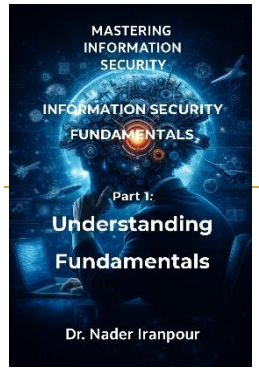
MASTERING INFORMATION SECURITY

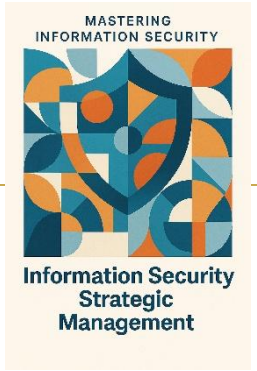
Six-Volume Series

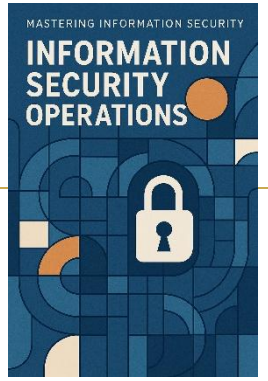
Dr. Nader Iranpour

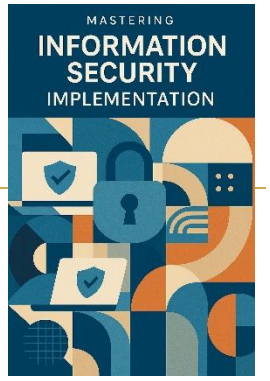
Mapping each chapter to the domains of 8 leading cybersecurity certifications

CISSP · CISM · CISA · CompTIA Security+ · ISO 27001 LI · CCSP · CEH · CRISC









How to Use This Document

This matrix maps every chapter of the Mastering Information Security six-volume series to the knowledge domains of eight leading cybersecurity certifications. It is designed to help readers, instructors, and certification candidates identify which chapters address which certification domains — and to demonstrate how the complete series, when finished, will serve as a comprehensive, unified reference for all eight credentials.

Important Notes:

- Volumes 1 & 2 are finalized and content-verified — coverage ratings are based on actual chapter content.
- Volumes 3–6 are structured templates — chapter topics are defined but content is not yet finalized. Coverage ratings are based on the chapter scope as declared in the series structure. Final verification will occur upon content completion.
- Coverage ratings use three levels: Full (●), Partial (◐), and Foundational (○). These indicate the depth at which a chapter addresses a certification domain.
- A chapter may appear under multiple certification domains when its subject matter spans multiple knowledge areas.
- The goal of the complete series is to provide a single, unified reference covering all domains of all eight certifications at depth.

Coverage Level Key

Symbol	Meaning	Description
●	**Full Coverage**	The chapter addresses this domain comprehensively as a primary subject.
◐	**Partial Coverage**	The chapter covers significant aspects of the domain as part of a broader scope.
○	**Foundational Coverage**	The chapter provides foundational context that supports understanding of the domain.

Series Overview

Vol.	Book Title	Chapters
Vol. 1	**Information Security Fundamentals** ✓ *Content Finalized*	Ch.1 The Essence of Information Security Ch.2 Information Security Principles Ch.3 Information Security Management Ch.4 Information Security Ecosystem Ch.5 Information Security Implementation
Vol. 2	**Blueprint of Security Excellence** ✓ *Content Finalized*	Ch.1 Information Security Guidance Ch.2 Information Security Frameworks Ch.3 Information Security Standards & Regulations Ch.4 Vendors' Best Practices & Real-World Application
Vol. 3	**Information Security Strategic Management** ○ *Template — Content Pending*	Ch.1 Risk Management Ch.2 Information Security Strategic Plan Ch.3 Information Security Architecture Ch.4 Information Security Governance Ch.5 Information Security Policies and Procedures Ch.6 Compliance, Legal and Regulatory Requirements Ch.7 Information Security Metrics
Vol. 4	**Information Security Engineering** ○ *Template — Content Pending*	Ch.1 Data Security Ch.2 Software Security Ch.3 Endpoint Security Ch.4 Wireless & Mobile Security Ch.5 Network Security Ch.6 Physical Security Ch.7 Human Resource Security & Privacy Management Ch.8 Industrial Systems Security Ch.9 Virtualization & Cloud Security Ch.10 DevSecOps, Secure Supply Chain & 3rd Party Risk
Vol. 5	**Information Security Operations** ○ *Template — Content Pending*	Ch.1 Cryptography Ch.2 Identity and Access Management Ch.3 Business Continuity and Disaster Recovery Ch.4 Incident Management Ch.5 Digital Forensics Ch.6 Logging and Monitoring Ch.7 Configuration & Change Management Ch.8 Patch Management Ch.9 Security Awareness Ch.10 Security Audit, Compliance and Assessment
Vol. 6	**Information Security Implementation** ○ *Template — Content Pending*	Ch.1 Methodology Overview Ch.2 Phase 1: Initiate Ch.3 Phase 2: Implement Ch.4 Phase 3: Intelligence Ch.5 Phase 4: Improve

Master Coverage Summary

The table below shows how many domains of each certification are addressed by each volume, and the total coverage across the complete six-volume series. A value of 100% indicates that every domain of that certification is covered by at least one chapter in the series.

Certification	Total Domains	Vol.1	Vol.2	Vol.3	Vol.4	Vol.5	Vol.6	Series Coverage
CISSP	8	4/8	3/8	4/8	4/8	4/8	4/8	**100%**
CISM	4	2/4	3/4	3/4	—	2/4	4/4	**100%**
CISA	5	2/5	2/5	2/5	2/5	3/5	3/5	**100%**
CompTIA Security+	5	4/5	1/5	3/5	2/5	2/5	2/5	**100%**
ISO 27001 LI	7	1/7	2/7	6/7	1/7	2/7	7/7	**100%**
CCSP	6	1/6	2/6	1/6	5/6	3/6	2/6	**100%**
CEH	20	1/20	—	1/20	17/20	12/20	—	**100%**
CRISC	4	1/4	2/4	3/4	1/4	1/4	2/4	**100%**

Note: Series Coverage = 100% for all certifications, as it is the design intent of this series that — upon completion of all six volumes — every knowledge domain of every mapped certification will be addressed in depth.

CISSP

Certified Information Systems Security Professional (ISC²)

8 Knowledge Domains

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
Security and Risk Management	● Ch.1: The Essence of Information Security ○ Ch.2: Information Security Principles ○ Ch.3: Information Security Management	◐ Ch.1: Information Security Guidance ◐ Ch.2: Information Security Frameworks	◐ Ch.1: Risk Management ◐ Ch.2: Information Security Strategic Plan ◐ Ch.4: Information Security Governance ◐ Ch.5: Information Security Policies and Procedures ◐ Ch.6: Compliance, Legal and Regulatory Requirements	—	—	◐ Ch.2: Phase 1: Initiate
Asset Security	● Ch.1: The Essence of Information Security ○ Ch.4: Information Security Ecosystem	—	◐ Ch.1: Risk Management	◐ Ch.1: Data Security ◐ Ch.7: Human Resource Security & Privacy Management	—	—
Security Architecture and Engineering	● Ch.4: Information Security Ecosystem	◐ Ch.2: Information Security Frameworks ◐ Ch.3: Information Security Standards & Regulations	◐ Ch.3: Information Security Architecture	◐ Ch.5: Network Security ◐ Ch.8: Industrial Systems Security ◐ Ch.9: Virtualization & Cloud Security	—	◐ Ch.3: Phase 2: Implement
Communication and Network Security	—	—	—	● Ch.4: Wireless & Mobile Security ● Ch.5: Network Security	◐ Ch.1: Cryptography	—
Identity and Access Management (IAM)	● Ch.2: Information Security Principles	—	—	—	● Ch.2: Identity and Access Management	—
Security Assessment and Testing	—	● Ch.1: Information Security Guidance ◐ Ch.2: Information Security Frameworks	◐ Ch.7: Information Security Metrics	—	◐ Ch.10: Security Audit, Compliance and Assessment	◐ Ch.4: Phase 3: Intelligence
Security Operations	—	—	—	—	● Ch.4: Incident Management ◐ Ch.5: Digital Forensics ◐ Ch.6: Logging and Monitoring ◐ Ch.7: Configuration & Change Management ◐ Ch.8: Patch Management	◐ Ch.4: Phase 3: Intelligence
Software Development Security	—	—	—	● Ch.2: Software Security ● Ch.10: DevSecOps, Secure Supply Chain & 3rd Party Risk	—	—

CISM

Certified Information Security Manager (ISACA)

4 Knowledge Domains

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
Information Security Governance	● Ch.3: Information Security Management	◐ Ch.2: Information Security Frameworks	◐ Ch.2: Information Security Strategic Plan ◐ Ch.4: Information Security Governance ◐ Ch.5: Information Security Policies and Procedures	—	—	◐ Ch.2: Phase 1: Initiate
Information Risk Management	● Ch.1: The Essence of Information Security	◐ Ch.1: Information Security Guidance ◐ Ch.2: Information Security Frameworks	◐ Ch.1: Risk Management	—	—	◐ Ch.2: Phase 1: Initiate
Information Security Program Development and Management	—	● Ch.1: Information Security Guidance ◐ Ch.2: Information Security Frameworks	◐ Ch.2: Information Security Strategic Plan ◐ Ch.3: Information Security Architecture ◐ Ch.7: Information Security Metrics	—	◐ Ch.9: Security Awareness	◐ Ch.3: Phase 2: Implement
Information Security Incident Management	—	—	—	—	● Ch.4: Incident Management ● Ch.5: Digital Forensics	◐ Ch.4: Phase 3: Intelligence

CISA

Certified Information Systems Auditor (ISACA)

5 Knowledge Domains

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
Information Systems Auditing Process	—	● Ch.1: Information Security Guidance ◐ Ch.2: Information Security Frameworks	◐ Ch.7: Information Security Metrics	—	◐ Ch.10: Security Audit, Compliance and Assessment	◐ Ch.4: Phase 3: Intelligence
Governance and Management of IT	● Ch.3: Information Security Management	● Ch.2: Information Security Frameworks	◐ Ch.4: Information Security Governance ◐ Ch.6: Compliance, Legal and Regulatory Requirements	—	—	—
Information Systems Acquisition, Development and Implementation	—	—	—	● Ch.2: Software Security ● Ch.10: DevSecOps, Secure Supply Chain & 3rd Party Risk	—	◐ Ch.3: Phase 2: Implement
Information Systems Operations and Business Resilience	—	—	—	—	● Ch.3: Business Continuity and Disaster Recovery ● Ch.7: Configuration & Change Management ◐ Ch.8: Patch Management	◐ Ch.4: Phase 3: Intelligence
Protection of Information Assets	● Ch.2: Information Security Principles	—	—	◐ Ch.1: Data Security ◐ Ch.6: Physical Security	◐ Ch.1: Cryptography ◐ Ch.2: Identity and Access Management ◐ Ch.6: Logging and Monitoring	—

CompTIA Security+

CompTIA Security+ (SY0-701)

5 Knowledge Domains

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
General Security Concepts	● Ch.1: The Essence of Information Security ◐ Ch.2: Information Security Principles ◐ Ch.3: Information Security Management ◐ Ch.4: Information Security Ecosystem	◐ Ch.1: Information Security Guidance	—	—	—	—
Threats, Vulnerabilities and Mitigations	● Ch.1: The Essence of Information Security	—	◐ Ch.1: Risk Management	◐ Ch.3: Endpoint Security ◐ Ch.5: Network Security	◐ Ch.4: Incident Management	—
Security Architecture	● Ch.4: Information Security Ecosystem	—	◐ Ch.3: Information Security Architecture	◐ Ch.5: Network Security ◐ Ch.9: Virtualization & Cloud Security	—	◐ Ch.3: Phase 2: Implement
Security Operations	—	—	—	—	● Ch.4: Incident Management ◐ Ch.6: Logging and Monitoring ◐ Ch.7: Configuration & Change Management ◐ Ch.8: Patch Management	◐ Ch.4: Phase 3: Intelligence
Security Program Management and Oversight	● Ch.3: Information Security Management	—	◐ Ch.2: Information Security Strategic Plan ◐ Ch.4: Information Security Governance ◐ Ch.5: Information Security Policies and Procedures ◐ Ch.6: Compliance, Legal and Regulatory Requirements ◐ Ch.7: Information Security Metrics	—	—	—

ISO 27001 LI

ISO/IEC 27001 Lead Implementer

7 Knowledge Domains

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
Organizational Context and Scope	● Ch.3: Information Security Management	—	◐ Ch.2: Information Security Strategic Plan ◐ Ch.4: Information Security Governance	—	—	◐ Ch.1: Methodology Overview ◐ Ch.2: Phase 1: Initiate
Leadership and Commitment	—	—	● Ch.4: Information Security Governance ● Ch.5: Information Security Policies and Procedures	—	—	◐ Ch.2: Phase 1: Initiate
Planning (Risk Assessment & Treatment)	—	● Ch.2: Information Security Frameworks	● Ch.1: Risk Management ◐ Ch.6: Compliance, Legal and Regulatory Requirements	—	—	◐ Ch.2: Phase 1: Initiate
Support (Resources, Competence, Awareness, Communication)	—	—	● Ch.5: Information Security Policies and Procedures	—	● Ch.9: Security Awareness	◐ Ch.2: Phase 1: Initiate
Operation (Controls Implementation)	—	● Ch.1: Information Security Guidance ◐ Ch.3: Information Security Standards & Regulations	—	◐ Ch.1: Data Security ◐ Ch.2: Software Security ◐ Ch.3: Endpoint Security ◐ Ch.4: Wireless & Mobile Security ◐ Ch.5: Network Security ◐ Ch.6: Physical Security	—	◐ Ch.3: Phase 2: Implement
Performance Evaluation (Monitoring & Audit)	—	—	● Ch.7: Information Security Metrics	—	● Ch.6: Logging and Monitoring ◐ Ch.10: Security Audit, Compliance and Assessment	◐ Ch.4: Phase 3: Intelligence
Improvement (Nonconformity & Continual Improvement)	—	—	● Ch.7: Information Security Metrics	—	—	● Ch.5: Phase 4: Improve

CCSP

Certified Cloud Security Professional (ISC²)

6 Knowledge Domains

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
Cloud Concepts, Architecture and Design	● Ch.4: Information Security Ecosystem	● Ch.2: Information Security Frameworks	—	◐ Ch.9: Virtualization & Cloud Security	—	—
Cloud Data Security	—	—	—	● Ch.1: Data Security ● Ch.9: Virtualization & Cloud Security	◐ Ch.1: Cryptography	—
Cloud Platform and Infrastructure Security	—	—	—	● Ch.5: Network Security ● Ch.9: Virtualization & Cloud Security	◐ Ch.7: Configuration & Change Management	—
Cloud Application Security	—	—	—	● Ch.2: Software Security ● Ch.9: Virtualization & Cloud Security ◐ Ch.10: DevSecOps, Secure Supply Chain & 3rd Party Risk	—	—
Cloud Security Operations	—	—	—	● Ch.9: Virtualization & Cloud Security	◐ Ch.6: Logging and Monitoring ◐ Ch.7: Configuration & Change Management ◐ Ch.8: Patch Management	◐ Ch.4: Phase 3: Intelligence
Legal, Risk and Compliance	—	● Ch.3: Information Security Standards & Regulations	● Ch.1: Risk Management ◐ Ch.6: Compliance, Legal and Regulatory Requirements	—	—	◐ Ch.2: Phase 1: Initiate

CEH

Certified Ethical Hacker (EC-Council)

20 Knowledge Domains

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
Introduction to Ethical Hacking	● Ch.1: The Essence of Information Security ● Ch.2: Information Security Principles ○ Ch.4: Information Security Ecosystem	—	—	—	—	—
Footprinting and Reconnaissance	—	—	—	● Ch.5: Network Security	● Ch.6: Logging and Monitoring	—
Scanning Networks	—	—	—	● Ch.5: Network Security	● Ch.6: Logging and Monitoring	—
Enumeration	—	—	—	● Ch.5: Network Security	● Ch.6: Logging and Monitoring	—
Vulnerability Analysis	—	—	● Ch.1: Risk Management	—	● Ch.10: Security Audit, Compliance and Assessment	—
System Hacking	—	—	—	● Ch.3: Endpoint Security	● Ch.7: Configuration & Change Management	—
Malware Threats	—	—	—	● Ch.3: Endpoint Security	● Ch.4: Incident Management	—
Sniffing	—	—	—	● Ch.5: Network Security	● Ch.6: Logging and Monitoring	—
Social Engineering	—	—	—	● Ch.7: Human Resource Security & Privacy Management	● Ch.9: Security Awareness	—
Denial-of-Service	—	—	—	● Ch.5: Network Security	● Ch.4: Incident Management	—
Session Hijacking	—	—	—	● Ch.5: Network Security	● Ch.1: Cryptography	—
IDS, Firewalls and Honeypots	—	—	—	● Ch.5: Network Security	● Ch.6: Logging and Monitoring	—
Hacking Web Servers	—	—	—	● Ch.2: Software Security ● Ch.5: Network Security	—	—
Hacking Web Applications	—	—	—	● Ch.2: Software Security	—	—

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
SQL Injection	—	—	—	• Ch.2: Software Security	—	—
Hacking Wireless Networks	—	—	—	• Ch.4: Wireless & Mobile Security	—	—
Hacking Mobile Platforms	—	—	—	• Ch.4: Wireless & Mobile Security	—	—
IoT and OT Hacking	—	—	—	• Ch.8: Industrial Systems Security	—	—
Cloud Computing	—	—	—	• Ch.9: Virtualization & Cloud Security	—	—
Cryptography	—	—	—	—	• Ch.1: Cryptography	—

CRISC

Certified in Risk and Information Systems Control (ISACA)

4 Knowledge Domains

Certification Domain	Vol. 1 Information Security Fundamentals	Vol. 2 Blueprint of Security Excellence	Vol. 3 Information Security Strategic Management	Vol. 4 Information Security Engineering	Vol. 5 Information Security Operations	Vol. 6 Information Security Implementation
Governance	● Ch.3: Information Security Management	◐ Ch.2: Information Security Frameworks	◐ Ch.4: Information Security Governance ◐ Ch.5: Information Security Policies and Procedures	—	—	◐ Ch.2: Phase 1: Initiate
IT Risk Assessment	—	● Ch.1: Information Security Guidance ● Ch.2: Information Security Frameworks	◐ Ch.1: Risk Management ◐ Ch.7: Information Security Metrics	—	—	—
Risk Response and Reporting	—	—	● Ch.1: Risk Management ● Ch.7: Information Security Metrics	—	—	◐ Ch.4: Phase 3: Intelligence
Information Technology and Security	—	—	—	● Ch.1: Data Security ◐ Ch.5: Network Security	◐ Ch.1: Cryptography ◐ Ch.2: Identity and Access Management ◐ Ch.6: Logging and Monitoring	—

Reverse Index: Chapter-to-Certification Coverage

This section lists, for each chapter of each volume, which certification domains that chapter addresses. Use this as a quick reference when studying a specific chapter to understand its certification relevance.

Volume 1: Information Security Fundamentals

Chapter 1: The Essence of Information Security

Certification	Domains Covered
CISSP	• Security and Risk Management • Asset Security
CISM	• Information Risk Management
CompTIA Security+	• General Security Concepts • Threats, Vulnerabilities and Mitigations
CEH	• Introduction to Ethical Hacking

Chapter 2: Information Security Principles

Certification	Domains Covered
CISSP	• Security and Risk Management • Identity and Access Management (IAM)
CISA	• Protection of Information Assets
CompTIA Security+	• General Security Concepts
CEH	• Introduction to Ethical Hacking

Chapter 3: Information Security Management

Certification	Domains Covered
CISSP	• Security and Risk Management
CISM	• Information Security Governance
CISA	• Governance and Management of IT
CompTIA Security+	• General Security Concepts • Security Program Management and Oversight

ISO 27001 LI	• Organizational Context and Scope
CRISC	• Governance

Chapter 4: Information Security Ecosystem

Certification	Domains Covered
CISSP	• Asset Security • Security Architecture and Engineering
CompTIA Security+	• General Security Concepts • Security Architecture
CCSP	• Cloud Concepts, Architecture and Design
CEH	• Introduction to Ethical Hacking

Chapter 5: Information Security Implementation

No direct certification domain mapping identified.

Volume 2: Blueprint of Security Excellence

Chapter 1: Information Security Guidance

Certification	Domains Covered
CISSP	• Security and Risk Management • Security Assessment and Testing
CISM	• Information Risk Management • Information Security Program Development and Management
CISA	• Information Systems Auditing Process
CompTIA Security+	• General Security Concepts
ISO 27001 LI	• Operation (Controls Implementation)
CRISC	• IT Risk Assessment

Chapter 2: Information Security Frameworks

Certification	Domains Covered
CISSP	• Security and Risk Management • Security Architecture and Engineering • Security Assessment and Testing
CISM	• Information Security Governance • Information Risk Management • Information Security Program Development and Management
CISA	• Information Systems Auditing Process • Governance and Management of IT
ISO 27001 LI	• Planning (Risk Assessment & Treatment)
CCSP	• Cloud Concepts, Architecture and Design
CRISC	• Governance • IT Risk Assessment

Chapter 3: Information Security Standards & Regulations

Certification	Domains Covered
CISSP	• Security Architecture and Engineering
ISO 27001 LI	• Operation (Controls Implementation)
CCSP	• Legal, Risk and Compliance

Chapter 4: Vendors' Best Practices & Real-World Application

No direct certification domain mapping identified.

Volume 3: Information Security Strategic Management

Chapter 1: Risk Management

Certification	Domains Covered
CISSP	• Security and Risk Management • Asset Security
CISM	• Information Risk Management
CompTIA Security+	• Threats, Vulnerabilities and Mitigations
ISO 27001 LI	• Planning (Risk Assessment & Treatment)

CCSP	• Legal, Risk and Compliance
CEH	• Vulnerability Analysis
CRISC	• IT Risk Assessment • Risk Response and Reporting

Chapter 2: Information Security Strategic Plan

Certification	Domains Covered
CISSP	• Security and Risk Management
CISM	• Information Security Governance • Information Security Program Development and Management
CompTIA Security+	• Security Program Management and Oversight
ISO 27001 LI	• Organizational Context and Scope

Chapter 3: Information Security Architecture

Certification	Domains Covered
CISSP	• Security Architecture and Engineering
CISM	• Information Security Program Development and Management
CompTIA Security+	• Security Architecture

Chapter 4: Information Security Governance

Certification	Domains Covered
CISSP	• Security and Risk Management
CISM	• Information Security Governance
CISA	• Governance and Management of IT
CompTIA Security+	• Security Program Management and Oversight
ISO 27001 LI	• Organizational Context and Scope • Leadership and Commitment
CRISC	• Governance

Chapter 5: Information Security Policies and Procedures

Certification	Domains Covered
CISSP	• Security and Risk Management
CISM	• Information Security Governance
CompTIA Security+	• Security Program Management and Oversight
ISO 27001 LI	• Leadership and Commitment • Support (Resources, Competence, Awareness, Communication)
CRISC	• Governance

Chapter 6: Compliance, Legal and Regulatory Requirements

Certification	Domains Covered
CISSP	• Security and Risk Management
CISA	• Governance and Management of IT
CompTIA Security+	• Security Program Management and Oversight
ISO 27001 LI	• Planning (Risk Assessment & Treatment)
CCSP	• Legal, Risk and Compliance

Chapter 7: Information Security Metrics

Certification	Domains Covered
CISSP	• Security Assessment and Testing
CISM	• Information Security Program Development and Management
CISA	• Information Systems Auditing Process
CompTIA Security+	• Security Program Management and Oversight
ISO 27001 LI	• Performance Evaluation (Monitoring & Audit) • Improvement (Nonconformity & Continual Improvement)
CRISC	• IT Risk Assessment • Risk Response and Reporting

Volume 4: Information Security Engineering

Chapter 1: Data Security

Certification	Domains Covered
CISSP	• Asset Security
CISA	• Protection of Information Assets
ISO 27001 LI	• Operation (Controls Implementation)
CCSP	• Cloud Data Security
CRISC	• Information Technology and Security

Chapter 2: Software Security

Certification	Domains Covered
CISSP	• Software Development Security
CISA	• Information Systems Acquisition, Development and Implementation
ISO 27001 LI	• Operation (Controls Implementation)
CCSP	• Cloud Application Security
CEH	• Hacking Web Servers • Hacking Web Applications • SQL Injection

Chapter 3: Endpoint Security

Certification	Domains Covered
CompTIA Security+	• Threats, Vulnerabilities and Mitigations
ISO 27001 LI	• Operation (Controls Implementation)
CEH	• System Hacking • Malware Threats

Chapter 4: Wireless & Mobile Security

Certification	Domains Covered
CISSP	• Communication and Network Security
ISO 27001 LI	• Operation (Controls Implementation)
CEH	• Hacking Wireless Networks • Hacking Mobile Platforms

Chapter 5: Network Security

Certification	Domains Covered
CISSP	• Security Architecture and Engineering • Communication and Network Security
CompTIA Security+	• Threats, Vulnerabilities and Mitigations • Security Architecture
ISO 27001 LI	• Operation (Controls Implementation)
CCSP	• Cloud Platform and Infrastructure Security
CEH	• Footprinting and Reconnaissance • Scanning Networks • Enumeration • Sniffing • Denial-of-Service • Session Hijacking • IDS, Firewalls and Honeypots • Hacking Web Servers
CRISC	• Information Technology and Security

Chapter 6: Physical Security

Certification	Domains Covered
CISA	• Protection of Information Assets
ISO 27001 LI	• Operation (Controls Implementation)

Chapter 7: Human Resource Security & Privacy Management

Certification	Domains Covered
CISSP	• Asset Security
CEH	• Social Engineering

Chapter 8: Industrial Systems Security

Certification	Domains Covered
CISSP	• Security Architecture and Engineering
CEH	• IoT and OT Hacking

Chapter 9: Virtualization & Cloud Security

Certification	Domains Covered
CISSP	• Security Architecture and Engineering
CompTIA Security+	• Security Architecture
CCSP	• Cloud Concepts, Architecture and Design • Cloud Data Security • Cloud Platform and Infrastructure Security • Cloud Application Security • Cloud Security Operations
CEH	• Cloud Computing

Chapter 10: DevSecOps, Secure Supply Chain & 3rd Party Risk

Certification	Domains Covered
CISSP	• Software Development Security
CISA	• Information Systems Acquisition, Development and Implementation
CCSP	• Cloud Application Security

Volume 5: Information Security Operations

Chapter 1: Cryptography

Certification	Domains Covered
CISSP	• Communication and Network Security
CISA	• Protection of Information Assets
CCSP	• Cloud Data Security
CEH	• Session Hijacking • Cryptography
CRISC	• Information Technology and Security

Chapter 2: Identity and Access Management

Certification	Domains Covered
CISSP	• Identity and Access Management (IAM)
CISA	• Protection of Information Assets
CRISC	• Information Technology and Security

Chapter 3: Business Continuity and Disaster Recovery

Certification	Domains Covered
CISA	• Information Systems Operations and Business Resilience

Chapter 4: Incident Management

Certification	Domains Covered
CISSP	• Security Operations
CISM	• Information Security Incident Management
CompTIA Security+	• Threats, Vulnerabilities and Mitigations • Security Operations
CEH	• Malware Threats • Denial-of-Service

Chapter 5: Digital Forensics

Certification	Domains Covered
CISSP	• Security Operations
CISM	• Information Security Incident Management

Chapter 6: Logging and Monitoring

Certification	Domains Covered
CISSP	• Security Operations
CISA	• Protection of Information Assets
CompTIA Security+	• Security Operations
ISO 27001 LI	• Performance Evaluation (Monitoring & Audit)
CCSP	• Cloud Security Operations
CEH	• Footprinting and Reconnaissance • Scanning Networks • Enumeration • Sniffing • IDS, Firewalls and Honeypots
CRISC	• Information Technology and Security

Chapter 7: Configuration & Change Management

Certification	Domains Covered
CISSP	• Security Operations
CISA	• Information Systems Operations and Business Resilience
CompTIA Security+	• Security Operations
CCSP	• Cloud Platform and Infrastructure Security • Cloud Security Operations
CEH	• System Hacking

Chapter 8: Patch Management

Certification	Domains Covered
CISSP	• Security Operations
CISA	• Information Systems Operations and Business Resilience
CompTIA Security+	• Security Operations
CCSP	• Cloud Security Operations

Chapter 9: Security Awareness

Certification	Domains Covered
CISM	• Information Security Program Development and Management
ISO 27001 LI	• Support (Resources, Competence, Awareness, Communication)
CEH	• Social Engineering

Chapter 10: Security Audit, Compliance and Assessment

Certification	Domains Covered
CISSP	• Security Assessment and Testing
CISA	• Information Systems Auditing Process
ISO 27001 LI	• Performance Evaluation (Monitoring & Audit)
CEH	• Vulnerability Analysis

Volume 6: Information Security Implementation

Chapter 1: Methodology Overview

Certification	Domains Covered
ISO 27001 LI	• Organizational Context and Scope

Chapter 2: Phase 1: Initiate

Certification	Domains Covered
CISSP	• Security and Risk Management
CISM	• Information Security Governance • Information Risk Management
ISO 27001 LI	• Organizational Context and Scope • Leadership and Commitment • Planning (Risk Assessment & Treatment) • Support (Resources, Competence, Awareness, Communication)
CCSP	• Legal, Risk and Compliance
CRISC	• Governance

Chapter 3: Phase 2: Implement

Certification	Domains Covered
CISSP	• Security Architecture and Engineering
CISM	• Information Security Program Development and Management
CISA	• Information Systems Acquisition, Development and Implementation
CompTIA Security+	• Security Architecture
ISO 27001 LI	• Operation (Controls Implementation)

Chapter 4: Phase 3: Intelligence

Certification	Domains Covered
CISSP	• Security Assessment and Testing • Security Operations
CISM	• Information Security Incident Management

CISA	• Information Systems Auditing Process • Information Systems Operations and Business Resilience
CompTIA Security+	• Security Operations
ISO 27001 LI	• Performance Evaluation (Monitoring & Audit)
CCSP	• Cloud Security Operations
CRISC	• Risk Response and Reporting

Chapter 5: Phase 4: Improve

Certification	Domains Covered
ISO 27001 LI	• Improvement (Nonconformity & Continual Improvement)

www.TerminuSys.com/book-series