packt

Certified Information Security Manager Exam Prep Guide

2ND EDITION

Gain the confidence to pass the CISM exam using test-oriented study material

HEMANG DOSHI

WITH FREE ONLINE CONTENT

FLASHCARDS PRACTICE QUESTIONS EXAM TIPS

Certified Information Security Manager Exam Prep Guide

Second Edition

Gain the confidence to pass the CISM exam using test-oriented study material

Hemang Doshi

BIRMINGHAM—MUMBAI

Certified Information Security Manager Exam Prep Guide

Second Edition

Author: Hemang Doshi

Reviewers: Zeshan Ahmad, Pushkar Nagle, Kartik Sharma, and Wei Tschang

Publishing Product Manager: Anindya Sil

Acquisitions Editor: Sneha Shinde

Development Editor: Shubhra Mayuri

Production Editor: Shantanu Zagade

Editorial Board: Vijin Boricha, Megan Carlisle, Elliot Dallow, Ketan Giri, Heather Gopsill, Akin Babu Joseph, Bridget Kenningham, Alex Mazonowicz, Monesh Mirpuri, Aaron Nash, Abhishek Rane, Ankita Thakur, Nitesh Thakur, and Jonathan Wray

First published: November 2021

Second edition: December 2022

Production reference: 1141222

ISBN 978-1-80461-063-3

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

Packt.com

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

Why subscribe?

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

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

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

Contributors

About the author

Hemang Doshi has more than 15 years of experience in the field of system audit, IT risk and compliance, internal audit, risk management, information security audit, third-party risk management, and operational risk management. He has authored several books for certification such as CISA, CRISC, CISM, DISA, and enterprise risk management.

About the reviewers

Zeshan Ahmad is a specialist in cybersecurity who has worked with Fortune 500 companies and clients across banking and finance, life sciences, telecom, and technology sectors on application security, project management, program design and maturity, risk management, and information security governance.

He presently works as a senior analyst for a Fortune 100 financial services company and is certified as a CISM, CISA and ISO 27001:2013 Lead Auditor.

Pushkar Nagle is an InfoSec professional with 12 years of experience, holding professional IT certifications including CISM, CISSP, CEH, and CCNA. Pushkar attained a Licentiate Diploma in Electronics from VJTI, a B.Engg. in Electronics from Mumbai University, and currently pursuing an M.Sc. in Cyber Security from the University of York. Pushkar has held several positions, including penetration tester, vulnerability manager, risk management advisor, and application security consultant. Pushkar has experience in handling large and complex penetration testing projects, providing risk advisory to businesses, and assisting organizations in vulnerability remediation.

Pushkar has managed 500+ onsite/offsite Web Application pentests, Mobile applications, Infrastructure, Build & Code reviews, and other risk-based security testing projects.

"I would like to thank my parents, Sanjay and Kavita, and my wife, Ashvini for their motivation and support."

– Pushkar

Kartik Sharma has over 18 years of experience in information technology. He holds certifications like CISSP, CISM, CRISC, CDPSE, and Security certifications from all major cloud providers like AWS, Google, Azure, Oracle, and Alibaba. He has contributed to the development of various certification exams for ISC2, AWS, and Adobe, by serving as a subject matter expert (SME). He is currently working as a Director, Solution Architect at Wiley. His areas of expertise include Cloud Technologies, Cloud Security, Information Security, Data Privacy, Marketing Technologies, Identity & Access Management, and Microservices.

He can be reached via LinkedIn at `https://www.linkedin.com/in/kartiksharma84`. You can find more about him at his personal site `http://www.kartiksharma.us`.

"I would like to thank my wife, Punima Sharma, for her support, understanding, and patience during the long hours of work. I would also like to thank my parents, siblings, and friends for their constant encouragement."

– Kartik

Wei Tschang has more than 20 years of experience spanning various information technology disciplines within the banking, legal, and manufacturing industries. He is a passionate member of the ISACA Community, serving as a board member in various leadership roles for his local ISACA chapter since 2013. He has received multiple volunteer awards for his contributions to the chapter. He presented at conferences on cybersecurity topics. Wei holds the following certifications: CISA, CISM, CGEIT, CISSP, CIPP, SSCP, and ABCP. Wei lives in New Jersey with his wife, daughter, and golden retriever.

Packt is searching for authors like you

If you are interested in becoming an author for Packt, please visit authors.`packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Table of Contents

Preface

Apart from being well-versed in fundamentals and advanced information security concepts, a candidate must be quick and accurate in solving questions to ace ISACA's **Certified Information Security Manager (CISM)** certification. This book covers all four domains of the CISM Review Manual and provides complete coverage of the exam content through comprehensive explanations of core concepts.

With this book, you will unlock access to a powerful exam-prep platform that includes interactive practice questions, exam tips, and flashcards. The platform perfectly complements the book and even lets you clarify your doubts directly with the author.

This blended learning approach of shoring up key concepts through the book and applying them to answer practice questions online is designed to help build your confidence in acing the CISM certification.

By the end of this book, you will have everything you need to succeed in your information security career and pass the CISM certification exam with this handy, on-the-job desktop reference guide.

Online Exam-Prep Tools

With this book, you will unlock unlimited access to our online exam-prep platform (*Figure 0.1*). This is your place to practice everything you have learned in the book.

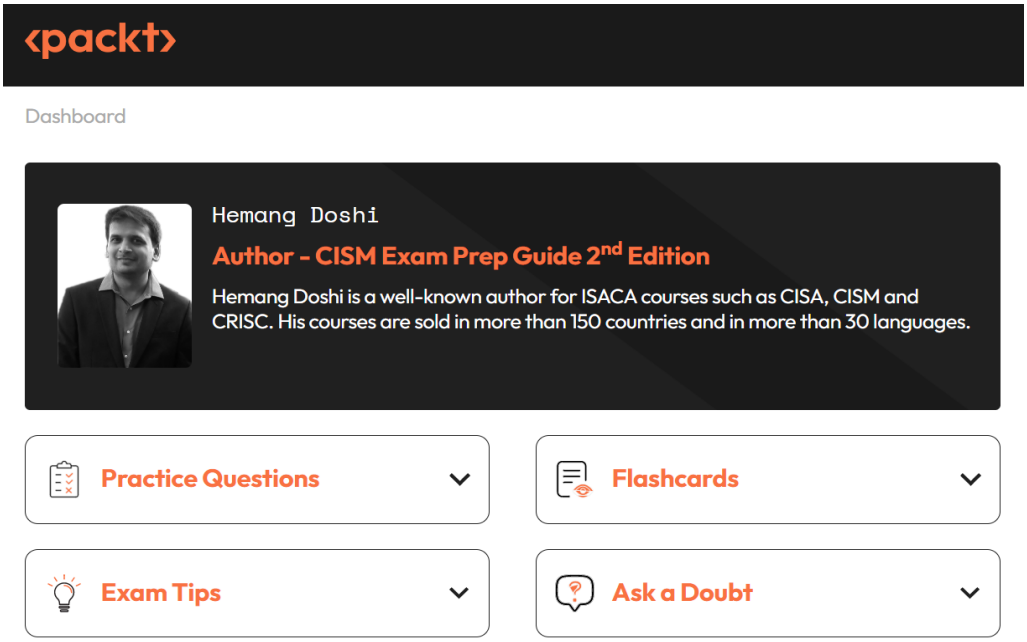

Figure 0.1: Online exam-prep platform

Sharpen your understanding of concepts with multiple sets of practice questions and interactive flashcards, accessible from all modern web browsers. If you get stuck, you can raise your concerns with the author directly through the website. Before doing that, make sure to go through the list of resolved doubts as well. These are based on questions asked by other users. Finally, go through the exam tips on the website to make sure you are well prepared.

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

This book is aligned with the *CISM Review Manual* (16th Edition; 2022) and encompasses the following topics:

Chapter 1: *Enterprise Governance* provides an overview of information security governance as a whole. It covers aspects such as the importance of information security governance, the role of organizational culture in information security, and security governance metrics.

Chapter 2: *Information Security Strategy* discusses information security strategy and highlights areas such as security strategy development, senior management's role in an organization's security strategy, and the security architecture.

Chapter 3: Information Risk Assessment covers the basic aspects of risk management and deals with the basic definition of risk and its components, risk identification, analysis and evaluation, and the security baseline.

Chapter 4: *Information Risk Response* covers the tools and techniques used for risk response: namely, risk avoidance, risk mitigation, risk transfer, and risk acceptance. The chapter also details change management and risk management integration with the project life cycle.

Chapter 5: *Information Security Program Development* explores the different procedures and techniques for developing an information security program and also deals with the information security program roadmap.

Chapter 6: *Information Security Program Management* discusses the basics of information security program management and covers information security program objectives, the security baseline, and security awareness and training.

Chapter 7: *Information Security Infrastructure and Architecture* defines information security architecture and explores how to implement it effectively.

Chapter 8: *Information Security Monitoring Tools and Techniques* emphasizes the importance of monitoring tools and techniques and introduces some of the most commonly used and most useful ones, such as intrusion detection systems, intrusion prevention systems, and firewalls.

Chapter 9: *Incident Management Readiness* sets out what it means to be ready for information security incidents. It covers aspects such as incident classification, business impact analysis, and insurance.

Chapter 10: *Incident Management Operations* covers the implementation of business continuity and disaster recovery processes and also deals with post-incident review practices.

How to Get the Most Out of This Book

This book is directly aligned with the *CISM Review Manual* (16th Edition; 2022) from ISACA. It is advisable to stick to the following steps when preparing for the CISM exam:

Step 1: Read this book from end to end.

Step 2: Go through ISACA's QAE book or database.

Step 3: Refer to ISACA's *CISM Review Manual*.

Step 4: Memorize key concepts using the flashcards on the website.

Step 5: Attempt the online practice question sets. Make a note of the concepts you are weak in, revisit those in the book, and re-attempt the practice questions.

Step 6: Keep repeating the practice question sets till you are able to answer all the questions in each practice set correctly within the time limit.

Step 7: Review exam tips on the website.

CISM aspirants will gain a lot of confidence if they approach their CISM preparation as per these mentioned steps.

Recorded Lectures

This book is also available in video lecture format along with 200+ exam-oriented practice questions on Udemy. Buyers of this book are entitled to 30% off on Hemang Doshi's recorded lectures. For a discount coupon, please write to `training@hemangdoshiacademy.in`.

Requirements for the Online Content

The online content includes interactive elements like practice questions, flashcards, and exam tips. For optimal experience, it is recommended that you use the latest version of a modern, desktop (or mobile) web browser such as Edge, Chrome, Safari, or Firefox.

Instructions for Unlocking the Online Content

To unlock the online content, you will need to create an account on our exam-prep website using the unique sign-up code provided in this book.

> **Where to find the sign-up code**
>
> You can find your unique sign-up code at the start of *Chapter 5, Information Security Program Development*.

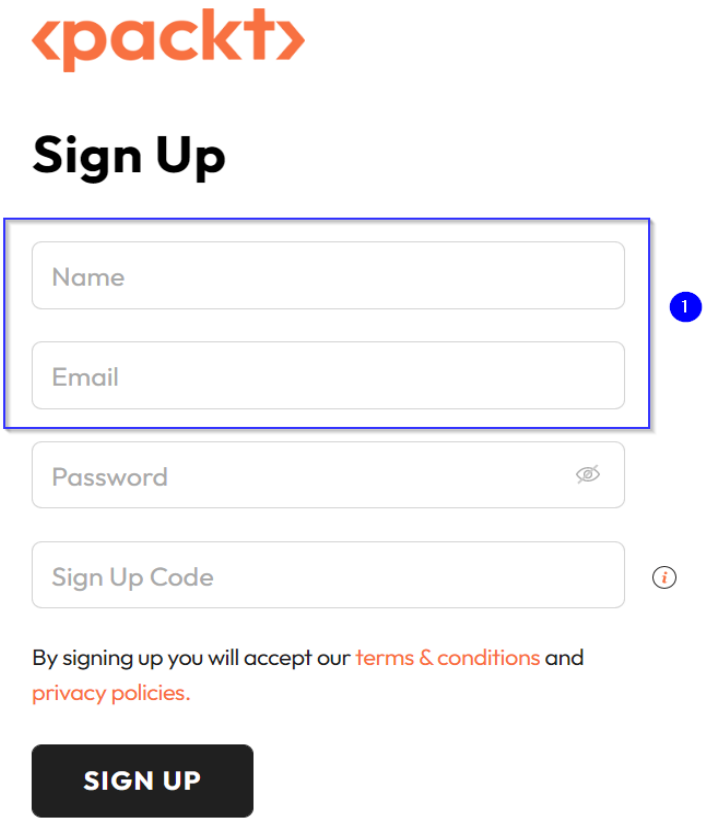

Figure 0.2: Enter your name and email address in the sign-up form

1. Create a strong alphanumeric password (**2**) (minimum 6 characters in length):

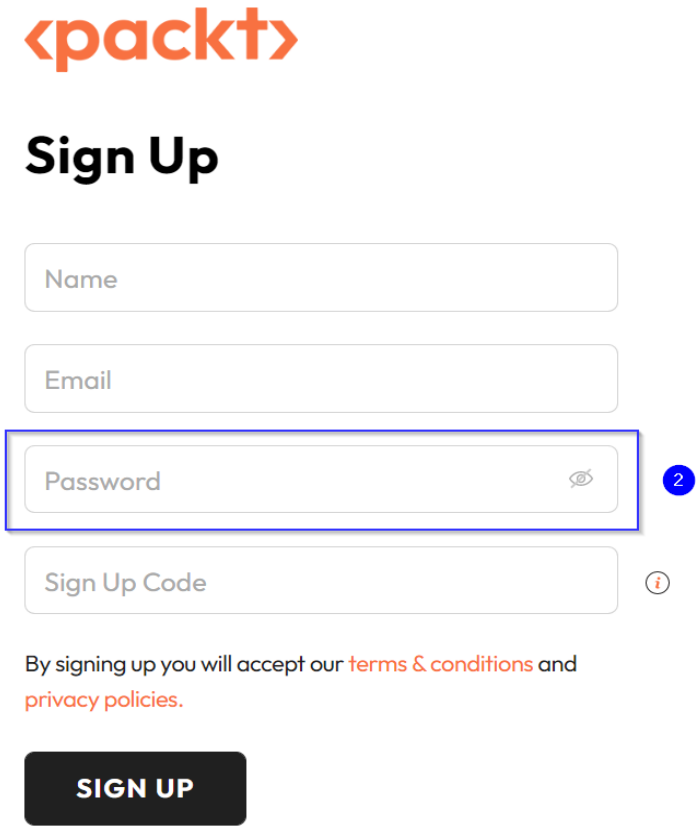

Figure 0.3: Create a strong password in the sign-up form

2. Enter the unique sign-up code (**3**). Once you have entered the code, click the `Sign Up` button.

> **Note**
> You only need to input the sign-up code once. After your account is created, you will be able to access the website from any device with only your email address and password.

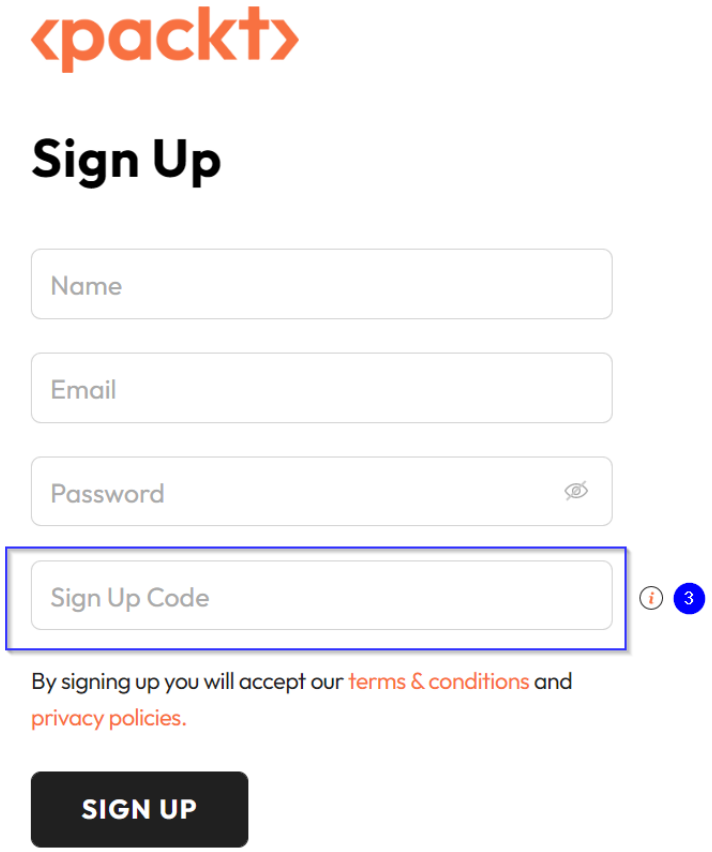

Figure 0.4: Enter the unique sign-up code

3. Upon a successful sign-up, you will be redirected to the dashboard (*see Figure 0.5*).

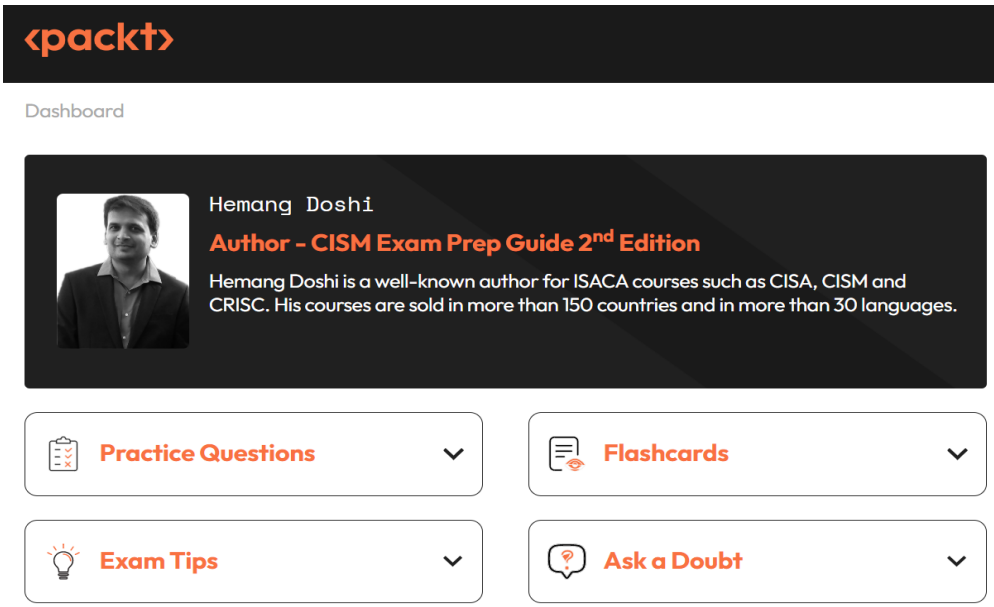

Figure 0.5: Online exam-prep platform dashboard

Going forward, you will simply need to login using your email address and password.

> **Note**
>
> If you are facing issues signing up, reach out to `customercare@packt.com`.

Quick Access to the Website

If you have successfully signed up, it is recommended that you bookmark this link for quick access to the website: `https://packt.link/cismexamguidewebsite`. Click the `Login` link on the top-right corner of the page to open the login page. Use the credentials you created in *Steps 2* and *3* of the *Instructions for Unlocking the Online Content* section above.

Alternatively, you can scan the following QR code to open the website:

Figure 0.6: QR Code for the CISM online exam-prep platform

CISM Syllabus – 2022

The CISM exam content was updated on June 1, 2022. There are minor changes in domain nomenclature and substantial changes in the weightage of each domain tested in the new exam. The following table presents the domains and their corresponding weightage:

Earlier Domains (Applicable up to May 31, 2022)	**Updated Domains (Applicable from June 1, 2022)**
Information Security Governance (24%)	Information Security Governance (17%)
Information Risk Management (30%)	Information Security Risk Management (20%)
Information Security Program Development and Management (27%)	Information Security Program (33%)
Information Security Incident Management (19%)	Incident Management (30%)

Figure 0.7: Previous and updated domains for CISM

Candidates who have based their studies so far on the previous weightings should take careful note of the changes and adjust their preparations accordingly.

The CISM exam contains 150 questions and covers the 4 information security management areas mentioned in the preceding table in *Figure 0.7*.

The following are the key topics that candidates will be tested on **starting from June 1, 2022**:

Number	Key Domains and Topics
1	**Information Security Governance**
A	Enterprise Governance
1A1	Organizational Culture
1A2	Legal, Regulatory, and Contractual Requirements
1A3	Organizational Structures, Roles, and Responsibilities
B	Information Security Strategy
1B1	Information Security Strategy Development
1B2	Information Governance Frameworks and Standards
1B3	Strategic Planning (e.g., budgets, resources, and business case)
2	**Information Security Risk Management**
A	Information Security Risk Assessment
2A1	Emerging Risk and Threat Landscape
2A2	Vulnerability and Control Deficiency Analysis
2A3	Risk Assessment and Analysis
B	Information Security Risk Response
2B1	Risk Treatment/Risk Response Options
2B2	Risk and Control Ownership
2B3	Risk Monitoring and Reporting
3	**Information Security Program**
A	Information Security Program Development
3A1	Information Security Program Resources (e.g., people, tools, and technologies)
3A2	Information Asset Identification and Classification
3A3	Industry Standards and Frameworks for Information Security
3A4	Information Security Policies, Procedures, and Guidelines

Number	Key Domains and Topics
3A5	Information Security Program Metrics
B	Information Security Program Management
3B1	Information Security Control Design and Selection
3B2	Information Security Control Implementation and Integrations
3B3	Information Security Control Testing and Evaluation
3B4	Information Security Awareness and Training/td>
3B5	Management of External Services (e.g., providers, suppliers, third parties, and fourth parties)
3B6	Information Security Program Communications and Reporting
4	**Incident Management**
A	Incident Management Readiness
4A1	Incident Response Plan
4A2	Business Impact Analysis (BIA)
4A3	Business Continuity Plan (BCP)
4A4	Disaster Recovery Plan (DRP)
4A5	Incident Classification/Categorization
4A6	Incident Management Training, Testing, and Evaluation
B	Incident Management Operations
4B1	Incident Management Tools and Techniques
4B2	Incident Investigation and Evaluation
4B3	Incident Containment Methods
4B4	Incident Response Communications (e.g., reporting, notification, and escalation)
4B5	Incident Eradication and Recovery
4B6	Post-Incident Review Practices

Figure 0.8: Key CISM topics

Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere? Is your eBook purchase not compatible with the device of your choice?

Don't worry, now with every Packt book you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, and on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there; you can get exclusive access to discounts, newsletters, and great free content in your inbox daily.

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below:

`https://packt.link/free-ebook/9781804610633`

2. Submit your proof of purchase.
3. That's it! We'll send your free PDF and other benefits to your email directly.

1
Enterprise Governance

Accessing the Online Content

With this book, you get unlimited access to web-based CISM exam prep tools which include practice questions, flashcards, exam tips, and more. To unlock the content, you'll need to create an account using your unique sign-up code provided with this book. Refer to the *Instructions for Unlocking the Online Content* section in the *Preface* on how to do that.

If you've already created your account using those instructions, visit this link `http://packt.link/cismexamguidewebsite` or scan the following QR code to quickly open the website. Once there, click the `Login` link in the top-right corner of the page to access the content using your credentials.

Governance is an important aspect of the **certified information security manager** (**CISM**) exam. In simple terms, governance means a set of policies, procedures, and standards used to monitor and control an activity. **Enterprise governance** refers to policies, procedures, and standards put in place to monitor an entire organization. **Information security governance** is a subset of overall enterprise governance, and its objective is to monitor and control activities related to information security.

In this chapter, you will gain an overview of information security governance and understand the impact of good governance on the effectiveness of information security projects.

You will learn about how organizational structure and culture impact information security governance and details about the various roles and responsibilities of the security function. You will also be introduced to the best practices for implementing information security governance.

This chapter will cover the following topics:

- Importance of Information Security Governance
- Organizational Culture
- Legal, Regulatory, and Contractual Requirements
- Retention of Business Records
- Organizational Structure
- Maturity Model
- Governance of Third-Party Relationships
- Information Security Governance Metrics

Importance of 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 in the form 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 its objectives, vision, mission and strategy, different function units, different product lines, hierarchy, and leadership structure. A review of organizational structure helps the security manager to understand the roles and responsibilities of information security governance, as discussed in the next section.

Information is one of the most important assets for any organization and its governance is mandated by various laws and regulations. For these reasons, information security governance is of critical importance.

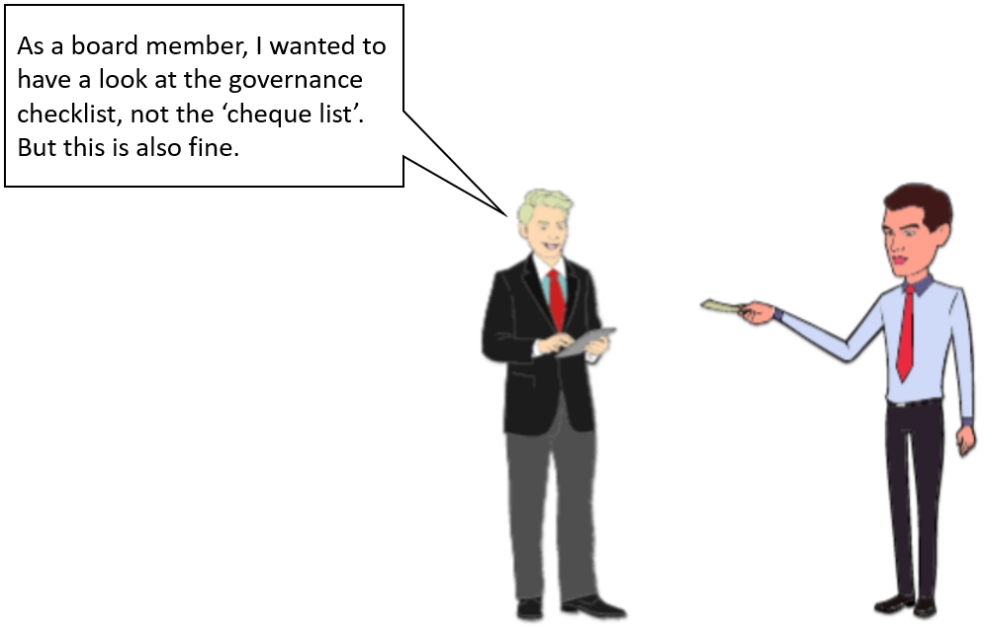

Figure 1.1: Information security governance

Desired Outcomes of Good Information Security Governance

A well-structured information security governance model aims to achieve the following outcomes:

- To ensure that security initiatives are aligned with the business strategy and that they 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

Responsibility for Information Security Governance

The responsibility for information security governance primarily resides with the board of directors, senior management, and the **steering committee**. They are required to make security an important part of governance by monitoring its key aspects. Information security governance is a subset of enterprise governance.

Senior management is responsible for ensuring that security aspects are integrated with business processes. The involvement of senior management and the steering committee in discussions and 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 of the organization's security environment.

Steps for Establishing Governance

Governance is effective if it is established in a structured manner. A CISM aspirant should understand the following steps for establishing security governance:

1. First, determine the objectives of the information security program. Most often, these objectives are derived from risk management and the acceptable level of risk that the organization is willing to take. For example, an objective for a bank may be that their system should always be available for customers – that is, there should be zero downtime. In this manner, information security objectives must align with and be guided by the organization's business objectives.
2. Next, the information security manager develops a strategy and a set of requirements based on these objectives. The security manager is required to conduct a gap analysis and identify the best strategy to move to the desired state of security from its current state of security. The desired state of security is also termed 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, security budget, and laws and regulations.

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

Governance Framework

A **governance framework** is a structure or outline that supports the implementation of information security strategies. It provides the best practices for a structured security program. Frameworks are flexible structures that any organization can adopt as per their environment and requirements. COBIT and ISO 27001 are both examples of widely accepted and implemented frameworks for security governance.

As 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. This ensures better integration between the two.

Top-Down and Bottom-Up Approaches

There are two possible approaches to governance: top-down and bottom-up.

In a top-down approach, policies, procedures, and goals are reviewed and approved by senior management, hence policies and procedures are directly aligned with business objectives.

A bottom-up approach may not directly address management priorities. In a bottom-up approach, operational level risks are given more importance.

Key Aspects from the CISM Exam Perspective

The following are some key aspects from the exam perspective:

Question	Possible Answer
Which approach (that is, top-down or bottom-up) is more effective for governance?	The effectiveness of governance is best ensured by a top-down approach. In a top-down approach, policies, procedures, and goals are set 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 are the most important aspects of an information security strategy from a senior management perspective?	Business priorities, objectives, and goals.
What is a governance framework?	A governance framework is a structure that provides the outline to support processes and methods.

Figure 1.2: Key aspects from the CISM exam perspective

A Note on the Practice Questions

Throughout this book, and within the CISM certification exam itself, more than one of the answers may address the problem posed by the question. For that reason, it is very important to carefully read the question and ensure you pick the answer that represents the most important element of the solution.

Please also note, as ISACA recommends only those with "technical expertise and experience in IS/IT security and control" seek CISM certification, that this book assumes some prior experience in the field. With that in mind, you will face some questions intended to test your expected pre-existing knowledge. Do not worry if you do not get these questions right the first time; full explanations are given after every question to help you fill any gaps in your understanding.

> **Note**
> You can find the answer key and explanations for all practice and revision questions for this chapter under the section *Chapter 1, Enterprise Governance* of the solution set titled *Answers to Practice Questions* located at the end of the book.

Practice Question Set 1

1. An information security manager has been asked to determine the effectiveness of the information security governance model. Which of the following will help them decide whether the information security governance model is effective?
   A. Security projects are discussed and approved by a steering committee
   B. Security training is mandatory for all executive-level employees
   C. Security training module is available on the intranet for all employees
   D. Patches are tested before deployment
2. An information security manager is reviewing the information security governance model. The information security governance model is primarily impacted by:
   A. The number of workstations
   B. The geographical spread of business units
   C. The complexity of the organizational structure
   D. The information security budget

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
4. Which of the following factors primarily drives information security governance?
   A. Technology requirements
   B. Compliance requirements
   C. The business strategy
   D. Financial constraints
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 information security projects
   D. To provide access to critical systems
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
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 derive from a globally accepted risk management framework
   C. be able to address regulatory compliance
   D. To promote a risk-aware culture

8. Effective governance is best indicated by:
   A. An approved security architecture
   B. Certification from an international body
   C. Frequent audits
   D. 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. Compliance-oriented approach
   D. 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
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 business functions
   D. To align with organizational goals
12. 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

13. 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
14. The security manager notices 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
15. 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
16. 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 processes
    C. To support operational processes
    D. To address operational risks
17. 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. Business objectives supporting the information security strategy
    D. Security guidelines supporting regulatory requirements

18. 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

Organizational Culture

The culture of an organization and its service provider is the most important factor that determines the implementation of an information security program. An organization's culture influences its **risk appetite**, that is, its 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 compared to a culture that is risk averse.

Figure 1.3: Organizational culture

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.

For some organizations, financial data is more important than privacy data. So, it is important to determine whether the culture of the service provider is aligned with the culture of the organization. Cultural differences and their impact on data security are generally not considered during security reviews.

Acceptable Usage Policy

An **acceptable usage policy** (**AUP**) generally includes rules for access controls, information classification, incident reporting requirements, confidentiality requirements, email, and internet usage requirements. All participants must understand which behaviors and acts are acceptable and which are not. This maintains a risk-aware culture.

A well-defined and documented AUP helps spread awareness about the dos and don'ts of information security.

It is essential that the AUP is conveyed to all users, and acknowledgment should be obtained from the users that they have read and understood the AUP. For new users, an AUP should be part of their induction training.

Ethics Training

The information security manager should also consider implementing periodic training on ethics. Ethical training includes emphasizing moral principles that govern a person's behavior or the conduct of an activity. It includes guidance on what the company considers legal and appropriate behavior.

Training on ethics is of utmost importance for employees engaged in sensitive activities, such as monitoring user activities or accessing sensitive personal data.

Some examples of unethical behavior include improper influence on other employees or service providers, use of corporate information or assets for private benefit, accepting gifts or bribes, and multiple employments.

Acknowledgment should be obtained from employees on understanding ethical behavior and the code of conduct and this should be retained as part of the employment records.

Practice Question Set 2

1. A newly appointed information security manager is reviewing the design and implementation of the information security program. Which of the following elements will have a major influence on the design and implementation of the information security program?

   A. Types of vulnerabilities

   B. The culture of the organization

   C. The business objectives

   D. The complexity of the business

2. Which of the following is the most important factor to consider while developing a control policy?

   A. Protecting data

   B. Protecting life

   C. Protecting the business's reputation

   D. Protecting the business objectives

3. Which of the following risks is most likely to be 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

4. 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

5. What factor has the greatest impact on the security strategy?
   A. IT technology
   B. System vulnerabilities
   C. Network bandwidth
   D. Organizational goals
6. What is the most important consideration when 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 cultures of the different countries
   D. The capability of the security tools
7. What is the most important factor in determining 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
8. 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

Legal, Regulatory, and Contractual Requirements

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.

Processes should be in place to scan all new regulations and determine their applicability 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 any new regulations. If not, further controls should be implemented to address the new regulations.

Departments affected by any new regulations are in the best position to determine the impact of new regulatory requirements on their processes, as well as the best ways to address them.

Key Aspects from the CISM Exam Perspective

The following are some key aspects from the exam perspective:

Question	Possible Answer
Who should determine the control processes for any new regulatory requirements?	The affected department (as they are in the best position to determine the impact of new regulatory requirements on their processes and the best way to address them)
What is the first step of an information security manager who notices a new regulation impacting one of the organization's processes?	To determine the processes and activities that may be impacted To assess whether existing controls meet the regulations
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

Figure 1.4: Key aspects from the CISM exam perspective

Practice Question Set 3

1. An information security steering committee has approved the implementation of a **bring your own device** (**BYOD**) policy for mobile devices. As an information security manager, what should your first step be?
   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
2. 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
3. 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
4. Which of the following should be the first step of an information security manager who notices a new regulation impacting one of the organization's processes?
   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

5. Privacy laws are mainly focused on which of the following?
   A. Big data analytics
   B. Corporate data
   C. Identity theft
   D. Identifiable personal data
6. The information security manager notices a regulation that impacts the handling of sensitive data. Which of the following should they do first?
   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.
7. The information security manager should address laws and regulations in which way?
   A. To the extent that they impact the organization
   B. To meet the certification standards
   C. To address the requirements of policies
   D. To reduce the cost of compliance
8. 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
9. What should be the next step for the board of directors when they notice new regulations are impacting some of the organization's processes?
   A. Instruct the information security department to implement 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

10. 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
11. What should the next step be for an information security manager upon 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

Retention of Business Records

The information security manager should ensure that an adequate **record retention policy** is in place and that this is followed throughout the organization. A record retention policy will specify what types of data and documents are required to be preserved, and what must be destroyed. It also specifies the number of years for which that data is required to be preserved.

Figure 1.5: Record retention

Record retention should primarily be based on the following two factors:

- Business requirements
- Legal requirements

If a record is required to be maintained for three years as per the business requirements, and for two years from a legal perspective, then it should be maintained for three years.

Organizations generally design their record retention policy in line with the relevant laws and regulations.

Electronic Discovery

Electronic discovery (e-discovery) is the process of the identification, collection, and submission of electronic records in a lawsuit or investigation. The best way to ensure the availability of electronic records is to implement comprehensive retention policies. A retention policy dictates the terms for storing, backing up, and accessing the records.

Key Aspects from the CISM Exam Perspective

The following are some key aspects from the exam perspective:

Question	Possible Answer
What is e-discovery?	E-discovery is the process of identifying, collecting, and submitting electronic records in a lawsuit or investigation.
What are the factors on which record retention is based?	Business requirements. Legal requirements. (If both options are available, then preference should be given to business requirements as it is generally assumed that business requirements already include consideration of legal requirements.)

Figure 1.6: Key aspects from the CISM exam perspective