PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CISSP

Fourth Edition

ROBIN ABERNATHY
Dr. DARREN R. HAYES

CISSP Cert Guide

Fourth Edition

Robin Abernathy
Darren Hayes

CISSP Cert Guide

ISBN-13: 978-0-13-750747-4

ISBN-10: 0-13-750747-X

Library of Congress Control Number: 2022943249

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Executive Editor
James Manly

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Chuck Hutchinson

Indexer
Erika Millen

Proofreader
Jen Hinchliffe

Technical Editors
R. Sarma Danturthi
Ben Mayo

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Contents at a Glance

Introduction xlvii

CHAPTER 1 Security and Risk Management 5

CHAPTER 2 Asset Security 165

CHAPTER 3 Security Architecture and Engineering 213

CHAPTER 4 Communication and Network Security 377

CHAPTER 5 Identity and Access Management (IAM) 535

CHAPTER 6 Security Assessment and Testing 601

CHAPTER 7 Security Operations 637

CHAPTER 8 Software Development Security 733

CHAPTER 9 Final Preparation 791

Index 797

Online Elements

APPENDIX A Memory Tables

APPENDIX B Memory Tables Answer Key

Glossary

Table of Contents

Introduction xlvii

Chapter 1 Security and Risk Management 5

Security Terms 6

CIA 6

Confidentiality 6

Integrity 7

Availability 7

Auditing and Accounting 7

Non-repudiation 8

Default Security Posture 8

Defense in Depth 9

Abstraction 10

Data Hiding 10

Encryption 10

Security Governance Principles 10

Security Function Alignment 12

Organizational Strategies and Goals 12

Organizational Mission and Objectives 12

Business Case 13

Security Budget, Metrics, and Efficacy 13

Resources 14

Organizational Processes 14

Acquisitions and Divestitures 15

Governance Committees 16

Organizational Roles and Responsibilities 16

Board of Directors 16

Management 17

Audit Committee 18

Data Owner 18

Data Custodian 19

System Owner 19

System Administrator 19

Security Analyst 19

Application Owner 19

Supervisor 20

User 20

Auditor 20

Security Control Frameworks 20

ISO/IEC 27000 Series 21

Zachman Framework 25

The Open Group Architecture Framework (TOGAF) 25

Department of Defense Architecture Framework (DoDAF) 25

British Ministry of Defence Architecture Framework (MODAF) 25

Sherwood Applied Business Security Architecture (SABSA) 25

Control Objectives for Information and Related Technology (COBIT) 27

National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series 27

HITRUST CSF 30

CIS Critical Security Controls 31

Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework 32

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) 32

Information Technology Infrastructure Library (ITIL) 33

Six Sigma 34

Capability Maturity Model Integration (CMMI) 35

CCTA Risk Analysis and Management Method (CRAMM) 36

Top-Down Versus Bottom-Up Approach 36

Security Program Life Cycle 37

Due Care and Due Diligence 38

Compliance 38

Contractual, Legal, Industry Standards, and Regulatory Compliance 40

Privacy Requirements Compliance 40

Legal and Regulatory Issues 41

Computer Crime Concepts 41

Computer-Assisted Crime 41

Computer-Targeted Crime 41
Incidental Computer Crime 42
Computer Prevalence Crime 42
Hackers Versus Crackers 42
Computer Crime Examples 42
Major Legal Systems 43
Civil Law 44
Common Law 44
Criminal Law 44
Civil/Tort Law 45
Administrative/Regulatory Law 45
Customary Law 45
Religious Law 45
Mixed Law 45
Licensing and Intellectual Property 46
Patent 46
Trade Secret 47
Trademark 47
Copyright 48
Software Piracy and Licensing Issues 49
Internal Protection 49
Digital Rights Managements (DRM) 50
Cyber Crimes and Data Breaches 50
Import/Export Controls 51
Trans-Border Data Flow 51
Privacy 52
Personally Identifiable Information (PII) 52
Laws and Regulations 53
Investigation Types 62
Operations/Administrative 63
Criminal 63
Civil 64
Regulatory 64

Industry Standards 64
eDiscovery 67
Professional Ethics 67
(ISC)^2 Code of Ethics 67
Computer Ethics Institute 68
Internet Architecture Board 68
Organizational Code of Ethics 69
Security Documentation 69
Policies 70
Organizational Security Policy 71
System-Specific Security Policy 72
Issue-Specific Security Policy 72
Policy Categories 72
Processes 72
Procedures 72
Standards 73
Guidelines 73
Baselines 73
Business Continuity 73
Business Continuity and Disaster Recovery Concepts 73
Disruptions 74
Disasters 74
Disaster Recovery and the Disaster Recovery Plan (DRP) 75
Continuity Planning and the Business Continuity Plan (BCP) 76
Business Impact Analysis (BIA) 76
Contingency Plan 76
Availability 77
Reliability 77
Scope and Plan 77
Personnel Components 77
Scope 78
Business Contingency Planning 78
BIA Development 81
Identify Critical Processes and Resources 82

Identify Outage Impact and Estimate Downtime 82
Identify Resource Requirements 84
Identify Recovery Priorities 84
Personnel Security Policies and Procedures 85
Candidate Screening and Hiring 85
Employment Agreements and Policies 87
Employee Onboarding and Offboarding Policies 88
Vendor, Consultant, and Contractor Agreements and Controls 88
Compliance Policy Requirements 89
Privacy Policy Requirements 89
Job Rotation 89
Separation of Duties 89
Risk Management Concepts 90
Asset and Asset Valuation 90
Vulnerability 91
Threat 91
Threat Agent 91
Exploit 91
Risk 91
Exposure 92
Countermeasure 92
Risk Appetite 92
Attack 93
Breach 93
Risk Management Policy 94
Risk Management Team 94
Risk Analysis Team 94
Risk Assessment 95
Information and Asset (Tangible/Intangible) Value and Costs 95
Identity Threats and Vulnerabilities 96
Risk Assessment/Analysis 96
Countermeasure (Safeguard) Selection 98
Inherent Risk Versus Residual Risk 99
Handling Risk and Risk Response 99

Implementation 100
Control Categories 100
Compensative 101
Corrective 101
Detective 101
Deterrent 102
Directive 102
Preventive 102
Recovery 102
Control Types 102
Administrative (Management) 103
Logical (Technical) 105
Physical 105
Controls Assessment, Monitoring, and Measurement 108
Reporting and Continuous Improvement 108
Risk Frameworks 109
NIST 109
ISO/IEC 27005:2018 126
Open Source Security Testing Methodology Manual (OSSTMM) 127
COSO's Enterprise Risk Management (ERM) Integrated Framework 127
A Risk Management Standard *by the Federation of European Risk Management Associations (FERMA) 128*
Geographical Threats 129
Internal Versus External Threats 129
Natural Threats 130
Hurricanes/Tropical Storms 130
Tornadoes 130
Earthquakes 130
Floods 131
Volcanoes 131
System Threats 131
Electrical 131
Communications 132
Utilities 133

Human-Caused Threats 133
Explosions 133
Fire 133
Vandalism 134
Fraud 135
Theft 135
Collusion 135
Politically Motivated Threats 135
Strikes 136
Riots 136
Civil Disobedience 136
Terrorist Acts 136
Bombing 137
Threat Modeling 137
Threat Modeling Concepts 138
Threat Modeling Methodologies 138
STRIDE Model 139
Process for Attack Simulation and Threat Analysis (PASTA) Methodology 139
Trike Methodology 139
Visual, Agile, and Simple Threat (VAST) Model 140
NIST SP 800-154 140
Identifying Threats 141
Potential Attacks 142
Remediation Technologies and Processes 143
Security Risks in the Supply Chain 143
Risks Associated with Hardware, Software, and Services 144
Third-Party Assessment and Monitoring 144
Onsite Assessment 144
Document Exchange/Review 145
Process/Policy Review 145
Other Third-Party Governance Issues 145
Minimum Service-Level and Security Requirements 145
Service-Level Requirements 146

Security Education, Training, and Awareness 147
Levels Required 147
Methods and Techniques 148
Periodic Content Reviews 148
Review All Key Topics 148
Complete the Tables and Lists from Memory 150
Define Key Terms 150
Answers and Explanations 157
Chapter 2 Asset Security 165
Asset Security Concepts 166
Asset and Data Policies 166
Data Quality 167
Data Documentation and Organization 168
Identify and Classify Information and Assets 169
Data and Asset Classification 170
Sensitivity and Criticality 170
PII 171
PHI 173
Proprietary Data 175
Private Sector Data Classifications 175
Military and Government Data Classifications 176
Information and Asset Handling Requirements 177
Marking, Labeling, and Storing 178
Destruction 178
Provision Resources Securely 179
Asset Inventory and Asset Management 179
Data Life Cycle 180
Databases 182
DBMS Architecture and Models 182
Database Interface Languages 185
Data Warehouses and Data Mining 185
Database Maintenance 186
Database Threats 186
Database Views 187

Database Locks 187
Polyinstantiation 187
Database ACID Test 187
Roles and Responsibilities 188
Data Owner 188
Data Controller 189
Data Custodian 189
System Owners 189
System Custodians 190
Business/Mission Owners 190
Data Processors 190
Data Users and Subjects 191
Data Collection and Limitation 191
Data Location 192
Data Maintenance 192
Data Retention 193
Data Remanence and Destruction 193
Data Audit 194
Asset Retention 195
Data Security Controls 197
Data Security 197
Data States 197
Data at Rest 198
Data in Transit 198
Data in Use 198
Data Access and Sharing 198
Data Storage and Archiving 199
Baselines 200
Scoping and Tailoring 201
Standards Selection 201
Data Protection Methods 202
Cryptography 202
Digital Rights Management (DRM) 203

Data Loss Prevention (DLP) 204
Cloud Access Security Broker (CASB) 204
Review All Key Topics 205
Define Key Terms 205
Answers and Explanations 207
Chapter 3 Security Architecture and Engineering 213
Engineering Processes Using Secure Design Principles 214
Objects and Subjects 215
Closed Versus Open Systems 215
Threat Modeling 215
Least Privilege 216
Defense in Depth 216
Secure Defaults 216
Fail Securely 217
Separation of Duties (SoD) 217
Keep It Simple 218
Zero Trust 218
Privacy by Design 218
Trust but Verify 219
Shared Responsibility 219
Security Model Concepts 220
Confidentiality, Integrity, and Availability 220
Confinement 220
Bounds 221
Isolation 221
Security Modes 221
Dedicated Security Mode 221
System High Security Mode 221
Compartmented Security Mode 222
Multilevel Security Mode 222
Assurance and Trust 222
Security Model Types 222
State Machine Models 223
Multilevel Lattice Models 223

Matrix-Based Models 223
Noninterference Models 224
Information Flow Models 224
Take-Grant Model 225
Security Models 226
Bell-LaPadula Model 226
Biba Model 228
Clark-Wilson Integrity Model 228
Lipner Model 229
Brewer-Nash (Chinese Wall) Model 229
Graham-Denning Model 230
Harrison-Ruzzo-Ullman Model 230
Goguen-Meseguer Model 230
Sutherland Model 230
System Architecture Steps 230
ISO/IEC 42010:2011 231
Computing Platforms 231
Mainframe/Thin Clients 232
Distributed Systems 232
Middleware 232
Embedded Systems 232
Mobile Computing 233
Virtual Computing 233
Security Services 234
Boundary Control Services 234
Access Control Services 234
Integrity Services 234
Cryptography Services 234
Auditing and Monitoring Services 234
System Components 235
CPU 235
Memory and Storage 238
Input/Output Devices 241
Input/Output Structures 241

Firmware 242
Operating Systems 243
Memory Management 244
System Security Evaluation Models 244
TCSEC 245
Rainbow Series 245
ITSEC 248
Common Criteria 250
Security Implementation Standards 252
ISO/IEC 27001 253
ISO/IEC 27002 254
Payment Card Industry Data Security Standard (PCI DSS) 255
Controls and Countermeasures 255
Certification and Accreditation 256
Control Selection Based on Systems Security Requirements 256
Security Capabilities of Information Systems 257
Memory Protection 257
Trusted Platform Module 258
Interfaces 259
Fault Tolerance 259
Policy Mechanisms 260
Separation of Privilege 260
Accountability 260
Encryption/Decryption 260
Security Architecture Maintenance 261
Vulnerabilities of Security Architectures, Designs, and Solution Elements 261
Client-Based Systems 262
Server-Based Systems 263
Data Flow Control 263
Database Systems 264
Inference 264
Aggregation 264
Contamination 264

Data Mining Warehouse 264
Cryptographic Systems 265
Industrial Control Systems 265
Cloud-Based Systems 268
Large-Scale Parallel Data Systems 274
Distributed Systems 275
Grid Computing 275
Peer-to-Peer Computing 275
Internet of Things 276
IoT Examples 277
Methods of Securing IoT Devices 277
NIST Framework for Cyber-Physical Systems 278
Microservices 280
Containerization 281
Serverless Systems 281
High-Performance Computing Systems 282
Edge Computing Systems 282
Virtualized Systems 283
Vulnerabilities in Web-Based Systems 283
Maintenance Hooks 284
Time-of-Check/Time-of-Use Attacks 284
Web-Based Attacks 285
XML 285
SAML 285
OWASP 286
Vulnerabilities in Mobile Systems 286
Device Security 287
Application Security 287
Mobile Device Concerns 287
NIST SP 800-164 290
Vulnerabilities in Embedded Systems 291
Cryptographic Solutions 292
Cryptography Concepts 292
Cryptography History 294

Julius Caesar and the Caesar Cipher 295
Vigenere Cipher 295
Kerckhoffs's Principle 297
World War II Enigma 297
Lucifer by IBM 298
Cryptosystem Features 298
Authentication 298
Confidentiality 298
Integrity 298
Authorization 299
Non-repudiation 299
NIST SP 800-175A and B 299
Cryptographic Mathematics 300
Boolean 300
Logical Operations (And, Or, Not, Exclusive Or) 300
Modulo Function 302
One-Way Function 302
Nonce 302
Split Knowledge 302
Cryptographic Life Cycle 302
Key Management 303
Algorithm Selection 304
Cryptographic Types 304
Running Key and Concealment Ciphers 305
Substitution Ciphers 305
One-Time Pads 306
Steganography 307
Transposition Ciphers 307
Symmetric Algorithms 308
Stream-Based Ciphers 309
Block Ciphers 310
Initialization Vectors (IVs) 310
Asymmetric Algorithms 310
Hybrid Ciphers 311

Elliptic Curves 312
Quantum Cryptography 312
Symmetric Algorithms 312
DES and 3DES 313
DES Modes 313
3DES and Modes 316
AES 316
IDEA 317
Skipjack 317
Blowfish 317
Twofish 318
RC4/RC5/RC6/RC7 318
CAST 318
Asymmetric Algorithms 319
Diffie-Hellman 320
RSA 320
El Gamal 321
ECC 321
Knapsack 322
Zero-Knowledge Proof 322
Public Key Infrastructure and Digital Certificates 322
Certificate Authority and Registration Authority 323
Certificates 323
Certificate Life Cycle 324
Enrollment 325
Verification 326
Revocation 326
Renewal and Modification 327
Certificate Revocation List 327
OCSP 327
PKI Steps 327
Cross-Certification 328
Key Management Practices 328
Message Integrity 332

Hashing 333
One-Way Hash 333
MD2/MD4/MD5/MD6 335
SHA/SHA-2/SHA-3 336
HAVAL 337
RIPEMD-160 337
Tiger 337
Message Authentication Code 337
HMAC 337
CBC-MAC 338
CMAC 338
Salting 339
Digital Signatures and Non-repudiation 339
DSS 340
Non-repudiation 340
Applied Cryptography 340
Link Encryption Versus End-to-End Encryption 340
Email Security 340
Internet Security 341
Cryptanalytic Attacks 341
Ciphertext-Only Attack 342
Known Plaintext Attack 342
Chosen Plaintext Attack 342
Chosen Ciphertext Attack 342
Social Engineering 342
Brute Force 343
Differential Cryptanalysis 343
Linear Cryptanalysis 343
Algebraic Attack 343
Frequency Analysis 343
Birthday Attack 344
Dictionary Attack 344
Replay Attack 344

Analytic Attack 344
Statistical Attack 344
Factoring Attack 344
Reverse Engineering 344
Meet-in-the-Middle Attack 345
Ransomware Attack 345
Side-Channel Attack 345
Implementation Attack 345
Fault Injection 345
Timing Attack 346
Pass-the-Hash Attack 346
Digital Rights Management 346
Document DRM 347
Music DRM 347
Movie DRM 347
Video Game DRM 348
E-book DRM 348
Site and Facility Design 348
Layered Defense Model 348
CPTED 348
Natural Access Control 349
Natural Surveillance 349
Natural Territorials Reinforcement 349
Physical Security Plan 350
Deter Criminal Activity 350
Delay Intruders 350
Detect Intruders 350
Assess Situation 350
Respond to Intrusions and Disruptions 350
Facility Selection Issues 351
Visibility 351
Surrounding Area and External Entities 351
Accessibility 351
Construction 352

Internal Compartments 352
Computer and Equipment Rooms 353
Site and Facility Security Controls 353
Doors 353
Door Lock Types 354
Turnstiles and Mantraps 354
Locks 355
Biometrics 356
Type of Glass Used for Entrances 356
Visitor Control 357
Wiring Closets/Intermediate Distribution Facilities 357
Restricted and Work Areas 357
Secure Data Center 357
Restricted Work Area 358
Server Room 358
Media Storage Facilities 358
Evidence Storage 358
Environmental Security and Issues 358
Fire Protection 359
Power Supply 360
HVAC 361
Water Leakage and Flooding 362
Environmental Alarms 362
Equipment Physical Security 362
Corporate Procedures 362
Safes, Vaults, and Locking 364
Review All Key Topics 364
Complete the Tables and Lists from Memory 366
Define Key Terms 366
Answers and Explanations 372
Chapter 4 Communication and Network Security 377
Secure Network Design Principles 378
OSI Model 378
Application Layer 379

Presentation Layer 379
Session Layer 380
Transport Layer 380
Network Layer 380
Data Link Layer 381
Physical Layer 381
TCP/IP Model 383
Application Layer 383
Transport Layer 384
Internet Layer 386
Link Layer 388
Encapsulation and De-encapsulation 388
IP Networking 389
Common TCP/UDP Ports 389
Logical and Physical Addressing 391
IPv4 392
IP Classes 393
Public Versus Private IP Addresses 394
NAT 394
MAC Addressing 399
Network Transmission 399
Analog Versus Digital 399
Asynchronous Versus Synchronous 400
Broadband Versus Baseband 401
Unicast, Multicast, and Broadcast 402
Wired Versus Wireless 403
IPv6 403
NIST SP 800-119 404
IPv6 Major Features 406
IPv4 Versus IPv6 Threat Comparison 409
IPv6 Addressing 410
Shorthand for Writing IPv6 Addresses 412
IPv6 Address Types 414
IPv6 Address Scope 415

Network Types 416
Local-Area Network (LAN) 417
Intranet 417
Extranet 418
MAN 418
WAN 419
WLAN 420
SAN 420
CAN 421
PAN 421
Protocols and Services 421
ARP/RARP 422
DHCP/BOOTP 423
DNS 424
FTP, FTPS, SFTP, and TFTP 424
HTTP, HTTPS, and S-HTTP 425
ICMP 425
IGMP 426
IMAP 426
LDAP 426
LDP 426
NAT 426
NetBIOS 426
NFS 427
PAT 427
POP 427
CIFS/SMB 427
SMTP 427
SNMP 427
SSL/TLS 428
Multilayer Protocols 428
Converged Protocols 429
FCoE 429
MPLS 430

VoIP 431
iSCSI 431
Wireless Networks 431
FHSS, DSSS, OFDM, VOFDM, FDMA, TDMA, CDMA, OFDMA, and GSM 432
802.11 Techniques 432
Cellular or Mobile Wireless Techniques 433
5G 434
Satellites 435
WLAN Structure 435
Access Point 435
Service Set Identifier (SSID) 436
Infrastructure Mode Versus Ad Hoc Mode 436
WLAN Standards 436
802.11 436
802.11a 436
802.11b 437
802.11g 437
802.11n (Wi-Fi 4) 437
802.11ac (Wi-Fi 5) 437
802.11ax (Wi-Fi 6) 438
802.11be (Wi-Fi 7) 438
Bluetooth 438
Infrared 439
Near Field Communication (NFC) 439
Zigbee 439
WLAN Security 439
Open System Authentication 440
Shared Key Authentication 440
WEP 440
WPA 440
WPA2 441
Personal Versus Enterprise 441
WPA3 441
802.1X 442

SSID Broadcast 443
MAC Filter 444
Wireless Site Surveys 444
Antenna Placement and Power Levels 444
Antenna Types 445
Communications Cryptography 445
Link Encryption 445
End-to-End Encryption 446
Email Security 446
PGP 446
MIME and S/MIME 447
Quantum Cryptography 448
Internet Security 448
Remote Access 448
HTTP, HTTPS, and S-HTTP 449
Secure Electronic Transaction (SET) 449
Cookies 449
SSH 450
IPsec 450
Secure Network Components 450
Hardware 450
Network Devices 450
Network Routing 468
Transmission Media 471
Cabling 471
Network Topologies 475
Network Technologies 479
WAN Technologies 486
Network Access Control Devices 491
Quarantine/Remediation 492
Firewalls/Proxies 493
Endpoint Security 493
Content-Distribution Networks 494

Secure Communication Channels 495
Voice 495
Multimedia Collaboration 495
Remote Meeting Technology 496
Instant Messaging 496
Remote Access 497
Remote Connection Technologies 497
VPN Screen Scraper 506
Virtual Application/Desktop 506
Telecommuting/Teleworking 506
Data Communications 507
Virtualized Networks 507
SDN 507
Virtual SAN 508
Guest Operating Systems 508
Federated Identity with a Third-Party 508
Network Attacks 509
Cabling 509
Noise 509
Attenuation 509
Crosstalk 510
Eavesdropping 510
Network Component Attacks 510
Non-Blind Spoofing 510
Blind Spoofing 511
Man-in-the-Middle Attack 511
MAC Flooding Attack 511
802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack 511
Double-Encapsulated 802.1Q/Nested VLAN Attack 512
ARP Attack 512
ICMP Attacks 512
Ping of Death 512
Smurf 512
Fraggle 513
ICMP Redirect 513

Ping Scanning 513
Traceroute Exploitation 513
DNS Attacks 514
DNS Cache Poisoning 514
DoS 514
DDoS 515
DNSSEC 515
URL Hiding 515
Domain Grabbing 516
Cybersquatting 516
Email Attacks 516
Email Spoofing 516
Spear Phishing 517
Whaling 518
Spam 518
Wireless Attacks 518
Wardriving 518
Warchalking 519
Remote Attacks 519
Other Attacks 519
SYN ACK Attacks 519
Session Hijacking 519
Port Scanning 520
Teardrop 520
IP Address Spoofing 520
Zero-Day 521
Ransomware 521
Review All Key Topics 521
Define Key Terms 522
Answers and Explanations 529

Chapter 5 Identity and Access Management (IAM) 535

Access Control Process 536
Identify Resources 536
Identify Users 536
Identify the Relationships Between Resources and Users 537

Physical and Logical Access to Assets 537
Access Control Administration 538
Centralized 538
Decentralized 539
Information 539
Systems 539
Devices 540
Facilities 540
Applications 541
Identification and Authentication Concepts 541
NIST SP 800-63 542
Five Factors for Authentication 546
Knowledge Factors 546
Ownership Factors 550
Characteristic Factors 551
Location Factors 556
Time Factors 557
Single-Factor Versus Multifactor Authentication 557
Device Authentication 557
Identification and Authentication Implementation 558
Separation of Duties 558
Least Privilege/Need-to-Know 559
Default to No Access 560
Directory Services 560
Single Sign-on 561
Kerberos 562
SESAME 564
OpenID Connect (OIDC)/Open Authorization (Oauth) 564
Security Assertion Markup Language (SAML) 564
Federated Identity Management (IdM) 564
Security Domains 565
Session Management 566
Registration, Proof, and Establishment of Identity 566
Credential Management Systems 567

Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+) 568
Accountability 568
Auditing and Reporting 569
Just-In-Time (JIT) 570
Identity as a Service (IDaaS) Implementation 571
Third-Party Identity Services Integration 571
Authorization Mechanisms 572
Permissions, Rights, and Privileges 572
Access Control Models 572
Discretionary Access Control 573
Mandatory Access Control 573
Role-Based Access Control 574
Rule-Based Access Control 574
Attribute-Based Access Control 575
Content-Dependent Versus Context-Dependent 578
Risk-Based Access Control 578
Access Control Matrix 579
Access Control Policies 580
Provisioning Life Cycle 580
Provisioning 581
Identity and Account Management 581
User, System, and Service Account Access Review 582
Account Transfers 582
Account Revocation 583
Role Definition 583
Privilege Escalation 583
Access Control Threats 584
Password Threats 585
Dictionary Attack 585
Brute-Force Attack 585
Birthday Attack 586
Rainbow Table Attack 586
Sniffer Attack 586

Social Engineering Threats 586
Phishing/Pharming 586
Shoulder Surfing 587
Identity Theft 587
Dumpster Diving 587
DoS/DDoS 588
Buffer Overflow 588
Mobile Code 588
Malicious Software 589
Spoofing 589
Sniffing and Eavesdropping 589
Emanating 590
Backdoor/Trapdoor 590
Access Aggregation 590
Advanced Persistent Threat 591
Prevent or Mitigate Access Control Threats 591
Review All Key Topics 592
Define Key Terms 593
Answers and Explanations 596

Chapter 6 Security Assessment and Testing 601

Design and Validate Assessment and Testing Strategies 602
Security Testing 602
Security Assessments 603
Red Team versus Blue Team 603
Security Auditing 604
Internal, External, and Third-party Security Assessment, Testing, and Auditing 604
Conduct Security Control Testing 605
Vulnerability Assessment 605
Network Discovery Scan 606
Network Vulnerability Scan 607
Web Application Vulnerability Scan 609
Penetration Testing 609
Log Reviews 611

NIST SP 800-92 612
Synthetic Transactions 616
Code Review and Testing 616
Code Review Process 618
Static Testing 618
Dynamic Testing 618
Fuzz Testing 619
Misuse Case Testing 619
Test Coverage Analysis 619
Interface Testing 620
Collect Security Process Data 620
NIST SP 800-137 620
Account Management 621
Management Review and Approval 622
Key Performance and Risk Indicators 622
Backup Verification Data 623
Training and Awareness 623
Disaster Recovery and Business Continuity 624
Analyze Test Outputs and Generate a Report 624
Conduct or Facilitate Security Audits 624
Review All Key Topics 626
Define Key Terms 627
Answers and Explanations 630
Chapter 7 Security Operations 637
Investigations 638
Forensic and Digital Investigations 638
Identify Evidence 640
Preserve and Collect Evidence 640
Examine and Analyze Evidence 641
Present Findings 641
Decide 641
Forensic Procedures 641
Reporting and Documentation 642
IOCE/SWGDE and NIST 642

Crime Scene 643
MOM 644
Chain of Custody 644
Interviewing 645
Investigative Techniques 645
Evidence Collection and Handling 646
Five Rules of Evidence 646
Types of Evidence 647
Surveillance, Search, and Seizure 649
Media Analysis 650
Software Analysis 650
Network Analysis 650
Hardware/Embedded Device Analysis 651
Digital Forensic Tools, Tactics, and Procedures 651
Logging and Monitoring Activities 654
Audit and Review 654
Log Types 655
Audit Types 656
Intrusion Detection and Prevention 656
Security Information and Event Management (SIEM) 656
Continuous Monitoring 657
Egress Monitoring 657
Log Management 658
Threat Intelligence 658
User and Entity Behavior Analytics (UEBA) 659
Configuration and Change Management 659
Resource Provisioning 661
Asset Inventory and Management 661
Baselining 664
Automation 664
Security Operations Concepts 664
Need to Know/Least Privilege 664
Managing Accounts, Groups, and Roles 665
Separation of Duties and Responsibilities 666

Privilege Account Management 666
Job Rotation and Mandatory Vacation 666
Two-Person Control 667
Sensitive Information Procedures 667
Record Retention 667
Information Life Cycle 668
Service-Level Agreements 668
Resource Protection 669
Protecting Tangible and Intangible Assets 669
Facilities 669
Hardware 670
Software 670
Information Assets 671
Asset Management 671
Redundancy and Fault Tolerance 671
Backup and Recovery Systems 672
Identity and Access Management 672
Media Management 672
Media History 678
Media Labeling and Storage 678
Sanitizing and Disposing of Media 678
Network and Resource Management 679
Incident Management 680
Event Versus Incident 680
Incident Response Team and Incident Investigations 681
Rules of Engagement, Authorization, and Scope 681
Incident Response Procedures 682
Incident Response Management 682
Detect 683
Respond 683
Mitigate 683
Report 684
Recover 684
Remediate 684
Review and Lessons Learned 684

Detective and Preventive Measures 684
IDS/IPS 685
Firewalls 685
Whitelisting/Blacklisting 685
Third-Party Security Services 686
Sandboxing 686
Honeypots/Honeynets 686
Anti-malware/Antivirus 686
Clipping Levels 686
Deviations from Standards 687
Unusual or Unexplained Events 687
Unscheduled Reboots 687
Unauthorized Disclosure 687
Trusted Recovery 688
Trusted Paths 688
Input/Output Controls 688
System Hardening 688
Vulnerability Management Systems 689
Machine Learning and Artificial Intelligence (AI)-Based Tools 689
Patch and Vulnerability Management 689
Recovery Strategies 690
Create Recovery Strategies 691
Categorize Asset Recovery Priorities 691
Business Process Recovery 692
Supply and Technology Recovery 692
User Environment Recovery 695
Data Recovery 696
Training Personnel 699
Backup Storage Strategies 699
Recovery and Multiple Site Strategies 700
Hot Site 701
Cold Site 702
Warm Site 702
Tertiary Site 702

Reciprocal Agreements *703*
Redundant Sites *703*
Redundant Systems, Facilities, and Power 703
Fault-Tolerance Technologies 704
Insurance 704
Data Backup 705
Fire Detection and Suppression 705
High Availability 705
Quality of Service 706
System Resilience 706
Disaster Recovery 706
Response 707
Personnel 707
Damage Assessment Team *708*
Legal Team *708*
Media Relations Team *708*
Recovery Team *708*
Relocation Team *709*
Restoration Team *709*
Salvage Team *709*
Security Team *709*
Communications 709
Assessment 710
Restoration 710
Training and Awareness 710
Lessons Learned 710
Testing Disaster Recovery Plans 711
Read-Through Test 711
Checklist Test 712
Table-Top Exercise 712
Structured Walk-Through Test 712
Simulation Test 712
Parallel Test 712
Full-Interruption Test 712

Functional Drill 713
Evacuation Drill 713
Business Continuity Planning and Exercises 713
Physical Security 713
Perimeter Security Controls 713
Gates and Fences 714
Perimeter Intrusion Detection 716
Lighting 718
Patrol Force 719
Access Control 719
Building and Internal Security Controls 719
Personnel Safety and Security 719
Duress 720
Travel 720
Monitoring 720
Emergency Management 721
Security Training and Awareness 721
Review All Key Topics 722
Define Key Terms 723
Answers and Explanations 727
Chapter 8 Software Development Security 733
Software Development Concepts 734
Machine Languages 734
Assembly Languages and Assemblers 734
High-Level Languages, Compilers, and Interpreters 734
Object-Oriented Programming 735
Polymorphism 736
Polyinstantiation 736
Encapsulation 736
Cohesion 737
Coupling 737
Data Structures 737
Distributed Object-Oriented Systems 737
CORBA 737

COM and DCOM 738
OLE 738
Java 738
SOA 739
Mobile Code 739
Java Applets 739
ActiveX 739
NIST SP 800-163 740
Security in the System and Software Development Life Cycle 743
System Development Life Cycle 743
Initiate 744
Acquire/Develop 744
Implement 745
Operate/Maintain 745
Dispose 745
Software Development Life Cycle 746
Plan/Initiate Project 746
Gather Requirements 747
Design 747
Develop 748
Test/Validate 748
Release/Maintenance 749
Certify/Accredit 749
Change Management and Configuration Management/Replacement 749
DevSecOps 750
Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) 750
Security Orchestration and Automated Response (SOAR) 751
Software Development Methods and Maturity Models 751
Build and Fix Model 752
Waterfall Model 753
V-Shaped Model 754
Prototyping 754

Modified Prototype Model (MPM) 755
Incremental Model 755
Spiral Model 756
Agile Model 756
Continuous Integration and Continuous Delivery (CI/CD) 757
Rapid Application Development (RAD) 758
Joint Analysis Development (JAD) 758
Cleanroom Model 758
Structured Programming Development Model 759
Exploratory Model 759
Computer-Aided Software Engineering (CASE) 759
Component-Based Development 759
CMMI 759
ISO 9001:2015/90003:2014 760
IDEAL Model 761
Operation and Maintenance 762
Integrated Product Team 763
Security Controls in Development 764
Software Development Security Best Practices 764
WASC 764
OWASP 765
BSI 765
ISO/IEC 27000 765
Software Environment Security 765
Source Code Analysis Tools 766
Code Repository Security 766
Software Threats 766
Malware 767
Malware Protection 771
Scanning Types 772
Security Policies 772
Software Protection Mechanisms 772

Assess Software Security Effectiveness 774
Auditing and Logging 774
Risk Analysis and Mitigation 774
Regression and Acceptance Testing 775
Security Impact of Acquired Software 775
Secure Coding Guidelines and Standards 776
Security Weaknesses and Vulnerabilities at the Source Code Level 776
Buffer Overflow 776
Escalation of Privileges 778
Backdoor 778
Rogue Programmers 778
Covert Channel 779
Object Reuse 779
Mobile Code 779
Time of Check/Time of Use (TOC/TOU) 779
Security of Application Programming Interfaces 780
Secure Coding Practices 780
Validate Input 780
Heed Compiler Warnings 780
Design for Security Policies 781
Implement Default Deny 781
Adhere to the Principle of Least Privilege, and Practice Defense in Depth 781
Sanitize Data Prior to Transmission to Other Systems 781
Review All Key Topics 782
Define Key Terms 782
Answers and Explanations 786

Chapter 9 Final Preparation 791

Tools for Final Preparation 791
Pearson Test Prep Practice Test Engine and Questions on the Website 791
Accessing the Pearson Test Prep Practice Test Software Online 792
Accessing the Pearson Test Prep Practice Test Software Offline 792
Customizing Your Exams 793
Updating Your Exams 794

Premium Edition 794
Memory Tables 795
Chapter-Ending Review Tools 795
Suggested Plan for Final Review/Study 795
Summary 796
Index 797

Online Elements

Appendix A Memory Tables
Appendix B Memory Tables Answer Key
Glossary

About the Authors

Robin M. Abernathy has been working in the IT certification preparation industry for more than 20 years. She has written and edited certification preparation materials for many $(ISC)^2$, Microsoft, CompTIA, PMI, ITIL, ISACA, and GIAC certifications and holds multiple IT certifications from these vendors.

Robin provides training on computer hardware and software, networking, security, and project management. Over the past decade, she has ventured into the traditional publishing industry by technically editing several publications and co-authoring Pearson's *CISSP Cert Guide* and *CASP+ Cert Guide* and authoring Pearson's *Project+ Cert Guide*. She presents at technical conferences and hosts webinars on IT certification topics.

Dr. Darren R. Hayes has close to 20 years of academic and professional experience in computer security and digital forensics. He has authored numerous publications in these fields, including *A Practical Guide to Digital Forensics Investigations*, which is published by Pearson. He is Associate Professor at Pace University, where he is the founder and director of the Seidenberg Digital Forensics Research Lab. He holds numerous IT certifications in security and digital forensics and holds a PhD from Sapienza University in Italy and a doctorate from Pace University.

Darren is also a professional digital forensics examiner and has supported both criminal and civil investigations over the past decade and a half. He has also been declared an expert witness in federal court.

Dedications

To all those out there on a certification journey!

—Robin

To all our cyber warriors who protect our businesses and our national security. Your careers are so demanding and your ambition to gain certifications is to be commended.

—Darren

Acknowledgments

My first thanks goes to God for blessing me with the ability to learn and grow in any field I choose. With Him, all things are possible!

For me, it is hard to believe that I am on the fourth edition of this book. I appreciate my family and my friends, who have supported me in my publishing journey through three titles and multiple editions.

It is my hope that you, the reader, succeed in your IT certification goals!

—Robin

To my beautiful wife, Nalini, and my children, Aine, Fiona, Nicolai, and Shay, I cannot thank you enough for your support and love over the years. Also, to my parents, Ted and Annette, who inspired me to be an eternal learner and try to help others to gain knowledge. I would like to acknowledge my fellow teachers who make immeasurable sacrifices to see their students succeed. My sincere thanks to all of the tremendous reviewers, editors, and other staff at Pearson who I have had the honor of working with for many years.

—Darren

About the Technical Reviewers

R. Sarma Danturthi, PhD, PMP, CISSP, has a doctoral degree in engineering from the University of Memphis, Memphis, Tennessee, and has taught graduate-level courses in engineering, microprocessors, and computer science. He has been in the IT field for more than 20 years. His earlier experience included designing processor-level boards with interfaces and programming with several languages such as C and C++ on various platforms such as Windows, Linux, UNIX, and VAX/VMS. He has been a funding proposal reviewer, scientific paper peer reviewer for universities in the USA and Taiwan, book reviewer and exam preparation subject matter expert for Pearson, $(ISC)^2$, and CompTIA.

His current experience includes information and cybersecurity, database security, software and application security, project team lead, and project management. He has published several papers in peer-reviewed journals and has written book chapters on software interfaces, modeling, IT security, and simulation. His interests include evolving cybersecurity, cloud computing, intelligent interfaces, and mobile application development. Besides being proficient in various programming languages, databases, information, and cybersecurity, he has certifications in Java, Project Management Institute's PMP, CompTIA Sec+, and $(ISC)^2$'s CISSP.

Dr. Danturthi published *70 Tips and Tricks for Mastering the CISSP Exam* (Apress) in 2020. He can be contacted at danturthi@gmail. com.

Ben Mayo, CCIE No. 24861, CISSP, is the head of security and lead engineer for Montana's largest independent network and data center provider. He has more than 19 years of experience in the network and security fields. Ben's experience spans multiple industries, including electrical power generation, education, and telecommunications. Ben takes a "purple team" approach to security, applying both offensive and defensive security practices to enhance his organization's security posture. Though security is his passion, he most enjoys spending time with his three awesome kids and his amazing wife. You can follow Ben on Twitter at @ping_18024.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *CISSP Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780137507474 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Certified Information Systems Security Professional (CISSP) is one of the most respected and sought-after security certifications available today. It is a globally recognized credential which demonstrates that the holder has knowledge and skills across a broad range of security topics.

As the number of security threats to organizations grows and the nature of these threats broadens, companies large and small have realized that security can no longer be an afterthought. It must be built into the DNA of the enterprise to be successful. Consequently, trained professionals must be versed not only in technology security but all aspects of security. It also requires a holistic approach to protecting the enterprise.

Security today is no longer a one-size-fits-all proposition. The CISSP credential is a way security professionals can demonstrate the ability to design, implement, and maintain the correct security posture for an organization, based on the complex environments in which today's organizations exist.

The Goals of the CISSP Certification

The CISSP certification is created and managed by one of the most prestigious security organizations in the world and has a number of stated goals. Although not critical for passing the exam, having knowledge of the organization and of these goals is helpful in understanding the motivation behind the creation of the exam.

Sponsoring Bodies

The CISSP is created and maintained by the International Information System Security Certification Consortium $(ISC)^2$. The $(ISC)^2$ is a global not-for-profit organization that provides both a vendor-neutral certification process and supporting educational materials.

The CISSP is one of a number of security-related certifications offered by $(ISC)^2$. Other certifications offered by this organization include the following:

- Systems Security Certified Practitioner (SSCP)
- Certified Cloud Security Professional (CCSP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Life Cycle Professional (CSSLP)
- HealthCare Information Security and Privacy Practitioner (HCISPP)

Several additional versions of the CISSP are offered that focus in particular areas:

- CISSP-Information Systems Security Architecture Professional (CISSP-ISSAP)
- CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)
- CISSP-Information Systems Security Management Professional (CISSP-ISSMP)

$(ISC)^2$ derives some of its prestige from the fact that it was the first security certification body to meet the requirements set forth by ANSI/ISO/IEC Standard 17024, a global benchmark for personnel certification. This ensures that certifications offered by this organization are both highly respected and sought after.

Stated Goals

The goal of $(ISC)^2$, operating through its administration of the CISSP and other certifications, is to provide a reliable instrument to measure an individual's knowledge of security. This knowledge is not limited to technology issues alone but extends to all aspects of security that face an organization.

In that regard, the topics are technically more shallow than those tested by some other security certifications, while also covering a much wider range of issues than those other certifications. Later, we cover the topics that comprise the eight domains of knowledge in detail, but it is a wide range of topics. This vast breadth of knowledge and the experience needed to pass the exam are what set the CISSP certification apart.

The Value of the CISSP Certification

The CISSP certification holds value for both the exam candidate and the enterprise. This certification is routinely in the top 10 of yearly lists that rank the relative demand for various IT certifications.

To the Security Professional

A security professional would spend the time and effort required to achieve this credential for numerous reasons:

- To meet growing demand for security professionals
- To become more marketable in an increasingly competitive job market
- To enhance skills in a current job

- To qualify or compete more successfully for a promotion
- To increase salary

In short, this certification demonstrates that the holder not only has the knowledge and skills tested in the exam but also has the wherewithal to plan and implement a study plan that addresses an unusually broad range of security topics.

To the Enterprise

For an organization, the CISSP certification offers a reliable benchmark to which job candidates can be measured by validating knowledge and experience. Candidates who successfully pass the rigorous exam are required to submit documentation verifying experience in the security field. Individuals holding this certification will stand out from the rest, not only making the hiring process easier but also adding a level of confidence in the final hire.

The Common Body of Knowledge

The material contained in the CISSP exam is divided into eight domains, which comprise what is known as the Common Body of Knowledge. This book devotes a chapter to each of these domains. Inevitable overlap occurs between the domains, leading to some overlap between topics covered in the chapters; the topics covered in each chapter are described next.

Security and Risk Management

The Security and Risk Management domain, covered in Chapter 1, encompasses a broad spectrum of general information security and risks management topics and is 15 percent of the exam. Topics include

- Professional ethics
- Concepts of confidentiality, integrity, availability, authenticity, and nonrepudiation
- Security governance principles
- Compliance requirements
- Legal and regulatory issues
- Investigation types
- Security policy, standards, procedures, and guidelines
- Business continuity (BC) requirements

- Personnel security policies and procedures
- Risk management concepts
- Threat modeling concepts and methodologies
- Supply chain risk management (SCRM) concepts
- Security awareness, education, and training program

Asset Security

The Asset Security domain, covered in Chapter 2, focuses on the collection, handling, and protection of information throughout its life cycle and is 10 percent of the exam. Topics include

- Information and asset identification and classification
- Information and asset handling requirements
- Resource provisioning
- Data life cycle
- Asset retention
- Data security controls and compliance requirements

Security Architecture and Engineering

The Security Architecture and Engineering domain, covered in Chapter 3, addresses the practice of building information systems and related architecture that deliver the required functionality when threats occur and is 13 percent of the exam. Topics include

- Engineering processes using secure design principles
- Fundamental concepts of security models
- Control selection based on systems security requirements
- Security capabilities of information systems
- Vulnerabilities of security architectures, designs, and solution elements
- Cryptography
- Cryptanalytic attacks
- Security principles of site and facility design
- Site and facility security controls

Communication and Network Security

The Communication and Network Security domain, covered in Chapter 4, focuses on protecting data in transit and securing the underlying networks over which the data travels and is 13 percent of the exam. Topics include

- Secure design principles in network architectures
- Network components security
- Secure communication channels

Identity and Access Management (IAM)

The Identity and Access Management domain, covered in Chapter 5 and comprising 13 percent of the exam, discusses provisioning and managing the identities and access used in the interaction of humans and information systems, of disparate information systems, and even between individual components of information systems. Topics include

- Physical and logical access to assets
- Identification and authentication of people, devices, and services
- Federated identity as a third-party service
- Authorization mechanisms
- Identity and access provisioning life cycle
- Authentication systems

Security Assessment and Testing

The Security Assessment and Testing domain, covered in Chapter 6 and comprising 12 percent of the exam, encompasses the evaluation of information assets and associated infrastructure using tools and techniques for the purpose of identifying and mitigating risk due to architectural issues, design flaws, configuration errors, hardware and software vulnerabilities, coding errors, and any other weaknesses that may affect an information system's ability to deliver its intended functionality in a secure manner. The topics include

- Assessment, test, and audit strategies design and validation
- Security control testing
- Security process data collection
- Test output analysis and reporting
- Security audits

Security Operations

The Security Operations domain, covered in Chapter 7, surveys the execution of security measures and maintenance of proper security posture and is 13 percent of the exam. Topics include

- Investigations compliance
- Logging and monitoring activities
- Configuration management
- Security operations concepts
- Resource protection
- Incident management
- Detective and preventive measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery (DR) processes
- Disaster recovery plan (DRP) testing
- Business continuity (BC) planning and exercises
- Physical security implementation and management
- Personnel safety and security concerns

Software Development Security

The Software Development Security domain, covered in Chapter 8, explores the software development life cycle and development best practices and is 11 percent of the exam. Topics include

- Software development life cycle (SDLC) security
- Security controls in development environments
- Software security effectiveness
- Security impact of acquired software
- Secure coding guidelines and standards

Steps to Becoming a CISSP

To become a CISSP, a test candidate must meet certain prerequisites and follow specific procedures. Test candidates must qualify for the exam and sign up for the exam.

Qualifying for the Exam

Candidates must have a minimum of five years of paid full-time professional security work experience in two or more of the eight domains in the Common Body of Knowledge. You may receive a one-year experience waiver with a four-year college degree or additional credential from the approved list, available at the (ISC)^2 website, thus requiring four years of direct full-time professional security work experience in two or more of the eight domains of the CISSP.

If you lack this experience, you can become an Associate of (ISC)^2 by successfully passing the CISSP exam. You'll then have six years to earn your experience to become a CISSP.

Signing Up for the Exam

The steps required to sign up for the CISSP are as follows:

1. Create a Pearson Vue account and schedule your exam.
2. Complete the Examination Agreement, attesting to the truth of your assertions regarding professional experience and legally committing to the adherence of the (ISC)^2 Code of Ethics.
3. Review the Candidate Background Questions.
4. Submit the examination fee.

When you are notified that you have successfully passed the examination, you will be required to subscribe to the (ISC)^2 Code of Ethics and have your application endorsed before the credential can be awarded. An endorsement form for this purpose must be completed and signed by an (ISC)^2 certified professional who is an active member and who is able to attest to your professional experience.

Facts About the CISSP Exam

The CISSP exam is a computer-based test that the candidate can spend up to three to six hours completing (depending on whether you take the CAT version that is available in English only or the linear format that is available in all other languages). There are no formal breaks, but you are allowed to bring a snack and eat it at the back of the test room, but any time used for that break counts toward the three to six hours. You must bring a government-issued identification card. No other forms of ID will be accepted. You may be required to submit to a palm vein scan.

The CAT test consists of a maximum 175 questions, while the linear format consists of 250 questions. As of May 2022, the CISSP exam will be in a computerized adaptive testing (CAT) format for those who take the English-language version, whereas all other languages have only the linear format. With the CAT format, the computer evaluates the certification candidate's ability to get the next question right based on the candidate's previous answers and the difficulty of those questions. The questions get harder as the certification candidate answers questions correctly, and the questions get easier as the certification candidate answers questions incorrectly. Each answer affects the questions that follow. Therefore, unlike the linear test format where the certification candidate can go back and forth in the question pool and change answers, a CAT format exam does *not* allow the certification candidate to change the answer or even view a previously answered question. The certification candidate may receive a pass or fail score without seeing 175 questions. To find out more about the CAT format, please go to www.isc2.org/Certifications/CISSP/CISSP-CAT#.

Although the majority of the questions will be multiple-choice questions with four options, test candidates may also encounter drag-and-drop and hotspot questions. The passing grade is 700 out of a possible 1,000 points. Candidates will receive the unofficial results at the test center from the test administrator. (ISC)^2 will then follow up with an official result via email.

About the *CISSP Cert Guide*, Fourth Edition

This book maps to the topic areas of the (ISC)^2 Certified Information Systems Security Professional (CISSP) exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass the exam only by memorization; it seeks to help you to truly learn and understand the topics. This book is designed to help you pass the CISSP exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" section lists a series of study activities that you should do at the end of the chapter:
  - **Review All Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
  - **Define Key Terms:** Although the CISSP exam may be unlikely to ask a question such as "Define this term," the exam does require that you learn and know a lot of information systems security terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
  - **Review Questions:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Cert Practice Test engine that allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains eight core chapters—Chapters 1 through 8. Chapter 9 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CISSP exam. The core chapters map directly to the CISSP exam topic areas and cover the concepts and technologies that you will encounter on the exam.

Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the authors that provide further insight into the more troublesome topics on the exam. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

Step 1. Go to www.pearsonitcertification.com/register and log in or create a new account.

Step 2. Enter the ISBN: **9780137507474**.

Step 3. Answer the challenge question as proof of purchase.

Step 4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Please note that many of the companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following these steps, please visit www.pearsonITcertification.com/contact and select the **Site Problems/Comments** option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

Step 1. Go to www.PearsonTestPrep.com.

Step 2. Select **Pearson IT Certification** as your product group.

Step 3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you will need to establish one by going to PearsonITCertification.com/join.

Step 4. In the **My Products** tab, click the **Activate New Product** button.

Step 5. Enter the access code printed on the insert card in the back of your book to activate your product.

Step 6. The product will now be listed in your My Products page. Click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can just enter this link in your browser:

www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, simply follow these steps:

Step 1. Register your book by going to PearsonITCertification.com/register and entering the ISBN: **9780137507474**.

Step 2. Answer the challenge questions.

Step 3. Go to your account page and click the **Registered Products** tab.

Step 4. Click the **Access Bonus Content** link under the product listing.

Step 5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.

Step 6. After the software finishes downloading, unzip all the files on your computer.

Step 7. Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.

Step 8. After the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.

Step 9. Click the **Activate a Product** button in the Activate Product Wizard.

Step 10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.

Step 11. Click **Next** and then click **Finish** to download the exam data to your application.

Step 12. Start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded on one version will be available to you on the other as well.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters; then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up,

whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

Figure Credits

Chapter Opener: Charlie Edwards/Getty Images

Figure 1.1: Joseph Steinberg, CloudMask Inc.

Figure 1.27: The Committee of Sponsoring Organizations (COSO)

Figure 3.25: EnggCyclopedia.com

Figure 4.46: Cisco Systems

Figure 8.7: The National Aeronautics and Space Administration (NASA)

This chapter covers the following topics:

- **Security Terms:** Concepts discussed include confidentiality, integrity, and availability (CIA); auditing and accounting; non-repudiation; default security posture; defense in depth; abstraction; data hiding; and encryption.
- **Security Governance Principles:** Concepts discussed include security function alignment, organizational processes, organizational roles and responsibilities, security control frameworks, and due care and due diligence.
- **Compliance:** Concepts discussed include contractual, legal, industry standards, and regulatory compliance and privacy requirements compliance.
- **Legal and Regulatory Issues:** Concepts discussed include computer crime concepts, major legal systems, licensing and intellectual property, cyber crimes and data breaches, import/export controls, trans-border data flow, and privacy.
- **Investigation Types:** Concepts discussed include operations/administrative, criminal, civil, regulatory, industry standards, and eDiscovery investigations.
- **Professional Ethics:** Concepts discussed include (ISC)2 Code of Ethics, Computer Ethics Institute, Internet Architecture Board, and organizational code of ethics.
- **Security Documentation:** Documentation types include policies, processes, procedures, standards, guidelines, and baselines.
- **Business Continuity:** Concepts discussed include business continuity and disaster recovery concepts, scope and plan, and BIA development.
- **Personnel Security Policies and Procedures:** Policies and procedures discussed include candidate screening and hiring; employment agreements and policies; onboarding and offboarding processes; vendor, consultant, and contractor agreements and controls; compliance policy requirements; privacy policy requirements, job rotation, and separation of duties.

- **Risk Management Concepts:** Concepts discussed include asset; asset valuation; vulnerability; threat; threat agent; exploit; risk; exposure; countermeasure; risk appetite; attack; breach; risk management policy; risk management team; risk analysis team; risk assessment; implementation; control categories; control types; control assessment, monitoring, and measurement; reporting and continuous improvement; and risk frameworks.
- **Geographical Threats:** Concepts discussed include internal versus external threats, natural threats, system threats, human threats, and politically motivated threats.
- **Threat Modeling:** Concepts discussed include threat modeling concepts, threat modeling methodologies, identifying threats, potential attacks, and remediation technologies and processes.
- **Security Risks in the Supply Chain:** Concepts discussed include risks associated with hardware, software, and services; third-party assessment and monitoring; minimum security requirements; and service-level requirements.
- **Security Education, Training, and Awareness:** Concepts discussed include levels required, methods and techniques, and periodic content reviews.

The Security and Risk Management domain addresses a broad array of topics, including the fundamental information security principles of confidentiality, integrity, and availability; governance; legal systems; privacy; the regulatory environment; personnel security; risk management; threat modeling; business continuity; supply chain risk; and professional ethics. Out of 100 percent of the exam, this domain carries an average weight of 15 percent, which is the highest weight of all the eight domains. So, pay close attention to the many details in this chapter!

This page intentionally left blank

CHAPTER 1

Security and Risk Management

Information security governance involves the principles, frameworks, and methods that establish criteria for protecting information assets, including security awareness. Risk management allows organizations to identify, measure, and control organizational risks. Threat modeling allows organizations to identify threats and potential attacks and implement appropriate mitigations against these threats and attacks. These facets ensure that security controls that are implemented are in balance with the operations of the organization. Each organization must develop a well-rounded, customized security program that addresses the needs of the organization while ensuring that the organization exercises due care and due diligence in its security plan. Acquisitions present special risks that management must understand prior to completing acquisitions.

Security professionals must take a lead role in their organization's security program and act as risk advisors to management. In addition, security professionals must ensure that they understand current security issues and risks, governmental and industry regulations, and security controls that can be implemented. They also must understand professional ethics for security personnel. Security is an ever-evolving, continuous process, and security professionals must be watchful.

Business continuity and disaster recovery ensure that the organization can recover from any attack or disaster that affects operations. Using the results from the risk assessment, security professionals should ensure that the appropriate business continuity and disaster recovery plans are created, tested, and revised at appropriate intervals.

In this chapter, you learn how to use the information security governance and risk management components to assess risks, implement controls for identified risks, monitor control effectiveness, and perform future risk assessments.

Foundation Topics

Security Terms

When implementing security and managing risk, you must keep in mind several important security principles and terms, including confidentiality, integrity, and availability; auditing and accounting; non-repudiation; default security posture; defense in depth; abstraction; data hiding; and encryption.

CIA

The three fundamentals of security are confidentiality, integrity, and availability (CIA), often referred to as the ***CIA triad***. Although the CIA triad is being introduced here, each principle of the triad should be considered in every aspect of security design. The CIA triad could easily be discussed in any domain of the CISSP exam.

Most security issues result in a violation of at least one facet of the CIA triad. Understanding these three security principles will help security professionals ensure that the security controls and mechanisms implemented protect at least one of these principles.

Every security control that an organization puts into place fulfills at least one of the security principles of the CIA triad. Understanding how to circumvent these security principles is just as important as understanding how to provide them.

A balanced security approach should be implemented to ensure that all three facets are considered when security controls are implemented. When implementing any control, you should identify the facet that the control addresses. For example, Redundant Array of Inexpensive Disks (RAID) addresses data availability, file hashes address data integrity, and encryption addresses data confidentiality. A balanced approach ensures that no facet of the CIA triad is ignored.

Confidentiality

To ensure ***confidentiality***, you must prevent the disclosure of data or information to unauthorized entities. As part of confidentiality, the sensitivity level of data must be determined before putting any access controls in place. Data with a higher sensitivity level will have more access controls in place than data at a lower sensitivity level. Identification, authentication, and authorization can be used to maintain data confidentiality.

The opposite of confidentiality is open access. Encryption is probably the most popular example of a control that provides confidentiality.

Integrity

Integrity, the second part of the CIA triad, ensures that data and systems are protected from unauthorized modification or data corruption. The goal of integrity is to preserve consistency, specifically:

- **Data integrity:** Implies that the data can be trusted, is complete, consistent, and accurate.
- **System integrity:** Implies that a system will work as intended—that is, store, process, and display data correctly.

The opposite of integrity is corruption. Hashing can be used to prove (or disprove) data integrity.

Availability

Availability means ensuring that information, systems, and supporting infrastructure are operating and accessible when needed. The two main instances in which availability is affected are (1) when attacks are carried out that disable or cripple a system and (2) when service loss occurs during and after disasters. Each system should be assessed in terms of its criticality to organizational operations. Controls should be implemented based on each system's criticality level.

Availability is the opposite of destruction or inoperability. Fault-tolerant technologies, such as RAID or alternate sites, are examples of controls that help improve availability.

Auditing and Accounting

Auditing and *accounting* are two related terms in organizational security. ***Auditing*** is an internal or external process of providing a manual or systematic measurable technical assessment of a system or application, whereas ***accounting*** is the logging of access and use of information resources. Auditing requires an analysis, which may be used to form an opinion. Accountability is the process of tracing actions to the source. Security professionals can perform audits of user or service accounts, account usage, application usage, device usage, and even permission usage. An audit is often used to identify corporate assets, detect risks to those assets, and improve security protocols. Regular audits should be carried out to ensure that the security policies in place are enforced and are being followed. Accounting is used to determine what changes need to be made.

Organizations should have a designated party who is responsible for ensuring that auditing and accounting of enterprise security are being completed regularly.

Although computer security audits can be performed by internal personnel, such as corporate internal auditors, the audits may also need to be completed by federal or state regulators, external auditors, or consultants.

Keep in mind that in many contexts auditing can also be a third-party activity whereby an organization gains independent assurance based on evidence. With this type of auditing, the third party is usually assessing an organization's compliance with standards or other organizational guidelines.

Non-repudiation

Non-repudiation is the assurance that a sender cannot deny an action, and often involves the sender being sent proof of delivery, while the receiver is provided with proof of the sender's identity. This behavior is usually seen in electronic communications where one party denies sending a contract, document, or email. Non-repudiation means putting measures in place that will prevent the sender from denying that it sent a message.

A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and when encrypted with a signature, that the message was not altered in transit (integrity).

Default Security Posture

An organization's approach to information security directly affects its access control strategy. For a ***default security posture***, organizations must choose between the allow-by-default or deny-by-default options. As implied by its name, an allow-by-default posture permits access to any data unless a need exists to restrict access. The deny-by-default posture is much stricter because it denies any access that is not explicitly permitted. Government and military institutions and many commercial organizations use a deny-by-default posture.

Today, few organizations implement either of these postures to its fullest. Most organizations use some mixture of the two. Access control protocols enable an organization to balance both protocols. Although the core posture should guide the organization, organizations often find that this mixture is necessary to ensure that data is still protected while providing access to a variety of users. For example, a public website might grant all HTTP and HTTPS content but deny all other content.

Defense in Depth

A ***defense-in-depth*** strategy refers to the practice of using multiple layers of security between data and the resources on which it resides and securing that data from possible attackers (see Figure 1-1). It is derived from a military strategy, whereby multiple layers of defense are used rather than one line of defense, thereby slowing down the advancement of an attacker.

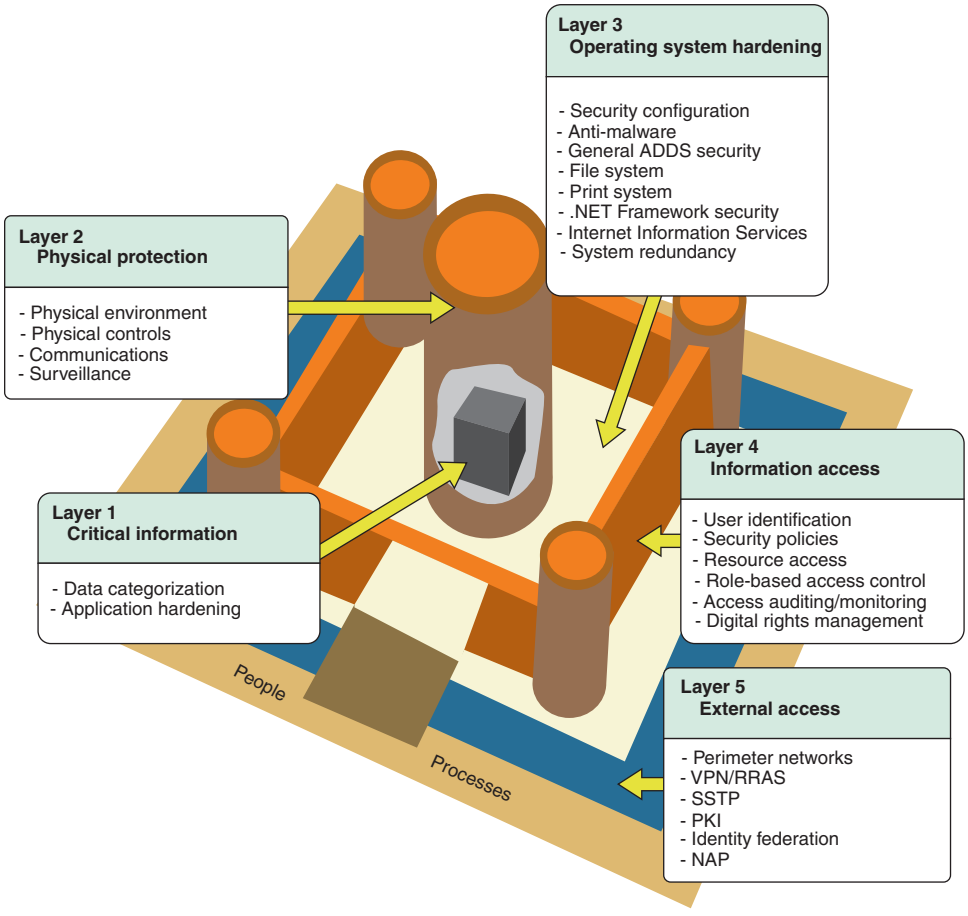

Figure 1-1 Defense-in-Depth Example

The first layer of a good defense-in-depth strategy is appropriate access control strategies. Access controls exist in all areas of an information systems (IS) infrastructure (more commonly referred to as an IT infrastructure), but a defense-in-depth strategy goes beyond access control. It also considers software development security, asset security, and all other domains of the CISSP realm.