CISO**) is a senior-level officer who has been entrusted with making security-related decisions and is responsible for implementing security programs. The CISO should be an executive-level officer directly reporting to the **chief executive officer** (**CEO**). The role of the CISO is fundamentally a regulatory role, whereas the role of the CIO is to generally focus on IT performance.

Chief operating officer

The **chief operating officer** (**COO**) is the head of operational activities in the organization. Operational processes are reviewed and approved by the COO. The COO has a thorough knowledge of the business operations and objectives. The COO is most likely the sponsor for the implementation of security projects as they have a strong influence across the organization. **Sponsoring** means supporting the project financially or through products or services. Although the CISO should provide security advice and recommendations, the sponsor should be the COO for effective *ground-level* implementation.

Data custodian

The **data custodian** is a staff member who is entrusted with the safe custody of data. The data custodian is different from the **data owner**, though in some cases, both data custodian and data owner may be the same individual. A data custodian is responsible for managing the data on behalf of the data owner in terms of data backup, ensuring data integrity, and providing access to data for different individuals through the approval of the data owner. From a security perspective, a data custodian is responsible for ensuring that appropriate security measures are implemented and are consistent with organizational policy.

Communication channel

A well-defined **communication channel** is of utmost importance in the management of information security. A mature organization has dedicated systems to manage risk-related communication. This should be a two-way system, wherein management can reach all the employees and at the same time employees can reach a designated risk official to report identified risks. This will help in the timely reporting of events as well as to disseminate the security information. In the absence of an appropriate communication channel, the identification of events may be delayed.

Indicators of a security culture

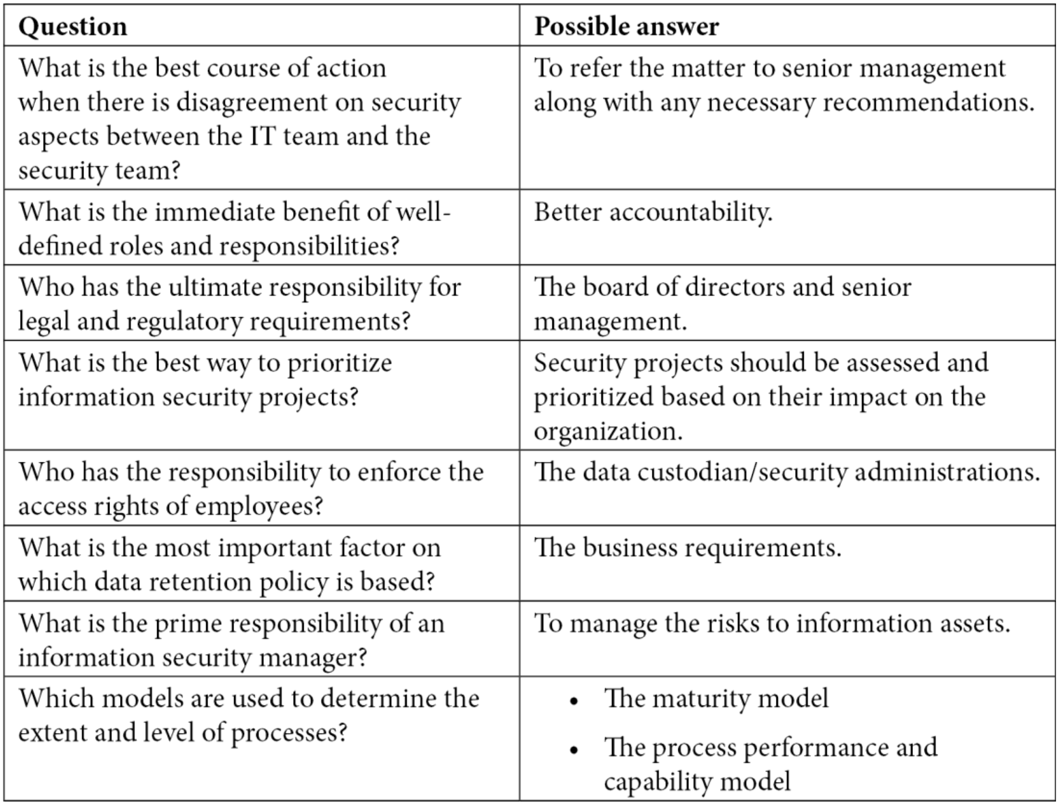
The following list consists of some of the indicators of a successful security culture:

- The involvement of the information security department in business projects.
- The end users are aware of the identification and reporting of the incidents.
- There is an appropriate budget for information security programs.
- The employees are aware of their roles and responsibilities with regard to information security.

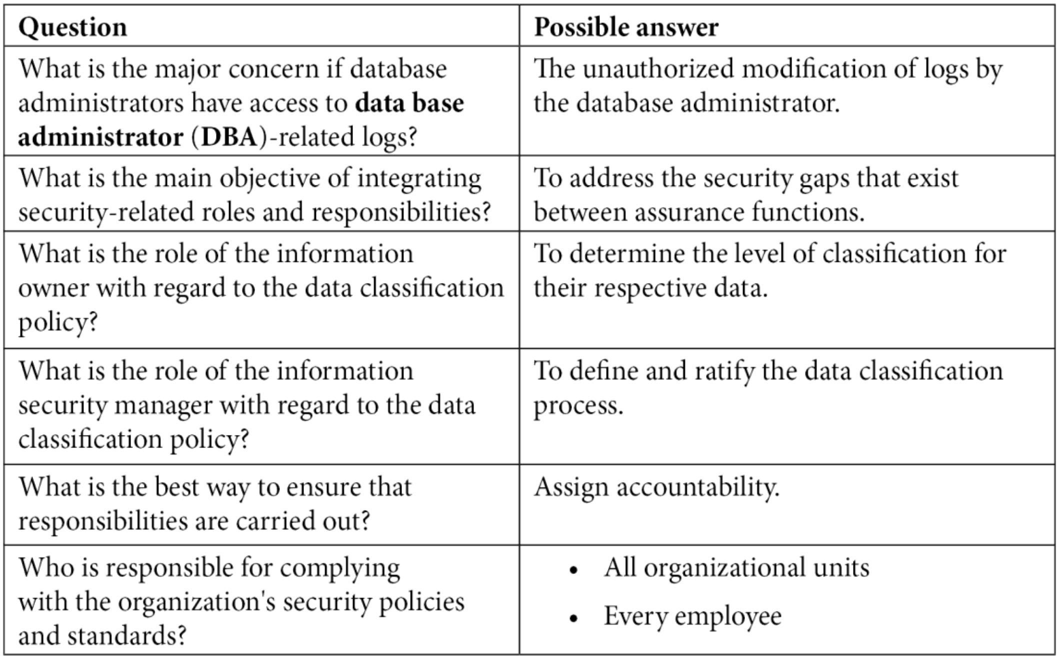
Understanding the roles and responsibilities as covered in this section will help the security manager to implement an effective security strategy.

Key aspects from the CISM exam perspective

The following are some of the key aspects from the CISM exam perspective:



Question	**Possible answer**
What is the best course of action when there is disagreement on security aspects between the IT team and the security team?	To refer the matter to senior management along with any necessary recommendations.
What is the immediate benefit of well-defined roles and responsibilities?	Better accountability.
Who has the ultimate responsibility for legal and regulatory requirements?	The board of directors and senior management.
What is the best way to prioritize information security projects?	Security projects should be assessed and prioritized based on their impact on the organization.
Who has the responsibility to enforce the access rights of employees?	The data custodian/security administrations.
What is the most important factor on which data retention policy is based?	The business requirements.
What is the prime responsibility of an information security manager?	To manage the risks to information assets.
Which models are used to determine the extent and level of processes?	• The maturity model • The process performance and capability model



Question	**Possible answer**
What is the major concern if database administrators have access to **data base administrator** (**DBA**)-related logs?	The unauthorized modification of logs by the database administrator.
What is the main objective of integrating security-related roles and responsibilities?	To address the security gaps that exist between assurance functions.
What is the role of the information owner with regard to the data classification policy?	To determine the level of classification for their respective data.
What is the role of the information security manager with regard to the data classification policy?	To define and ratify the data classification process.
What is the best way to ensure that responsibilities are carried out?	Assign accountability.
Who is responsible for complying with the organization's security policies and standards?	• All organizational units • Every employee

Table 1.4 – Key aspects from the CISM exam perspective

Questions

1. The process of mapping job descriptions to relevant data access rights will help in adherence to which of the following security principles?

   A. The principle of accountability.

   B. The principle of proportionality.

   C. The principle of integration.

   D. The principle of the code of ethics.

   Answer: B. The principle of proportionality.

   Explanation: The principle of proportionality requires that the access should be proportionate to the criticality of the assets and access should be provided on a need-to-know basis. The principle of accountability is important for the mapping of job descriptions; however, people with access to data may not always be accountable. Options *C* and *D* are not directly relevant to mapping job descriptions.

2. The data custodian is primarily responsible for which of the following?

   A. Approving access to the data.

   B. The classification of assets.

   C. Enhancing the value of data.

   D. Ensuring all security measures are in accordance with organizational policy.

   Answer: D. Ensuring all security measures are in accordance with organizational policy.

   Explanation: The data custodian is responsible for ensuring that appropriate security measures are implemented and are consistent with organizational policy. The other options are not the responsibility of the data custodian.

3. In the case of a disagreement between the IT team and security team on a security aspect, the security manager should do which of the following?

   A. Refer the matter to an external third party for resolution.

   B. Request senior management to discontinue the relevant project immediately.

   C. Ask the IT team to accept the risk.

   D.Refer the matter to senior management along with any necessary recommendations.

   Answer: D. Refer the matter to senior management along with any necessary recommendations.

   Explanation: The best option for a security manager in this case is to highlight the issue to senior management. Senior management will be in the best position to take a decision after considering business as well security aspects.

4. Which of the following is an immediate benefit of having well-defined roles and responsibilities from an information security perspective?

   A. The adherence to security policies throughout the organization.

   B. Well-structured process flows.

   C. The implementation of **segregation of duties** (**SoD**).

   D. Better accountability.

   Answer: D. Better accountability.

Explanation: Having clearly set out roles and responsibilities ensures better accountability, as individuals are aware of their key performance area and expected outcomes. The other options may be indirect benefits, but the only direct benefit is better accountability.

5. What is the prime role of an information security manager in a data classification process?

A. To define and ratify the data classification process.

B. To map all data to different classification levels.

C. To provide data security, as per the classification.

D. To confirm that data is properly classified.

Answer: A. To define and ratify the data classification process.

Explanation: The primary role of an information security manager is to define the structure of data classification. They need to ensure that the data classification policy is consistent with the organization's risk appetite. The mapping of data as per the classification is the responsibility of the data owner. Providing security is the responsibility of the data custodian. Confirming proper classification may be the role of the information security manager or the information security auditor.

6. Which of the following is the area of most concern for the information security manager?

A. That there are vacant positions in the information security department.

B. That the information security policy is approved by senior management.

C. That the steering committee only meets on a quarterly basis.

D. That security projects are reviewed and approved by the data center manager.

Answer: D. That security projects are reviewed and approved by the data center manager.

Explanation: Security projects should be approved by the steering committee consisting of senior management. The data center manager may not be in a position to ensure the alignment of security projects with the overall enterprise objectives. This will have an adverse impact on security governance. The approval of the security policy by senior management indicates good governance. Vacant positions are not a major concern. The steering committee meeting on a quarterly basis is also not an issue.

7. An information security manager should have a thorough understanding of business operations with a prime objective of which of the following?

   A. Supporting organizational objectives.

   B. Ensuring regulatory compliance.

   C. Concentrating on high-risk areas.

   D. Evaluating business threats.

   Answer: A. Supporting organizational objectives.

   Explanation: The main objective of the security manager having a thorough understanding of the business operations is to support the organization's objectives. The other options are specific actions to support the business objectives.

8. In a big multi-national organization, the best approach to identify security events is to do which of the following?

   A. Conduct frequent audits of the business processes.

   B. Deploy a firewall and **intrusion detection system** (**IDS**).

   C. Develop communication channels across the organization.

   D. Conduct vulnerability assessments of new systems.

   Answer: C. Develop communication channels across the organization.

   Explanation: The best approach is to develop communication channels that will help in the timely reporting of events as well as to disseminate security information. The other options are good practices; however, without an appropriate communication channel, the identification of events may be delayed.

9. Legal and regulatory liability is the responsibility of which of the following?

   A. The chief information security officer.

   B. The head of legal.

   C. The board of directors and senior management.

   D. The steering committee.

   Answer: C. The board of directors and senior management.

   Explanation: The ultimate responsibility for compliance with legal and regulatory requirements is with the board of directors and senior management. The CISO, head of legal, and steering committee implement the directive of the board and senior management, but they are not individually liable for the failure of security.

10. What is the best way to gain support from senior management for information security projects?

    A. Lower the information security budget.

    B. Conduct a risk assessment.

    C. Highlight industry best practices.

    D. Design an information security policy.

    Answer: B. Conduct a risk assessment.

    Explanation: The best way to gain the support of senior management is to conduct a risk assessment and present it to management in the form of an impact analysis. A risk assessment will help management to understand areas of concern. The other options may be considered secondary factors.

11. Prioritization of information security projects should be best conducted based on which of the following?

    A. The turnaround time of the project.

    B. The impact on the organization's objectives.

    C. The budget of the security project.

    D. The resource requirements for the project.

    Answer: B. The impact on the organization's objectives.

    Explanation: Security projects should be assessed and prioritized based on their impact on the organization. The other options are secondary factors.

12. Who is responsible for enforcing the access rights of employees?

    A. The process owner.

    B. The data owner.

    C. The steering committee.

    D. The security administrators.

    Answer: D. The security administrators.

    Explanation: The security administrators are custodians of the data and they need to ensure that data is in safe custody. They are responsible for enforcing and implementing security measures in accordance with the information security policy. The data owner and process owner are responsible for classifying the data and approving access rights. However, they do not enforce and implement the security controls. The steering committee is not responsible for enforcement.

13. Who is responsible for information classification?

    A. The data administrator.

    B. The information security manager.

    C. The information system auditor.

    D. The data owner.

    Answer: D. The data owner.

    Explanation: The data owner has responsibility for the classification of their data in accordance with the organization's data classification policy. The data administrator is required to implement security controls as per the security policy. The security manager and system auditor oversee the data classification and handling process to ensure conformance to the policy.

14. What is the data retention policy primarily based on?

    A. Industry practices.

    B. Business requirements.

    C. Regulatory requirements.

    D. Storage requirements.

    Answer: B. Business requirements.

    Explanation: The primary basis for defining the data retention period is the business requirements. Business requirements will consider any legal and regulatory aspects. If its data is not retained as per business needs, it may have a negative impact on the business objectives.

15. What is the most important security aspect for a multi-national organization?

    A. The local security programs should comply with the corporate data privacy policy.

    B. The local security program should comply with the data privacy policy of the location where the data is collected.

    C. The local security program should comply with the data privacy policy of the country where the headquarters are located.

    D. Local security program should comply with industry best practices.

    Answer: B. The local security program should comply with the data privacy policy of the location where the data is collected.

Explanation: Data privacy laws are country-specific. It is very important to ensure adherence to local laws. The organization's privacy policy may not be able to address all the local laws and requirements. The organization's data privacy policy cannot supersede the local laws.

16. Ultimate accountability for the protection of sensitive data is with which of the following?

A. The security administrators.

B. The steering committee.

C. The board of directors.

D. The security manager.

Answer: C. The board of directors.

Explanation: The board of directors has the ultimate accountability for information security. The other options such as the security administrators, steering committee, and security managers are responsible for implementing, enforcing, and monitoring security controls as per the directive of the board.

17. The most likely authority to sponsor the implementation of new security infrastructure for business processes is which of the following?

A. The CISO.

B. The COO.

C. The head of legal.

D. The data protection officer.

Answer: B. The COO.

Explanation: The chief operating officer is the head of operational activities in the organization. Operational processes are reviewed and approved by the COO. The COO has the most thorough knowledge of the business operations and objectives. The COO is most likely the sponsor for the implementation of security projects as they have a strong influence across the organization. Sponsoring means supporting the project financially or through products or services. Although the CISO should provide security advice and recommendations, the sponsor should be the COO for effective ground-level implementation.

18. Who should determine the requirements for access to data?

    A. The security officer.

    B. The data protection officer.

    C. The compliance officer.

    D. The business owner.

    Answer: D. The business owner.

    Explanation: The business owner needs to ensure that their data is appropriately protected, and access is provided on a need-to-know basis only. The security officer, data protection officer, and compliance officer can advise on security aspects, but they do not have final responsibility.

19. The responsibility for establishing information security controls in an application resides with which of the following?

    A. The information security steering committee.

    B. The data owner.

    C. The system auditor.

    D. The system owner.

    Answer: B. The data owner.

    Explanation: The data owner is responsible for determining the level of security controls for the data, as well as for the application that stores the data. The system owner is generally responsible for platforms rather than applications or data. The system auditor is responsible for evaluating the security controls. The steering committee consists of senior-level officials and is responsible for aligning the security strategy with the business objectives.

20. The information security manager observes that not enough details are documented in the recovery plan and this may prevent meeting the recovery time objective. Which of the following compensates for the lack of details in the recovery plan and ensures that the recovery time objective is met?

    A. Establishing more than one operation center.

    B. Delegating authority for the recovery execution.

    C. Outsourcing the recovery process.

    D. Taking incremental backups of the database.

    Answer: B. Delegating authority for recovery execution.

Explanation: During an incident, considerable time is taken up in escalation procedures, as decisions need to be made at each management level. The delegation of authority for the recovery execution makes the recovery process faster and more effective. However, the scope of the recovery delegation must be assessed beforehand and appropriately documented. Having multiple operation centers is too expensive to implement. Outsourcing is not a feasible option. Incremental backups do facilitate faster backups; however, they generally increase the time needed to restore the data.

21. The effectiveness of SoD is best ensured by which of the following?

A. Implementing strong password rules.

B. Making available a security awareness poster on the intranet.

C. Frequent information security training.

D. Reviewing access privileges when an operator's role changes.

Answer: D. Reviewing access privileges when an operator's role changes.

Explanation: In the absence of access privilege reviews, there is the risk that a single staff member can acquire excess operational capabilities. This will defeat the objective of SoD. In order to maintain the effectiveness of SoD, it is important to review access privileges more frequently and more specifically when an operator's role changes.

22. What is the prime responsibility of an information security manager?

A. To manage the risk to information assets.

B. To implement the security configuration for IT assets.

C. To conduct disaster recovery testing.

D. To close identified vulnerabilities.

Answer: A. To manage the risk to information assets.

Explanation: The prime responsibility of an information security manager is to evaluate and manage the information security risk by involving risk owners. Implementing the security configuration is the responsibility of the asset owner. Disaster recovery testing should be conducted by the process owner, and the closing of vulnerabilities is the responsibility of the asset owner.

23. To determine the extent of sound processes, the maturity model is used. Another approach is to use which of the following?

    A. The Monte Carlo method.

    B. Process performance and capabilities.

    C. Vulnerability assessments.

    D. Risk analysis.

    Answer: B. Process performance and capabilities.

    Explanation: Process performance and capabilities provide a detailed perspective of the maturity levels, just like the maturity model. The other options will not help to determine the level of maturity of the process. The Monte Carlo method is a risk assessment method that uses simulations.

24. Information system access should be primarily authorized by which of the following?

    A. The information owner.

    B. The system auditor.

    C. The CISO.

    D. The system administrator.

    Answer: A. The information owner.

    Explanation: The information owner is ultimately responsible for the protection of their data. The information owner is the best person to know the criticality of the data and who should have access to the data. Therefore, information system access should be primarily authorized by the information owner.

25. The information security manager observed that the incident log is stored on a production database server. Which of the following is a major concern?

    A. The unavailability of log details if the server crashes.

    B. The unauthorized modification of logs by the database administrator.

    C. Log capturing makes the transaction process slow.

    D. Critical information may not be captured in the log files.

    Answer: B. The unauthorized modification of logs by the database administrator.

Explanation: The database administrator will have access to logs if they are stored in the database server. The database administrator can modify or delete the log entries. This is a major cause of concern. Backup of the logs will address the issue of server crashes. Log capturing may not always impact transaction processing. If critical information is not captured in logs, it is a design failure and has nothing to do with log entries stored in the production database. The database administrator should not have access to logs related to the database.

26. Appointing a CISO indicates which of the following?

A. The organization wants to enhance the role of senior management.

B. The organization is committed to its responsibility for information security.

C. The board of directors wants to pass on their accountability.

D. The organization wants to improve its technology architecture.

Answer: B. The organization is committed to its responsibility for information security.

Explanation: Appointing a CISO indicates that the organization wants to have a clear line of responsibility for information security. Information security is one of the focus areas for the organization. Having a CISO does not impact the role of senior management. Even if the CISO is appointed, accountability lies with the board of directors. The CISO is generally not accountable for technology projects.

27. The main objective of integrating security-related roles and responsibilities is which of the following?

A. To address the security gaps that exist between assurance functions.

B. To address the unavailability of manpower.

C. To address the gap in business continuity and disaster recovery.

D. To address the complications in system development processes.

Answer: A. To address the security gaps that exist between assurance functions.

Explanation: Whenever there are shared responsibilities for information security, gaps tend to exist. Integrating the roles and responsibilities is the best way to address these gaps and ensure consistent risk management. The other options are secondary factors.

28. Which of the following is the best compensating control when the same employee is responsible for updating servers, maintaining the access control, and reviewing the logs?

    A. To verify that only approved changes are made.

    B. To conduct penetration tests.

    C. To conduct risk assessments.

    D. To conduct reviews of log files by the manager.

    Answer: A. To verify that only approved changes are made.

    Explanation: In the absence of SoD, the best compensatory control is to ensure that only approved changes are made by the employee. This verification can either be done for all cases or on a sample basis depending on the risk involved. The review of logs by the manager may not be meaningful as an employee can manipulate the logs and hide activities from the supervisor. Penetration tests and risk assessments may not be able to detect the unauthorized activities.

29. What is the responsibility of the information owner when complying with the information classification scheme?

    A. To implement security measures to protect their data.

    B. To determine the level of classification for their data.

    C. To arrange backups of their data.

    D. To delegate the processes of information classification to the system administrator.

    Answer: B. To determine the level of classification for their data.

    Explanation: The information owner is required to determine the level of classification for their respective data. Based on its classification, the system administrator implements the required security measures and data backups. The information owner may delegate the process of classification to some other responsible employee but not to the system administrator.

30. The effectiveness of the organization's security measures is the final responsibility of which of the following?

    A. The security administrator.

    B. The CISO.

    C. Senior management.

    D. The information security auditor.

    Answer: C. Senior management.

    Explanation: Senior management has the final responsibility for the effectiveness of the organization's security measures. Although the authority to implement, monitor, and evaluate the security measures is delegated to the security administrator, CISO, and the information security auditor, the responsibility cannot be delegated. The final responsibility rests with senior management.

31. What is the best way to ensure that responsibilities are carried out?

    A. Signed non-disclosure agreements.

    B. Heavy penalties for non-compliance.

    C. Assigned accountability.

    D. Documented policies.

    Answer: C. Assigned accountability.

    Explanation: If accountability is properly assigned and made known to the individuals, individuals will be more proactive and concerned about their responsibilities, and this will ensure that duties are properly carried out.

32. Who is responsible for complying with the organization's security policies and standards?

    A. The CISO.

    B. Senior management.

    C. The compliance officer.

    D. All organizational units.

    Answer: D. All organizational units.

    Explanation: Every employee is required to comply with security policies and standards, as applicable to their performance areas. Though CISO and senior management monitor the level of compliance, all organizational units should adhere to policies and standards.

33. Continuous improvement of the risk management process is most likely ensured by which of the following?

    A. The regular review of implemented security controls.

    B. Implementing an information classification policy.

    C. The adoption of a maturity model.

    D. Regular audits of risk management processes.

    Answer: C. The adoption of a maturity model.

    Explanation: A maturity model like the CMM can be used to determine the maturity level of the risk management process from *Level 0* (that is, initial) to *Level 5* (that is, optimized). The organization can know where it falls and can gradually move towards higher levels and thus improve its risk management process. The other options are secondary factors.

34. Information security is the responsibility of which of the following?

    A. All personnel.

    B. IT personnel.

    C. Security personnel.

    D. Operational personnel.

    Answer: A. All personnel.

    Explanation: It is the responsibility of all personnel to adhere to the security requirements of the organization.

35. Who should security policies be finally approved by?

    A. Operation managers.

    B. The CISO.

    C. Senior management.

    D. The **chief technical officer** (**CTO**)

    Answer: C. Senior management.

    Explanation: Senior management is in the best position to understand the key business objectives and how they should be protected by way of policies and procedures. Other officials (for example, the operation manager, CISO, and CTO) may provide necessary inputs, but final approval should be provided by senior management.

36. Confidentiality of information can be best ensured by which of the following?

    A. Implementing an information classification policy.

    B. Implementing SoD.

    C. Implementing the principle of least privilege.

    D. Implementing information security audits.

    Answer: C. Implementing the principle of least privilege.

    Explanation: The most effective method to protect the confidentiality of information assets is to follow the principle of least privilege. The principle of least privilege ensures that access is provided only on a need-to-know basis and it should be restricted for all other users. The other options are good measures; however, in the absence of the principle of least privilege, they may not be effective.

Finding out about the governance of third-party relationships

In today's world, most organizations are heavily reliant on a **third party** to achieve business objectives. The primary reason to obtain the services of a third party is to avail yourself of expert services in a cost-effective manner. These third parties can be in the form of a **service provider**, **trading partners**, **group companies**, or others.

These third parties are connected to the systems of the organization and have access to the data and other resources of the organization. To protect the organization, it is very important for an information security manager to assess the risk of such third-party relationships and ensure relevant controls are in place.

Policies and requirements of information security should be developed before the creation of any third-party relationship.

Also, the security manager should understand the following challenges of third-party relationships:

- The cultural differences between an organization and the service provider.
- Technology incompatibilities.
- The business continuity arrangements of the service provider may not have aligned to the requirements of the organization.
- Differences in **incident management processes**.
- Differences in **disaster recovery capabilities**.

Effective governance is highly dependent on the culture of the organization. Let's discuss this in more detail in our next topic.

The culture of an organization

The culture of an organization and its service provider is the most important factor that determines the implementation of an *information security program*. The culture of the organization influences *risk appetite,* that is, the willingness to take risks. This will have a significant influence on the design and implementation of the information security program. A culture that favors taking risks will have a different implementation approach to a culture that is risk-averse.

Cultural differences and their impact on data security are generally not considered during security reviews. Different cultures have different perspectives on what information is considered sensitive and how it should be handled. This cultural practice may not be consistent with an organization's requirements.

Compliance with laws and regulations

An information security manager should be cautious about adherence to laws and regulations. Laws and regulations should be addressed to the extent that they impact the organization.

The process should be in place to scan all the new regulations and determine the applicability of regulations to the organization.

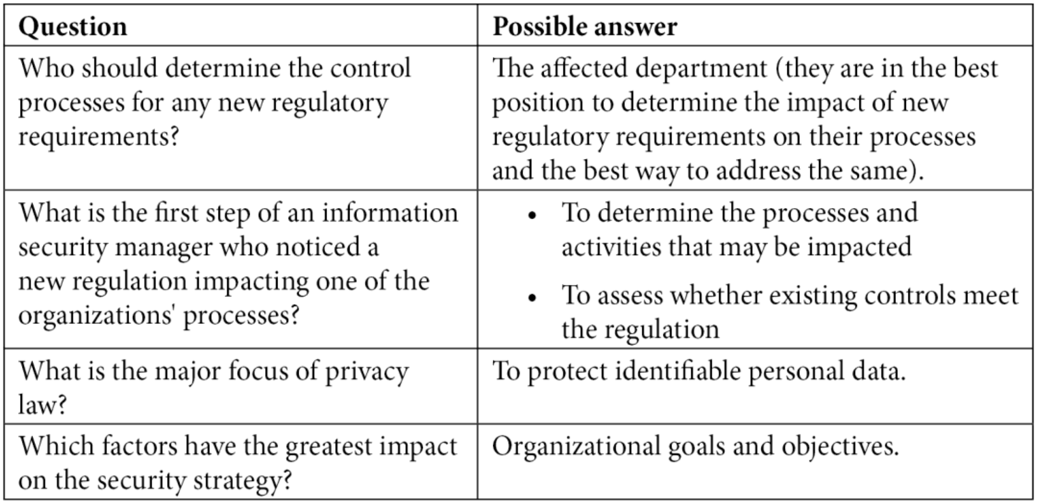
The information security manager is required to determine the processes and activities that may be impacted and whether existing controls are adequate to address the new regulations. If not, then further controls should be implemented to address the new regulations.

Departments affected by the new regulations are in the best position to determine the impact of new regulatory requirements on their processes and the best way to address them.

The information security manager is required to assess the impact of privacy law on business processes. The prime focus of privacy law is to protect the identifiable personal data held by an organization.

Key aspects from the CISM exam perspective

The following are some of the key aspects from the CISM exam perspective:



Question	Possible answer
Who should determine the control processes for any new regulatory requirements?	The affected department (they are in the best position to determine the impact of new regulatory requirements on their processes and the best way to address the same).
What is the first step of an information security manager who noticed a new regulation impacting one of the organizations' processes?	• To determine the processes and activities that may be impacted • To assess whether existing controls meet the regulation
What is the major focus of privacy law?	To protect identifiable personal data.
Which factors have the greatest impact on the security strategy?	Organizational goals and objectives.

Table 1.5 – Key aspects from the CISM exam perspective

Questions

1. What should be the first step of the information security manager when an organization plans to implement a **bring your own device** (**BYOD**) policy for mobile devices?

   A. To ask management to stop the BYOD policy implementation, stating the associated risk.

   B. To prepare a business case for the implementation of BYOD controls.

   C. To make the end users aware of BYOD risks.

   D. To determine the information security strategy for BYOD.

   Answer: D. To determine the information security strategy for BYOD.

   Explanation: The first step for the information security manager is to determine a strategy to protect the organization from the risks of BYOD. Option *A* is not feasible, as the role of the security manager is to facilitate business processes by mitigating the risk. Options *B* and *C* will be based on the security strategy.

2. The factor that influences the design and implementation of the information security program the most is which of the following?

   A. Types of vulnerabilities.

   B. The culture of the organization.

   C. The business objectives.

   D. The complexity of the business.

   Answer: B. The culture of the organization.

   Explanation: The culture of the organization influences the risk appetite which in turn has a significant influence on the design and implementation of the information security program. The business objective is important to prioritize the risk treatment. But the culture of the organization will have a major influence on the design and implementation of the security program. A pro-risk culture will have a different implementation approach to a risk-averse culture.

3. Which of the following will have the biggest influence while planning for business record retention?

   A. Potential changes in storage capacity.

   B. Potential changes in regulatory requirements.

   C. Potential changes in the business strategy.

   D. Potential changes in the application systems and media.

   Answer: D. Potential changes in the application systems and media.

   Explanation: The type and nature of the application systems and media and their capability to read and interpret different types of data formats is the most important factor for planning record retention. New application systems may not be able to read and interpret data generated by earlier applications. This is a major risk.

4. New regulatory requirements impacting information security will mostly come from which of the following?

   A. The chief legal officer.

   B. The chief audit officer.

   C. Affected departments.

   D. Senior management.

   Answer: C. Affected departments.

Explanation: Departments affected by the new regulations are most likely to raise the requirements. They are in the best position to determine the impact of new regulatory requirements on their processes and the best way to address them.

5. Due to changes in the business strategy, certain information now no longer supports the purpose of the business. What should be done with this information?

A. It should be analyzed under the retention policy.

B. It should have restricted access.

C. It should be frequently backed up.

D. It should be evaluated by a business impact analysis.

Answer: A. It should be analyzed under the retention policy.

Explanation: From an information security perspective, such data should be analyzed under the retention policy, and then it should be determined whether the data is required to be maintained for business or regulatory reasons. If the data is no longer required, it should be removed in a secure manner. The other options are not sensible for data if it is of no use.

6. Primarily, the requirements of an information security program are based on which of the following?

A. The IT policy.

B. The desired outcomes.

C. The management perceptions.

D. The security strategy.

Answer: B. The desired outcomes.

Explanation: The desired outcomes should dictate the input requirements of an information security program. It is the responsibility of the security manager to ensure that the program is implemented in such a way that it achieves the desired outcome. The security strategy should also be based on the desired outcomes of the information security program.

7. The first step of an information security manager who noticed a new regulation impacting one of the organizations' processes should be which of the following?

A. To pass on responsibility to the process owner for compliance.

B. To survey the industry practices.

C. To assess whether existing controls meet the regulation.

D. To update the IT security policy.

Answer: C. To assess whether existing controls meet the regulation.

Explanation: The first step is to determine whether existing controls are adequate to address the new regulation. If existing controls are adequate, the need to perform other options is not required.

8. Privacy laws are mainly focused on which of the following?

A. Big data analytics.

B. Corporate data.

C. Identity theft.

D. Identifiable personal data.

Answer: D. Identifiable personal data.

Explanation: The prime focus of privacy law is to protect identifiable personal data. Identity theft is one of the ways of misusing personal data. There can also be other consequences. If analytics are done on identifiable personal data, it could impact privacy only if this violates regulatory provisions.

9. The information security manager noticed a regulation that impacts the handling of sensitive data. They should first do which of the following?

A. Determine the processes and activities that may be impacted.

B. Present a risk treatment option to senior management.

C. Determine the cost of control.

D. Discuss the possible consequences with the process owner.

Answer: A. Determine the processes and activities that may be impacted.

Explanation: The very first step is to determine the processes and activities that may be impacted. Based on that, the security manager can do a risk assessment and determine the level of impact. The other options are subsequent steps.

10. The most important factor to consider while developing a control policy is which of the following?

    A. Protecting data.

    B. Protecting life.

    C. Protecting the business's reputation.

    D. Protecting the business objectives.

    Answer: B. Protecting life.

    Explanation: The most important consideration is to protect human life. For example, carbon dioxide fire extinguishers should be restricted for areas where employees are working. Also, electric door access should be set to fail open in case of fire. The other options are secondary factors.

11. The information security manager should address laws and regulations in which way?

    A. To the extent they impact the organization.

    B. To meet the certification standards.

    C. To address the requirements of policies.

    D. To reduce the cost of compliance.

    Answer: A. To the extent they impact the organization.

    Explanation: Laws and regulations should be addressed to the extent they impact the organization, irrespective of whether they are required for certification standards or the requirements of policies.

12. Which of the following is the most important consideration in the retention of business records?

    A. Strategic objectives

    B. Regulatory and legal requirements.

    C. Storage capacity.

    D. The level of controls implemented.

    Answer: B. Regulatory and legal requirements.

Explanation: Record retention should be primarily based on two factors: business requirements and legal requirements. If a record is required to be maintained for two years as per business requirements, and three years as per legal requirements, it should be maintained for three years. Organizations generally design their business requirements after considering the relevant laws and regulations.

13. What is the most important consideration for organizations involved in cross-border transactions?

A. The capability of the IT architecture.

B. The evolving data protection regulations.

C. The cost of network bandwidth.

D. The incident management process.

Answer: B. The evolving data protection regulations.

Explanation: Privacy laws vary from country to country and organizations must comply with the applicable laws from each country where their data is collected, processed, or stored. The other options are secondary factors.

14. What should be the next step for the board of directors when noticing new regulations impacting some of the organization's processes?

A. Instruct the information security department for specific controls.

B. Evaluate various solutions to address the new regulations.

C. Require management to report on compliance.

D. Evaluate the cost of implementing new controls.

Answer: C. Require management to report on compliance.

Explanation: The board of directors has oversight responsibilities, and they should monitor compliance. The board would not be directly involved in evaluating various alternatives and the cost of implementation. Also, the board will not directly instruct the information security department.

15. Which of the following factors is the most difficult to estimate?

A. Vulnerabilities in the system.

B. Legal and regulatory requirements.

C. Compliance timelines.

D. The threat landscape.

Answer: D. The threat landscape.

Explanation: A *threat* is something that *exploits* a vulnerability. Threat factors are not in the control of the organization. Examples of threat factors are hackers, fires, earthquakes, changes in the regulatory environment, and more. All of these factors are difficult to estimate and control. Other options are not as difficult to estimate as the threat landscape.

16. Which of the following is the risk that is likely to be most ignored during an onsite inspection of an offshore service provider?

A. Cultural differences.

B. Security controls.

C. The network security.

D. The documented IT policy.

Answer: A. Cultural differences.

Explanation: Cultural differences and their impact on data security are generally not considered during security reviews. Different cultures have different perspectives on what information is considered sensitive and how it should be handled. This cultural practice may not be consistent with the organization's requirements.

17. What does an organization's risk appetite mostly depend on?

A. The threat landscape.

B. The size of the information security team.

C. The security strategy.

D. The organization's culture.

Answer: D. The organization's culture.

Explanation: The culture of the organization determines the risk appetite of the organization. Pro-risk organizations generally tend to have more of a risk appetite as compared to risk-averse organizations. Other options do not directly impact the risk appetite.

18. What factor has the greatest impact on the security strategy?

A. IT technology.

B. System vulnerabilities.

C. Network bandwidth.

D. Organizational goals.

Answer: D. Organizational goals.

Explanation: The prime objective of a security strategy is to facilitate and support organizational goals. The other options are secondary factors.

19. What is the most important consideration for designing a security policy for a multi-national organization operating in different countries?

A. The cost of implementation.

B. The level of security awareness of the employees.

C. The culture of the different countries.

D. The capability of the security tools.

Answer: C. The culture of the different countries.

Explanation: Culture plays an important role for designing security policies. Different countries have different cultures and these impact their local legal requirements. The organization needs to ensure that the local laws of all the countries are appropriately addressed. Other options are not as significant as the local culture.

20. What should the next step be for the information security manager when noticing new regulations impacting some of the organization's processes?

A. To identify whether the current controls are adequate.

B. To update the audit department about the new regulations.

C. To present a business case to senior management.

D. To implement the requirements of new regulations.

Answer: A. To identify whether the current controls are adequate.

Explanation: The first step is to analyze and identify whether current controls are adequate. If current practice already adheres to the regulations, then there is no need to implement further controls.

21. What is the most important factor that determines the acceptable level of organizational standards?

A. The current level of vulnerability.

B. The risk appetite of the organization.

C. IT policies and processes.

D. The documented strategy.

Answer: B. The risk appetite of the organization.

Explanation: The risk appetite is the level of willingness of the organization to take risks. It sets the boundary of acceptable risks. This would determine the acceptable limit for the organizational standards. The other options do not directly impact the acceptable level of organizational standards.

22. What is the most important factor for promoting a positive information security culture?

    A. Monitoring by an audit committee.

    B. High budgets for security initiatives.

    C. Collaboration across business lines.

    D. Frequent information security audits.

    Answer: C. Collaboration across business lines.

    Explanation: Collaboration across business lines is of utmost importance to promote a positive information security culture. This will ensure collective efforts toward common security goals. The other options are not as significant as collaboration across business lines.

Obtaining commitment from senior management

For the effective implementation of security governance, support and commitment from **senior management** is the most important prerequisite. A lack of high-level sponsorship will have an adverse impact on the effectiveness of security projects.

It is very important for the information security manager to gain support from senior management. The most effective way to gain this is to ensure that the security program continues to be aligned with and supports the business objectives. This is critical in gaining management support. Senior management is more concerned with the achievement of business objectives and will be keen to address all the risks impacting them.

Obtaining commitment from senior management is very important to ensure appropriate investment in information security, as we'll cover in the next section.

Information security investment

Investment should be able to provide value to the business. The primary driver for investment in an information security project is **value analysis** and a sound **business case**. To obtain approval for an information security budget, the budget should primarily include a **cost-benefit analysis**. Senior management is more interested in the benefit that is derived from the budget.

For example, as a security manager, if you request a budget of $5,000 for security investment, the senior management may not be convinced. But if you also project annualized savings of $10,000 against an investment of $5,000, the senior management may be more willing to invest.

Strategic alignment

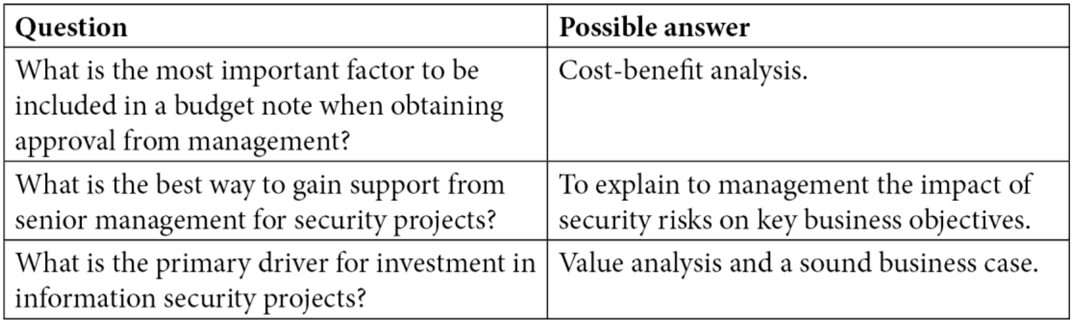
Information security activities are said to have a **strategic alignment** when it supports the requirements of key business stakeholders. Information security should support the achievement of organizational objectives by minimizing business disruptions. The most effective way to enhance the senior management's commitment toward information security is to conduct a periodic review of the alignment between security and business goals. A discussion with key business stakeholders will give a correct picture of the alignment of security programs with business objectives.

A survey of the organization's management is the best way to determine whether the security programs support business objectives. Achieving strategic alignment means business process owners and managers believe that information security is effectively supporting their goals. If business management is not confident in the security programs, the information security manager should redesign the processes to provide value to the business.

Another aspect of determining the strategic alignment is to review the business **balanced scorecard**. A business scorecard contains important metrics from a business perspective. It will help to determine the alignment of the security goals with the business goals.

Key aspects from the CISM exam perspective

The following are some of the key aspects from the CISM exam perspective:



Question	Possible answer
What is the most important factor to be included in a budget note when obtaining approval from management?	Cost-benefit analysis.
What is the best way to gain support from senior management for security projects?	To explain to management the impact of security risks on key business objectives.
What is the primary driver for investment in information security projects?	Value analysis and a sound business case.

Table 1.6 – Key aspects from the CISM exam perspective

Questions

1. To obtain approval for information security budgets, what should a budget primarily include?

   A. A cost-benefit analysis.

   B. Industry benchmarks.

   C. The total cost of ownership.

   D. All the resources required by business units.

   Answer: A. A cost-benefit analysis.

   Explanation: Senior management is more interested in the overall business benefit derived from the security budget. The other options are important considerations when evaluating and approving budgets, but the most important factor is the cost-benefit analysis.

2. What should senior management do to support information security?

   A. Evaluate the latest security products.

   B. Conduct risk assessments

   C. Approve policy statements and funding.

   D. Mandate information security audits.

   Answer: C. Approve policy statements and funding.

Explanation: Policy statements contain the intent and direction of the management. Senior management should approve policy statements and provide sufficient budgets to achieve the organization's information security objectives. The management may be involved in evaluating products and risk assessment and mandating information security audits, but their primary role is to provide direction, oversight, and governance.

3. When are information security activities are said to have strategic alignment?

   A. When they support the requirements of key business stakeholders.

   B. When they support the requirements of the IT team.

   C. When they support the requirements of globally accepted standards

   D. When they provide reliable and cost-effective services.

   Answer: A. When they support the requirements of key business stakeholders.

   Explanation: Information security should support the achievement of organizational objectives by minimizing business disruptions. When information security supports the requirements of key business units, there is alignment. The IT department is one of the stakeholders. The other options are secondary factors.

4. What is the best way to gain support from senior management?

   A. To provide examples of security breaches in other organizations.

   B. To provide details of technical risks applicable to the organization.

   C. To showcase industry best practices.

   D. To explain the impact of security risks on key business objectives.

   Answer: D. To explain the impact of security risks on key business objectives.

   Explanation: Senior management is more concerned about the achievement of business objectives and will be keen to address all the risks impacting these. The other options will not be as effective as mapping security risks to key business objectives.

5. How can support from senior management be obtained for implementing a new project?

   A. Conducting risk assessments.

   B. Explaining regulatory requirements.

   C. Developing a business case.

   D. Selecting the latest technology.

Answer: C. Developing a business case.

Explanation: The business case contains the need and justification for the project. It will be the most important document to gain support from senior management. The other options will not be as effective as the business case.

6. What is the most effective way to enhance the commitment from senior management toward information security?

A. To have security policies approved by the CEO.

B. To conduct frequent security awareness training.

C. To conduct periodic reviews of the alignment between security and business goals.

D. To conduct periodic information security audits

Answer: C. To conduct periodic reviews of the alignment between security and business goals.

Explanation: The most effective way to enhance the commitment from senior management toward information security is to ensure that the security program continues to be aligned with and support the business objectives. This is critical to management support. The other options will not have as much of an effect on management as ensuring alignment with the business goals.

7. What is the most effective way to justify the information security budget?

A. To consider the number of security breaches.

B. To consider the expected annual loss.

C. To consider a cost-benefit analysis.

D. To consider industry benchmarks.

Answer: C. To consider a cost-benefit analysis.

Explanation: The most effective way to justify the budget is to consider a cost-benefit analysis. Other options may be considered when conducting a cost-benefit analysis.

8. What best indicates commitment from senior management toward security programs?

A. Their involvement in the asset risk assessment.

B. Their review and approval of the risk management methodology.

C. Their review and approval of residual risks.

D. Their review and approval of inherent risks.

Answer: B. Their review and approval of the risk management methodology.

Explanation: The involvement of senior management in the review of the risk management methodology is the best indicator that management support and are committed to effective information security. The other options do show some level of management support and commitment, but not as much as option *B*.

9. What is the most effective justification to gain support from senior management for security investment?

A. The reduction in the security budget.

B. The adherence to regulatory requirements.

C. The protection of information assets.

D. The enhanced business value.

Answer: D. The enhanced business value.

Explanation: The objective of security investments is to increase the business value by addressing instances of business disruptions, thereby reducing losses and improving productivity. The protection of information assets is one of the elements of enhanced business value.

10. Who is most likely to sponsor the security steering committee?

A. The chief audit officer.

B. The information security manager.

C. The chief operating officer.

D. The head of legal.

Answer: C. The chief operating officer.

Explanation: The steering committee should be sponsored by an authority who is well versed in the business objectives and strategy. The COO has the most knowledge of the business operations and objectives. The COO is in the best position to align the security strategy with the business objectives.

11. What is the best driver for investment in information security projects?

    A. An information security audit report.

    B. Value analysis.

    C. The business environment.

    D. Penetration test reports.

    Answer: B. Value analysis.

    Explanation: Investment in security should be able to provide value to the business. The primary driver for investment in information security projects is value analysis and a sound business case. The other options are secondary factors.

12. What is the most important prerequisite for implementing the information security program?

    A. Senior management commitment.

    B. A documented framework.

    C. A documented policy.

    D. Frequent security awareness training.

    Answer: A. Senior management commitment.

    Explanation: The support and commitment from senior management is the most important prerequisite. Without that, the other options may not add value to the information security program.

13. Who is the best person to approve the information security governance plan?

    A. The system auditor.

    B. The security manager.

    C. The steering committee.

    D. The system administrator.

    Answer: C. The steering committee.

    Explanation: The steering committee consists of senior officials from different departments. They are well versed in the business objectives and strategy. They can ensure that the security governance is aligned with the business strategy and objectives.

14. What is the best method to change an organization's security culture?

    A. Stringent penalties for non-compliance.

    B. Obtaining strong management support.

    C. Implement strong security controls.

    D. Conducting frequent system audits.

    Answer: B. Obtaining strong management support.

    Explanation: The intention and support from senior management is of utmost importance in changing an organization's security culture. In the absence of support from management, the other options will not add value.

15. Which of the following will have the most adverse impact on the effective implementation of security governance?

    A. A complex organizational environment.

    B. A limited budget for information security.

    C. Improper business priorities.

    D. A lack of high-level sponsorship.

    Answer: D. A lack of high-level sponsorship.

    Explanation: A lack of high-level sponsorship means a lack of commitment and support from senior management. Support from senior management is a prerequisite for effective security governance. With high-level sponsorship, budget constraints and business priorities can be set right.

16. What is the best method to measure the strategic alignment of an information security program?

    A. To survey the business stakeholders.

    B. To conduct frequent audits.

    C. To analyze incident trends.

    D. To evaluate the business case.

    Answer: A. To survey the business stakeholders.

Explanation: Discussion with key business stakeholders will give a correct picture about the alignment of security programs to support business objectives. Incident trends will help us to understand the effectiveness of security programs but not directly about their alignment. A business case is prepared at the time of initiation of the project and a discussion with the business owner will help us to understand whether alignment, as indicated in the business case, is being adhered to.

17. What is the most important factor that affects the successful implementation of the information security program?

A. Support from senior management.

B. The level of the security budget.

C. The team size of the security team.

D. Regular information system audits.

Answer: A. Support from senior management.

Explanation: The most important factor that affects the successful implementation of an organization's information security program is the support and commitment from senior management. The other options are secondary factors. Without appropriate support, it will be difficult to achieve the desired objective of a security program.

18. What is the most effective method for achieving strategic alignment?

A. Periodically surveying the management.

B. Employing an industry-accepted governance framework.

C. Conducting frequent audits.

D. Developing enterprise risk management processes.

Answer: A. Periodically surveying the management.

Explanation: A survey of the management is the best way to determine whether security supports the business objectives. Achieving strategic alignment means the business process owners and managers believe that information security is effectively supporting their goals. If business management is not confident in security programs, the information security manager should redesign the process to provide value to the business. The other options do not directly indicate the strategic alignment.

19. What is the objective of aligning information security governance with corporate governance?

    A. To ensure that the security team understands the business objectives.

    B. To comply with regulations.

    C. To maximize the cost-effectiveness of the control.

    D. To reduce the number of rules required for governance.

    Answer: C. To maximize the cost-effectiveness of the control.

    Explanation: The alignment ensures that assurance functions are integrated to maximize the cost-effectiveness. A lack of alignment can result in potentially duplicate or contradictory controls, which negatively impacts cost-effectiveness. The others are secondary factors.

20. What is the best method for addressing the concerns of senior management about the effectiveness of the existing information security program?

    A. Redesign the program based on industry-recognized standards.

    B. Analyze the cost-benefit of the existing program.

    C. Discuss with senior management to understand their concerns.

    D. Show an approved business case to senior management.

    Answer: C. Discuss with senior management to understand their concerns.

    Explanation: The best method to address the concerns of senior management is to first discuss their concerns to better understand them. Following this, the security program can be redesigned to be more valuable to senior management.

21. What is the most effective method for obtaining a commitment from senior management for the implementation of the security program?

    A. Discuss industry best practices with senior management.

    B. Discuss various risk scenarios with the process owners.

    C. Discuss a cost-benefit analysis with senior management.

    D. Discuss the relationship between the security program and the business goals.

    Answer: D. Discuss the relationship between the security program and the business goals.

    Explanation: Senior management is keen to protect and achieve the business goals and objectives. If they see value in the project in terms of business support, there will not be any reluctance. The other options can be secondary factors.

22. What is the most effective method for obtaining a commitment from senior management for the implementation of the security program?

    A. Demonstrate the success of industry peers.

    B. Demonstrate the potential loss and other negative impacts due to lack of support.

    C. Demonstrate regulatory requirements related to security.

    D. Demonstrate support for the desired outcome.

    Answer: D. Demonstrate support for the desired outcome.

    Explanation: Demonstrating the support for the desired outcome is the best approach. This can be done by demonstrating improvement in performance metrics related to business objectives. Senior management is keen to protect and achieve the business goals and objectives. The other options are secondary factors.

23. What factor has the most influence on the success of an information security strategy?

    A. Its approval from the chief information officer.

    B. Its alignment with the IT plan.

    C. Its alignment with the goals set by the board of directors.

    D. If it is measured by key performance indicators.

    Answer: C. Its alignment with the goals set by the board of directors.

    Explanation: The security strategy is said to be successful if it supports the achievement of goals set up by the board of directors. The other options do not directly influence whether the security program is successful.

Introducing the business case and the feasibility study

A **business case** is a justification for a proposed project. The business case is prepared to justify the effort and investment in a proposed project. It captures the reasoning for initiating a project or task. Generally, the business case is the precursor to the start of the project.

The business case is a key element in decision-making for any project. The proposed **returns on investments** (**ROIs**), along with any other expected benefits, are the most important consideration for decision-making in any new project.

The first step of developing a business case is to define the need and justification of the problem.

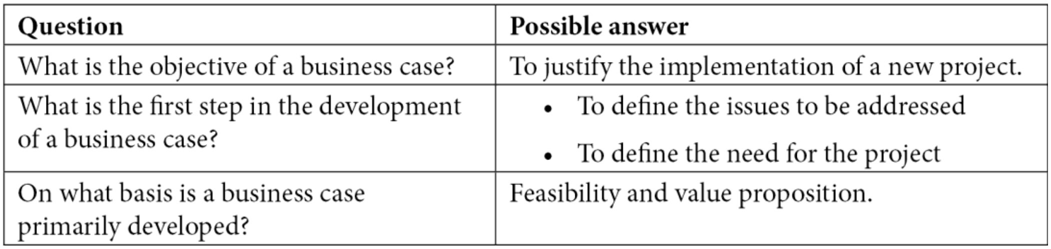
Feasibility analysis

A **feasibility study** is an analysis that takes various factors into account, including economic, technical, and legal factors, to ascertain the likelihood of completing the project successfully.

The feasibility study should consider how the project will impact the organization in terms of risks, costs, and benefits. It helps to assess whether a solution is practical and achievable within the established budgets and schedule requirements.

Key aspects from the CISM exam perspective

The following are some of the key aspects from the CISM exam perspective:



Question	**Possible answer**
What is the objective of a business case?	To justify the implementation of a new project.
What is the first step in the development of a business case?	• To define the issues to be addressed • To define the need for the project
On what basis is a business case primarily developed?	Feasibility and value proposition.

Table 1.7 – Key aspects from the CISM exam perspective

Questions

1. What should a business case primarily include?

    A. An appropriate justification.

    B. Results of a gap analysis.

    C. Legal requirements.

    D. Expected annual loss.

    Answer: A. An appropriate justification.

    Explanation: The objective of a business case is to justify the implementation of a new project. Its justification can be either the results of a gap analysis, legal requirements, the expected annual loss, or any other reason.

2. What is the first step of developing a business case?

   A. To determine the budget.

   B. To determine the vendor.

   C. To define the need.

   D. To determine the cost-efficiency.

   Answer: C. To define the need.

   Explanation: Without defining the need for the new project, the other options of the business case cannot be evaluated and determined. The first step of developing a business case is to define the need and the justification of the project.

3. For implementing a new project, support from senior management can be obtained by which of the following?

   A. Conducting a risk assessment.

   B. Explaining regulatory requirements.

   C. Developing a business case.

   D. Selecting the latest technology.

   Answer: C. Developing a business case.

   Explanation: The business case contains the need and justification for the project. It will be the most important document to gain support from senior management. The other options will not be as effective as the business case.

4. What are the main criteria for selecting a security technology?

   A. The technology can mitigate the risk.

   B. The technology is widely accepted in industry.

   C. It is the latest available technology.

   D. The technology provides benefits in comparison to its costs.

   Answer: D. The technology provides benefits in comparison to its costs.

   Explanation: The technology should provide benefits by mitigating risks and at the same time should be cost-efficient. The technology should be effective as well as efficient. If the technology is not cost-effective, then it will not be meaningful, even if it mitigates the risk.

5. Which of the following is the lowest concern for information security managers?

   A. Technical requirements.

   B. Regulatory requirements.

   C. Privacy requirements.

   D. Business requirements.

   Answer: A. Technical requirements.

   Explanation: Business requirements are the most important aspect for an information security manager, followed by privacy and other regulatory requirements. The other options (regulatory requirements, business requirements, and privacy requirements) are more important for a security manager as compared to technical requirements.

6. What is the most effective report while proposing the implementation of a new security solution?

   A. A vendor evaluation report.

   B. A risk analysis report.

   C. A business case.

   D. A budget utilization report.

   Answer: C. A business case.

   Explanation: A business case contains the need and justification of the proposed project. It helps to illustrate the costs and benefits of the project. The other options can be considered as part of the information required in the business case.

7. What is the biggest challenge in preparing the business case for obtaining approval from senior management for new security projects?

   A. To make the senior management understand the technical aspects of security.

   B. To demonstrate values and benefits.

   C. To present various risk scenarios.

   D. To provide comparative data of the industry.

   Answer: B. To demonstrate values and benefits.

   Explanation: It is very important and challenging to include the values and benefits in a business case in such a way as to convince the senior management. Technical aspects are generally not covered in a business case. Risk scenarios and comparative data is used to demonstrate values and benefits.

8. What is the best way to obtain support from senior management for information security initiatives?

   A. Develop and present a business case.

   B. Present various risk scenarios.

   C. Demonstrate the financial benefit of the project.

   D. Align the security initiative to the organization's goals.

   Answer: A. Develop and present a business case.

   Explanation: All the options are important, but a significant aspect is developing and presenting a business case to demonstrate that the security initiative is aligned to the organization's goal and provides value to the organization. A business case includes all of the other options.

9. Which of the following is the first step for the development of a business case?

   A. To conduct an industry survey.

   B. To work out the ROI.

   C. To evaluate cost-effective alternatives.

   D. To define the issues to be addressed.

   Answer: D. To define the issues to be addressed.

   Explanation: The first step for the development of a business case is to understand the issues that need to be addressed. Without clear requirements being defined, the other options may not add value.

10. What is a business case primarily based on?

    A. Various risk scenarios.

    B. The predicted ROI.

    C. Organizational objectives.

    D. The feasibility and value proposition.

    Answer: D. The feasibility and value proposition.

    Explanation: The most important basis for developing a business case is the feasibility and value proposition. It helps to determine whether a project should be implemented. The feasibility and value proposition indicates whether the project will be able to address risk with effective ROIs and whether it will help to achieve organizational objectives.

11. What is the best way to address the reluctance of the senior management in providing a budget for new security initiatives?

    A. To develop and present a business case.

    B. To develop various risk scenarios.

    C. To let the user management take the initiative.

    D. To organize security awareness training for the senior management.

    Answer: A. To develop and present a business case.

    Explanation: A business case is the best way to present the link between a new security project and organization's business objectives. Senior management is keen to protect and achieve the business objectives. If they see value in the project in terms of business support, there will not be any reluctance. Risk scenarios should be considered as a part of the business case. The other options will not be effective to address their concerns.

12. The information security manager is evaluating two technologies to address a particular risk and is required to select one for implementation. What is the best approach for the security manager with a limited budget to choose between the two technologies?

    A. A risk assessment.

    B. A business impact analysis.

    C. An ROI prediction.

    D. A cost-benefit analysis.

    Answer: D. A cost-benefit analysis.

    Explanation: A cost-benefit analysis will be the best approach to inform a decision. Cost-benefit analyses indicate the cost of implementing the control and its expected benefits. The cost of a control should not exceed the benefit to be derived from it. A risk assessment is a step prior to the evaluation and implementation of a control. In security parlance, ROI is difficult to calculate, as returns are in terms of safety and security.

13. How is an information security program best justified?

    A. An impact analysis.

    B. A detailed business case.

    C. Industry benchmarks

    D. Acceptance by users.

Answer: B. A detailed business case.

Explanation: A business case is the justification for the implementation of the program. It contains a rationale for making an investment. It indicates the cost of the project and its expected benefits. The other options by themselves are not sufficient to justify the information security program. User acceptance may not always be reliable for a security program, as security and performance often clash.

14. What factor is most likely to persuade the management of the approval of a new information security budget?

A. A detailed risk assessment.

B. Risk treatment options.

C. A well-developed business case.

D. Calculating the future value of a current budget

Answer: C. A well-developed business case.

Explanation: A business case is the justification for the implementation of the security program. It contains a rationale for making an investment. It indicates the cost of the project and its expected benefits. The other options by themselves are not sufficient to justify the information security budget.

15. Which of the following is the most important thing to consider in the development of a business case?

A. Various risk scenarios.

B. Industry benchmarks.

C. Implementation benefits.

D. Affordability.

Answer: C. Implementation benefits.

Explanation: A business case is the justification for the implementation of the security program. It contains a rationale for making an investment. It indicates the cost of the project and its expected benefits. The other options by themselves are not sufficient to justify the information security budget.

Understanding information security governance metrics

A **metric** is a measurement of a process to determine how well the process is performing. Security-related metrics indicate how well the controls can mitigate the risks. For example, a **system uptime metric** helps us to understand whether a system is available to the user as per requirements.

The objective of metrics

On the basis of effective metrics, an organization evaluates and measures the achievement and performance of various processes and controls. The main objective of a metric is to help the management in decision-making. A metric should be able to provide relevant information to the recipient so that informed decisions can be made.

Technical metrics vis-à-vis governance-level metrics

Technical metrics help us to understand the functioning of technical controls such as IDS, firewalls, antivirus software, and more. They are useful for tactical operational management. However, these metrics have little value from a governance standpoint.

Management is more concerned about the overall security posture of the organization. Full audits and comprehensive risk assessments are a few of the activities that help the management to understand security from a governance perspective.

Characteristics of effective metrics

Good metrics should be **SMART**. That is, **specific**, **measurable**, **attainable**, **relevant**, and **timely**. Let's look at those in more detail:

- **Specific**: The metric should be specific, clear, and concise.
- **Measurable**: The metric should be measurable so that it can be compared over a period.
- **Attainable**: The metric should be realistic and achievable.
- **Relevant**: The metric should be linked to specific risks or controls.
- **Timely**: The metric should be able to be monitored on a timely basis.

Key aspects from the CISM exam perspective

The following are some of the key aspects from the CISM exam perspective:

Question	Possible answer
What is the prime objective of a metric?	Decision making (on the basis of effective metrics, organizations evaluate and measure the achievements and performance of various processes and controls. Effective metrics are primarily used for security-related decision making).

Table 1.8 – Key aspects from the CISM exam perspective

Questions

1. What should information security decisions be based on primarily?

   A. Market research.

   B. Predicative analysis.

   C. Industry standards.

   D. Effective metrics.

   Answer: D. Effective metrics.

   Explanation: Based on effective metrics, organizations evaluate and measure the achievements and performance of various processes and controls. Effective metrics are primarily used for security-related decision making. The other options are secondary factors.

2. Which of the following is considered to have the most important strategic value?

   A. A privileged access management process.

   B. Trends in incident occurrence.

   C. System downtime analysis.

   D. Results of penetration tests.

   Answer: B. Trends in incident occurrence.

   Explanation: Trends in incidents will be more valuable from a strategic perspective as they will indicate whether a security program is heading in the right direction or not. The other options are more of an operational metric.

3. What is the most important metric that indicates the organizational risk?

   A. The expected annual loss.

   B. The number of security incidents.

   C. The number of unplanned business interruptions.

   D. The number of open vulnerabilities.

   Answer: C. The number of unplanned business interruptions.

   Explanation: The number of unplanned business interruptions is the best indication to evaluate organizational risk by determining how much business may be lost due to interruptions. Annual loss expectancy is based on projections and does not indicate actual value. Security incidents and open vulnerabilities do not reveal impact.

4. What is the best method to determine the level of alignment of the security objectives with the business objectives?

   A. Interview the security manager.

   B. Review the capability maturity model.

   C. Review the risk assessment report.

   D. Review the business balanced scorecard.

   Answer: D. Review the business balanced scorecard.

   Explanation: Reviewing the business balanced scorecard will help to determine the alignment of the security goals with the business goals. The business scorecard contains important metrics from the business perspective. The other options do not address the alignment directly.

5. What is the most essential attribute for a metric?

   A. Metrics should be easy to implement.

   B. Metrics should be meaningful to the process owner.

   C. Metrics should be qualitative.

   D. Metrics should be able to support regulatory requirements.

   Answer: B. Metrics should be meaningful to the process owner.

Explanation: Metrics are a measurement used to evaluate and monitor a particular process. Metrics are most effective when they are meaningful to the person receiving the information. The process owner should be able to take appropriate action based on the metrics. Metrics can be either quantifiable or qualitative based on the nature of the process. Options *A* and *D* are important, but more significant is the ability of metrics to convey meaning.

6. What is the most important attribute of a **key risk indicator** (**KRI**)?

A. A KRI should be flexible and adaptable.

B. A KRI should be arrived at by consistent methodologies and practices.

C. A KRI should be easy to understand.

D. A KRI should be convenient for the process owner to use.

Answer: B. A KRI should be arrived at by consistent methodologies and practices.

Explanation: A KRI will be effective only if it is arrived at by consistent methodologies and practices. In the absence of this, the KRI will be meaningless as it cannot be compared over different periods of time and hence it may not be able to indicate actual risk. Other options are good attributes but do not provide a consistent approach to determine deviation over the period.

7. What is the best indicator to determine the effectiveness of the security strategy?

A. The strategy helps to improve the risk appetite of the organization.

B. The strategy helps to implement countermeasures for all the threats.

C. The strategy helps to minimize the annual losses.

D. The strategy helps to achieve the control objective.

Answer: D. The strategy helps to achieve the control objective.

Explanation: The control objectives are developed to achieve the acceptable level of risk. The strategy is effective if the control objectives are met. The other options may be part of the control objectives, but the effectiveness of the security strategy is best measured by evaluating the extent to which the overall control objectives are met.

8. The information security manager has been asked to implement a particular security standard. Which of the following is the most effective to monitor this?

   A. The key success factor.

   B. The key objective indicator.

   C. The key performance indicator.

   D. The key goal indicator.

   Answer: C. The key performance indicator.

   Explanation: The key performance indicator measures how well a process is performing compared to its expectations. The key success factor determines the most important aspects or issues to achieve the goal. The key objective indicator and key goal indicator define the objective set by the organization.

Summary

In this chapter, you have learned about the importance of assurance functions, that is, governance, risk, and compliance, and how their integration is key to effective and efficient information security management. You have also understood how organizations can use the maturity model to improve their processes. We discussed the importance of the commitment of senior management toward the security aspects of an organization.

Reading this chapter will have helped the CISM aspirant to get an overview of information security governance.

In our next topic, we will discuss the practical aspects of information security governance.

2

Practical Aspects of Information Security Governance

In this chapter, we will discuss practical aspects of information security governance and understand how governance impacts the success of security projects. You will learn about different aspects of what a *security strategy* is. You will also understand the role of an information security manager in supporting business objectives.

The following topics will be covered in this chapter:

- Information security strategy and plan
- Information security program
- Enterprise information security architecture
- Organization structure
- Record retention
- Awareness and education

Let's understand each one of these topics in detail.