

PEARSON IT
CERTIFICATION



Practice
Tests



Flash
Cards



Review
Exercises

Cert Guide

Advance your IT career with hands-on learning

CISSP

Fifth Edition



ROBIN ABERNATHY
Dr. DARREN R. HAYES

CISSP Cert Guide, Fifth Edition

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **www.pearsonitcertification.com/register**.
2. Enter the **print book ISBN**: 9780135343999.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.ehelp.org**.

CISSP Cert Guide

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Contents at a Glance

Contents

Introduction

Chapter 1 Security and Risk Management

Foundation Topics

Security Terms

Five Pillars of Information Security

CIA Triad

Confidentiality

Integrity

Availability

Authenticity

Non-Repudiation

Auditing and Accounting

Default Security Posture

Defense in Depth

Abstraction

Data Hiding

Encryption

Table of Contents

Security Governance Principles

Security Function Alignment

Organizational Strategies and Goals

Organizational Mission and Objectives

Business Case

Security Budget, Metrics, and Efficacy

Resources

Organizational Processes

Acquisitions and Divestitures

Governance Committees

Organizational Roles and Responsibilities

Board of Directors

Management

Audit Committee

Data Owner

Data Custodian

System Owner

System Administrator

Security Administrator

Security Analyst

Application Owner

Supervisor

User

Auditor

Security Control Frameworks

ISO/IEC 27000 Series

Zachman Framework

The Open Group Architecture Framework (TOGAF)

Department of Defense Architecture Framework (DoDAF)

British Ministry of Defence Architecture Framework (MODAF)

Table of Contents

Sherwood Applied Business Security Architecture (SABSA)
Control Objectives for Information and Related Technology (COBIT)
National Institute of Standards and Technology (NIST) Special Publication
 (SP) 800 Series
HITRUST CSF
CIS Critical Security Controls
Committee of Sponsoring Organizations (COSO) of the Treadway Commission
 Framework
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
Information Technology Infrastructure Library (ITIL)
Six Sigma
Capability Maturity Model Integration (CMMI)
CCTA Risk Analysis and Management Method (CRAMM)
Federal Risk and Authorization Management Program (FedRAMP)
Payment Card Industry Data Security Standard (PCI DSS)
Top-Down Versus Bottom-Up Approach
Security Program Life Cycle
Due Care and Due Diligence

Compliance

Contractual, Legal, Industry Standards, and Regulatory Compliance
Privacy Requirements Compliance

Legal and Regulatory Issues

Computer Crime Concepts
Computer-Assisted Crime
Computer-Targeted Crime
Incidental Computer Crime
Computer Prevalence Crime
Hackers Versus Crackers
Computer Crime Examples
Major Legal Systems

Table of Contents

Civil Law
Common Law
Criminal Law
Civil/Tort Law
Administrative/Regulatory Law
Customary Law
Religious Law
Mixed Law
Licensing and Intellectual Property
Patent
Trade Secret
Trademark
Copyright
Software Piracy and Licensing Issues
Internal Protection
Digital Rights Managements (DRM)
Cyber Crimes and Data Breaches
Import/Export Controls
Trans-Border Data Flow
Privacy
Personally Identifiable Information (PII)
Laws and Regulations

Investigation Types

Operations/Administrative
Criminal
Civil
Regulatory
Industry Standards
eDiscovery
Scope and Plan

Table of Contents

Professional Ethics

- (ISC)2 Code of Ethics

- Computer Ethics Institute

- Internet Architecture Board

- Organizational Code of Ethics

Security Documentation

- Policies

- Organizational Security Policy

- System-Specific Security Policy

- Issue-Specific Security Policy

- Policy Categories

- Processes

- Procedures

- Standards

- Guidelines

- Baselines

Business Continuity

- Business Continuity and Disaster Recovery Concepts

- Disruptions

- Disasters

- Disaster Recovery and the Disaster Recovery Plan (DRP)

- Continuity Planning and the Business Continuity Plan (BCP)

- Business Impact Analysis (BIA)

- Contingency Plan

- Availability

- Reliability

- External Dependencies

- Scope and Plan

- Personnel Components

Table of Contents

Scope

Business Contingency Planning

BIA Development

Identify Critical Processes and Resources

Identify Outage Impact and Estimate Downtime

Identify Resource Requirements

Identify Recovery Priorities

Personnel Security Policies and Procedures

Candidate Screening and Hiring

Employment Agreements and Policies

Employee Onboarding and Offboarding Policies

Vendor, Consultant, and Contractor Agreements and Controls

Compliance Policy Requirements

Privacy Policy Requirements

Job Rotation

Separation of Duties

Risk Management Concepts

Asset and Asset Valuation

Vulnerability

Threat

Threat Agent

Exploit

Risk

Exposure

Countermeasure

Risk Appetite

Incident

Attack

Breach

Table of Contents

Risk Management Policy
Risk Management Team
Risk Analysis Team
Risk Assessment
Information and Asset (Tangible/Intangible) Value and Costs
Identity Threats and Vulnerabilities
Risk Assessment/Analysis
Countermeasure (Safeguard) Selection
Inherent Risk Versus Residual Risk
Handling Risk and Risk Response
Implementation
Control Categories
Compensative
Corrective
Detective
Deterrent
Directive
Preventive
Recovery
Control Types
Administrative (Management)
Logical (Technical)
Physical
Controls Assessment, Monitoring, and Measurement
Reporting and Continuous Improvement
Internal Reporting
External Reporting
Risk Frameworks
NIST
ISO/IEC 27005:2018

Table of Contents

COSO's Enterprise Risk Management (ERM) Integrated Framework

A Risk Management Standard by the Federation of European Risk Management
Associations (FERMA)

Geographical Threats

Internal Versus External Threats

Natural Threats

Hurricanes/Tropical Storms

Tornadoes

Earthquakes

Floods

Volcanoes

System Threats

Electrical

Communications

Utilities

Human-Caused Threats

Explosions

Fire

Vandalism

Fraud

Theft

Collusion

Politically Motivated Threats

Strikes

Riots

Civil Disobedience

Terrorist Acts

Active Shooter

Bombing

Threat Modeling

Table of Contents

Threat Modeling Concepts

Threat Modeling Methodologies

STRIDE Model

Process for Attack Simulation and Threat Analysis (PASTA) Methodology

Trike Methodology

Visual, Agile, and Simple Threat (VAST) Model

NIST SP 800-154

Identifying Threats

Potential Attacks

Remediation Technologies and Processes

Security Risks in the Supply Chain

Risks Associated with Hardware, Software, and Services

Third-Party Assessment and Monitoring

Onsite Assessment

Document Exchange/Review

Process/Policy Review

Other Third-Party Governance Issues

Supply Chain Assessment and Monitoring

Silicon Root of Trust

Physically Unclonable Function (PUF)

Software Bill of Materials (SBOM)

Minimum Service-Level and Security Requirements

Service-Level Agreements (SLAs)

Security Education, Training, and Awareness

Levels Required

Methods and Techniques

Periodic Content Reviews

Exam Preparation Tasks

Review All Key Topics

Table of Contents

Complete the Tables and Lists from Memory

Define Key Terms

Answer Review Questions

Answers and Explanations

Chapter 2 Asset Security

Foundation Topics

Asset Security Concepts

- Asset and Data Policies

- Data Quality

- Data Documentation and Organization

Identify and Classify Information and Assets

- Data and Asset Classification

- Sensitivity and Criticality

- PII

- PHI

- Proprietary Data

- Private Sector Data Classifications

- Military and Government Data Classifications

Information and Asset Handling Requirements

- Marking, Labeling, and Storing

- Destruction

Provision Resources Securely

- Asset Inventory and Asset Management

Data Life Cycle

- Databases

- DBMS Architecture and Models

- Database Interface Languages

- Data Warehouses and Data Mining

Table of Contents

Database Maintenance

Database Threats

Database Views

Database Locks

Polyinstantiation

Database ACID Test

Roles and Responsibilities

Data Owner

Data Controller

Data Custodian

System Owners

System Custodians

Business/Mission Owners

Data Processors

Data Users and Subjects

Data Collection and Limitation

Data Location

Data Maintenance

Data Retention

Data Remanence and Destruction

Data Audit

Asset Retention

Data Security Controls

Data Security

Data States

Data at Rest

Data in Transit

Data in Use

Data Access and Sharing

Table of Contents

Data Storage and Archiving

Baselines

Scoping and Tailoring

Standards Selection

Data Protection Methods

Cryptography

Digital Rights Management (DRM)

Data Loss Prevention (DLP)

Cloud Access Security Broker (CASB)

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Answer Review Questions

Answers and Explanations

Chapter 3 Security Architecture and Engineering

Foundation Topics

Information Systems Life Cycle

Stakeholders Needs and Requirements

Requirements Analysis

Architectural Design

Development/Implementation

Integration

Verification and Validation

Transition/Deployment

Operations and Maintenance/Sustainment

Retirement/Disposal

Engineering Processes Using Secure Design Principles

Objects and Subjects

Table of Contents

Closed Versus Open Systems

Threat Modeling

Least Privilege

Defense in Depth

Secure Defaults

Fail Securely

Separation of Duties (SoD)

Keep It Simple and Small

Zero Trust

Privacy by Design

Trust but Verify

Shared Responsibility

Secure Access Service Edge (SASE)

Security Model Concepts

Confidentiality, Integrity, and Availability

Confinement

Bounds

Isolation

Security Modes

Dedicated Security Mode

System High Security Mode

Compartmented Security Mode

Multilevel Security Mode

Assurance and Trust

Security Model Types

State Machine Models

Multilevel Lattice Models

Matrix-Based Models

Noninterference Models

Information Flow Models

Table of Contents

Take-Grant Model
Security Models
Bell-LaPadula Model
Biba Model
Clark-Wilson Integrity Model
Lipner Model
Brewer-Nash (Chinese Wall) Model
Graham-Denning Model
Harrison-Ruzzo-Ullman Model
Goguen-Meseguer Model
Sutherland Model
System Architecture Steps
ISO/IEC 42010:2011
Computing Platforms
Mainframe/Thin Clients
Distributed Systems
Middleware
Embedded Systems
Mobile Computing
Virtual Computing
Security Services
Boundary Control Services
Access Control Services
Integrity Services
Cryptography Services
Auditing and Monitoring Services
System Components
CPU
Memory and Storage
Input/Output Devices

Table of Contents

Input/Output Structures

Firmware

Operating Systems

Memory Management

System Security Evaluation Models

TCSEC

Rainbow Series

ITSEC

Common Criteria

Security Implementation Standards

ISO/IEC 27001

ISO/IEC 27002

Payment Card Industry Data Security Standard (PCI DSS)

Controls and Countermeasures

Security Architecture Maintenance

Certification and Accreditation

Control Selection Based on Systems Security Requirements

Security Capabilities of Information Systems

Memory Protection

Trusted Platform Module

Interfaces

Fault Tolerance

Policy Mechanisms

Separation of Privilege

Accountability

Encryption/Decryption

Vulnerabilities of Security Architectures, Designs, and Solution Elements

Client-Based Systems

Server-Based Systems

Table of Contents

Data Flow Control
Database Systems
Inference
Aggregation
Contamination
Data Mining Warehouse
Cryptographic Systems
Operational Technology/Industrial Control Systems
Cloud-Based Systems
Large-Scale Parallel Data Systems
Distributed Systems
Grid Computing
Peer-to-Peer Computing
Internet of Things
IoT Examples
Methods of Securing IoT Devices
NIST Framework for Cyber-Physical Systems
Microservices
Containerization
Serverless Systems
High-Performance Computing Systems
Edge Computing Systems
Virtualized Systems
Vulnerabilities in Web-Based Systems
Maintenance Hooks
Time-of-Check/Time-of-Use Attacks
Web-Based Attacks
XML
SAML
OWASP

Table of Contents

Vulnerabilities in Mobile Systems

- Device Security

- Application Security

- Mobile Device Concerns

- NIST SP 800-164

Vulnerabilities in Embedded Systems

Cryptographic Solutions

- Cryptography Concepts

- Cryptography History

- Julius Caesar and the Caesar Cipher

- Vigenere Cipher

- Kerckhoffss Principle

- World War II Enigma

- Lucifer by IBM

- Cryptosystem Features

- Authentication

- Confidentiality

- Integrity

- Authorization

- Non-repudiation

- NIST SP 800-175A and B

- Cryptographic Mathematics

- Boolean

- Logical Operations (And, Or, Not, Exclusive Or)

- Modulo Function

- One-Way Function

- Nonce

- Split Knowledge

- Cryptographic Life Cycle

Table of Contents

Key Management

Algorithm Selection

Cryptographic Types

Running Key and Concealment Ciphers

Substitution Ciphers

One-Time Pads

Steganography

Transposition Ciphers

Symmetric Algorithms

Stream-Based Ciphers

Block Ciphers

Initialization Vectors (IVs)

Asymmetric Algorithms

Hybrid Ciphers

Elliptic Curves

Quantum Cryptography

Symmetric Algorithms

DES and 3DES

DES Modes

3DES and Modes

AES

IDEA

Skipjack

Blowfish

Twofish

RC4/RC5/RC6/RC7

CAST

Asymmetric Algorithms

Diffie-Hellman

Table of Contents

RSA

El Gamal

ECC

Knapsack

Zero-Knowledge Proof

Public Key Infrastructure and Digital Certificates

Certificate Authority and Registration Authority

Certificates

Certificate Life Cycle

Enrollment

Verification

Revocation

Renewal and Modification

Certificate Revocation List

OCSP

PKI Steps

Cross-Certification

Quantum Key Distribution

Key Management Practices

Message Integrity

Hashing

One-Way Hash

MD2/MD4/MD5/MD6

SHA/SHA-2/SHA-3

HAVAL

RIPEMD-160

Tiger

Message Authentication Code

HMAC

Table of Contents

CBC-MAC

CMAC

Salting

Digital Signatures and Non-repudiation

DSS

Non-repudiation

Applied Cryptography

Link Encryption Versus End-to-End Encryption

Email Security

Internet Security

Cryptanalytic Attacks

Ciphertext-Only Attack

Known Plaintext Attack

Chosen Plaintext Attack

Chosen Ciphertext Attack

Social Engineering

Brute Force

Differential Cryptanalysis

Linear Cryptanalysis

Algebraic Attack

Frequency Analysis

Birthday Attack

Dictionary Attack

Replay Attack

Analytic Attack

Statistical Attack

Factoring Attack

Reverse Engineering

Meet-in-the-Middle Attack

Table of Contents

Ransomware Attack

Side-Channel Attack

Implementation Attack

Fault Injection

Timing Attack

Pass-the-Hash Attack

Digital Rights Management

Document DRM

Music DRM

Movie DRM

Video Game DRM

E-book DRM

Site and Facility Design

Layered Defense Model

CPTED

Natural Access Control

Natural Surveillance

Natural Territorials Reinforcement

Physical Security Plan

Deter Criminal Activity

Delay Intruders

Detect Intruders

Assess Situation

Respond to Intrusions and Disruptions

Facility Selection Issues

Visibility

Surrounding Area and External Entities

Accessibility

Construction

Table of Contents

Internal Compartments

Computer and Equipment Rooms

Site and Facility Security Controls

Doors

Door Lock Types

Turnstiles and Mantraps

Locks

Biometrics

Type of Glass Used for Entrances

Visitor Control

Wiring Closets/Intermediate Distribution Facilities

Restricted and Work Areas

Secure Data Center

Restricted Work Area

Server Room

Media Storage Facilities

Evidence Storage

Environmental Security and Issues

Fire Protection

Power Supply

HVAC

Water Leakage and Flooding

Environmental Alarms

Equipment Physical Security

Corporate Procedures

Safes, Vaults, and Locking

Exam Preparation Tasks

Review All Key Topics

Complete the Tables and Lists from Memory

Table of Contents

Define Key Terms

Answer Review Questions

Answers and Explanations

Chapter 4 Communication and Network Security

Foundation Topics

Secure Network Design Principles

- OSI Model

- Application Layer

- Presentation Layer

- Session Layer

- Transport Layer

- Network Layer

- Data Link Layer

- Physical Layer

- TCP/IP Model

- Application Layer

- Transport Layer

- Internet Layer

- Link Layer

- Encapsulation and De-encapsulation

IP Networking

- Common TCP/UDP Ports

- Logical and Physical Addressing

- IPv4

- IP Classes

- Public Versus Private IP Addresses

- NAT

- Media Access Control (MAC) Addressing

- Network Transmission

Table of Contents

Analog Versus Digital

Asynchronous Versus Synchronous

Broadband Versus Baseband

Unicast, Multicast, and Broadcast

Wired Versus Wireless

IPv6

NIST SP 800-119

IPv6 Major Features

IPv4 Versus IPv6 Threat Comparison

IPv6 Addressing

Shorthand for Writing IPv6 Addresses

IPv6 Address Types

IPv6 Address Scope

Network Types

LAN

Intranet

Extranet

MAN

WAN

WLAN

SAN

CAN

PAN

Protocols and Services

ARP/RARP

DHCP/BOOTP

DNS

FTP, FTPS, SFTP, and TFTP

HTTP, HTTPS, and S-HTTP

ICMP

Table of Contents

IGMP

IMAP

LDAP

LDP

NAT

NetBIOS

NFS

PAT

POP

CIFS/SMB

SMTP

SNMP

SSL/TLS

Multilayer Protocols

Converged Protocols

FCoE

InfiniBand

Compute Express Link (CXL)

MPLS

VoIP

iSCSI

Wireless Networks

FHSS, DSSS, OFDM, VOFDM, FDMA, TDMA, CDMA, OFDMA, GSM, and Massive
MIMO

802.11 Techniques

Cellular or Mobile Wireless Techniques

5G

Telecommunications and Hardware Support

Telecom Providers

Satellites

Table of Contents

Backhaul Networks

Hardware Support

WLAN Structure

Access Point

Service Set Identifier (SSID)

Infrastructure Mode Versus Ad Hoc Mode

WLAN Standards

802.11

802.11a (Wi-Fi 2)

802.11b (Wi-Fi 1)

802.11g (Wi-Fi 3)

802.11n (Wi-Fi 4)

802.11ac (Wi-Fi 5)

802.11ax (Wi-Fi 6)

802.11be (Wi-Fi 7)

802.11bn (Wi-Fi 8)

Bluetooth

Infrared

Near Field Communication (NFC)

Zigbee

WLAN Security

Open System Authentication

Shared Key Authentication

WEP

WPA

WPA2

Personal Versus Enterprise

WPA3

802.1X

SSID Broadcast

Table of Contents

MAC Filter

Wireless Site Surveys

Antenna Placement and Signal Power Levels

Antenna Types

Answers and Explanations

Communications Cryptography

Link Encryption

End-to-End Encryption

Email Security

PGP

MIME and S/MIME

Quantum Cryptography

Internet Security

Remote Access

HTTP, HTTPS, and S-HTTP

Secure Electronic Transaction (SET)

Cookies

SSH

IPsec

Secure Network Components

Network Monitoring and Management

Operation of Infrastructure

Hardware

Network Devices

Network Routing

Transmission Media

Cabling

Network Topologies

Performance Metrics

Table of Contents

Network Technologies

WAN Technologies

Network Access Control Devices

Quarantine/Remediation

Firewalls/Proxies

Network Access Control Systems

Endpoint Security

Content-Distribution Networks

Secure Communication Channels

Voice

Multimedia Collaboration

Remote Meeting Technology

Instant Messaging

Remote Access

Remote Connection Technologies

VPN Screen Scraper

Virtual Application/Desktop

Telecommuting/Teleworking

Data Communications

Virtualized Networks

Software-Defined Networking

Virtual Private Cloud (VPC)

Virtual SAN

Guest Operating Systems

Federated Identity with a Third Party

Network Attacks

Network Component Attacks

Non-Blind Spoofing

Blind Spoofing

Table of Contents

Man-in-the-Middle Attack

MAC Flooding Attack

802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack

Double-Encapsulated 802.1Q/Nested VLAN Attack

ARP Attack

ICMP Attacks

Ping of Death

Smurf

Fraggle

ICMP Redirect

Ping Scanning

Traceroute Exploitation

DNS Attacks

DNS Cache Poisoning

DoS

DDoS

DNSSEC

URL Hiding

Domain Grabbing

Cybersquatting

Email Attacks

Email Spoofing

Spear Phishing

Whaling

Spam

Wireless Attacks

Wardriving

Warchalking

Remote Attacks

Other Attacks

Table of Contents

SYN ACK Attacks

Session Hijacking

Port Scanning

Teardrop

IP Address Spoofing

Zero-Day

Ransomware

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Answer Review Questions

Chapter 5 Identity and Access Management (IAM)

Foundation Topics

Access Control Process

Identify Resources

Identify Users

Identify the Relationships Between Resources and Users

Physical and Logical Access to Assets

Access Control Administration

Centralized

Decentralized

Information

Systems

Devices

Facilities

Applications

Services

Identification and Authentication Concepts

Table of Contents

NIST SP 800-63

Five Factors for Authentication

Knowledge Factors

Ownership Factors

Characteristic Factors

Location Factors

Time Factors

Single-Factor Versus Multifactor Authentication

Device Authentication

Password-Less Authentication

Groups and Roles

Identification and Authentication Implementation

Authentication, Authorization, and Accounting (AAA)

Authentication

Authorization

Accounting

Separation of Duties

Least Privilege/Need-to-Know

Default to No Access

Directory Services

Single Sign-on

Kerberos

SESAME

OpenID Connect (OIDC)/Open Authorization (OAuth)

Security Assertion Markup Language (SAML)

Federated Identity Management (IdM)

Security Domains

Session Management

Registration, Proof, and Establishment of Identity

Credential Management Systems

Table of Contents

Remote Authentication Dial-In User Service (RADIUS)/Terminal Access

Controller Access Control System Plus (TACACS+)

Just-In-Time (JIT)

Identity as a Service (IDaaS) Implementation

Third-Party Identity Services Integration

Authorization Mechanisms

Permissions, Rights, and Privileges

Access Control Models

Discretionary Access Control

Mandatory Access Control

Role-Based Access Control

Rule-Based Access Control

Attribute-Based Access Control

Content-Dependent Versus Context-Dependent

Risk-Based Access Control

Access Control Matrix

Access Control Policies and Policy Enforcement

Provisioning Life Cycle

Provisioning

Identity and Account Management

User, System, and Service Account Access Review

Account Transfers

Account Revocation

Role Definition and Transition

Privilege Escalation

Service Account Management

Access Control Threats

Password Threats

Dictionary Attack

Table of Contents

Brute-Force Attack
Birthday Attack
Rainbow Table Attack
Sniffer Attack
Social Engineering Threats
Phishing/Pharming
Shoulder Surfing
Identity Theft
Dumpster Diving
DoS/DDoS
Buffer Overflow
Mobile Code
Malicious Software
Spoofing
Sniffing and Eavesdropping
Emanating
Backdoor/Trapdoor
Access Aggregation
Advanced Persistent Threat

Prevent or Mitigate Access Control Threats

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Answer Review Questions

Answers and Explanations

Chapter 6 Security Assessment and Testing

Foundation Topics

Design and Validate Assessment and Testing Strategies

Table of Contents

Security Testing

Security Assessments

Red Team versus Blue Team

Security Auditing

Internal, External, and Third-party Security Assessment, Testing, and
Auditing

Location

Conduct Security Control Testing

Vulnerability Assessment

Network Discovery Scan

Network Vulnerability Scan

Web Application Vulnerability Scan

Penetration Testing

Log Reviews

NIST SP 800-92

Synthetic Transactions

Code Review and Testing

Code Review Process

Static Testing

Dynamic Testing

Fuzz Testing

Misuse Case Testing

Test Coverage Analysis

Interface Testing

Collect Security Process Data

NIST SP 800-137

Account Management

Management Review and Approval

Key Performance and Risk Indicators

Table of Contents

Backup Verification Data

Training and Awareness

Disaster Recovery and Business Continuity

Analyze Test Outputs and Generate a Report

Conduct or Facilitate Security Audits

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Answer Review Questions

Answers and Explanations

Chapter 7 Security Operations

Foundation Topics

Investigations

Forensic and Digital Investigations

Identify Evidence

Preserve and Collect Evidence

Examine and Analyze Evidence

Present Findings

Decide

Forensic Procedures

Reporting and Documentation

IOCE/SWGDE and NIST

Crime Scene

MOM

Chain of Custody

Interviewing

Investigative Techniques

Evidence Collection and Handling

Table of Contents

Five Rules of Evidence

Types of Evidence

Surveillance, Search, and Seizure

Media Analysis

Software Analysis

Network Analysis

Hardware/Embedded Device Analysis

Digital Forensic Tools, Tactics, and Procedures

Artifacts

Logging and Monitoring Activities

Audit and Review

Log Types

Audit Types

Intrusion Detection and Prevention

Security Information and Event Management (SIEM)

Security Orchestration and Automated Response (SOAR)

Continuous Monitoring and Tuning

Egress Monitoring

Log Management

Threat Intelligence

User and Entity Behavior Analytics (UEBA)

Configuration and Change Management

Resource Provisioning

Asset Inventory and Management

Baselining

Automation

Security Operations Concepts

Need to Know/Least Privilege

Managing Accounts, Groups, and Roles

Table of Contents

Separation of Duties and Responsibilities

Privilege Account Management

Job Rotation and Mandatory Vacation

Two-Person Control

Sensitive Information Procedures

Record Retention

Information Life Cycle

Service-Level Agreements

Resource Protection

Protecting Tangible and Intangible Assets

Facilities

Hardware

Software

Information Assets

Protecting Data at Rest and Data in Transit

Asset Management

Redundancy and Fault Tolerance

Backup and Recovery Systems

Identity and Access Management

Media Management

Media History

Media Labeling and Storage

Sanitizing and Disposing of Media

Network and Resource Management

Incident Management

Event Versus Incident

Incident Response Team and Incident Investigations

Rules of Engagement, Authorization, and Scope

Incident Response Procedures

Table of Contents

Incident Response Management

Detect

Respond

Mitigate

Report

Recover

Remediate

Review and Lessons Learned

Detective and Preventive Measures

IDS/IPS

Firewalls

Whitelisting/Blacklisting

Third-Party Security Services

Sandboxing

Honeypots/Honeynets

Anti-malware/Antivirus

Clipping Levels

Deviations from Standards

Unusual or Unexplained Events

Unscheduled Reboots

Unauthorized Disclosure

Trusted Recovery

Trusted Paths

Input/Output Controls

System Hardening

Vulnerability Management Systems

Machine Learning and Artificial Intelligence (AI)-Based Tools

Patch and Vulnerability Management

Recovery Strategies

Table of Contents

Create Recovery Strategies
Categorize Asset Recovery Priorities
Business Process Recovery
Supply and Technology Recovery
User Environment Recovery
Data Recovery
Training Personnel
Backup Storage Strategies
Recovery and Multiple Site Strategies
Hot Site
Cold Site
Warm Site
Tertiary Site
Reciprocal Agreements
Redundant Sites
Resource Capacity Agreement
Redundant Systems, Facilities, and Power
Fault-Tolerance Technologies
Insurance
Data Backup
Fire Detection and Suppression
High Availability
Quality of Service
System Resilience
Disaster Recovery
 Response
 Personnel
 Damage Assessment Team
 Legal Team
 Media Relations Team

Table of Contents

- Recovery Team
- Relocation Team
- Restoration Team
- Salvage Team
- Security Team
- Communications
- Assessment
- Restoration
- Training and Awareness
- Lessons Learned

Testing Disaster Recovery Plans

- Read-Through Test
- Checklist Test
- Table-Top Exercise
- Structured Walk-Through Test
- Simulation Test
- Parallel Test
- Full-Interruption Test
- Functional Drill
- Evacuation Drill

Business Continuity Planning and Exercises

Physical Security

- Perimeter Security Controls
- Gates and Fences
- Perimeter Intrusion Detection
- Lighting
- Patrol Force
- Access Control
- Building and Internal Security Controls

Table of Contents

Personnel Safety and Security

- Duress

- Travel

- Monitoring

- Emergency Management

- Security Training and Awareness

Exam Preparation Tasks

- Review All Key Topics

- Define Key Terms

- Answer Review Questions

- Answers and Explanations

Chapter 8 Software Development Security

Foundation Topics

Software Development Concepts

- Machine Languages

- Assembly Languages and Assemblers

- High-Level Languages, Compilers, and Interpreters

- Object-Oriented Programming

- Polymorphism

- Polyinstantiation

- Encapsulation

- Cohesion

- Coupling

- Data Structures

- Distributed Object-Oriented Systems

- CORBA

- COM and DCOM

- OLE

Table of Contents

Java

SOA

Mobile Code

Java Applets

ActiveX

NIST SP 800-163

Security in the System and Software Development Life Cycle

System Development Life Cycle

Initiate

Acquire/Develop

Implement

Operate/Maintain

Dispose/Decommission

Software Development Life Cycle

Plan/Initiate Project

Gather Requirements

Design

Develop

Test/Validate

Release/Maintenance

Certify/Accredit

Change Management and Configuration Management/Replacement

DevSecOps

Static Application Security Testing (SAST) and Dynamic Application Security
Testing (DAST)

Interactive Application Security Test (IAST)

Software Composition Analysis

Software Development Methods and Maturity Models

Build and Fix Model

Waterfall Model

Table of Contents

V-shaped Model

Prototyping

Modified Prototype Model (MPM)

Incremental Model

Spiral Model

Agile Model

Scaled Agile Framework (SAFe)

Continuous Integration and Continuous Delivery (CI/CD)

Rapid Application Development (RAD) Model

Joint Analysis Development (JAD) Model

Cleanroom Model

Structured Programming Development Model

Exploratory Model

Computer-Aided Software Engineering (CASE)

Component-Based Development

CMMI

ISO 9001:2015/90003:2014

IDEAL Model

Operation and Maintenance

Integrated Product Team

Security Controls in Development

Software Development Security Best Practices

WASC

OWASP

BSI

ISO/IEC 27000

Software Environment Security

Source Code Analysis Tools

Code Repository Security

Software Threats

Table of Contents

Malware

Malware Protection

Scanning Types

Security Policies

Software Protection Mechanisms

Assess Software Security Effectiveness

Auditing and Logging

Risk Analysis and Mitigation

Regression and Acceptance Testing

Security Impact of Acquired Software

Secure Coding Guidelines and Standards

Security Weaknesses and Vulnerabilities at the Source Code Level

Buffer Overflow

Escalation of Privileges

Backdoor

Rogue Programmers

Covert Channel

Object Reuse

Mobile Code

Time of Check/Time of Use (TOC/TOU)

Security of Application Programming Interfaces

Secure Coding Practices

Validate Input

Heed Compiler Warnings

Design for Security Policies

Implement Default Deny

Adhere to the Principle of Least Privilege, and Practice Defense in Depth

Sanitize Data Prior to Transmission to Other Systems

Exam Preparation Tasks

Table of Contents

Review All Key Topics

Define Key Terms

Answer Review Questions

Answers and Explanations

Chapter 9 Final Preparation

Tools for Final Preparation

Pearson Test Prep Practice Test Engine and Questions on the Website

Accessing the Pearson Test Prep Practice Test Software Online

Accessing the Pearson Test Prep Practice Test Software Offline

Customizing Your Exams

Updating Your Exams

Premium Edition

Memory Tables

Chapter-Ending Review Tools

Suggested Plan for Final Review/Study

Summary

Index

Online Elements

Appendix A Memory Tables

Appendix B Memory Tables Answer Key

Glossary

A

B

C

D

E

F

G

Table of Contents

H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z