

# ExamLabs

**Certified Information Security  
Manager  
Study Guide  
Exam CISM**

---

## CONTENTS AT A GLANCE

- Chapter 1**    Becoming a CISM
  - Chapter 2**    Information Security Governance
  - Chapter 3**    Information Risk Management
  - Chapter 4**    Information Security Program Development and Management
  - Chapter 5**    Information Security Incident Management
- Glossary
- Index

---

## CONTENTS

Acknowledgments

Introduction

### **Chapter 1** Becoming a CISM

Benefits of CISM Certification

Becoming a CISM Professional

Experience Requirements

ISACA Code of Professional Ethics

The Certification Exam

Exam Preparation

Before the Exam

Day of the Exam

After the Exam

Applying for CISM Certification

Retaining Your CISM Certification

Continuing Education

CPE Maintenance Fees

Revocation of Certification

Summary

### **Chapter 2** Information Security Governance

Introduction to Information Security Governance

Reason for Security Governance

Security Governance Activities and Results

Business Alignment

# ExamLabs

- Roles and Responsibilities
- Monitoring Responsibilities
- Information Security Governance Metrics
- The Security Balanced Scorecard
- Business Model for Information Security
- Security Strategy Development
  - Strategy Objectives
  - Control Frameworks
  - Risk Objectives
  - Strategy Resources
  - Strategy Development
  - Strategy Constraints
- Chapter Review
  - Notes
  - Questions
  - Answers

## **Chapter 3** Information Risk Management

- Risk Management Concepts
  - The Importance of Risk Management
  - Outcomes of Risk Management
  - Risk Management Technologies
- Implementing a Risk Management Program
  - Risk Management Strategy
  - Risk Management Frameworks
  - Risk Management Context
  - Gap Analyses
  - External Support
- The Risk Management Life Cycle
  - The Risk Management Process
  - Risk Management Methodologies
  - Asset Identification and Valuation
  - Asset Classification
  - Asset Valuation

# ExamLabs

- Threat Identification
- Vulnerability Identification
- Risk Identification
- Risk, Likelihood, and Impact
- Risk Analysis Techniques and Considerations
- Operational Risk Management
  - Risk Management Objectives
  - Risk Management and Business Continuity Planning
  - Third-Party Risk Management
  - The Risk Register
  - Integration of Risk Management into Other Processes
  - Risk Monitoring and Reporting
  - Key Risk Indicators
  - Training and Awareness
  - Risk Documentation
- Chapter Review
  - Notes
  - Questions
  - Answers

## **Chapter 4** Information Security Program Development and Management

- Information Security Programs
  - Outcomes
  - Charter
  - Scope
  - Information Security Management Frameworks
  - Defining a Road Map
  - Information Security Architecture
- Security Program Management
  - Security Governance
  - Risk Management

# ExamLabs

- The Risk Management Program
- The Risk Management Process
- Risk Treatment
- Audits and Reviews
- Policy Development
- Third-Party Risk Management
- Administrative Activities
- Security Program Operations
  - Event Monitoring
  - Vulnerability Management
  - Secure Engineering and Development
  - Network Protection
  - Endpoint Protection and Management
  - Identity and Access Management
  - Security Incident Management
  - Security Awareness Training
  - Managed Security Services Providers
  - Data Security
  - Business Continuity Planning
- IT Service Management
  - Service Desk
  - Incident Management
  - Problem Management
  - Change Management
  - Configuration Management
  - Release Management
  - Service-Level Management
  - Financial Management
  - Capacity Management
  - Service Continuity Management
  - Availability Management
  - Asset Management
- Controls
  - Control Classification

# ExamLabs

- Internal Control Objectives
- Information Systems Control Objectives
- General Computing Controls
- Control Frameworks
- Controls Development
- Control Assessment
- Metrics and Monitoring
  - Types of Metrics
  - Audiences
- Continuous Improvement
- Chapter Review
  - Notes
  - Questions
  - Answers

## **Chapter 5** Information Security Incident Management

- Security Incident Response Overview
  - Phases of Incident Response
- Incident Response Plan Development
  - Objectives
  - Maturity
  - Resources
  - Roles and Responsibilities
  - Gap Analysis
  - Plan Development
- Responding to Security Incidents
  - Detection
  - Initiation
  - Evaluation
  - Eradication
  - Recovery
  - Remediation
  - Closure
  - Post-incident Review

# ExamLabs

Business Continuity and Disaster Recovery Planning

Business Continuity Planning

Disaster Recovery Planning

Testing BC and DR Plans

Chapter Review

Notes

Questions

Answers

**Appendix** About the Download

System Requirements

Installing and Running Total Tester

About Total Tester

Technical Support

**Glossary**

**Index**



## Figure Credits

Figure 2-2 Adapted from The Business Model for Information Security, ISACA.

Figure 2-4 Adapted from The University of Southern California, Marshall School of Business, Institute for Critical Information Infrastructure Protection, USA.

Figure 2-5 Courtesy Xhienne: SWOT pt.svg, CC BY-SA 2.5, <https://commons.wikimedia.org/w/index.php?curid=2838770>.

Figure 2-6 Courtesy High Tech Security Solutions Magazine.

Figure 3-2 Source: National Institute for Standards and Technology.

Figure 4-1 Courtesy The Open Group.

Figure 4-9 Courtesy Bluefoxicy at [en.wikipedia.org](https://en.wikipedia.org).

Figure 5-3 Source: NASA.

## Purpose of This Book

Let's get the obvious out of the way: this is a comprehensive study guide for the security management professional who needs a serious reference for individual or group-led study for the Certified Information Security Manager (CISM) certification. The content in this book contains the technical information that CISM candidates are required to know. This book is one source of information to help you prepare for the CISM exam but should not be thought of as the ultimate collection of all the information and experience that ISACA expects qualified CISM candidates to possess. No one publication covers all of this information.

This book is also a reference for aspiring and practicing IT security managers and CISOs. The content that is required to pass the CISM exam is the same content that practicing security managers need to be familiar with in their day-to-day work. This book is an ideal CISM exam study guide as well as a desk reference for those who have already earned their CISM certification.

This book is also invaluable for information security professionals who are not in a leadership position today. You will gain considerable insight into today's information security management challenges. This book is also useful for IT and business management professionals who work with information security leaders and need to better understand what they are doing and why.

This book is an excellent guide for anyone exploring a security management career. The study chapters explain all the relevant technologies, techniques, and processes used to manage a modern information security program. This is useful if you are wondering what the security management profession is all about.

## How This Book Is Organized

This book is logically divided into four major sections:

- **Introduction** The “front matter” of the book and [Chapter 1](#) provide an overview of the CISM certification and the information security

# ExamLabs

management profession.

- **CISM study material** [Chapters 2](#) through [5](#) contain everything a studying CISM candidate is responsible for. This same material is a handy desk reference for aspiring and practicing information security managers.
- **Glossary** There are more than 550 terms used in the information security management profession.
- **Practice exams** Appendix explains the online CISM practice exam and Total Tester software accompanying this book.