

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

FREE SAMPLE CHAPTER



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.echelp.org**.

This page intentionally left blank

CISSP Cert Guide

Fifth Edition

Robin M. Abernathy

Dr. Darren R. Hayes



Pearson

Hoboken, New Jersey

CISSP Cert Guide, Fifth Edition

Copyright © 2025 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose all such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

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

ISBN-13: 978-0-13-534399-9

ISBN-10: 0-13-534399-2

Library of Congress Control Number: 2024911820

\$PrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

**GM K12, Early Career
and Professional
Learning**
Soo Kang

Product Line Manager
Brett Bartow

Executive Editor
James Manly

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Mandie Frank

Copy Editor
Bill McManus

Indexer
Timothy Wright

Proofreader
Donna E. Mulder

Technical Editors
R. Sarma Danturthi
Ben Mayo

Publishing Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

	Introduction	xlix
CHAPTER 1	Security and Risk Management	5
CHAPTER 2	Asset Security	171
CHAPTER 3	Security Architecture and Engineering	219
CHAPTER 4	Communication and Network Security	391
CHAPTER 5	Identity and Access Management (IAM)	561
CHAPTER 6	Security Assessment and Testing	635
CHAPTER 7	Security Operations	673
CHAPTER 8	Software Development Security	773
CHAPTER 9	Final Preparation	835
	Index	841

Online Elements

APPENDIX A	Memory Tables
APPENDIX B	Memory Tables Answer Key
	Glossary

Table of Contents

Introduction	xlix
Chapter 1 Security and Risk Management	5
Foundation Topics	6
Security Terms	6
Five Pillars of Information Security	6
<i>CIA Triad</i>	6
<i>Confidentiality</i>	7
<i>Integrity</i>	7
<i>Availability</i>	7
<i>Authenticity</i>	7
<i>Non-Repudiation</i>	8
Auditing and Accounting	8
Default Security Posture	9
Defense in Depth	9
Abstraction	11
Data Hiding	11
Encryption	11
Security Governance Principles	11
Security Function Alignment	12
<i>Organizational Strategies and Goals</i>	12
<i>Organizational Mission and Objectives</i>	13
<i>Business Case</i>	14
<i>Security Budget, Metrics, and Efficacy</i>	14
<i>Resources</i>	15
Organizational Processes	15
<i>Acquisitions and Divestitures</i>	15
<i>Governance Committees</i>	17
Organizational Roles and Responsibilities	17
<i>Board of Directors</i>	17
<i>Management</i>	18
<i>Audit Committee</i>	19
<i>Data Owner</i>	19

<i>Data Custodian</i>	20
<i>System Owner</i>	20
<i>System Administrator</i>	20
<i>Security Administrator</i>	20
<i>Security Analyst</i>	20
<i>Application Owner</i>	20
<i>Supervisor</i>	21
<i>User</i>	21
<i>Auditor</i>	21
<i>Security Control Frameworks</i>	21
<i>ISO/IEC 27000 Series</i>	22
<i>Zachman Framework</i>	26
<i>The Open Group Architecture Framework (TOGAF)</i>	26
<i>Department of Defense Architecture Framework (DoDAF)</i>	26
<i>British Ministry of Defence Architecture Framework (MODAF)</i>	26
<i>Sherwood Applied Business Security Architecture (SABSA)</i>	26
<i>Control Objectives for Information and Related Technology (COBIT)</i>	28
<i>National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series</i>	28
<i>HITRUST CSF</i>	31
<i>CIS Critical Security Controls</i>	32
<i>Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework</i>	33
<i>Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)</i>	33
<i>Information Technology Infrastructure Library (ITIL)</i>	34
<i>Six Sigma</i>	35
<i>Capability Maturity Model Integration (CMMI)</i>	35
<i>CCTA Risk Analysis and Management Method (CRAMM)</i>	37
<i>Federal Risk and Authorization Management Program (FedRAMP)</i>	37
<i>Payment Card Industry Data Security Standard (PCI DSS)</i>	37
<i>Top-Down Versus Bottom-Up Approach</i>	38
<i>Security Program Life Cycle</i>	38
<i>Due Care and Due Diligence</i>	39

Compliance	40
Contractual, Legal, Industry Standards, and Regulatory Compliance	41
Privacy Requirements Compliance	42
Legal and Regulatory Issues	42
Computer Crime Concepts	42
<i>Computer-Assisted Crime</i>	43
<i>Computer-Targeted Crime</i>	43
<i>Incidental Computer Crime</i>	43
<i>Computer Prevalence Crime</i>	43
<i>Hackers Versus Crackers</i>	44
<i>Computer Crime Examples</i>	44
Major Legal Systems	45
<i>Civil Law</i>	45
<i>Common Law</i>	46
<i>Criminal Law</i>	46
<i>Civil/Tort Law</i>	46
<i>Administrative/Regulatory Law</i>	47
<i>Customary Law</i>	47
<i>Religious Law</i>	47
<i>Mixed Law</i>	47
Licensing and Intellectual Property	47
<i>Patent</i>	48
<i>Trade Secret</i>	48
<i>Trademark</i>	49
<i>Copyright</i>	49
<i>Software Piracy and Licensing Issues</i>	50
<i>Internal Protection</i>	51
<i>Digital Rights Managements (DRM)</i>	51
Cyber Crimes and Data Breaches	52
Import/Export Controls	52
Trans-Border Data Flow	53
Privacy	53
<i>Personally Identifiable Information (PII)</i>	53
<i>Laws and Regulations</i>	54

Investigation Types	65
Operations/Administrative	65
Criminal	66
Civil	66
Regulatory	66
Industry Standards	67
eDiscovery	70
Professional Ethics	70
(ISC) ² Code of Ethics	70
Computer Ethics Institute	71
Internet Architecture Board	71
Organizational Code of Ethics	72
Security Documentation	72
Policies	73
<i>Organizational Security Policy</i>	74
<i>System-Specific Security Policy</i>	75
<i>Issue-Specific Security Policy</i>	75
<i>Policy Categories</i>	75
Processes	75
Procedures	75
Standards	76
Guidelines	76
Baselines	76
Business Continuity	76
Business Continuity and Disaster Recovery Concepts	76
<i>Disruptions</i>	77
<i>Disasters</i>	78
<i>Disaster Recovery and the Disaster Recovery Plan (DRP)</i>	79
<i>Continuity Planning and the Business Continuity Plan (BCP)</i>	79
<i>Business Impact Analysis (BIA)</i>	79
<i>Contingency Plan</i>	79
<i>Availability</i>	80
<i>Reliability</i>	80
<i>External Dependencies</i>	80

Scope and Plan	81
<i>Personnel Components</i>	81
<i>Scope</i>	82
<i>Business Contingency Planning</i>	82
BIA Development	85
<i>Identify Critical Processes and Resources</i>	86
<i>Identify Outage Impact and Estimate Downtime</i>	86
<i>Identify Resource Requirements</i>	88
<i>Identify Recovery Priorities</i>	88
Personnel Security Policies and Procedures	89
Candidate Screening and Hiring	90
Employment Agreements and Policies	91
Employee Onboarding and Offboarding Policies	93
Vendor, Consultant, and Contractor Agreements and Controls	94
Compliance Policy Requirements	94
Privacy Policy Requirements	95
Job Rotation	95
Separation of Duties	95
Risk Management Concepts	95
Asset and Asset Valuation	96
Vulnerability	96
Threat	97
Threat Agent	97
Exploit	97
Risk	97
Exposure	97
Countermeasure	97
Risk Appetite	98
Incident	99
Attack	99
Breach	99
Risk Management Policy	99
Risk Management Team	99
Risk Analysis Team	100

Risk Assessment	100
<i>Information and Asset (Tangible/Intangible) Value and Costs</i>	101
<i>Identity Threats and Vulnerabilities</i>	101
<i>Risk Assessment/Analysis</i>	102
<i>Countermeasure (Safeguard) Selection</i>	104
<i>Inherent Risk Versus Residual Risk</i>	105
<i>Handling Risk and Risk Response</i>	105
Implementation	106
Control Categories	107
<i>Compensative</i>	107
<i>Corrective</i>	107
<i>Detective</i>	108
<i>Deterrent</i>	108
<i>Directive</i>	108
<i>Preventive</i>	108
<i>Recovery</i>	108
Control Types	109
<i>Administrative (Management)</i>	109
<i>Logical (Technical)</i>	111
<i>Physical</i>	111
Controls Assessment, Monitoring, and Measurement	114
Reporting and Continuous Improvement	114
<i>Internal Reporting</i>	115
<i>External Reporting</i>	115
Risk Frameworks	116
<i>NIST</i>	116
<i>ISO/IEC 27005:2018</i>	131
<i>COSO's Enterprise Risk Management (ERM) Integrated Framework</i>	132
<i>A Risk Management Standard by the Federation of European Risk Management Associations (FERMA)</i>	133
Geographical Threats	133
Internal Versus External Threats	134
Natural Threats	134
<i>Hurricanes/Tropical Storms</i>	134

<i>Tornadoes</i>	134
<i>Earthquakes</i>	135
<i>Floods</i>	135
<i>Volcanoes</i>	135
System Threats	135
<i>Electrical</i>	136
<i>Communications</i>	136
<i>Utilities</i>	137
Human-Caused Threats	137
<i>Explosions</i>	137
<i>Fire</i>	138
<i>Vandalism</i>	139
<i>Fraud</i>	139
<i>Theft</i>	139
<i>Collusion</i>	139
Politically Motivated Threats	140
<i>Strikes</i>	140
<i>Riots</i>	140
<i>Civil Disobedience</i>	141
<i>Terrorist Acts</i>	141
<i>Active Shooter</i>	141
<i>Bombing</i>	141
Threat Modeling	142
Threat Modeling Concepts	142
Threat Modeling Methodologies	143
<i>STRIDE Model</i>	143
<i>Process for Attack Simulation and Threat Analysis (PASTA) Methodology</i>	144
<i>Trike Methodology</i>	144
<i>Visual, Agile, and Simple Threat (VAST) Model</i>	144
<i>NIST SP 800-154</i>	145
Identifying Threats	146
Potential Attacks	147
Remediation Technologies and Processes	148

Security Risks in the Supply Chain	148
Risks Associated with Hardware, Software, and Services	148
Third-Party Assessment and Monitoring	150
<i>Onsite Assessment</i>	151
<i>Document Exchange/Review</i>	151
<i>Process/Policy Review</i>	151
<i>Other Third-Party Governance Issues</i>	151
Supply Chain Assessment and Monitoring	151
<i>Silicon Root of Trust</i>	152
<i>Physically Unclonable Function (PUF)</i>	152
<i>Software Bill of Materials (SBOM)</i>	152
<i>Minimum Service-Level and Security Requirements</i>	152
<i>Service-Level Agreements (SLAs)</i>	153
Security Education, Training, and Awareness	153
Levels Required	154
Methods and Techniques	154
Periodic Content Reviews	155
Exam Preparation Tasks	155
Review All Key Topics	155
Complete the Tables and Lists from Memory	157
Define Key Terms	157
Answer Review Questions	158
Answers and Explanations	164
Chapter 2 Asset Security	171
Foundation Topics	172
Asset Security Concepts	172
Asset and Data Policies	172
Data Quality	173
Data Documentation and Organization	174
Identify and Classify Information and Assets	175
Data and Asset Classification	176
Sensitivity and Criticality	176
<i>PII</i>	177
<i>PHI</i>	179

<i>Proprietary Data</i>	181
Private Sector Data Classifications	181
Military and Government Data Classifications	182
Information and Asset Handling Requirements	183
Marking, Labeling, and Storing	184
Destruction	184
Provision Resources Securely	185
Asset Inventory and Asset Management	185
Data Life Cycle	186
Databases	188
<i>DBMS Architecture and Models</i>	189
<i>Database Interface Languages</i>	191
<i>Data Warehouses and Data Mining</i>	191
<i>Database Maintenance</i>	192
<i>Database Threats</i>	192
<i>Database Views</i>	193
<i>Database Locks</i>	193
<i>Polyinstantiation</i>	193
<i>Database ACID Test</i>	193
Roles and Responsibilities	194
<i>Data Owner</i>	194
<i>Data Controller</i>	195
<i>Data Custodian</i>	195
<i>System Owners</i>	195
<i>System Custodians</i>	196
<i>Business/Mission Owners</i>	196
<i>Data Processors</i>	196
<i>Data Users and Subjects</i>	197
Data Collection and Limitation	197
Data Location	198
Data Maintenance	198
Data Retention	199
Data Remanence and Destruction	199
Data Audit	200

Asset Retention	201
Data Security Controls	203
Data Security	203
Data States	203
<i>Data at Rest</i>	204
<i>Data in Transit</i>	204
<i>Data in Use</i>	204
Data Access and Sharing	204
Data Storage and Archiving	205
Baselines	206
Scoping and Tailoring	207
Standards Selection	207
Data Protection Methods	208
<i>Cryptography</i>	208
<i>Digital Rights Management (DRM)</i>	209
<i>Data Loss Prevention (DLP)</i>	210
<i>Cloud Access Security Broker (CASB)</i>	210
Exam Preparation Tasks	211
Review All Key Topics	211
Define Key Terms	211
Answer Review Questions	212
Answers and Explanations	213
Chapter 3 Security Architecture and Engineering	219
Foundation Topics	220
Information Systems Life Cycle	220
Stakeholders' Needs and Requirements	221
Requirements Analysis	221
Architectural Design	222
Development/Implementation	222
Integration	222
Verification and Validation	222
Transition/Deployment	223
Operations and Maintenance/Sustainment	223
Retirement/Disposal	223

Engineering Processes Using Secure Design Principles	223
Objects and Subjects	225
Closed Versus Open Systems	225
Threat Modeling	225
Least Privilege	225
Defense in Depth	226
Secure Defaults	226
Fail Securely	227
Separation of Duties (SoD)	227
Keep It Simple and Small	228
Zero Trust	228
Privacy by Design	228
Trust but Verify	229
Shared Responsibility	229
Secure Access Service Edge (SASE)	230
Security Model Concepts	231
Confidentiality, Integrity, and Availability	231
Confinement	232
Bounds	232
Isolation	232
Security Modes	232
<i>Dedicated Security Mode</i>	232
<i>System High Security Mode</i>	233
<i>Compartmented Security Mode</i>	233
<i>Multilevel Security Mode</i>	233
<i>Assurance and Trust</i>	233
Security Model Types	234
<i>State Machine Models</i>	234
<i>Multilevel Lattice Models</i>	234
<i>Matrix-Based Models</i>	235
<i>Noninterference Models</i>	235
<i>Information Flow Models</i>	235
<i>Take-Grant Model</i>	236
Security Models	237
<i>Bell-LaPadula Model</i>	237

<i>Biba Model</i>	238
<i>Clark-Wilson Integrity Model</i>	239
<i>Lipner Model</i>	240
<i>Brewer-Nash (Chinese Wall) Model</i>	240
<i>Graham-Denning Model</i>	240
<i>Harrison-Ruzzo-Ullman Model</i>	241
<i>Goguen-Meseguer Model</i>	241
<i>Sutherland Model</i>	241
System Architecture Steps	241
ISO/IEC 42010:2011	242
Computing Platforms	242
<i>Mainframe/Thin Clients</i>	242
<i>Distributed Systems</i>	243
<i>Middleware</i>	243
<i>Embedded Systems</i>	243
<i>Mobile Computing</i>	244
<i>Virtual Computing</i>	244
Security Services	245
<i>Boundary Control Services</i>	245
<i>Access Control Services</i>	245
<i>Integrity Services</i>	245
<i>Cryptography Services</i>	245
<i>Auditing and Monitoring Services</i>	245
System Components	246
CPU	246
<i>Memory and Storage</i>	249
<i>Input/Output Devices</i>	252
<i>Input/Output Structures</i>	252
<i>Firmware</i>	253
<i>Operating Systems</i>	254
<i>Memory Management</i>	255
System Security Evaluation Models	255
TCSEC	256
<i>Rainbow Series</i>	256
ITSEC	259

Common Criteria	261
Security Implementation Standards	263
ISO/IEC 27001	264
ISO/IEC 27002	265
Payment Card Industry Data Security Standard (PCI DSS)	266
Controls and Countermeasures	267
Certification and Accreditation	267
Control Selection Based on Systems Security Requirements	268
Security Capabilities of Information Systems	269
Memory Protection	269
Trusted Platform Module	270
Interfaces	270
Fault Tolerance	271
Policy Mechanisms	271
Separation of Privilege	271
Accountability	272
Encryption/Decryption	272
Security Architecture Maintenance	272
Vulnerabilities of Security Architectures, Designs, and Solution Elements	273
Client-Based Systems	273
Server-Based Systems	275
Data Flow Control	275
Database Systems	275
Inference	275
Aggregation	276
Contamination	276
Data Mining Warehouse	276
Cryptographic Systems	276
Operational Technology/Industrial Control Systems	277
Cloud-Based Systems	281
Large-Scale Parallel Data Systems	287
Distributed Systems	288
Grid Computing	288
Peer-to-Peer Computing	288

Internet of Things	289
<i>IoT Examples</i>	290
<i>Methods of Securing IoT Devices</i>	290
<i>NIST Framework for Cyber-Physical Systems</i>	291
Microservices	293
Containerization	294
Serverless Systems	294
High-Performance Computing Systems	295
Edge Computing Systems	296
Virtualized Systems	296
Vulnerabilities in Web-Based Systems	296
Maintenance Hooks	297
Time-of-Check/Time-of-Use Attacks	297
Web-Based Attacks	298
XML	298
SAML	298
OWASP	299
Vulnerabilities in Mobile Systems	299
Device Security	300
Application Security	300
Mobile Device Concerns	300
NIST SP 800-164	303
Vulnerabilities in Embedded Systems	304
Cryptographic Solutions	305
Cryptography Concepts	305
Cryptography History	307
<i>Julius Caesar and the Caesar Cipher</i>	308
<i>Vigenere Cipher</i>	308
<i>Kerckhoffs's Principle</i>	310
<i>World War II Enigma</i>	310
<i>Lucifer by IBM</i>	311
Cryptosystem Features	311
Authentication	311
Confidentiality	311
Integrity	311

<i>Authorization</i>	312
<i>Non-repudiation</i>	312
NIST SP 800-175A and B	312
Cryptographic Mathematics	313
<i>Boolean</i>	313
<i>Logical Operations (And, Or, Not, Exclusive Or)</i>	313
<i>Modulo Function</i>	315
<i>One-Way Function</i>	315
<i>Nonce</i>	315
<i>Split Knowledge</i>	315
Cryptographic Life Cycle	315
<i>Key Management</i>	316
<i>Algorithm Selection</i>	317
Cryptographic Types	317
Running Key and Concealment Ciphers	318
Substitution Ciphers	318
<i>One-Time Pads</i>	319
<i>Steganography</i>	320
Transposition Ciphers	320
Symmetric Algorithms	321
<i>Stream-Based Ciphers</i>	322
<i>Block Ciphers</i>	322
<i>Initialization Vectors (IVs)</i>	323
Asymmetric Algorithms	323
Hybrid Ciphers	324
Elliptic Curves	324
Quantum Cryptography	325
Symmetric Algorithms	325
DES and 3DES	325
<i>DES Modes</i>	326
<i>3DES and Modes</i>	329
AES	329
IDEA	330
Skipjack	330

Blowfish	330
Twofish	331
RC4/RC5/RC6/RC7	331
CAST	331
Asymmetric Algorithms	332
Diffie-Hellman	333
RSA	333
El Gamal	334
ECC	334
Knapsack	335
Zero-Knowledge Proof	335
Public Key Infrastructure and Digital Certificates	335
Certificate Authority and Registration Authority	336
Certificates	336
Certificate Life Cycle	337
<i>Enrollment</i>	338
<i>Verification</i>	339
<i>Revocation</i>	339
<i>Renewal and Modification</i>	340
Certificate Revocation List	340
OCSP	340
PKI Steps	341
Cross-Certification	341
Quantum Key Distribution	342
Key Management Practices	343
Message Integrity	347
Hashing	348
<i>One-Way Hash</i>	348
MD2/MD4/MD5/MD6	349
SHA/SHA-2/SHA-3	350
HAVAL	351
RIPEMD-160	351
Tiger	351
Message Authentication Code	351

<i>HMAC</i>	352
<i>CBC-MAC</i>	352
<i>CMAC</i>	353
Salting	353
Digital Signatures and Non-repudiation	354
DSS	354
Non-repudiation	354
Applied Cryptography	354
Link Encryption Versus End-to-End Encryption	355
Email Security	355
Internet Security	355
Cryptanalytic Attacks	355
Ciphertext-Only Attack	356
Known Plaintext Attack	356
Chosen Plaintext Attack	356
Chosen Ciphertext Attack	357
Social Engineering	357
Brute Force	357
Differential Cryptanalysis	357
Linear Cryptanalysis	357
Algebraic Attack	357
Frequency Analysis	358
Birthday Attack	358
Dictionary Attack	358
Replay Attack	358
Analytic Attack	358
Statistical Attack	359
Factoring Attack	359
Reverse Engineering	359
Meet-in-the-Middle Attack	359
Ransomware Attack	359
Side-Channel Attack	359
Implementation Attack	360
Fault Injection	360

Timing Attack	360
Pass-the-Hash Attack	360
Digital Rights Management	360
Document DRM	361
Music DRM	361
Movie DRM	362
Video Game DRM	362
E-book DRM	362
Site and Facility Design	362
Layered Defense Model	363
CPTED	363
<i>Natural Access Control</i>	363
<i>Natural Surveillance</i>	364
<i>Natural Territorials Reinforcement</i>	364
Physical Security Plan	364
<i>Deter Criminal Activity</i>	364
<i>Delay Intruders</i>	364
<i>Detect Intruders</i>	364
<i>Assess Situation</i>	365
<i>Respond to Intrusions and Disruptions</i>	365
Facility Selection Issues	365
<i>Visibility</i>	365
<i>Surrounding Area and External Entities</i>	365
<i>Accessibility</i>	366
<i>Construction</i>	366
<i>Internal Compartments</i>	367
<i>Computer and Equipment Rooms</i>	367
Site and Facility Security Controls	368
Doors	368
<i>Door Lock Types</i>	368
<i>Turnstiles and Mantraps</i>	368
Locks	369
Biometrics	371
Type of Glass Used for Entrances	371

Visitor Control	371
Wiring Closets/Intermediate Distribution Facilities	372
Restricted and Work Areas	372
Secure Data Center	372
Restricted Work Area	372
Server Room	372
Media Storage Facilities	373
Evidence Storage	373
Environmental Security and Issues	373
Fire Protection	373
Power Supply	375
HVAC	376
Water Leakage and Flooding	376
Environmental Alarms	377
Equipment Physical Security	377
Corporate Procedures	377
Safes, Vaults, and Locking	379
Exam Preparation Tasks	379
Review All Key Topics	379
Complete the Tables and Lists from Memory	381
Define Key Terms	381
Answer Review Questions	382
Answers and Explanations	387

Chapter 4 Communication and Network Security 391

Foundation Topics	392
Secure Network Design Principles	392
OSI Model	392
Application Layer	393
Presentation Layer	393
Session Layer	394
Transport Layer	394
Network Layer	395
Data Link Layer	395
Physical Layer	395

TCP/IP Model	397
<i>Application Layer</i>	397
<i>Transport Layer</i>	398
<i>Internet Layer</i>	400
<i>Link Layer</i>	402
<i>Encapsulation and De-encapsulation</i>	402
IP Networking	403
Common TCP/UDP Ports	403
Logical and Physical Addressing	405
IPv4	406
<i>IP Classes</i>	407
<i>Public Versus Private IP Addresses</i>	408
<i>NAT</i>	408
<i>Media Access Control (MAC) Addressing</i>	413
Network Transmission	413
<i>Analog Versus Digital</i>	413
<i>Asynchronous Versus Synchronous</i>	414
<i>Broadband Versus Baseband</i>	415
<i>Unicast, Multicast, and Broadcast</i>	416
<i>Wired Versus Wireless</i>	416
IPv6	417
<i>NIST SP 800-119</i>	418
<i>IPv6 Major Features</i>	420
<i>IPv4 Versus IPv6 Threat Comparison</i>	423
<i>IPv6 Addressing</i>	423
<i>Shorthand for Writing IPv6 Addresses</i>	426
<i>IPv6 Address Types</i>	427
<i>IPv6 Address Scope</i>	429
Network Types	430
<i>LAN</i>	430
<i>Intranet</i>	431
<i>Extranet</i>	432
<i>MAN</i>	432
<i>WAN</i>	433

<i>WLAN</i>	434
<i>SAN</i>	434
<i>CAN</i>	435
<i>PAN</i>	435
Protocols and Services	435
ARP/RARP	436
DHCP/BOOTP	437
DNS	438
FTP, FTPS, SFTP, and TFTP	438
HTTP, HTTPS, and S-HTTP	439
ICMP	439
IGMP	440
IMAP	440
LDAP	440
LDP	440
NAT	440
NetBIOS	440
NFS	441
PAT	441
POP	441
CIFS/SMB	441
SMTP	441
SNMP	441
SSL/TLS	442
Multilayer Protocols	442
Converged Protocols	443
FCoE	443
InfiniBand	444
Compute Express Link (CXL)	445
MPLS	446
VoIP	447
iSCSI	447
Wireless Networks	448
FHSS, DSSS, OFDM, VOFDM, FDMA, TDMA, CDMA, OFDMA, GSM, and Massive MIMO	448

<i>802.11 Techniques</i>	448
<i>Cellular or Mobile Wireless Techniques</i>	449
5G	450
<i>Telecommunications and Hardware Support</i>	451
<i>Telecom Providers</i>	452
<i>Satellites</i>	454
<i>Backhaul Networks</i>	455
<i>Hardware Support</i>	456
WLAN Structure	457
<i>Access Point</i>	457
<i>Service Set Identifier (SSID)</i>	458
<i>Infrastructure Mode Versus Ad Hoc Mode</i>	458
WLAN Standards	458
802.11	458
802.11a (Wi-Fi 2)	458
802.11b (Wi-Fi 1)	459
802.11g (Wi-Fi 3)	459
802.11n (Wi-Fi 4)	459
802.11ac (Wi-Fi 5)	459
802.11ax (Wi-Fi 6)	460
802.11be (Wi-Fi 7)	460
802.11bn (Wi-Fi 8)	460
<i>Bluetooth</i>	461
<i>Infrared</i>	462
<i>Near Field Communication (NFC)</i>	462
<i>Zigbee</i>	462
WLAN Security	462
<i>Open System Authentication</i>	462
<i>Shared Key Authentication</i>	463
WEP	463
WPA	463
WPA2	463
<i>Personal Versus Enterprise</i>	464
WPA3	464

- 802.1X* 464
- SSID Broadcast* 466
- MAC Filter* 466
- Wireless Site Surveys* 467
- Antenna Placement and Signal Power Levels* 467
- Antenna Types* 468

Communications Cryptography 468

- Link Encryption 468
- End-to-End Encryption 468
- Email Security 469
- PGP* 469
- MIME and S/MIME* 470
- Quantum Cryptography* 470
- Internet Security 470
- Remote Access* 471
- HTTP, HTTPS, and S-HTTP* 471
- Secure Electronic Transaction (SET)* 471
- Cookies* 472
- SSH* 472
- IPsec* 473

Secure Network Components 473

- Network Monitoring and Management 473
- Operation of Infrastructure* 475
- Hardware 475
- Network Devices* 475
- Network Routing* 492
- Transmission Media 495
- Cabling* 495
- Network Topologies* 500
- Performance Metrics* 503
- Network Technologies* 504
- WAN Technologies* 510
- Network Access Control Devices 516
- Quarantine/Remediation* 517
- Firewalls/Proxies* 517

Network Access Control Systems	517
Endpoint Security	518
Content-Distribution Networks	519
Secure Communication Channels	520
Voice	520
Multimedia Collaboration	520
<i>Remote Meeting Technology</i>	521
<i>Instant Messaging</i>	521
Remote Access	522
<i>Remote Connection Technologies</i>	522
<i>VPN Screen Scraper</i>	531
<i>Virtual Application/Desktop</i>	531
<i>Telecommuting/Teleworking</i>	531
Data Communications	532
Virtualized Networks	532
<i>Software-Defined Networking</i>	532
<i>Virtual Private Cloud (VPC)</i>	533
<i>Virtual SAN</i>	534
<i>Guest Operating Systems</i>	534
<i>Federated Identity with a Third Party</i>	534
Network Attacks	535
Network Component Attacks	535
<i>Non-Blind Spoofing</i>	535
<i>Blind Spoofing</i>	535
<i>Man-in-the-Middle Attack</i>	536
<i>MAC Flooding Attack</i>	536
<i>802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack</i>	536
<i>Double-Encapsulated 802.1Q/Nested VLAN Attack</i>	536
<i>ARP Attack</i>	536
ICMP Attacks	537
<i>Ping of Death</i>	537
<i>Smurf</i>	537
<i>Fraggle</i>	538
<i>ICMP Redirect</i>	538
<i>Ping Scanning</i>	538

Traceroute Exploitation 538

DNS Attacks 538

DNS Cache Poisoning 539

DoS 539

DDoS 539

DNSSEC 540

URL Hiding 540

Domain Grabbing 540

Cybersquatting 541

Email Attacks 541

Email Spoofing 541

Spear Phishing 542

Whaling 542

Spam 543

Wireless Attacks 543

Wardriving 543

Warchalking 543

Remote Attacks 544

Other Attacks 544

SYN ACK Attacks 544

Session Hijacking 544

Port Scanning 544

Teardrop 545

IP Address Spoofing 545

Zero-Day 545

Ransomware 546

Exam Preparation Tasks 547

Review All Key Topics 547

Define Key Terms 548

Answer Review Questions 550

Answers and Explanations 555

Chapter 5 Identity and Access Management (IAM) 561

Foundation Topics 562

Access Control Process 562

Identify Resources 562

Identify Users	562
Identify the Relationships Between Resources and Users	563
Physical and Logical Access to Assets	563
Access Control Administration	564
<i>Centralized</i>	564
<i>Decentralized</i>	565
Information	565
Systems	565
Devices	566
Facilities	566
Applications	567
Services	567
Identification and Authentication Concepts	568
NIST SP 800-63	569
Five Factors for Authentication	573
<i>Knowledge Factors</i>	573
<i>Ownership Factors</i>	577
<i>Characteristic Factors</i>	579
<i>Location Factors</i>	584
<i>Time Factors</i>	584
Single-Factor Versus Multifactor Authentication	584
Device Authentication	585
Password-Less Authentication	585
Groups and Roles	586
Identification and Authentication Implementation	588
Authentication, Authorization, and Accounting (AAA)	588
<i>Authentication</i>	588
<i>Authorization</i>	589
<i>Accounting</i>	589
Separation of Duties	591
Least Privilege/Need-to-Know	592
Default to No Access	593
Directory Services	593
Single Sign-on	594
Kerberos	595

<i>SESAME</i>	597
<i>OpenID Connect (OIDC)/Open Authorization (OAuth)</i>	597
<i>Security Assertion Markup Language (SAML)</i>	597
<i>Federated Identity Management (IdM)</i>	597
<i>Security Domains</i>	598
Session Management	599
Registration, Proof, and Establishment of Identity	599
Credential Management Systems	600
Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)	601
Just-In-Time (JIT)	601
Identity as a Service (IDaaS) Implementation	602
Third-Party Identity Services Integration	602
Authorization Mechanisms	603
Permissions, Rights, and Privileges	603
Access Control Models	603
<i>Discretionary Access Control</i>	604
<i>Mandatory Access Control</i>	604
<i>Role-Based Access Control</i>	605
<i>Rule-Based Access Control</i>	605
<i>Attribute-Based Access Control</i>	606
<i>Content-Dependent Versus Context-Dependent</i>	609
<i>Risk-Based Access Control</i>	609
<i>Access Control Matrix</i>	610
Access Control Policies and Policy Enforcement	611
Provisioning Life Cycle	612
Provisioning	613
<i>Identity and Account Management</i>	613
User, System, and Service Account Access Review	614
Account Transfers	615
Account Revocation	615
Role Definition and Transition	615
Privilege Escalation	616
Service Account Management	617

Access Control Threats	618
Password Threats	619
<i>Dictionary Attack</i>	619
<i>Brute-Force Attack</i>	619
<i>Birthday Attack</i>	619
<i>Rainbow Table Attack</i>	619
<i>Sniffer Attack</i>	620
Social Engineering Threats	620
<i>Phishing/Pharming</i>	620
<i>Shoulder Surfing</i>	621
<i>Identity Theft</i>	621
<i>Dumpster Diving</i>	621
DoS/DDoS	621
Buffer Overflow	622
Mobile Code	622
Malicious Software	622
Spoofing	623
Sniffing and Eavesdropping	623
Emanating	623
Backdoor/Trapdoor	624
Access Aggregation	624
Advanced Persistent Threat	624
Prevent or Mitigate Access Control Threats	625
Exam Preparation Tasks	625
Review All Key Topics	625
Define Key Terms	626
Answer Review Questions	627
Answers and Explanations	630
Chapter 6 Security Assessment and Testing	635
Foundation Topics	636
Design and Validate Assessment and Testing Strategies	636
Security Testing	636
Security Assessments	637
Red Team versus Blue Team	637
Security Auditing	638

Internal, External, and Third-party Security Assessment, Testing, and Auditing	638
Location	639
Conduct Security Control Testing	639
Vulnerability Assessment	639
<i>Network Discovery Scan</i>	640
<i>Network Vulnerability Scan</i>	642
<i>Web Application Vulnerability Scan</i>	643
Penetration Testing	643
Log Reviews	646
<i>NIST SP 800-92</i>	646
Synthetic Transactions	650
Code Review and Testing	651
<i>Code Review Process</i>	652
<i>Static Testing</i>	653
<i>Dynamic Testing</i>	653
<i>Fuzz Testing</i>	653
Misuse Case Testing	653
Test Coverage Analysis	654
Interface Testing	654
Collect Security Process Data	655
NIST SP 800-137	655
Account Management	656
Management Review and Approval	656
Key Performance and Risk Indicators	657
Backup Verification Data	658
Training and Awareness	658
Disaster Recovery and Business Continuity	658
Analyze Test Outputs and Generate a Report	659
Conduct or Facilitate Security Audits	659
Exam Preparation Tasks	661
Review All Key Topics	661
Define Key Terms	662
Answer Review Questions	662
Answers and Explanations	665

Chapter 7 Security Operations 673

Foundation Topics 674

Investigations 674

Forensic and Digital Investigations 674

Identify Evidence 676 *Preserve and Collect Evidence* 676 *Examine and Analyze Evidence* 677 *Present Findings* 677 *Decide* 677 *Forensic Procedures* 677 *Reporting and Documentation* 678 *IOCE/SWGDE and NIST* 678 *Crime Scene* 679 *MOM* 680 *Chain of Custody* 680 *Interviewing* 681 *Investigative Techniques* 681

Evidence Collection and Handling 682

Five Rules of Evidence 682 *Types of Evidence* 683 *Surveillance, Search, and Seizure* 685 *Media Analysis* 685 *Software Analysis* 686 *Network Analysis* 686 *Hardware/Embedded Device Analysis* 687

Digital Forensic Tools, Tactics, and Procedures 687

Artifacts 689

Logging and Monitoring Activities 690

Audit and Review 691

Log Types 691

Audit Types 692

Intrusion Detection and Prevention 692

Security Information and Event Management (SIEM) 693

Security Orchestration and Automated Response (SOAR) 693

Continuous Monitoring and Tuning	694
Egress Monitoring	695
Log Management	696
Threat Intelligence	697
User and Entity Behavior Analytics (UEBA)	697
Configuration and Change Management	697
Resource Provisioning	699
<i>Asset Inventory and Management</i>	700
Baselining	702
Automation	702
Security Operations Concepts	702
Need to Know/Least Privilege	703
Managing Accounts, Groups, and Roles	703
Separation of Duties and Responsibilities	704
Privilege Account Management	704
Job Rotation and Mandatory Vacation	705
Two-Person Control	705
Sensitive Information Procedures	705
Record Retention	706
Information Life Cycle	706
Service-Level Agreements	706
Resource Protection	707
Protecting Tangible and Intangible Assets	707
<i>Facilities</i>	707
<i>Hardware</i>	708
<i>Software</i>	708
<i>Information Assets</i>	709
Protecting Data at Rest and Data in Transit	709
Asset Management	710
<i>Redundancy and Fault Tolerance</i>	711
<i>Backup and Recovery Systems</i>	711
<i>Identity and Access Management</i>	711
<i>Media Management</i>	712
<i>Media History</i>	717

<i>Media Labeling and Storage</i>	717
<i>Sanitizing and Disposing of Media</i>	718
<i>Network and Resource Management</i>	718
Incident Management	719
Event Versus Incident	719
Incident Response Team and Incident Investigations	720
Rules of Engagement, Authorization, and Scope	720
Incident Response Procedures	721
Incident Response Management	722
Detect	722
Respond	722
Mitigate	723
Report	723
Recover	723
Remediate	723
Review and Lessons Learned	724
Detective and Preventive Measures	724
IDS/IPS	724
Firewalls	724
Whitelisting/Blacklisting	725
Third-Party Security Services	725
Sandboxing	725
Honeypots/Honeynets	725
Anti-malware/Antivirus	726
Clipping Levels	726
Deviations from Standards	726
Unusual or Unexplained Events	726
Unscheduled Reboots	727
Unauthorized Disclosure	727
Trusted Recovery	727
Trusted Paths	727
Input/Output Controls	727
System Hardening	728
Vulnerability Management Systems	728
Machine Learning and Artificial Intelligence (AI)-Based Tools	728

Patch and Vulnerability Management	729
Recovery Strategies	729
Create Recovery Strategies	730
<i>Categorize Asset Recovery Priorities</i>	731
<i>Business Process Recovery</i>	731
<i>Supply and Technology Recovery</i>	732
<i>User Environment Recovery</i>	734
<i>Data Recovery</i>	735
<i>Training Personnel</i>	738
Backup Storage Strategies	738
Recovery and Multiple Site Strategies	739
<i>Hot Site</i>	740
<i>Cold Site</i>	741
<i>Warm Site</i>	741
<i>Tertiary Site</i>	742
<i>Reciprocal Agreements</i>	742
<i>Redundant Sites</i>	742
<i>Resource Capacity Agreement</i>	742
Redundant Systems, Facilities, and Power	744
Fault-Tolerance Technologies	744
Insurance	744
Data Backup	745
Fire Detection and Suppression	745
High Availability	745
Quality of Service	746
System Resilience	746
Disaster Recovery	747
Response	747
Personnel	747
<i>Damage Assessment Team</i>	748
<i>Legal Team</i>	748
<i>Media Relations Team</i>	748
<i>Recovery Team</i>	749
<i>Relocation Team</i>	749

<i>Restoration Team</i>	749
<i>Salvage Team</i>	749
<i>Security Team</i>	749
Communications	749
Assessment	750
Restoration	750
Training and Awareness	750
Lessons Learned	751
Testing Disaster Recovery Plans	751
Read-Through Test	752
Checklist Test	752
Table-Top Exercise	752
Structured Walk-Through Test	752
Simulation Test	753
Parallel Test	753
Full-Interruption Test	753
Functional Drill	753
Evacuation Drill	753
Business Continuity Planning and Exercises	753
Physical Security	754
Perimeter Security Controls	754
<i>Gates and Fences</i>	755
<i>Perimeter Intrusion Detection</i>	756
<i>Lighting</i>	758
<i>Patrol Force</i>	759
<i>Access Control</i>	759
Building and Internal Security Controls	760
Personnel Safety and Security	760
Duress	760
Travel	761
Monitoring	762
Emergency Management	762
Security Training and Awareness	762

	Exam Preparation Tasks	763
	Review All Key Topics	763
	Define Key Terms	764
	Answer Review Questions	764
	Answers and Explanations	768
Chapter 8	Software Development Security	773
	Foundation Topics	774
	Software Development Concepts	774
	Machine Languages	774
	Assembly Languages and Assemblers	774
	High-Level Languages, Compilers, and Interpreters	774
	Object-Oriented Programming	775
	<i>Polymorphism</i>	776
	<i>Polyinstantiation</i>	776
	<i>Encapsulation</i>	776
	<i>Cohesion</i>	777
	<i>Coupling</i>	777
	<i>Data Structures</i>	777
	Distributed Object-Oriented Systems	777
	CORBA	777
	COM and DCOM	778
	OLE	778
	Java	778
	SOA	779
	Mobile Code	779
	Java Applets	779
	ActiveX	779
	NIST SP 800-163	780
	Security in the System and Software Development Life Cycle	783
	System Development Life Cycle	783
	<i>Initiate</i>	784
	<i>Acquire/Develop</i>	784
	<i>Implement</i>	785
	<i>Operate/Maintain</i>	785
	<i>Dispose/Decommission</i>	785

Software Development Life Cycle	786
<i>Plan/Initiate Project</i>	786
<i>Gather Requirements</i>	787
<i>Design</i>	787
<i>Develop</i>	788
<i>Test/Validate</i>	788
<i>Release/Maintenance</i>	789
<i>Certify/Accredit</i>	789
<i>Change Management and Configuration Management/Replacement</i>	789
DevSecOps	790
Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST)	790
Interactive Application Security Test (IAST)	791
Software Composition Analysis	791
Software Development Methods and Maturity Models	792
<i>Build and Fix Model</i>	793
<i>Waterfall Model</i>	794
<i>V-shaped Model</i>	795
<i>Prototyping</i>	795
<i>Modified Prototype Model (MPM)</i>	796
<i>Incremental Model</i>	796
<i>Spiral Model</i>	797
<i>Agile Model</i>	797
<i>Scaled Agile Framework (SAFe)</i>	798
<i>Continuous Integration and Continuous Delivery (CI/CD)</i>	799
<i>Rapid Application Development (RAD) Model</i>	800
<i>Joint Analysis Development (JAD) Model</i>	800
<i>Cleanroom Model</i>	800
<i>Structured Programming Development Model</i>	801
<i>Exploratory Model</i>	801
<i>Computer-Aided Software Engineering (CASE)</i>	801
<i>Component-Based Development</i>	801
CMMI	801
ISO 9001:2015/90003:2014	802
IDEAL Model	803

Operation and Maintenance	804
Integrated Product Team	804
Security Controls in Development	806
Software Development Security Best Practices	806
WASC	806
OWASP	807
BSI	807
ISO/IEC 27000	807
Software Environment Security	807
Source Code Analysis Tools	808
Code Repository Security	808
Software Threats	808
Malware	809
Malware Protection	813
Scanning Types	814
Security Policies	814
Software Protection Mechanisms	814
Assess Software Security Effectiveness	815
Auditing and Logging	816
Risk Analysis and Mitigation	816
Regression and Acceptance Testing	817
Security Impact of Acquired Software	817
Secure Coding Guidelines and Standards	819
Security Weaknesses and Vulnerabilities at the Source Code Level	819
Buffer Overflow	819
Escalation of Privileges	821
Backdoor	821
Rogue Programmers	822
Covert Channel	822
Object Reuse	822
Mobile Code	822
Time of Check/Time of Use (TOC/TOU)	823
Security of Application Programming Interfaces	823
Secure Coding Practices	823

	<i>Validate Input</i>	824
	<i>Heed Compiler Warnings</i>	824
	<i>Design for Security Policies</i>	824
	<i>Implement Default Deny</i>	824
	<i>Adhere to the Principle of Least Privilege, and Practice Defense in Depth</i>	824
	<i>Sanitize Data Prior to Transmission to Other Systems</i>	825
	Exam Preparation Tasks	825
	Review All Key Topics	825
	Define Key Terms	825
	Answer Review Questions	826
	Answers and Explanations	830
Chapter 9	Final Preparation	835
	Tools for Final Preparation	835
	Pearson Test Prep Practice Test Engine and Questions on the Website	835
	<i>Accessing the Pearson Test Prep Practice Test Software Online</i>	836
	<i>Accessing the Pearson Test Prep Practice Test Software Offline</i>	836
	Customizing Your Exams	837
	Updating Your Exams	838
	<i>Premium Edition</i>	838
	Memory Tables	839
	Chapter-Ending Review Tools	839
	Suggested Plan for Final Review/Study	839
	Summary	840
	Index	841

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 fifth 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 whom 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 9780135343999 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*, Fifth 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.

How to Access the Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials, as well as additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box indicating 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: **9780135343999**.
- 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 our 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 the steps above, 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 below.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- You can get your access code by registering the print ISBN (9780135343999) on pearsonitcertification.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. After you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code

are available on the book's companion website by clicking the Access Bonus Content link.

- If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at pearsonitcertification.com, click Account to see details of your account, and click the Digital Purchases tab.

NOTE After you register your book, your code can always be found in your account on the Registered Products tab.

Once you have the access code, to find instructions about both the Pearson Test Prep web app and the desktop app, follow these steps:

- Step 1.** Open this book's companion website, as shown earlier in this Introduction, under the heading, "How to Access the Companion Website."
- Step 2.** Click the **Practice Test Software** button.
- Step 3.** Follow the instructions listed there for both installing the desktop app and using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

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

Figures 4.47 and 4.49: Microsoft

Figure 7.13: Ratchat/Shutterstock

This page intentionally left blank

Asset Security

Assets are any entities that are valuable to an organization and include *tangible* and *intangible assets*. As mentioned in Chapter 1, “Security and Risk Management,” tangible assets include computers, facilities, supplies, and personnel. Intangible assets include intellectual property, data, and organizational reputation. All assets in an organization must be protected to ensure the organization’s future success. Although securing some assets is as easy as locking them in a safe, other assets require more advanced security measures. The most valuable asset of any organization is its data.

The Asset Security domain addresses a broad array of topics, including information and asset identification and classification, information and asset handling, information and asset ownership, asset inventory and asset management, data life cycle, asset retention, and data security controls and compliance requirements. Out of 100 percent of the exam, this domain carries an average weight of 10 percent, which is the lowest weight of the domains.

A security professional must be concerned with all aspects of asset security. The most important factor in determining the controls used to ensure asset security is an asset’s value. Although some assets in the organization may be considered more important because they have greater value, you should ensure that no assets are forgotten. This chapter covers all the aspects of asset security that you, as an IT security professional, must understand.

NOTE Throughout this chapter, the terms *information* and *data* are used interchangeably, as commonly happens in the real world.

Foundation Topics

Asset Security Concepts

Asset security concepts that you must understand include

- Asset and data policies
- Data quality
- Data documentation and organization

Asset and Data Policies

As a security professional, you should ensure that your organization implements a data *policy* that defines long-term goals for data management and asset policies that define long-term goals for each asset type at a minimum. In some cases, each asset may need its own defined policy to ensure that it is properly administered. Business units will need to define asset policies and data policies for any assets and data owned by that business unit. Asset and data policies should be based on the organization's overall asset and data policies. Individual roles and responsibilities should be defined to ensure that personnel understand their job tasks as related to these policies.

After the overall policies are created, asset and data management practices and procedures should be documented to ensure that the day-to-day tasks related to assets and data are completed. In addition, the appropriate quality assurance and quality control procedures must be put into place for data quality to be ensured. Storage and backup procedures must be defined to ensure that assets and data can be restored.

As part of a data policy, any databases implemented within an organization should be carefully designed based on user requirements and the type of data to be stored. All databases should comply with the data policies that are approved, created, and implemented. Data policies should be strictly enforced.

Prior to establishing a data policy, you should consider several issues that can affect it. These issues include risks, cost, liability, legal and regulatory requirements, privacy, sensitivity, and ownership.

The cost of any data management mechanism is usually the primary consideration of any organization. Often organizations do not implement a data policy because they think it is easier to allow data to be stored in whatever way each business unit or user desires. However, if an organization does not adopt formal data policies and

procedures, data security issues can arise because of the different storage methods used. For example, suppose an organization's research department decides to implement a Microsoft SQL Server database to store all research data, but the organization does not have a data policy. If the database is implemented without a thorough understanding of the types of data that will be stored and the users' needs, the research department may end up with a database that is difficult to navigate and manage. In addition, the proper access control mechanism may not be in place, resulting in users being able to edit the data that should only have view access.

Liability involves protecting the organization from legal issues. Liability is directly affected by legal and regulatory requirements that apply to the organization. Issues that can affect liability include asset or data misuse, data inaccuracy, data corruption, data breach, and data loss or a data leak.

Data privacy is determined as part of data analysis. Data classifications must be determined based on the value of the data to the organization. After the data classifications are determined, data controls should be implemented to ensure that the appropriate security controls are implemented based on data classifications. Privacy laws and regulations must also be considered.

Sensitive data is any data that could adversely affect an organization or individual if it were released to the public or obtained by attackers. When determining sensitivity, you should understand the types of threats that can occur, the vulnerability of the data, and the data type. For example, Social Security numbers are more sensitive than physical address data.

Data ownership is the final issue that you must consider as part of data policy design. This issue is particularly important if multiple organizations store their data within the same asset or database. One organization may want completely different security controls in place to protect its data. Understanding legal ownership of data is important to ensure that you design a data policy that takes into consideration the different requirements of multiple data owners. While this is most commonly a consideration when multiple organizations are involved, it can also be an issue with different business units in the same organization. For example, data from the human resources department has different owners and therefore different requirements than research department data.

Data Quality

Data quality is defined as data's fitness for use. The integrity factor of the security triad drives the data quality. Data quality must be maintained throughout the data life cycle, including during data capture, data modification, data storage, data distribution, data usage, and data archiving. These terms are also known as *data in use*,

data at rest, and *data in transit*. Security professionals must ensure that their organization adopts the appropriate quality control and quality assurance measures so that data quality does not suffer. Data quality is most often safeguarded by ensuring data integrity, which protects data from unintentional, unauthorized, or accidental changes. With data integrity, data is known to be good, and information can be trusted as being complete, consistent, and accurate. System integrity ensures that a system will work as intended.

Security professionals should work to document data standards, processes, and procedures to monitor and control data quality. In addition, internal processes should be designed to periodically assess data quality. When data is stored in databases, quality control and assurance are easier to ensure using the internal data controls in the database. For example, you can configure a field to only a valid number. By doing this, you would ensure that only numbers could be input into the field. This is an example of input validation. Input validation can occur on both the client side (using regular expressions) and the server side (using code or in the database) to avoid SQL injection attacks.

Data **contamination** occurs when data errors occur. Data can be corrupt due to network or hash corruptions, lack of integrity policies, transmission errors, and bad encryption algorithms. Data errors can be reduced through implementation of the appropriate quality control and assurance mechanisms. Data verification, an important part of the process, evaluates how complete and correct the data is and whether it complies with standards. Data verification can be carried out by personnel who have the responsibility of entering the data. Data validation evaluates data after data verification has occurred and tests data to ensure that data quality standards have been met. Data validation must be carried out by personnel who have the most familiarity with the data.

Organizations should develop procedures and processes that keep two key data issues in the forefront: error prevention and correction. Error prevention is provided at data entry, whereas error correction usually occurs during data verification and validation.

Data Documentation and Organization

Data documentation ensures that data is understood at its most basic level and can be properly organized into data sets. Data sets ensure that data is arranged and stored in a relational way so that the data can be used for multiple purposes. Data sets should be given unique, descriptive names that indicate their contents.

By documenting the data and organizing data sets, organizations can also ensure that duplicate data is not retained in multiple locations. For example, the sales department may capture all demographic information for all customers. However, the

shipping department may also need access to this same demographic information to ensure that products are shipped to the correct address. In addition, the accounts receivable department will need access to customer demographic information for billing purposes. There is no need for each business unit to have separate data sets for this information. Identifying the customer demographic data set as being needed by multiple business units prevents duplication of efforts across business units.

Within each data set, documentation must be created for each type of data. In the customer demographic data set example, customer name, address, and phone number are all collected. For each of the data types, the individual parameters for each data type must be created. Whereas an address may allow a mixture of numerals and characters, a phone number should allow only numerals. In addition, each data type may have a maximum length. Finally, it is important to document which data is required—meaning that it must be collected and entered. For example, an organization may decide that fax numbers are not required but phone numbers are required. Remember that each of these decisions is best made by the personnel working most closely with the data.

After all the documentation has been completed, the data organization must be mapped out. This organization will include all interrelationships between the data sets. It should also include information on which business units will need access to data sets or subsets of a data set.

NOTE *Big data* is a term for data sets that are so large or complex that they cannot be analyzed by traditional data processing applications. Specialized applications have been designed to help organizations with their big data. The big data challenges that may be encountered include data analysis, data capture, data search, data sharing, data storage, data mining, and data privacy.

Identify and Classify Information and Assets

Security professionals should ensure that the organizations they work for properly identify and classify all organizational information and assets. The first step in this process is to identify all information and assets the organization owns and uses. To perform information and asset identification, security professionals should work with the representatives from each department or functional area. After the information and assets are identified, security professionals should perform data and asset classification and document sensitivity and criticality of data.

Security professionals must understand private sector classifications, military and government classifications, the information life cycle, databases, and data audit.

Data and Asset Classification

Data and assets should be classified based on their value to the organization and their sensitivity to disclosure. Assigning a value to data and assets allows an organization to determine the resources that should be used to protect them. Resources that are used to protect data include personnel resources, monetary resources, access control resources, and so on. Classifying data and assets allows you to apply different protective measures. Data classification is critical to all systems to protect the *confidentiality*, *integrity*, and *availability* (CIA) of data.

After data is classified, the data can be segmented based on its level of protection needed. The classification levels ensure that data is handled and protected in the most cost-effective manner possible. The assets could then be configured to ensure that data is isolated or protected based on these classification levels. An organization should determine the classification levels it uses based on the needs of the organization. A number of private sector classifications and military and government information classifications are commonly used.

NOTE The common private sector classifications and military and government classifications are discussed in a later section.

The information life cycle, covered in more detail later in this chapter, should also be based on the classification of the data. Organizations are required to retain certain information, particularly financial data, based on local, state, or government laws and regulations.

Sensitivity and Criticality

Data sensitivity is a measure of how freely data can be handled. Some data requires special care and handling, especially when inappropriate handling could result in penalties, identity theft, financial loss, invasion of privacy, or unauthorized access by an individual or many individuals. Some data is also subject to regulation by state or federal laws and requires notification in the event of a disclosure.

Data is assigned a level of sensitivity based on who should have access to it and how much harm would be done if it were disclosed. This assignment of sensitivity is called data classification.

Data criticality is a measure of the importance of the data. Data that is considered sensitive may not necessarily be considered critical. Assigning a level of criticality to a particular data set requires considering the answers to a few questions:

- Will you be able to recover the data in case of disaster?
- How long will it take to recover the data?

- How safely, accurately and quickly can an organization recover the data in case of an incident or disaster?
- What is the effect of this downtime, including loss of public standing?

Data is considered essential when it is critical to the organization's business. When essential data is not available, even for a brief period of time, or when its integrity is questionable, the organization is unable to function at its optimal level. Data is considered required when it is important to the organization but organizational operations would continue for a predetermined period of time even if the data were not available. Data is nonessential if the organization is able to operate without it during extended periods of time.

When the sensitivity and criticality of data are understood and documented, the organization should then work to create a data classification system. Most organizations either use a private sector classification system or a military and government classification system.

PII

Personally identifiable information (PII) was defined and explained in Chapter 1. PII is considered information that should be classified and protected. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122 gives ***guidelines*** on protecting the confidentiality of PII.

According to SP 800-122, organizations should implement the following recommendations to effectively protect PII:



- Organizations should identify all PII residing in their environment.
- Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.
- Organizations should categorize their PII by the PII confidentiality impact level.
- Organizations should apply the appropriate safeguards for PII based on the PII confidentiality impact level.
- Organizations should develop an incident response plan to handle breaches involving PII.
- Organizations should encourage close coordination among their chief privacy officers, senior agency officials for privacy, chief information officers, chief information security officers, and legal counsel when addressing issues related to PII.

SP 800-122 defines PII as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.” To distinguish an individual is to identify an individual. To trace an individual is to process sufficient information to make a determination about a specific aspect of an individual’s activities or status. Linked information is information about or related to an individual that is logically associated with other information about the individual. In contrast, linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual.

All PII should be assigned confidentiality impact levels based on the FIPS 199 designations. Those designations are

- **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Determining the impact from a loss of confidentiality of PII should take into account relevant factors. Several important factors that organizations should consider are as follows:

- **Identifiability:** How easily PII can be used to identify specific individuals
- **Quantity of PII:** How many individuals are identified in the information
- **Data field sensitivity:** The sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together
- **Context of use:** The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated
- **Obligation to protect confidentiality:** The laws, regulations, standards, and operating practices that dictate an organization’s responsibility for protecting PII
- **Access to and location of PII:** The nature of authorized access to PII

PII should be protected through a combination of measures, including operational safeguards, privacy-specific safeguards, and security controls. Operational safeguards should include policy and procedure creation and awareness, training, and education programs. Privacy-specific safeguards help organizations collect, maintain, use, and disseminate data in ways that protect the confidentiality of the data and include minimizing the use, collection, and retention of PII; conducting privacy impact assessments; de-identifying information; and anonymizing information. Security controls include separation of duties, least privilege, auditing, identification and authorization, and others from NIST SP 800-53.

NOTE NIST SP 800-53 is covered in more detail in Chapter 1.

Organizations that collect, use, and retain PII should use NIST SP 800-122 to help guide the organization's efforts to protect the confidentiality of PII.

PHI

Protected health information (PHI), also referred to as electronic protected health information (**EPHI** or **ePHI**), is any individually identifiable health information. PHI is treated as a special case of PII with different standards and frameworks. NIST SP 800-66 provides guidelines for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The Security Rule applies to the following covered entities:

- **Covered healthcare providers:** Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which HHS (U.S. Department of Health and Human Services) has adopted a standard.
- **Health plans:** Any individual or group plan that provides or pays the cost of medical care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- **Healthcare clearinghouses:** A public or private entity that processes another entity's healthcare transactions from a standard format to a nonstandard format, or vice versa.
- **Medicare prescription drug card sponsors:** A nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act.

Each covered entity must ensure the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits; protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI; and protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

The Security Rule is separated into six main sections as follows:

- **Security Standards General Rules:** Includes the general requirements all covered entities must meet; establishes flexibility of approach; identifies standards and implementation specifications (both required and addressable); outlines decisions a covered entity must make regarding addressable implementation specifications; and requires maintenance of security measures to continue reasonable and appropriate protection of PHI.
- **Administrative Safeguards:** Defined in the Security Rule as the “administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”
- **Physical Safeguards:** Defined as the “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”
- **Technical Safeguards:** Defined as the “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”
- **Organizational Requirements:** Includes standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans.
- **Policies and Procedures and Documentation Requirements:** Requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the Security Rule; maintenance of written documentation (which may be also in electronic form such as email) and/or records that include policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation.

NIST SP 800-66 includes a relationship linking the NIST Risk Management Framework (RMF) and the Security Rule. It also includes key activities that should be carried out for each of the preceding six main sections of the Security Rule. Organizations that collect, use, and retain PHI should use NIST SP 800-66 to help guide the organization's efforts to provide confidentiality, integrity, and availability for PHI.

Proprietary Data

Proprietary data is defined as internally generated data or documents that contain technical or other types of information controlled by an organization to safeguard its competitive edge. Proprietary data may be protected under copyright, patent, or trade secret laws. While there are no specific and different standards or frameworks to govern the protection of proprietary data, organizations must ensure that the confidentiality, integrity, and availability of proprietary data are protected. Because of this, many organizations protect proprietary data with the same types of controls that are used for PII and PHI.

Security professionals should ensure that proprietary data is identified and properly categorized to ensure that the appropriate controls are put into place.

Private Sector Data Classifications

Organizations in the private sector can generally classify their data using four main classification levels, listed from highest sensitivity level (1) to lowest (4):

Key Topic

1. Confidential
2. Private
3. Sensitive
4. Public

NOTE It is up to each organization to determine the number and type of classifications. Other classification options that an organization can choose to use include “protected” to indicate legally protected data and “proprietary” to indicate company-owned data (in a legal sense).

Data that is confidential includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred. Data at this level would be available only to personnel in the organization whose work needs, or is directly related to, the accessed data.

Access to confidential data usually requires authorization for each access. In most cases, the only way for external entities to have authorized access to confidential data is as follows:

- After signing a confidentiality agreement
- When complying with a court order
- As part of a government project or contract procurement agreement

Data that is private includes any information related to personnel, including human resources records, medical records, and salary information, that is used only within the organization. Data that is sensitive includes organizational financial information and requires extra measures to ensure its CIA and accuracy. Public data is data that is generally shared with the public and would not cause a negative impact on the organization. Examples of public data include how many people work in the organization and what products an organization manufactures or sells.

Military and Government Data Classifications

Military and governmental entities usually classify data using five main classification levels, listed from highest sensitivity level to lowest:

Key Topic

1. **Top Secret:** Disclosure would cause exceptionally grave danger to national security.
2. **Secret:** Disclosure would cause serious damage to national security.
3. **Confidential:** Disclosure would cause damage to national security.
4. **Sensitive but Unclassified:** Disclosure might harm national security.
5. **Unclassified:** Any information that can generally be distributed to the public without any threat to national interest.

U.S. federal agencies use the Sensitive but Unclassified (SBU) designation when information is not classified but still needs to be protected and requires strict controls over its distribution. There are over 100 different labels for SBU, including

- For official use only (FOUO)
- Limited official use
- Sensitive security information
- Critical infrastructure information

Executive order 13556 created a standard designation Controlled Unclassified Information (CUI). Implementation is in progress.

Data that is top secret includes weapon blueprints, technology specifications, spy satellite information, and other military information that could gravely damage national security if disclosed. Data that is secret includes deployment plans, missile placement, and other information that could seriously damage national security if disclosed. Data that is confidential includes strength of forces in the United States and overseas, technical information used for training and maintenance, and other information that could seriously affect the government if unauthorized disclosure occurred. Data that is sensitive but unclassified includes medical or other personal data that might not cause serious damage to national security if disclosed but could cause citizens to question the reputation of the government and may even lead to legal battles with lawsuits. Military and government information that does not fall into any of the four other categories is considered unclassified and usually available to the public based on the Freedom of Information Act.

NOTE Enacted on July 4, 1966, and taking effect one year later, the Freedom of Information Act (FOIA) provides a powerful tool to advocates for access to information. Under the FOIA, anyone may request and receive any records from federal agencies unless the documents are officially declared exempt based upon specific categories, such as top secret, secret, and confidential. To learn more about how to explore for FOIA data or make a FOIA request, visit www.foia.gov.

Information and Asset Handling Requirements

Organizations should establish the appropriate information and asset handling requirements to protect their assets. As part of these handling requirements, personnel should be instructed on how to mark, label, store, and destroy or dispose of media.

Handling requirements are spelled out in organizational standards and other documentation. Organizational standards and documentations must be enforced to ensure proper asset handling. Handling requirements inform custodians and users how to protect the information they use and systems with which they interact. Handling requirements dictate by classification level how information must be stored, transmitted, communicated, accessed, retained, and destroyed. Handling requirements can extend to incident management and breach notification. Handling requirements extend to automated tools, such as data loss prevention (DLP) solutions. Handling requirements should be succinctly documented in a usable format. Handling requirements compliance should be referenced in the acceptable use policy (AUP). Users should be introduced to handling requirements during the onboarding process. Handling requirements should be reinforced throughout the user life cycle.

Marking, Labeling, and Storing

Plainly label all forms of storage media (tapes, optical drives, and so on) and store them safely. Some guidelines in the area of media control are to

- Accurately and promptly mark all data storage media.
- Ensure proper environmental storage of the media.
- Ensure the safe and clean handling of the media.
- Log data media to provide a physical inventory control.

The environment where the media will be stored is also important. For example, damage could occur to magnetic media above 100 degrees Fahrenheit (38 degrees Celsius).

Media marking refers to the use of human-readable information about the media, while *media labeling* refers to the use of security attributes in internal **data structures**. Marking is usually written on the media itself so the correct media can be easily identified. Labeling is internal to the media itself. A backup tape may be marked with a server name or other identifier of the asset to which the backup belongs. If an administrator accesses the backups on the backup tape, each backup will be labeled with a descriptive name that usually includes the date, time, and type of backup. In addition, ACLs may be configured on the different backup files to limit the users who can access the backup files.

Labeling is the vehicle for communicating the assigned classification to custodians, users, and applications (for example, access control and DLP). Labels make it easy to identify the data classification. Labels can take many forms: electronic, print, audio, or visual. Labeling recommendations are tied to media type. In electronic form, the classification label should be a part of the document name (for example, Customer Transaction History_Protected). On written or printed documents, the classification label should be clearly watermarked, as well as in either the document header or footer. For physical media, the classification label should be clearly marked on the case using words or symbols.

Destruction

During media disposal, you must ensure no data remains on the media. The most reliable, secure means of removing data from magnetic storage media, such as a magnetic tape cassette, is through *degaussing*, which exposes the media to a powerful, alternating magnetic field. It removes any previously written data, leaving the media in a magnetically randomized (blank) state. More information on the destruction of media is given earlier in this chapter, later in the “Data Remanence and Destruction” section, and in Chapter 7, “Security Operations.”

Provision Resources Securely

While information and assets within an organization are ultimately owned by the organization, it is usually understood that information and assets within the organization are owned and managed by different business units. These business units must work together to ensure that the organizational mission is achieved and that the information and assets are protected.

For this reason, security professionals must understand where the different information and assets are located and work with the various owners to ensure that the information and assets are protected. The owners that security professionals need to work with include data owners, system owners, and business/mission owners. As part of asset ownership, security professionals should ensure that appropriate asset management procedures are developed and followed, as described in Chapter 7.

Asset Inventory and Asset Management

To properly secure organizational assets, security professionals must ensure that an accurate inventory of all assets is obtained. After all assets are inventoried, assets must be managed by the asset owners. To fully understand asset inventory and management, security professionals must understand the asset life cycle. According to the National Institute of Standards (NIST), the asset life cycle is an eight-phase process, as shown in Figure 2-1.

**Key
Topic**

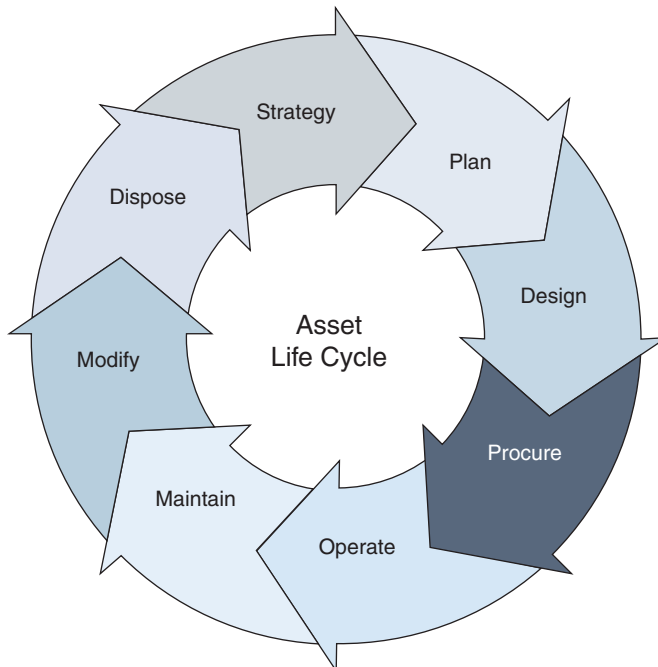


Figure 2-1 Asset Life Cycle

In a typical life cycle, an asset goes through the enrollment, operation, and end-of-life phases. The enrollment process involves manual IT staff activities, such as assigning and tagging the asset with a serial number and barcode, loading a baseline IT image, assigning the asset to an owner, and, finally, recording the serial number as well as other attributes into a database. The attributes might also include primary location, hardware model, baseline IT image, and owner. This process can also be referred to as the inventory phase.

As the asset goes through the operations phase, changes can occur. Such changes could include introduction of new or unauthorized software, the removal of certain critical software, or the removal of the physical asset itself from the enterprise. These changes need to be tracked and recorded. As a consequence, asset monitoring, anomaly detection, reporting, and policy enforcement are the primary activities in this phase.

The assets within the enterprise are monitored using installed agents that reside on the asset, as well as network-based monitoring systems that scan and capture network traffic. These monitoring systems collect data from and about the assets and send periodic reports to the analytics engine.

As an asset reaches the end of its operational life, it goes through activities within the end-of-life phase that include returning the asset to IT support for data removal and removing the serial number (or other organization labeling information) from the registration database and other associated databases. Finally, the asset is prepared for physical removal from the enterprise facility.

Asset management includes the operate, maintain, and modify phases of the asset life cycle. After an asset is configured as it should be with all updates and settings, administrators should document the configuration baseline, which is a description of an asset's attributes at a point in time, which serves as a basis for defining change. (Configuration and change management are discussed in more detail in Chapter 7.) As part of asset management, an asset's security and configuration baseline should be enforced by configuration management agents, and installed software is captured by software asset management agents. Both categories of agents forward reports to their respective servers, which serve as data storage facilities. Reports can be compiled based on the data received from the agents and sent to those responsible for managing the assets. Regular examination of these reports should be a priority to ensure that assets have the appropriate security controls.

Data Life Cycle

A *data life cycle* refers to the entire period of time that an organization retains data. The following sections discuss the data life cycle, databases, roles and

responsibilities, data collection and limitation, data location, data maintenance, data retention, data remanence and destruction, and data audit.

Organizations should ensure that any information they collect and store is managed throughout the life cycle of that information. If no information life cycle is followed, the data would be retained indefinitely, never discarded, and rarely, if ever, updated. Security professionals must therefore ensure that data owners and custodians understand the information life cycle.

For most organizations, the five phases of the information life cycle are as follows:



1. Create/receive
2. Distribute
3. Use
4. Maintain
5. Dispose/store

During the create/receive phase, data is either created by organizational personnel or received by the organization via the data entry portal. If the data is created by organizational personnel, it is usually placed in the location from which it will be distributed, used, and maintained. However, if the data is received via some other mechanism, you might need to copy or import the data to an appropriate location. In this case, the data will not be available for distribution, usage, and maintenance until after the copy or import. Not all data is used by all users. As such, data needs to be sorted, stored, and distributed in various ways as the needs arise from each user or business unit. This phase also must contain data classification after receiving and creating. Received or created data must be given a classification and sensitivity before it can be distributed or data will be going everywhere.

After the create/receive phase, organizational personnel must ensure that the data is properly distributed. In most cases, this step involves placing the data in the appropriate location and possibly configuring the access permissions as defined by the data owner. Keep in mind, however, that in many cases the storage location and appropriate user and group permissions may already be configured. In such a case, it is just a matter of ensuring that the data is in the correct distribution location. Distribution locations include databases, shared folders, *network-attached storage (NAS)*, storage-area networks (SANs), and data libraries.

After data has been distributed, personnel within the organization can use the data in their day-to-day operations. Whereas some personnel will have only read access to data, others may have write or full control permissions. Remember that the

permissions allowed or denied are designated by the data owner but configured by the data custodian.

Now that data is being used in day-to-day operations, data maintenance is key to ensuring that data remains accessible and secure. Maintenance includes auditing, performing backups, performing data integrity checks, and managing data leaks and loss.

When data becomes old, invalid, and not fit for any further use, it is considered to be in the disposition stage. You should either properly dispose of it or ensure that it is securely stored. Some organizations must maintain data records for a certain number of years per local, state, or federal laws or regulations. This type of data should be archived for the required period. In addition, any data that is part of litigation should be retained as requested by the court of law, and organizations should follow appropriate chain of custody and evidence documentation processes. Data archival and destruction procedures should be clearly defined by the organization.

All organizations need policies in place for the retention and destruction of data. Data retention and destruction must follow all local, state, and government regulations and laws. Documenting proper procedures ensures that information is maintained for the required time to prevent financial fines and possible incarceration of high-level organizational officers. These procedures must include both the retention period and destruction process.

Figure 2-2 shows the information life cycle.

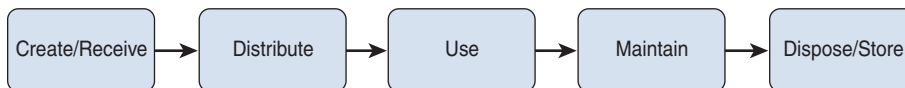


Figure 2-2 Information Life Cycle

A discussion of data would be incomplete without a discussion of databases.

Databases

Databases have become the technology of choice for storing, organizing, and analyzing large sets of data. End users who use data from databases generally access a database through a client interface. As the need arises to provide access to entities outside the enterprise, the opportunities for misuse increase. In the following sections, concepts necessary to discuss database security are covered as well as the security concerns surrounding database management and maintenance.

DBMS Architecture and Models

Databases contain data, and the main difference in database models is how that information is stored and organized. The model describes the relationships among the data elements, how the data is accessed, how integrity is ensured, and acceptable operations. The five models or architectures we discuss are

- Relational
- Hierarchical
- Network
- Object-oriented
- Object-relational

The *relational* model uses *attributes* (columns) and *tuples* (rows) to organize the data in two-dimensional tables. Each cell in the table represents the intersection of an attribute, and a tuple represents a record.

When working with relational database management systems (RDBMSs), you should understand the following terms:

- **Relation:** A connection between one or more tables. One column in a table is a primary key that relates to another table as a foreign key.
- **Tuple:** A *row* in a table.
- **Attribute:** A column in a table.
- **Schema:** Description of a *relational database*.
- **Record:** A collection of related data items.
- **Base relation:** In SQL, a relation that is actually existent in the database.
- **View:** The set of data derived from one or more tables or views available to a given user. Security is enforced through the use of views for users needing read-only access to the data.
- **Degree:** The number of columns in a table.
- **Cardinality:** The number of rows in a relation.
- **Domain:** The set of allowable values that an attribute can take.
- **Primary key:** One or more columns that identify each row of a table unique.
- **Foreign key:** An attribute in one relation that has values matching the primary key in another relation. Matches between the foreign key and the primary key

are important because they represent references from one relation to another and establish the connection among these relations.

- **Candidate key:** An attribute in a row that uniquely identifies that row.
- **Referential integrity:** A requirement that for any foreign key attribute, the referenced relation must have a tuple with the same value for its primary key.

An important element of database design that ensures that the attributes in a table depend only on the primary key is a process called *normalization*. Normalization includes

- Eliminating repeating groups by putting them into separate tables
- Eliminating redundant data (occurring in more than one table)
- Eliminating attributes in a table that are not dependent on the primary key of that table

In the **hierarchical database** model, data is organized into a hierarchy. An object can have one child (an object that is a subset of the parent object), multiple children, or no children. To navigate this hierarchy, you must know the branch in which the object is located. An example of the use of this system is the Windows Registry and a Lightweight Directory Access Protocol (LDAP) directory.

In the **network** model, as in the hierarchical model, data is organized into a hierarchy, but unlike the hierarchical model, objects can have multiple parents. Because of this, knowing which branch to find a data element in is not necessary because there will typically be multiple paths to it.

The **object-oriented** model can handle a variety of data types and is more dynamic than a relational database. **Object-oriented database (OODB)** systems are useful in storing and manipulating complex data, such as images and graphics. Consequently, complex applications involving multimedia, computer-aided design (CAD), video, graphics, and expert systems are more suited to the object-oriented model. It also has the characteristics of ease of reusing code and analysis and reduced maintenance.

Objects can be created as needed, and the data and the procedures (or methods) go with the object when it is requested. A **method** is the code defining the actions that the object performs in response to a message. This model uses some of the same concepts of a relational model. In the object-oriented model, the relation, column, and tuple (relational terms) are referred to as class, attribute, and instance objects.

The **object-relational** model is the marriage of object-oriented and relational technologies, combining the attributes of both. This is a relational database with a software interface that is written in an **object-oriented programming (OOP)** language. The

Index

Numbers

2FA (two-factor authentication), 223

3DES, 329

5G, 450

 CUPS (Control and User Plane
 Separation), 450–451

 D2D (device-to-device
 communication), 451

 MEC (multi-access Edge
 Computing), 450–451

 voice over, 451

0802.1X, 464–466

A

AAA (Authentication, Authorization,
 and Accounting), 588

 accounting, 589–591

 authentication, 588–589

 authorization, 589

abstraction, 11, 775–776

acceptance test, 789, 817

access control, 10, 267, 709. *See also*
 facility security; physical security

 applications, 567

 attribute-based, 606–608

 centralized, 564

 compensative, 107

 content-dependent, 609

 context-dependent, 609

 corrective, 107–108

 decentralized, 565

 default no access, 593

 detective, 108

 deterrent, 108

 devices, 566

 directive, 108

 discretionary, 604

 identify resources, 562

 identify the relationship between
 resources and users, 563

 identify users, 562–563

 mandatory, 604–605

 matrix, 610–611

 natural, 363

 policy, 611–612

 preventive, 108

 recovery, 108

 risk-based, 609–610

 role-based, 568, 605

 rule-based, 605–606

 services, 245, 567–568

 systems, 565–566

 threats

 access aggregation, 624

 advanced persistent, 624

 backdoor, 624

 buffer overflow, 622

 DoS/DDoS, 621

 eavesdropping, 623

 emanating, 623

 malware, 622–623

 mobile code, 622

 password, 619–620

 prevent or mitigate, 625

- social engineering, 620–621
 - spoofing, 623
 - types, 109
- account, 703–704
 - maintenance, 297
 - management, 656
 - revocation, 615
 - review, 614–615
 - transfers, 615
- accountability, 272
- accounting, 8–9, 589–591
- accreditation, 267–268, 785, 789
- ACL (access control list), 564
- acoustical systems, 757
- acquisitions and mergers, 15–16, 17
- ActiveX, 779
- ad hoc mode, 458
- address bus, 247
- administrative controls, 109–110
- administrative investigation, 65–66
- administrative law, 47
- administrator account, 703
- advanced distance vector protocol, 493
- adware, 811
- AES (Advanced Encryption Standard), 329–330
- aggregation, 276
- Agile model, 797–798
- agreement
 - employee, 92–93
 - reciprocal, 742
 - resource capacity, 742–743
 - service-level, 81, 152–153, 706–707, 718–719
- AI (artificial intelligence), 728
- alarm, environmental, 377
- ALE (annual loss expectancy), 102–103, 104–105
- algebraic attack, 357
- algorithm. *See also* asymmetric algorithm; symmetric algorithm
 - asymmetric, 323–324
 - cryptographic, 317
 - MD, 349–350
 - Rijndael, 330
 - Secure Hash, 350–351
 - symmetric, 321–322
- ALU (arithmetic logic unit), 246
- analog signal, 413
- analysis, risk
 - qualitative, 104
 - quantitative, 102–104
- analytic attack, 358
- analytics, user behavior, 697
- antenna, 467–468
- anti-malware, 726, 814
- antivirus, 726, 813
- anycast address, 429
- AP (access point), 457–458
- API (application programming interface), 393
 - NetBIOS (Network Basic Input/Output System), 440
 - security, 823
- APIPA (Automatic Private IP Addressing), 412
- app
 - security, 782–783
 - vetting process, 780–782
- applet, 274
 - ActiveX, 779
 - Java, 779
- Application layer
 - OSI model, 393
 - TCP/IP model, 397–398
- application/s, 702
 - access control, 567
 - owner, 20–21
 - security, 300
 - virtual, 531
- APT (advanced persistent threat), 624
- architecture
 - data flow, 275
 - firewall, 483–484
 - service-oriented, 779
 - superscalar, 254

- system, 241–242
 - access control services, 245
 - auditing and monitoring services, 245–246
 - boundary control services, 245
 - cryptography services, 245
 - integrity services, 245
- archiving, 205–206
- ARO (annualized rate of occurrence), 103, 104–105
- ARP (Address Resolution Protocol), 401, 436–442
 - broadcast, 436
 - cache, 436–437
 - poisoning, 536–537
 - reverse, 437
- artifacts, 689–690
- assembly language, 774
- assessment
 - internal, 638
 - location, 639
 - risk, 100–101
 - security, 637
 - security control, 114
 - third-party, 150–151
 - vulnerability, 639–640
- asset/s, 96, 101. *See also* data
 - classification, 175–176
 - cloud, 701–702
 - information, 709
 - intangible, 707
 - inventory, 700
 - life cycle, 185–186
 - physical, 701
 - policies, 172–173
 - tangible
 - facilities, 707–708
 - software, 708–709
 - virtual, 701
- assurance, 233–234, 303
- asymmetric algorithm, 323–324
 - Diffie-Hellman, 333
 - ECC (Elliptic Curve Cryptosystem), 334–335
 - El Gamal, 334
 - Knapsack, 335
 - RSA, 333–334
- asynchronous transmission, 414
- ATM (Asynchronous Transfer Mode), 513
- attack/s, 99
 - ARP, 536–537
 - birthday, 619
 - blind spoofing, 535–536
 - brute force, 619
 - cryptography, 355–360
 - DDoS (distributed denial-of-service), 539–540, 621
 - denial of service, 539
 - dictionary, 619
 - DNS cache poisoning, 539
 - DoS (denial-of-service), 621
 - double-encapsulated 802.1Q/nested VLAN, 536
 - email, 541
 - spear phishing, 542
 - whaling, 542
 - ICMP-based, 537
 - fraggle, 538
 - ping of death, 537
 - ping scanning, 538
 - smurf, 537
 - MAC flooding, 536
 - man-in-the-middle, 536
 - non-blind spoofing, 535
 - phishing, 472
 - potential, 147–148
 - rainbow table, 619–620
 - remote, 544
 - sniffer, 620
 - SYN ACK, 544
 - tagging, 536
 - teardrop, 545
 - time-of-check/time-of-use, 297–298
 - TOC (time of check)/TOU (time of use), 823

- vector, 143
- wireless
 - warchalking, 543
 - wardriving, 543
- attenuation, 496
- attribute-based access control, 606–608
- audit/ing, 8–9, 590–591, 691
 - committee, 19
 - data, 200–201
 - record retention, 706
 - security, 638–639, 659–661
 - software, 816
 - trails, 591
 - types, 692
- auditor, 21
- AUP (acceptable use policy), 91–92, 674
- authentication, 569, 573, 588–589
 - behavioral characteristic, 581
 - characteristic factor, 579–580
 - device, 585
 - Kerberos, 595–596
 - knowledge factor, 573–577
 - location factor, 584
 - multifactor, 584–585
 - ownership factor, 577
 - memory cards, 578
 - smart cards, 578
 - synchronous and asynchronous token devices, 577
- password, 570–573
- password-less, 585–586
- RADIUS (Remote Authentication Dial-In User Service), 528–529, 601
- remote, 529–530
- separation of duties, 591–592
- SESAME (Secure European System for Applications in a Multi-vendor Environment), 597
- session management, 599
- single-factor, 584
- SSO (single sign-on), 594–595

- TACACS+ (Terminal Access Controller Access-Control System Plus), 528–529, 601
- time factor, 584
- authenticity, 7–8
- authorization, 238, 569, 589
 - Open, 597
 - permissions, 603
 - privileges, 603
 - rights, 603
 - separation of duties, 591–592
- automation, 702
- availability, 7, 745–746

B

- backdoor, 624, 821–822
- background investigation, 90
- backhaul, 455–456
- backup, 658, 711
 - differential, 736
 - electronic, 737–738
 - full, 736
 - HSM (hierarchical storage management), 716–717
 - incremental, 736
 - strategies, 738–739
 - transaction log, 737
- balanced security, 6
- bandwidth, 503–504
- base-16 notation, IPv6, 423–424
- baseband transmission, 415
- Basel II, 60
- baseline, 76, 206–207, 702, 726
- bastion host, 483
- BCP (business continuity plan), 79.
 - See also* business continuity
- behavior, object, 775
- behavioral characteristic
 - authentication, 581
- Bell-LaPadula model, 237–238
- best evidence, 683
- BGP (Border Gateway Protocol), 495

BIA (business impact analysis), 79,
 84, 731
 development, 85–86
 identify critical processes and
 resources, 86
 identify outage impact and estimate
 downtime, 86–88
 identify recovery priorities, 88–89
 identify resource requirements, 88
 Biba model, 238–239
 big data, 175
 biometric systems, 579–580, 581–583
 accuracy, 581
 enrollment time, 581
 throughput rate, 581
 birthday attack, 358, 619
 black hat, 44
 black-box testing, 652
 blacklisting, 725
 blind spoofing attack, 535–536
 blind test, 644
 block cipher, 322–323
 Blowfish, 330
 bluejacking, 461
 bluesnarfing, 461
 Bluetooth, 461
 board of directors, 13, 17–18
 bollards, 755
 botnet, 811–812
 boundary control services, 245
 bounds, 232
 breach, data, 52, 99
 Brewer-Nash (Chinese Wall) model, 240
 bridge, 477
 broadcast transmission, 416, 429
 brownout, 136
 brute force attack, 357, 619
 BSI (Build Security In), 807
 budget, security, 14
 buffer overflow, 622, 819–821
 build and fix model, 793–794
 bus topology, 501
 business case, 14

business continuity, 5, 76–77. *See also*
 disaster/disaster recovery
 BIA (business impact analysis), 79
 contingency plan, 82–84
 disaster, 77–78
 man-made, 78
 natural, 78
 technological, 78
 disruption, 77
 external dependencies, 80–81
 personnel components, 81–82
 scope, 82
 business interruption insurance, 745
 business owner, 196
 business process recovery, 731

C

CA (certificate authority), 336, 341
 cable Internet, 524–525
 cabling
 attenuation, 496
 coaxial, 497–498
 data rate, 496
 fiber optic, 499–500
 installation, 497
 noise, 495–496
 plenum, 137
 security, 497
 twisted pair, 498–499
 Caesar cipher, 308
 CALEA (Communications Assistance
 for Law Enforcement Act of
 1994), 57
 CAM (content-addressable memory), 275
 CAN (campus-area network), 435
 capability table, 610–611
 capacitance detector, 757
 capacity management, 474
 CASB (cloud access security broker), 210
 CASE (common application service
 element) sublayer, OSI (Open
 Systems Interconnection) model,
 393–394

- CASE (computer-aided software engineering), 801
- catastrophe, 77
- CBC (Cipher Block Chaining), 327–328
- CBC (Cipher Block Chaining) MAC, 352–353
- CC (Common Criteria), 261–263
- CCPA (California Consumer Privacy Act), 58
- CCTV (closed-circuit television), 758
- CD (continuous delivery), 799
- CDMA (code-division multiple access), 449
- CDN (content-distribution network), 519
- cellular network, 5G, 450
 - CUPS (Control and User Plane Separation), 450–451
 - D2D (device-to-device communication), 451
 - MEC (multi-access Edge Computing), 450–451
 - voice over, 451
- centralized access control, 564
- CEO (chief executive officer), 18
- CER (crossover error rate), 582
- certification, 267–268, 341, 785, 789
- CFAA (Computer Fraud and Abuse Act of 1986), 56
- CFB (Cipher Feedback), 327–328
- CFO (chief financial officer), 18
- chain of custody, 680–681
- change management, 699
- characteristic factor authentication, 579–580
- checklist test, 752
- checksum, 347
- China, PIPL (Personal Information Protection Law), 64
- chosen ciphertext attack, 357
- chosen plaintext attack, 356
- CI (continuous integration), 799
- CIA triad, 6, 231–232
 - availability, 7, 80
 - confidentiality, 7
 - integrity, 7
- CIDR (Classless Inter-Domain Routing), 407
- CIFS (Common Internet File System), 441
- CIO (chief information officer), 18
- CIP (critical infrastructure protection)
 - plan, 83
- cipher
 - block, 322–323
 - Caesar, 308
 - concealment, 318
 - hybrid, 324
 - Kerckhoff's principle, 310
 - lock, 368
 - running key, 318
 - scytale, 307
 - stream-based, 322
 - substitution, 318–319
 - transposition, 320–321
 - Vigenere, 308–309
- circuit-level proxy, 481–482
- circuit-switching, 512–513
- circumstantial evidence, 684
- CIS (Center for Internet Security), Critical Security Controls, 32–33
- CISC (Complex Instruction Set Computer), 247
- CISO (chief information security officer), 14
- civil investigation, 685
- civil law, 45–47
- civil trial, 66
- Clark-Wilson integrity model, 239–240
- classful IP addressing, 407–408
- classification, data, 175–176
 - military and government, 182–183
 - private sector, 181–182
- Cleanroom model, 800
- client-based systems, vulnerabilities, 273–274
- client/server architecture, 243

- clipping level, 726
- closed system, 225
- CLOUD (Clarifying Lawful Overseas Use of Data), 61
- cloud/cloud computing, 281–282
 - assets, 701–702
 - deployments, 282
 - IDaaS (Identity as a Service), 602
 - levels of service, 282–283
 - NIST recommendations, 283–284, 286–287
 - security assessment, 639
 - security guidelines, 283–284
 - service agreement, 283–284
 - VPC (virtual private cloud), 533–534
- CMAC (Cipher-Based MAC), 353
- CMMI (Capability Maturity Model Integration), 35–36, 801–802
- coaxial cable, 497–498
- COBIT (Control Objectives for Information and Related Technology), 28
- code. *See also* software development
 - mobile, 244, 779, 822–823
 - repository, 808
 - review and testing, 651–653
 - testing
 - dynamic, 653
 - static, 653
- cohesion, 777
- cold site, 741
- collision domain, 507–508
- collusion, 139–140
- COM (Component Object Model), 778
- command, sudo, 616–617
- committee
 - audit, 19
 - governance, 17
- common law, 46
- communication, threats, 136–137
- compartmented security mode, 233
- compensative controls, 107
- compensatory damages, 46
- compliance, 40–42
 - legal, 42
 - privacy requirements, 42
 - regulatory, 41–42
 - risks, 149
- Component-Based Development, 801
- Computer Ethics Institute, 71
- Computer Security Act of 1987, 57
- computer/computing, 242
 - artifacts, 690
 - assisted crime, 43
 - CPU, 246–247
 - address bus, 247
 - ALU (arithmetic logic unit), 246
 - CISC (Complex Instruction Set Computer), 247
 - fetching, 246
 - multistate system, 248
 - multitasking, 247–248
 - multithreading, 248
 - process state, 249
 - RISC (Reduced Instruction Set Computer), 247
 - single-state system, 248
 - edge, 296
 - fail safe state, 255
 - firmware, 253
 - BIOS/UEFI, 253–254
 - device, 254
 - grid, 288
 - investigations. *See* digital forensic investigations
 - I/O (input/output) devices, 252–253
 - memory and storage, 249–250, 251
 - DMA (direct memory access), 250
 - RAM, 249
 - random versus sequential access, 252
 - ROM, 250
 - operating system, 254–255
 - peer-to-peer, 288–289
 - platform

- distributed system, 243
- embedded system, 243
- mainframe/thin client, 242–243
- middleware, 243
- mobile, 244
- virtual, 244
- prevalence crime, 43
- room, 367
- supervisor mode, 255
- surveillance, 685
- targeted crime, 43
- concealment cipher, 318
- conclusive evidence, 684
- confidentiality, 7, 238
- configuration management, 697–699
- confinement, 232
- connectivity
 - cable, 524–525
 - dial-up, 522–523
 - DSL (Digital Subscriber Line), 523–525
 - ISDN (Integrated Services Digital Network), 523
 - VPN (virtual private network), 525–528
- consent, credit history check, 90
- consultant, compliance policy
 - requirements, 94
- containerization, 294
- contamination, 276
- content-dependent access control, 609
- context-dependent access control, 609
- contingency plan, 79–80, 82–84
 - policy, 84
 - strategy, 85
- continuity planning, 79
- continuous monitoring, 694
- contractor, compliance policy
 - requirements, 94
- control/s. *See also* access control
 - administrative, 109–110
 - contingency plan, 79–80
 - critical security, 32–33
 - implementing, 106–107
 - import/export, 52–53
 - input/output, 727–728
 - logical, 111, 564
 - physical, 111–113, 564
 - preventive, 85
 - security, 114, 806
 - selection based on systems security
 - requirements, 268–269
- converged protocols, 443
 - CXL (Compute Express Link), 445–446
 - FCoE (Fibre Channel over Ethernet), 443–444
 - InfiniBand, 444–445
 - iSCSI (Internet Small Computer System Interface), 447–448
 - MPLS (Multiprotocol Label Switching), 446–447
 - VoIP (Voice over Internet Protocol), 447
- cookies, 472
- COOP (continuity of operations plan), 83
- copyright, 49–50
- CORBA (Common Object Request Broker Architecture), 777–778
- corporate governance, 11
- corrective controls, 107–108
- corroborative evidence, 684
- COSO (Committee of Sponsoring Organizations), 33, 132
- counterfeit products, 149
- countermeasure, 97–98, 104–105
- coupling, 777
- covert channel, 822
- CPO (chief privacy officer), 18
- CPS (cyber-physical systems), NIST
 - framework, 291–293
- CPTED (Crime Prevention Through Environmental Design), 363
- CPU, 246–247
 - address bus, 247

- ALU (arithmetic logic unit), 246
- CISC (Complex Instruction Set Computer), 247
- fetching, 246
- multistate system, 248
- multitasking, 247–248
- multithreading, 248
- process state, 249
- RISC (Reduced Instruction Set Computer), 247
- single-state system, 248
- cracker, 44
- CRAMM (CCTA Risk Analysis and Management Method), 37
- CRC (cyclic redundancy check), 347
- credential management system, 600–601
- credit history, 90
- crime
 - computer prevalence, 43
 - computer-assisted, 43
 - computer-targeted, 43
 - cyber, 52
 - incidental computer, 43
 - scene, 676, 679, 679–680, 681. *See also* investigation/s
- criminal history check, 90
- criminal investigation, 66
- crisis communications plan, 83
- CRL (certificate revocation list), 340
- cross-certification, 341
- crosstalk, 498
- cryptography/cryptographic, 305–307, 312–313. *See also* asymmetric algorithm; encryption; symmetric algorithm
 - algorithm selection, 317
 - applied, 354–355
 - asymmetric algorithm, 323–324
 - attack/s, 355–360
 - block cipher, 322–323
 - Caesar cipher, 308
 - concealment cipher, 318
 - elliptic curve, 324–325
 - Enigma machine, 310
 - history, 307–308
 - hybrid cipher, 324
 - IV (initialization vector), 323
 - Kerckhoff's principle, 310
 - key management, 316–317
 - life cycle, 315–316
 - logical operations, 313–315
 - Lucifer project, 311
 - modulo function, 315
 - NIST guidelines, 312–313
 - nonce, 315
 - one-time pad, 319–320
 - one-way function, 315
 - quantum, 325, 470
 - running key cipher, 318
 - services, 245
 - split knowledge, 315
 - steganography, 320
 - stream-based cipher, 322
 - substitution cipher, 318–319
 - symmetric algorithm, 321–322, 325
 - 3DES, 329
 - AES (Advanced Encryption Standard), 329–330
 - DES (Digital Encryption Standard), 325–329
 - system vulnerabilities, 276–277
 - transposition cipher, 320–321
 - Vigenere cipher, 308–309
- cryptosystem, features, 311–312
- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), 507, 509–510
- CSMA/CD (Carrier Sense Multiple Access/Collision Detection), 505, 507, 508–509
- CSO (chief security officer), 14, 18–19
- CSP (cloud service provider), 37
- CSU/DSU (channel service unit/data service unit), 512

CUPS (Control and User Plane Separation), 450–451

customary law, 47

CXL (Compute Express Link), 445–446

cyber crime, 52

cybersquatting, 541

D

D2D (device-to-device communication), 451

DAC (discretionary access control), 604

DAST (dynamic application security testing), 790–792

data

audit, 200–201

big, 175

breach, 52

classification, 175–176

military and government, 182–183

private sector, 181–182

clearing, 718

collection, 197

contamination, 174

controller, 195

criticality, 176–177

custodian, 20, 195

destruction, 199–200

documentation, 174–175

hiding, 11, 775–776

integrity, 7

interface languages, 191

life cycle, 186–188

location, 198

maintenance, 198–199

masking, 710

mining, 191

owner, 19, 194

policies, 172–173

processor, 196

proprietary, 181

purgin, 718

purging, 192

quality, 173–174

recovery, 735

differential backup, 736

electronic backup, 737–738

full backup, 736

incremental backup, 736

transaction log backup, 737

remanence, 199–200

at rest, 204, 709

retention, 199, 201–203

security, 203

sensitivity, 173, 176

sharing, 204–205

storage and archiving, 205–206

structure, 777

trans-border flow, 53

in transit, 204, 710

in use, 204

user, 197

warehouse, 191, 276

data center, security, 372

data flow architecture, 275

Data Link layer, OSI (Open Systems Interconnection) model, 395

database, 188

ACID test, 193

aggregation, 276

contamination, 276

hierarchical, 190

inference, 275–276

locks, 193

maintenance, 192

network model, 190

normalization, 190

object-oriented, 190

object-relational, 190

polyinstantiation, 193

relational, 189–190

threats, 192–193

views, 193

DCOM (Distributed Component Object Model), 778

- DDoS (distributed denial-of-service)
 - attack, 539–540, 621
- decentralized access control, 565
- decryption, 272
- dedicated security mode, 232
- default no access, 593
- default security posture, 9
- defense-in-depth, 9–10, 226, 824
- degaussing, 184
- denial of service, 7
- dependency
 - external, 80–81
 - supply chain, 149
- deployments, cloud computing, 282
- DES (Digital Encryption Standard), 325–329
- detective controls, 108
- deterrent controls, 108
- device
 - access control, 566
 - authentication, 585
 - multiplexer, 476
 - portable media, 700
 - tampering, 700
 - telco concentrator, 476
 - token, 577
- DevOps, 806
- DevSecOps, 790
 - DAST (dynamic application security testing), 790–792
 - IAST (interactive application security test), 791
 - SAST (static application security testing), 790
 - SCA (software composition analysis), 791–792
- DHCP (Dynamic Host Configuration Protocol), 437–438
- dial-up, 522–523
- dictionary attack, 619
- differential backup, 736
- differential cryptanalysis, 357
- Diffie-Hellman, 333
- digital certificate, 336–337
 - CRL (certificate revocation list), 340
 - enrollment, 338
 - life cycle, 337–338
 - revocation, 339–340
 - renewal and modification, 340
 - verification, 339
- digital forensic investigations, 674–675
 - artifacts, 689–690
 - digital toolkit, 687–689
 - examine and analyze evidence, 677
 - expertise, 677
 - identify evidence, 676
 - IOCE guidelines, 678–679
 - lessons learned, 677
 - present findings, 677
 - preserve and collect evidence, 676–677
 - reporting and documentation, 678
 - standards, 67–68
 - training, 689
- digital signal, 413–414
- digital signature, 8, 354
- digital toolkit, 687–689
- direct evidence, 683–684
- directive controls, 108
- directory service, 593
- disaster/disaster recovery, 5, 77–78, 79, 83, 658–659, 732, 747. *See also* testing, disaster recovery plans
 - assessment, 750
 - cold site, 741
 - communications, 749–750
 - damage assessment team, 748
 - documentation, 734
 - fault tolerance, 744
 - hardware backup, 732
 - hot site, 740–741
 - human resources, 733–734
 - insurance, 744–745
 - legal team, 748
 - lessons learned, 751

- man-made, 78
- media relations team, 748
- multiple site strategies, 739–740
- natural, 78
- personnel, 747–748
- reciprocal agreement, 742
- recovery team, 749
- redundant site, 742
- redundant systems, facilities, and
 - power, 744
- resource capacity agreement, 742–743
- restoration team, 749
- salvage team, 749
- security team, 749
- software backup, 733
- supplies, 734
- technological, 78
- tertiary site, 742
- training and awareness, 750–751
- warm site, 741
- disclosure, 7, 727
- disruption, 77
- distance vector protocol, 493
- distributed object-oriented systems, 777
 - ActiveX, 779
 - COM (Component Object Model), 778
 - CORBA (Common Object Request Broker Architecture), 777–778
 - DCOM (Distributed Component Object Model), 778
 - Java, 778–779
 - mobile code, 779
 - OLE (Object Linking and Embedding), 778
 - SOA (service-oriented architecture), 779
- distributed system, 243
- divestiture, 16–17
- DLP (data loss prevention), 210, 695–696
- DMA (direct memory access), 250, 252
- DMZ (demilitarized zone), 483
- DNS (Domain Name System), 393, 438, 539
- DNSSEC (Domain Name Security Extensions), 540
- documentation
 - business case, 14
 - data, 174–175
 - disaster recovery, 734
 - DRM (digital rights management), 361
 - FIPS 199, 117–119
 - investigation, 678
 - ITIL core publications and processes, 34
 - NIST SP 800 Series, 28–31, 119–128.
 - See also* NIST (National Institute of Standards and Technology)
 - security, 72–73
- DoDAF (Department of Defense Architecture Framework), 26
- domain grabbing, 540–541
- doors, 368
 - glass, 371
 - locks, 369–371
 - mantrap, 368–369
- DoS (denial-of-service) attack, 539, 621
- dotted decimal format, 406
- double-blind test, 644
- double-encapsulated 802.1Q/nested
 - VLAN attack, 536
- DPIA (Data Protection Impact Assessment), 63
- DPO (data protection officer), 18
- DRM (digital rights management), 51, 209–210, 360–361
 - document, 361
 - e-book, 362
 - movie, 362
 - music, 361–362
 - video game, 362
- DRP (disaster recovery plan), 83
- DSL (Digital Subscriber Line), 415, 523–525
- DSRC (dedicated short-range communications), 451
- DSS (digital signature standard), 354

- dual-homed firewall, 483
- due care, 18, 39, 51
- due diligence, 18, 39–40
- dumpster diving, 621
- duress, 760–761
- dwelt time, 581
- dynamic NAT, 412
- dynamic packet filtering firewall, 482
- dynamic testing, 653

E

- E lines, 511
- EAP (Extensible Authentication Protocol), 465–466
- eavesdropping, 623
- e-book DRM, 362
- ECB (Electronic Code Book), 326–327
- Economic Espionage Act of 1996, 60
- ECPA (Electronic Communications Privacy Act), 57
- edge computing systems, 296
- eDiscovery, 70
- EDR (Endpoint Detection and Response), 488
- EF (exposure factor), 103
- efficacy, security metric, 14
- egress monitoring, 695
- EIGRP (Enhanced IGRP), 494
- El Gamal, 334
- electronic backup, 737–738
- electrical threats, 136
- electromechanical systems, 757
- elliptic curve, 324–325
- email
 - attacks
 - spear phishing, 542
 - whaling, 542
 - header, 542
 - security, 355, 469
 - MIME (Multipurpose Internet Mail Extensions), 470
 - PGP (Pretty Good Privacy), 469–470
 - spam, 543

- emanating, 623
- embedded system, 243, 304
- emergency management, 762
- EMI (electromagnetic interference), 498
- employee
 - AUP (acceptable use policy), 91–92
 - duress, 760–761
 - job rotation, 95
 - monitoring, 762
 - onboarding and offboarding policies, 93–94
 - privacy issues, 61–62
 - privacy policy, 95
 - safety and security, 760
 - screening and hiring policy, 90–91
 - separation of duties, 95
 - spoofing, 541–542
 - termination, 94
 - threats, 16
- encapsulation, 11, 392, 402–403, 776
- encryption, 7, 11, 272, 355, 709
 - end-to-end, 209, 468–469
 - link, 208–209, 468
- endpoint security, 518–519
- end-to-end encryption, 209, 468–469
- Enigma machine, 310
- enrollment, digital certificate, 338
- enticement, 721
- entrapment, 721
- environmental security
 - alarms, 377
 - fire protection, 373–375
 - HVAC, 376
 - water leakage and flooding, 376–377
- escalation of privileges, 821
- ESI (electronically stored information), 70
- Ethernet, 504
 - CSMA/CD (Carrier Sense Multiple Access/Collision Detection), 505
 - frame, 504
 - implementations, 505
 - Metro, 433

ethics

- agreements, 92–93
- ISC² code of, 70–71
- organizational code of, 72
- professional, 70

EU (European Union)

- GDPR (General Data Protection Regulation), 63–64
- privacy laws and regulations, 62

evacuation drill, 753

evaluation models, 255–256

- CC (Common Criteria), 261–263
- ITSEC (Information Technology Security Evaluation Criteria), 259–261

Rainbow Series, 256

Green Book, 259

Orange Book, 256–259

Red Book, 256

- TSCEC (Trusted Computer System Evaluation Criteria), 256

events, 719–720

evidence

- best, 683
- chain of custody, 680–681
- circumstantial, 684
- conclusive, 684
- corroborative, 684
- direct, 683–684
- examine and analyze, 677
- five rules, 682
- hearsay, 684
- identifying, 676
- IOCE guidelines, 678–679
- legally permissible, 682
- opinion, 684
- order of volatility, 676
- preserve and collect, 676–677
- relevant, 682
- reliability, 682
- secondary, 683
- seizure, 685
- storage, 373

EXCLUSIVE OR operation, 314–315

expertise, forensic investigation, 677

exploit, 97

Exploratory model, 801

explosions, 137–138

exposure, 97

external dependency, 80–81

external reporting, 115–116

external threat, 134

extranet, 432

F

facial scan, 580

facility security, 566. *See also* physical security

data center, 372

doors, 368

evidence storage, 373

locks, 369–371

media storage facilities, 373

redundancy, 744

restricted and work areas, 372

server room, 372

turnstiles and mantraps, 368–369

type of glass used for entrances, 371

visitor control, 371

wiring closet/IDF, 372

factoring attack, 359

fail safe state, 255

fail securely, 227

FAR (false acceptance rate), 582

fault detection, 474

fault injection, 360

fault tolerance, 89, 271, 711, 718, 744

FBI (Federal Bureau of Investigation), 52

FCoE (Fibre Channel over Ethernet), 443–444

FDDI (Fiber Distributed Data Interface), 506

FDM (frequency-division multiplexing), 415

FDMA (frequency-division multiple access), 449

- Federal Privacy Act (US, 1974), 56
 - FedRAMP (Federal Risk and Authorization Management Program), 37
 - fencing, 756
 - fetching, 246
 - FHSS (frequency hopping spread spectrum), 448
 - fiber optic cable, 499–500
 - FIFO (first in, first out), 738
 - FIM (Federated Identity Management), 534–535, 597–598
 - fingerprint scan, 579–580
 - FIPS 199, 117–119
 - fire, 138–139
 - computer, 136
 - detection, 374
 - suppression, 374–375
 - firewall, 480, 724–725
 - architecture, 483–484
 - bastion host, 483
 - dual-homed, 483
 - dynamic packet filtering, 482
 - NAC (network access control), 517
 - packet filtering, 480–481
 - proxy, 481–482
 - SOCKS (Socket Secure), 482
 - stateful, 481
 - three-legged, 484
 - firmware, 253
 - BIOS/UEFI, 253–254
 - device, 254
 - FISA (Federal Intelligence Surveillance Act of 1978), 56
 - FISMA (Federal Information Security Management Act), 60
 - five pillars of information security
 - authenticity, 7–8
 - availability, 7
 - confidentiality, 7
 - integrity, 7
 - non-repudiation, 8
 - flight time, 581
 - fraggle attack, 538
 - Frame Relay, 513
 - framework/s, 21. *See also* NIST (Nationals Institute of Standards and Technology)
 - COBIT (Control Objectives for Information and Related Technology), 28
 - HITRUST Common Security, 31–32
 - MODAF (British Ministry of Defence Architecture Framework), 26
 - risk, NIST (Nationals Institute of Standards and Technology), 116–131
 - SABSA (Sherwood Applied Business Security Architecture), 26–27
 - TOGAF (The Open Group Architecture Framework), 26
 - Zachman, 26
 - fraud, 139
 - Freedom of Information Act (US, 1996), 183
 - frequency analysis, 358
 - FRR (false rejection rate), 582
 - FTP (File Transfer Protocol), 438
 - full backup, 736
 - full interruption test, 753
 - full-knowledge test, 645
 - functional drill, 753
 - fuzz testing, 653
- ## G
- gates, 756
 - gateway, 480
 - GDPR (General Data Protection Regulation), 63–64, 228
 - geo-fence, 756
 - GFS (grandfather/father/son) scheme, 738
 - glass, 371
 - GLBA (Gramm-Leach-Bliley Act) of 1999, 55–56
 - goals, organizational security, 12–13
 - Goguen-Meseguer model, 241

governance
 committee, 17
 information security, 5
 IT, 12
 third-party, 151
 Graham-Denning model, 240
 gray hat, 44
 gray-box testing, 652
 GRC (governance, risk management, and compliance), 41
 Green Book, 259
 grid computing, 288
 group, 587–588
 GSM (Global System for Mobile communication), 449–450
 guest operating system, 534
 guidelines, 76

H

hacker, 44
 hand scan, 580
 hardware
 analysis, 687
 backup, 732
 mobile communication, 456–457
 redundant, 718
 risks, 148–150
 segmentation, 269–270
 Harrison-Ruzzo-Ullman model, 241
 hash/ing, 348. *See also* algorithm
 HAVAL, 351
 MAC (Message Authentication Code), 352
 one-way, 348–349
 RIPEMD-160, 351
 salting, 353
 Tiger, 351
 HAVAL, 351
 header, 402–403
 Health Care and Education
 Reconciliation Act of 2010, 61
 hearsay evidence, 684

HIDS (host-based IDS), 486
 hierarchical database, 190
 high availability, 745–746
 HIPAA (Health Insurance Portability and Accountability Act), 40, 55
 HITRUST CSF (Common Security Framework), 31–32
 honeypot, 485, 725–726
 horizontal privilege escalation, 616
 hot site, 740–741
 HPC (High-Performance Computing) systems, 295
 HSM (hierarchical storage management), 716–717
 HSSI (High-Speed Serial Interface), 514
 HTTP (Hypertext Transfer Protocol), 393, 439
 HTTPS (Hypertext Transfer Protocol Secure), 439
 hub, 476
 human resources, 733–734
 human-caused threats, 137
 collusion, 139–140
 explosions, 137–138
 fire, 138–139
 fraud, 139
 theft, 139
 vandalism, 139
 HVAC, 376
 hybrid cipher, 324
 hybrid topology, 503
 hygrometer, 377

I

IAB (Internal Architecture Board), 71–72
 IAST (interactive application security test), 791
 ICMP (Internet Control Message Protocol), 401, 439
 attacks, 537
 fraggle, 538
 ping of death, 537

- ping scanning, 538
- smurf, 537
- redirect, 538
- ICS (Industrial Control Systems),
277–281, 442–443
- IDaaS (Identity as a Service), 602
- IDEA (International Data Encryption
Algorithm), 330
- IDEAL model, 803–804
- identification, 568–569
- identifying, threats, 146–147
- identity. *See also* authentication
 - and access management, 711–712
 - and account management, 613–614
 - credential management system, 600–601
 - federated management, 597–598
 - JIT (Just-In-Time) access, 601–602
 - proof of, 599–600
 - theft, 621
 - third-party services, 602
- IDS (intrusion detection system), 486–487,
692–693, 724
- IEC (International Electrotechnical
Commission), 208
- IETF (Internet Engineering Task
Force), 404
- IGMP (Internet Group Management
Protocol), 401, 440
- IGRP (Interior Gateway Routing
Protocol), 494
- IMAP (Internet Message Access
Protocol), 440
- implants, 149
- implementation attack, 360
- import/export controls, 52–53
- incident, 99
- incident response, 83, 693–694, 719,
721–722, 747
 - detect, 722
 - detective and preventive measures, 724
 - lessons learned, 724
 - mitigate, 723
 - recover, 723
 - remediate, 723–724
 - report, 723
 - respond, 722–723
 - rules of engagement, 720–721
 - team, 720
- incidental computer crime, 43
- incremental backup, 736
- Incremental model, 796
- India, Information Technology (Reasonable
Security Practices and Procedures
and Sensitive Personal Data or
Information) Rules 2011, 59
- industry standards, 67–69
- inference, 275–276
- InfiniBand, 444–445
- information systems
 - encryption/decryption, 272
 - fault tolerance, 271
 - interface, 271
 - life cycle, 220, 706
 - architectural design, 222
 - development/implementation, 222
 - integration, 222
 - requirements analysis, 221–222
 - retirement/disposal, 223
 - stakeholders' needs and require-
ments, 221
 - transition/deployment, 223
 - verification and validation, 222–223
- memory protection, 269–270
- policy mechanisms
 - accountability, 272
 - separation of privilege, 271–272
- TPM (Trusted Platform Module), 270
- Information Technology (Reasonable
Security Practices and Procedures
and Sensitive Personal Data or
Information) Rules 2011 (India), 59
- information/information security, 565
 - abstraction, 11
 - authenticity, 7–8

- CIA triad, 6, 231–232
 - availability, 7, 80
 - confidentiality, 7
 - integrity, 7
- data hiding, 11
- defense-in-depth, 9–10
- destruction, 184
- encryption, 11
- flow model, 235–236
- governance, 5, 11
- handling requirements, 183
- marking, labeling, and storing, 184
- non-repudiation, 8
- infrared, 462
- infrastructure, network, 475
- infrastructure mode, 458
- inherent risk, 105
- inheritance, object, 775
- input validation, 821, 824
- input/output controls, 727–728
- instant messaging, 521–522
- insurance, 744–745
- intangible assets, 96, 707
- integration test, 789
- integrity, 7
 - message, 347–348
 - services, 245
- intellectual property, 47–48
 - copyright, 49–50
 - patent, 48
 - trade secret, 48–49
 - trademark, 49
- interface, 271, 654
- internal reporting, 115
- internal threat, 134
- Internet
 - connectivity
 - cable, 524–525
 - dial-up, 522–523
 - DSL (Digital Subscriber Line), 523–525
 - ISDN (Integrated Services Digital Network), 523
 - VPN (virtual private network), 525–528
 - security
 - cookies, 472
 - remote access, 471
 - SET (Secure Electronic Transaction), 471–472
 - SSH (Secure Shell), 472
- Internet layer, TCP/IP model, 400–402
- interpreted code, 775
- interviewing, 681
- intranet, 431
- inventory, asset, 700
- investigation/s. *See also* evidence; incident response
 - administrative, 65–66
 - background, 90
 - civil, 685
 - criminal, 66
 - digital forensic, 674–675
 - artifacts, 689–690
 - digital toolkit, 687–689
 - examine and analyze evidence, 677
 - expertise, 677
 - identify evidence, 676
 - IOCE guidelines, 678–679
 - lessons learned, 677
 - present findings, 677
 - preserve and collect evidence, 676–677
 - hardware analysis, 687
 - interviewing, 681
 - media analysis, 685–686
 - MOM (motive, opportunity, and means), 680
 - network analysis, 686–687
 - operations, 65–66
 - regulatory, 66
 - reporting and documentation, 678
 - search warrant, 685
 - software analysis, 686
 - surveillance, 685
 - techniques, 681

- training, 689
 - warrant, 681
- I/O (input/output) devices, 252
- IOCE (International Organization on Computer Evidence), 678–679
- IoT (Internet of Things), 289–290
 - methods of securing devices, 290
 - NIST framework, 291–293
- IP (Internet Protocol), 401
 - convergence, 443
 - voice over, 447
- IP address
 - APIPA (Automatic Private IP Addressing), 412
 - classful, 407–408
 - NAT (Network Address Translation), 408–411
 - dynamic, 412
 - stateful, 411–412
 - static, 412
 - PAT (Port Address Translation), 410–411
 - public versus private, 408
 - spoofing, 545
- IPPD (Integrated Product and Process Development), 804–805
- IPS (intrusion prevention system), 488, 692–693, 724
- IPsec, 421, 526–528
- IPT (integrated product team), 804–806
- IPv4, 406–407
 - versus IPv6, 417–418
 - subnet mask, 406
 - subnets, 406
- IPv6, 417
 - address scope, 429–430
 - address types, 427–429
 - base-16 notation, 423–424
 - versus IPv4, 417–418
 - major features
 - autoconfiguration, 420
 - efficient transmission, 422–423
 - extended address space, 420
 - extension headers, 421
 - header structure, 420–421
 - mandatory IPsec support, 421
 - mobile compatibility, 421
 - QoS (quality of service), 421–422
 - route aggregation, 422
 - network prefix, 424–426
 - NIST guidelines, 418–420
 - shorthand, 426–427
 - subnet ID, 424
 - threats, 423
- iris scan, 580
- IRQ (interrupt request), 252
- ISACA (Information Systems Audit and Control Association), 12
- ISC² Certified Information Systems Security Professional (CISSP) exam
 - customizing your practice exams, 837–838
 - suggested plan for final review, 839–840
 - tools for final preparation, 835–837
 - updating your practice exams, 838
- ISC² code of ethics, 70–71
- ISCP (information system contingency plan), 84
- iSCSI (Internet Small Computer System Interface), 447–448
- ISDN (Integrated Services Digital Network), 523
- IS-IS (Intermediate System to Intermediate System), 495
- ISO (International Organization for Standardization)
 - 9001:2015/90003:2014, 802–803
 - OSI (Open Systems Interconnection) model. *See* OSI (Open Systems Interconnection) model
- ISO/IEC 27000 Series, 11–12, 22–25, 264–266
 - ISO/IEC 27005:2018, 131–132
 - software development security best practices, 807
- ISO/IEC 42010:2011, 242

isolation, 232

IT

governance, 12
system, 223–224

ITAR (Internal Traffic in Arms Regulations), 58

ITGI (IT Governance Institute), 12

ITIL (Information Technology Infrastructure Library), 11–12, 34, 34

ITSEC (Information Technology Security Evaluation Criteria), 259–261

IV (initialization vector), 323

J

JAD (Joint Analysis Development) model, 800

Java, 778–779

JDBC (Java Database Connectivity), 191

JIT (Just-In-Time), 601–602

jitter, 503–504

job rotation, 95, 705

jurisdiction, 53

JVM (Java virtual machine), 779

K

keep it simple and small, 228

Kerberos, 595–596

Kerckhoff's principle, 310

kernel proxy firewall, 482

key management, 316–317, 343–347

keylogger, 813

keystroke dynamics, 581

Knapsack, 335

knowledge factor authentication, 573–577

known plaintext attack, 356

KPI (key performance indicator), 657

L

LAN (local-area network), 430–431

large-scale parallel data systems, 287–288

latency, 503–504

layered defense model, 363

LDAP (Lightweight Directory Access Protocol), 440, 593

LDP (Label Distribution Protocol), 440

least privilege, 225–226, 568, 592, 703, 824

legacy system, 16

legal system

administrative law, 47

civil law, 45–46

civil/tort law, 46–47

common law, 46

compliance, 42

criminal law, 46

customary law, 47

mixed law, 47

religious law, 47

liability, 173

life cycle

asset, 185–186

cryptographic, 315–316

data, 186–188

digital certificate, 337–338

information, 706

information systems, 220

architectural design, 222

development/implementation, 222

integration, 222

requirements analysis, 221–222

retirement/disposal, 223

stakeholders' needs and

requirements, 221

transition/deployment, 223

verification and validation, 222–223

patch management, 729

provisioning, 612–613

security program, 38–39

software development, 786

certify/accredit, 789

change management and

configuration management/

replacement, 789–790

- CMMI (Capability Maturity Model Integration), 801–802
 - design, 787
 - develop, 788
 - gather requirements, 787
 - plan/initiate project, 786–787
 - release/maintenance, 789
 - test/validate, 788–789
 - system development, 783–784
 - acquire/develop, 784–785
 - dispose/decommission, 785
 - implement, 785
 - initiate, 784
 - operate/maintain, 785
 - lighting, 758–759
 - linear cryptanalysis, 357
 - link encryption, 208–209, 468
 - Link layer, TCP/IP model, 402
 - link state protocol, 493
 - Linux
 - root account, 577, 703
 - sudo command, 616–617
 - Lipner model, 240
 - location factor authentication, 584
 - locks, 368, 369–371
 - logic bomb, 811
 - logical addressing, 405–406
 - logical controls, 111, 564
 - logical operations, cryptography, 313–315
 - log/s, 691–692. *See also* reporting
 - management, 696–697
 - management policy, 650
 - review, 646–650
 - software, 816
 - Lucifer project, 311
- M**
- MAC (mandatory access control), 604–605
 - MAC (media access control) address, 395, 413, 466
 - MAC (Message Authentication Code), 351
 - Cipher Block Chaining, 352–353
 - Cipher-Based, 353
 - hash, 352
 - MAC flooding attack, 536
 - machine language, 774
 - machine learning, 728
 - mainframe/thin client, 242–243
 - maintenance
 - account, 297
 - data, 198–199
 - database, 192
 - hooks, 297
 - security architecture, 272–273
 - malware, 622–623
 - anti-, 726, 814
 - botnet, 811–812
 - keylogger, 813
 - logic bomb, 811
 - mobile, 813
 - ransomware, 44, 359, 546, 813
 - rootkit, 812
 - scanning, 814
 - scareware, 45
 - spyware/adware, 811
 - Trojan horse, 811
 - virus, 809–810
 - worm, 810
 - MAN (metropolitan-area network), 432–433
 - management controls, 109–110
 - man-in-the-middle attack, 536
 - man-made disaster, 78
 - mantrap, 368–369
 - matrix-based model, 235
 - maturity model, 272–273
 - MD algorithm, 349–350
 - MEC (multi-access Edge Computing), 450–451
 - media analysis, 685–686
 - media management
 - destruction, 184
 - handling requirements, 183
 - history, 717
 - labeling and storage, 184, 717
 - NAS (network-attached storage), 716

- RAID (Redundant Array of Inexpensive Disks), 712–715
- SAN (storage-area network), 716
 - sanitizing and disposal, 718
- media relations team, 748
- media storage facilities, security, 373
- meet-in-the-middle attack, 359
- memorized secret, 570–571
- memory, 249–250, 251. *See also* storage
 - ARP cache, 436–437
 - cards, 578
 - content-addressable, 275
 - DMA (direct memory access), 250
 - protection, 269–270
 - RAM, 249
 - random versus sequential access, 252
 - ROM, 250
- mesh topology, 502
- message integrity, 347–348
- methods, 775
- metrics, security, 14
- Metro Ethernet, 433
- microservices, 293
- middleware, 243
- MIME (Multipurpose Internet Mail Extensions), 470
- MIMO (multiple input, multiple output), 450
- mission, organizational, 13
- mission owner, 196
- misuse case testing, 653–654
- mixed law, 47
- MNOs (mobile network operators), 452–454
- mobile code, 622, 779, 822–823
- mobile communication, 244, 451–452
 - 5G, 450
 - CUPS (Control and User Plane Separation), 450–451
 - D2D (device-to-device communication), 451
 - MEC (multi-access Edge Computing), 450–451
 - voice over, 451
 - application security, 300
 - backhaul, 455–456
 - device security, 300
 - hardware support, 456–457
 - malware, 813
 - mobile device concerns, 300–302
 - NIST guidelines, 303–304
 - RoTs (Roots of Trust), 303
 - satellite, 454
 - security, 488–492
 - telecom providers, 452–454
 - third-party connectivity, 451–452
 - vulnerabilities, 299–300
- MODAF (British Ministry of Defence Architecture Framework), 26
- model. *See also* OSI (Open Systems Interconnection) model
 - evaluation, 255–256
 - CC (Common Criteria), 261–263
 - ITSEC (Information Technology Security Evaluation Criteria), 259–261
 - Rainbow Series, 256–259
 - TSCEC (Trusted Computer System Evaluation Criteria), 256
- maturity, 272–273
- security
 - Bell-LaPadula, 237–238
 - Biba, 238–239
 - Brewer-Nash (Chinese Wall), 240
 - Clark-Wilson integrity, 239–240
 - Goguen-Meseguer, 241
 - Graham-Denning, 240
 - Harrison-Ruzzo-Ullman, 241
 - information flow, 235–236
 - Lipner, 240
 - matrix-based, 235
 - multilevel lattice, 234–235
 - noninterference, 235
 - state machine, 234
 - Sutherland, 241
 - Take-Grant, 236

- software development. *See* software development
- modified Waterfall model, 795
- modulo function, 315
- MOM (motive, opportunity, and means), 680
- monitoring
 - continuous, 694
 - egress, 695
 - employee, 762
 - network, 473
 - real user, 651
 - supply chain, 151–153
 - synthetic transaction, 650
 - third-party, 150–151
- mono-alphabetic substitution cipher, 307
- movie DRM, 362
- MPLS (Multiprotocol Label Switching), 446–447
- MPM (Modified Prototype Model), 796
- MTBF (mean time between failure), 87, 719
- MTD (maximum tolerable downtime), 86
- MTTR (mean time to repair), 87, 719
- MU MIMO (multi-user multiple-input, multiple-output), 459
- multicast, 416, 428–429
- multifactor authentication, 584–585
- multilayer protocol, 442–443
- multilevel lattice model, 234–235
- multilevel security mode, 233
- multimedia collaboration, 520–521
- multiplexer, 476
- multiplexing, 415
- multitasking, 247–248
- multithreading, 248
- music DRM, 361–362

N

- NAC (network access control), 516–518
 - firewalls/proxies, 517
 - quarantine/remediation, 517
- NAS (network-attached storage), 716
- NAT (Network Address Translation), 408–411, 440
 - dynamic versus static, 412
 - stateful, 411–412
- natural access control, 363
- natural disaster, 78
- natural languages, 775
- natural surveillance, 364
- natural territorials reinforcement, 364
- natural threats, 134–135
- need-to-know, 592, 703
- NetBIOS (Network Basic Input/Output System), 440
- network. *See also* Ethernet; transmission; wireless networks and communication
 - analysis, 686–687
 - artifacts, 690
 - bridge, 477
 - campus-area, 435
 - capacity management, 474
 - content-distribution, 519
 - contention methods, 507
 - collision domain, 507–508
 - CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), 509–510
 - CSMA/CD (Carrier Sense Multiple Access/Collision Detection), 507, 508–509
 - polling, 510
 - token passing, 510
 - discovery scan, 640, 641
 - endpoint security, 518–519
 - extranet, 432
 - fault detection, 474
 - firewall, 480
 - dynamic packet filtering, 482
 - packet filtering, 480–481
 - proxy, 481–482
 - SOCKS (Socket Secure), 482
 - stateful, 481
 - gateway, 480

- hub, 476
- infrastructure, 475
- intranet, 431
- local-area, 430–431
- management, 718–719
- metropolitan-area, 432–433
- monitoring, 473
- observability, 473
- OSI (Open Systems Interconnection)
 - model. *See* OSI (Open Systems Interconnection) model
- patch panel, 475–476
- performance metrics, 503–504
- perimeter, 484
- personal-area, 435
- repeater, 477
- router, 479
- security
 - EDR (Endpoint Detection and Response), 488
 - IDS (intrusion detection system), 486–487
 - IPS (intrusion prevention system), 488
- software-defined, 532–533
- storage-area, 434
- switch, 477–478
- TCP/IP model. *See* TCP/IP model
- telco concentrator, 476
- topology
 - bus, 501
 - hybrid, 503
 - mesh, 502
 - ring, 500
 - star, 502
- virtual local-area, 479
- virtual storage-area, 534
- vulnerability scan, 642–643
- wide area, 433–434
 - ATM (Asynchronous Transfer Mode), 513
 - CSU/DSU, 512
 - E lines, 511
 - Frame Relay, 513
 - HSSI (High-Speed Serial Interface), 514
 - PPP (Point-to-Point Protocol), 514
 - PSTN (public switched telephone network), 514–515
 - SMDS (Switched Multimegabit Data Service), 514
 - SONET (Synchronous Optical Networking), 512
 - T lines, 510–511
 - X.25, 513
 - wireless local-area, 434
- Network layer, OSI (Open Systems Interconnection) model, 395
- NFC (Near Field Communication), 462
- NFS (Network File System), 441
- NIACAP (National Information Assurance Certification and Accreditation Process), 267–268
- NIDS (network-based IDS), 486
- NIST (National Institute of Standards and Technology), 11–12
 - CPS Framework, 291–293
 - FIPS 199, 117–119
 - FIPS 201–2, 599
 - Framework for Improving Critical Infrastructure Cybersecurity, 128–131, 657–658
 - Risk Management Framework, 268
 - SP 800 Series, 28–31
 - SP 800–37 Rev. 2, 125–127
 - SP 800–39, 127–128
 - SP 800–53 Rev. 5, 121–122
 - SP 800–60 Vol. 1 Rev. 1, 119–121
 - SP 800–63, 569–573
 - SP 800–79-2, 600
 - SP 800–86, 679
 - SP 800–92, 646–647
 - SP 800–119, 418–420
 - SP 800–124, 488–492
 - SP 800–128, 518–519

- SP 800–137, 655
- SP 800–144, 283–284, 285–286
- SP 800–146, 286–287
- SP 800–154, 145
- SP 800–160, 123–125
- SP 800–163, 780–783
- SP 800–164, 303–304
- SP 800–175A and B, 312–313
- NNTP (Network News Transfer Protocol), 393
- noise, 495–496
- non-blind spoofing attack, 535
- nonce, 315
- noninterference model, 235
- non-repudiation, 8, 354
- normalization, 190
- NOT operation, 314
- NYS DFS Rule 500, 58

O

- OAuth (Open Authorization), 597
- object, 225
 - behavior, 775
 - inheritance, 775
 - methods, 775
 - reuse, 822
- objectives, organizational, 13
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), 33
- ODBC (Open Database Connectivity), 191
- OFB (Output Feedback), 328–329
- OFDMA (orthogonal frequency-division multiple access), 449
- offboarding, 94
- OIDC (OpenID Connect), 597
- OLE (Object Linking and Embedding), 191, 778
- onboarding, 93–94
- one-time pad, 319–320
- one-way function, 315
- one-way hash, 348–349
- onsite assessment, 151
- OOP (object-oriented programming), 775
 - cohesion, 777
 - coupling, 777
 - data structure, 777
 - distributed object-oriented systems, 777
 - ActiveX, 779
 - COM (Component Object Model), 778
 - CORBA (Common Object Request Broker Architecture), 777–778
 - DCOM (Distributed Component Object Model), 778
 - Java, 778–779
 - mobile code, 779
 - OLE (Object Linking and Embedding), 778
 - SOA (service-oriented architecture), 779
 - encapsulation, 776
 - polyinstantiation, 776
 - polymorphism, 776
- Open Group Security Forum, 594
- open system, 225
- Open System Authentication, 462
- open-source solution, 225
- operating system, 254–255
 - fingerprinting, 641
 - guest, 534
- AND operation, 313–314
- OR operation, 314
- operations investigation, 65–66
- operations security
 - audit and review, 691, 692
 - continuous monitoring, 694
 - identity and access management, 711–712
 - information assets, 709
 - least privilege, 703
 - log types, 691–692
 - media management

- history, 717
 - HSM (hierarchical storage management), 716–717
 - labeling and storage, 717
 - NAS (network-attached storage), 716
 - RAID (Redundant Array of Inexpensive Disks), 712–715
 - SAN (storage-area network), 716
 - sanitizing and disposal, 718
 - need-to-know, 703
 - network and resource management, 718–719
 - privilege/s, 704–705
 - separation of duties, 704
 - SIEM (security information and event management), 693
 - tuning, 694–695
 - two-person control, 705
 - opinion evidence, 684
 - Orange Book, 256–259, 814
 - order of volatility, 676
 - organization/al
 - acquisitions and mergers, 15–16, 17
 - board of directors, 17–18
 - code of ethics, 72
 - compliance
 - legal, 42
 - privacy requirements, 42
 - regulatory, 41–42
 - divestiture, 16–17
 - due care, 39, 51
 - due diligence, 39–40
 - legacy system, 16
 - management, 18–19
 - mission and objectives, 13
 - resources, 15
 - security, 12
 - accounting, 8–9
 - auditing, 8–9
 - corporate governance, 11
 - posture, 9
 - strategies and goals, 12–13
 - security budget, 14
 - OSCP (Online Certificate Status Protocol), 340
 - OSI (Open Systems Interconnection) model
 - Application layer, 393
 - Data Link layer, 395
 - encapsulation, 392
 - Network layer, 395
 - Physical layer, 395–396
 - Presentation layer, 393–394
 - Session layer, 394
 - Transport layer, 394
 - OSPF (Open Shortest Path First), 494
 - OT (Operational Technology), 277
 - OWASP (Open Web Application Security Project), 299, 807
 - owner
 - application, 20–21
 - data, 19, 173
 - system, 20
 - ownership factor authentication, 577
 - memory cards, 578
 - smart cards, 578
 - synchronous and asynchronous token devices, 577
- ## P
- packet
 - encryption/de-encapsulation, 402–403
 - filtering, 480–481
 - shaping, 473–474
 - switching, 512–513
 - PAN (personal-area network), 435
 - parallel test, 753
 - partial-knowledge test, 645
 - pass-the-hash attack, 360
 - password
 - access control threats, 619–620
 - reset policies, 576
 - storage, 576–577
 - password-less authentication, 585–586

- passwords, 570–573
 - PASTA (Process for Attack Simulation and Threat Analysis) methodology, 144
 - PAT (Port Address Translation),
 - 410–411, 441
 - patch management, 729
 - patch panel, 475–476
 - patent, 48
 - patrol force, 759
 - PBX (private branch exchange), 485
 - PCI DSS (Payment Card Industry Data Security Standard), 37–38, 266–267
 - PDPA (Personal Data Protection Act (Singapore)), 59
 - peer-to-peer computing, 288–289
 - penetration testing, 637–638, 643–645
 - perimeter
 - network, 484
 - security, 754
 - bollards, 755
 - fencing, 756
 - gates, 756
 - intrusion detection, 757–758
 - lighting, 758–759
 - patrol force, 759
 - walls, 756
 - permissions, 603
 - personnel, 747–748
 - duress, 760–761
 - monitoring, 762
 - safety and security, 760
 - training, 658, 738
 - personnel components, BCP (business continuity plan), 81–82. *See also* employee
 - personnel security policy, candidate screening and hiring, 90–91
 - PGP (Pretty Good Privacy), 469–470
 - pharming, 620
 - PHI (protected health information), 171–179
 - phishing, 472, 620
 - photoelectric systems, 757
 - physical addressing, 405–406, 413
 - physical asset, 96
 - physical assets, 701
 - physical controls, 111–113, 564
 - Physical layer, OSI (Open Systems Interconnection) model, 395–396
 - physical security, 710
 - accessibility, 366
 - computer and equipment rooms, 367
 - construction, 366–367
 - CPTED (Crime Prevention Through Environmental Design), 363
 - equipment
 - corporate procedures, 377–379
 - safes, vaults and locking, 379
 - internal compartments, 367
 - layered defense model, 363
 - natural access control, 363
 - natural surveillance, 364
 - natural territorials reinforcement, 364
 - perimeter, 754
 - bollards, 755
 - fencing, 756
 - gates, 756
 - intrusion detection, 757
 - lighting, 758–759
 - patrol force, 759
 - walls, 756
 - plan, 364–365
 - surrounding area and external entities, 365–366
 - visibility, 365
- physiological characteristic
 - authentication, 579–580
- PII (personally identifiable information), 53–54, 177–179
- ping of death, 537
- ping scanning, 538
- PIPEDA (Personal Information and Electronic Documents Act), 57–58

- pipelined processor, 254
- PIPL (Personal Information Protection Law), 64
- PIR (passive infrared system), 757
- pirating, 210
- PKI (public key infrastructure), 335, 341, 528
 - key management practices, 343–347
 - QKD (Quantum Key Distribution), 342–343
- plaintiff, 46
- Plan B, 79–80
- Plan–Do–Check–Act cycle, 114–115
- plan/planning
 - contingency, 79–80, 84
 - continuity, 79
 - disaster recovery, 83, 752. *See also* disaster/disaster recovery
 - information system contingency, 84
 - physical security, 364–365
- plenum, 137
- policy/ies, 13, 73–74
 - acceptable use, 91–92, 674
 - access control, 611–612
 - accountability, 272
 - asset, 172–173
 - contingency plan, 84
 - data, 172
 - decision point, 611
 - enforcement point, 611–612
 - issue-specific security, 75
 - log management, 650
 - organizational security, 74
 - password reset, 576
- personnel
 - candidate screening and hiring, 90–91
 - employee onboarding and offboarding, 93–94
 - job rotation, 95
 - privacy, 95
 - separation of duties, 95
 - regulatory, 75
 - security, 814
 - separation of privilege, 271–272
 - system-specific security, 75
- politically motivated threats, 140–141
- polling, 510
- polyalphabetic substitution cipher, 307
- polyinstantiation, 193, 776
- polymorphism, 776
- POPIA (Protection of Personal Information Act), 64–65
- pop-ups, 44
- port
 - numbers, TCP/UDP, 403–405
 - scanning, 544–545
- portable media device, 700
- posture, security, 9
- potential attacks, 147–148
- power supply
 - preventive measures, 375–376
 - redundant, 744
 - types of outages, 375
- power user account, 704
- PPP (Point-to-Point Protocol), 514
- Presentation layer, OSI (Open Systems Interconnection) model, 393–394
- preventive controls, 85, 108
- principle of least functionality, 226
- principle of least privilege, 225–226, 592
- privacy, 53
 - by design, 228–229
 - employee, 61–62
 - laws and regulations, 54–55
 - Basel II, 60
 - CALEA (Communications Assistance for Law Enforcement Act of 1994), 57
 - CCPA (California Consumer Privacy Act), 58
 - CFAA (Computer Fraud and Abuse Act of 1986), 56
 - CLOUD (Clarifying Lawful Overseas Use of Data), 61
 - Computer Security Act of 1987, 57

- Economic Espionage Act of 1996, 60
- ECPA (Electronic Communications Privacy Act), 57
- EU, 62
- Federal Privacy Act of 1974, 56
- FISA (Federal Intelligence Surveillance Act of 1978), 56
- FISMA (Federal Information Security Management Act), 60
- GDPR (General Data Protection Regulation), 63–64
- GLBA (Gramm-Leach-Bliley Act) of 1999, 55–56
- Health Care and Education Reconciliation Act of 2010, 61
- HIPAA (Health Insurance Portability and Accountability Act), 55
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India), 59
- Investigatory Powers Act of 2016, 58–59
- ITAR (Internal Traffic in Arms Regulations), 58
- NYS DFS Rule 500, 58
- PDPA (Personal Data Protection Act (PDPA, Singapore), 59
- PIPEDA (Personal Information and Electronic Documents Act), 57–58
- PIPL (Personal Information Protection Law), 64
- POPIA (Protection of Personal Information Act), 64–65
- SOX (Sarbanes-Oxley Act), 55
- US Federal Sentencing Guidelines of 1991, 57
- USA Freedom Act of 2015, 61
- USA PATRIOT Act of 2001, 60–61
- personnel, 95
- PHI (protected health information), 171–179
- PII (personally identifiable information), 53–54, 177–179
 - requirements, compliance, 42
- private IP address, 408
- private sector data classification, 181–182
- privilege, 603, 616–617, 704–705, 821
- procedure, 75
- process/es, 75, 224. *See also* CPU;
 - system/s
 - bounds, 232
 - confinement, 232
 - isolation, 232
 - state, 249
 - thread, 254
- product
 - fail safe, 227
 - tampering, 149
- professional ethics, 70
- programming language, 774. *See also*
 - software development
 - assembly, 774
 - interpreter, 775
 - machine, 774
 - natural, 775
 - object-oriented, 775–776. *See also*
 - distributed object-oriented systems
 - cohesion, 777
 - coupling, 777
 - data structure, 777
 - encapsulation, 776
 - polymorphism, 776
 - polymorphism, 776
 - very-high level, 774–775
- proof of identity, 599–600
- proprietary data, 181
- protocol, 392
 - ARP (Address Resolution Protocol), 436–442
 - broadcast, 436
 - cache, 436–437
 - converged, 443
 - CXL (Compute Express Link), 445–446

- FCoE (Fibre Channel over Ethernet), 443–444
 - InfiniBand, 444–445
 - iSCSI (Internet Small Computer System Interface), 447–448
 - MPLS (Multiprotocol Label Switching), 446–447
 - VoIP (Voice over Internet Protocol), 447
 - DHCP (Dynamic Host Configuration Protocol), 437–438
 - DNS (Domain Name System), 438
 - FTP (File Transfer Protocol), 438–439
 - HTTP (Hypertext Transfer Protocol), 439
 - HTTPS (Hypertext Transfer Protocol Secure), 439
 - ICMP (Internet Control Message Protocol), 439
 - IGMP (Internet Group Management Protocol), 440
 - IMAP (Internet Message Access Protocol), 440
 - LDAP (Lightweight Directory Access Protocol), 440
 - LDP (Label Distribution Protocol), 440
 - multilayer, 442–443
 - NFS (Network File System), 441
 - POP (Post Office Protocol), 441
 - RARP (Reverse ARP), 437
 - routing, 493
 - BGP (Border Gateway Protocol), 495
 - EIGRP (Enhanced IGRP), 494
 - IGRP (Interior Gateway Routing Protocol), 494
 - IS-IS (Intermediate System to Intermediate System), 495
 - OSPF (Open Shortest Path First), 494
 - RIP (Routing Information Protocol), 493–494
 - VRRP (Virtual Router Redundancy Protocol), 494–495
 - secure, 710
 - S-HTTP (secure HTTP), 439
 - SMTP (Simple Mail Transfer Protocol), 441
 - SNMP (Simple Network Management Protocol), 441–442
 - SSL (Secure Sockets Layer), 442
 - prototyping, 795–796
 - provisioning
 - life cycle, 612–613
 - resource, 185, 699
 - user, identity and account management, 613–614
 - proximity authentication device, 368
 - proxy, 481, 484
 - application-level, 482
 - circuit-level proxy, 481–482
 - kernel, 482
 - NAC (network access control), 517
 - prudent-man rule, 18
 - PSTN (public switched telephone network), 514–515
 - public IP address, 408
 - PUF (physically unclonable function), 152
 - punitive damages, 46
- ## Q
- QKD (Quantum Key Distribution), 342–343
 - QoS (quality of service), 421–422, 473–474, 746
 - qualitative risk analysis, 104
 - quality, data, 173–174
 - quality improvement, 114–115
 - quantitative risk analysis, 102–104
 - quantum cryptography, 325, 470
- ## R
- RA (registration authority), 336
 - RAD (Rapid Application Development), 800
 - RADIUS (Remote Authentication Dial-In User Service), 528–529, 601

- RAID (Redundant Array of Inexpensive Disks), 711, 712–715
- Rainbow Series, 256
 - Green Book, 259
 - Orange Book, 256–259, 814
 - Red Book, 256
- rainbow table attack, 619–620
- random access device, 252
- ransomware, 44, 359, 546, 813
- RARP (Reverse ARP), 437
- RBAC (role-based access control), 568, 605
- RC algorithm, 331
- rcp, 530
- RDC (Remote Desktop Connection), 471
- read-through test, 752
- reciprocal agreement, 742
- record retention, 706
- recoverability, 89
- recovery
 - business process, 731
 - controls, 108
 - data, 735
 - differential backup, 736
 - electronic backup, 737–738
 - full backup, 736
 - incremental backup, 736
 - transaction log backup, 737
 - disaster, 732
 - documentation, 734
 - hardware backup, 732
 - human resources, 733–734
 - software backup, 733
 - supplies, 734
 - strategies, 729–731
 - user environment, 734–735
- Red Book, 256
- Red Team versus Blue Team, 637–638
- redundancy, 711
- reference check, 91
- reference monitor, 815
- regression test, 789
- regression testing, 817
- regulatory compliance, 41–42
- regulatory investigation, 66
- regulatory policy, 75
- relational database, 189–190
- reliability, 80, 682
- religious law, 47
- remanence, 718
- remediation technology, 148
- remote access, 471
 - rlogin/rsh/rcp, 530
 - Telnet, 530
 - TLS/SSL, 530–531
- remote meeting technology, 521
- remote wiping, 700
- repeater, 477
- replay attack, 358
- reporting, 659
 - external, 115–116
 - incident, 723
 - internal, 115
 - investigation, 678
 - SOC (Service Organization Control), 660–661
- residual risk, 105
- resource/s
 - capacity agreement, 742–743
 - human, 733–734
 - management, 718–719
 - organizational, 15
 - protection, 707
 - provisioning, 185, 699
- restoration team, 749
- retina scan, 580
- reverse engineering, 359
- RFI (radio frequency interference), 498
- rights, 603
- Rijndael algorithm, 330
- ring topology, 500
- RIP (Routing Information Protocol), 493–494
- RIPEMD-160, 351

RISC (Reduced Instruction Set Computer), 247

risk, 5, 13, 97

acceptance, 106

analysis

CRAMM (CCTA Risk Analysis and Management Method), 37

qualitative, 104

quantitative, 102–104

software, 816–817

team, 100

appetite, 98

assessment, 100–101

identify threats and vulnerabilities, 101–102

information and asset value and costs, 101

scope, 102

avoidance, 105

-based access control, 609–610

geopolitical, 150

hardware, software, and services, 148–150

indicator, 657

inherent, 105

management team, 99–100

mitigation, 106

reduction, 105

residual, 105

supply chain, 148

transfer, 105

Risk Management Standard, A, 133

rlogin, 530

rogue programmers, 822

role, 587–588

definition, 615

transition, 615–616

ROM, 250

root account, 703

rootkit, 812

RoTs (Roots of Trust), 303

route aggregation, 422

router, 479

routing protocol, 493

BGP (Border Gateway Protocol), 495

EIGRP (Enhanced IGRP), 494

IGRP (Interior Gateway Routing Protocol), 494

IS-IS (Intermediate System to Intermediate System), 495

OSPF (Open Shortest Path First), 494

RIP (Routing Information Protocol), 493–494

VRRP (Virtual Router Redundancy Protocol), 494–495

RPO (recovery point objective), 87, 731

RSA algorithm, 333–334

rsh, 530

RTO (recovery time objective), 87, 731

rule-based access control, 605–606

RUM (real user monitoring), 651

running key cipher, 318

S

SABSA (Sherwood Applied Business Security Architecture), 26–27

SAFe (Scaled Agile Framework), 798–799

salting, 353

salvage, 89, 749

SAM (Security Accounts Manager), 577

SAML (Security Assertion Markup Language), 298, 597, 598

SAN (storage-area network), 434, 716

sandboxing, 725

SASE (Secure Access Service Edge), 230–231

SASE (specific application service element) sublayer, OSI (Open Systems Interconnection) model, 393–394

SAST (static application security testing), 790

satellite communication, 454

SBOM (software bill of materials), 152

- SCA (security control assessment), 114
- SCA (software composition analysis)
 - tools, 791–792
- SCADA (Supervisory Control and Data Acquisition), 277–278
- scareware, 45
- scope/scoping, 207
 - BCP (business continuity plan), 82
 - IPv6 address, 429–430
 - risk assessment, 102
- screen scraper, 531
- screened host, 484
- scytale cipher, 307
- SDLC (system development life cycle), 783–784
 - acquire/develop, 784–785
 - dispose/decommission, 785
 - implement, 785
 - initiate, 784
 - operate/maintain, 785
- SDN (software-defined networking), 532–533
- search warrant, 685
- secondary evidence, 683
- secure design principles
 - assurance and trust, 233–234
 - defense-in-depth, 226
 - fail securely, 227
 - keep it simple and small, 228
 - least privilege, 225–226
 - mode, multilevel, 233
 - objects and subjects, 225
 - privacy by design, 228–229
 - SASE (Secure Access Service Edge), 230–231
 - secure defaults, 226–227
 - shared responsibility, 229
 - SoD (separation of duties), 227
 - threat modeling, 225
 - trust but verify, 229
 - zero trust, 228
- security. *See also* access control; authentication; DevSecOps; facility security; information security; operationssecurity; organizational security
 - administrator, 20
 - analyst, 20
 - API (application programming interface), 823
 - assessment, 637
 - auditing, 638–639
 - awareness training, 16, 153–155
 - balanced approach, 6
 - budget, 14
 - cabling, 497
 - data, 203
 - domain, 598
 - email, 355, 469
 - MIME (Multipurpose Internet Mail Extensions), 470
 - PGP (Pretty Good Privacy), 469–470
 - endpoint, 518–519
 - governance principles, 11–12
 - implementation standards
 - ISO/IEC 27000 Series, 264–266
 - PCI DSS (Payment Card Industry Data Security Standard), 266–267
 - Internet, 355
 - cookies, 472
 - remote access, 471
 - SET (Secure Electronic Transaction), 471–472
 - SSH (Secure Shell), 472
 - kernel, 815
 - management review and approval, 656–657
 - message integrity, 347–348
 - metrics, 14
 - mobile communication, 488–492
 - mode, 233

- compartmented, 233
- dedicated, 232
- system high, 233
- model
 - Bell-LaPadula, 237–238
 - Biba, 238–239
 - Brewer-Nash (Chinese Wall), 240
 - Clark-Wilson integrity, 239–240
 - Goguen-Meseguer, 241
 - Graham-Denning, 240
 - Harrison-Ruzzo-Ullman, 241
 - information flow, 235–236
 - Lipner, 240
 - matrix-based, 235
 - multilevel lattice, 234–235
 - noninterference, 235
 - state machine, 234
 - Sutherland, 241
 - Take-Grant, 236
- network
 - EDR (Endpoint Detection and Response), 488
 - firewall, 480–484
 - honeypot, 485
 - IDS (intrusion detection system), 486–487
 - IPS (intrusion prevention system), 488
- physical. *See* physical security
- policy, 73–74, 814
 - issue-specific, 75
 - organizational, 74
 - regulatory, 75
 - system-specific, 75
- posture, 9
- program
 - life cycle, 38–39
 - top-down versus bottom-up, 38
- remediation technology, 148
- testing, 636–637
- training and awareness, 658
- wireless
 - 0802.1X, 464–466
 - MAC filter, 466
 - Open System Authentication, 462
 - Shared Key Authentication, 463
 - WEP (Wired Equivalent Privacy), 463
 - WPA (Wi-Fi Protected Access), 463
 - WPA2, 463–464
 - WPA3, 464
- seizure of evidence, 685
- sensitive information procedures, 705–706
- separation of duties, 591–592, 704
- separation of privilege, 271–272
- separation of duties, 95
- sequential access device, 252
- server room, security, 372
- server-based system, vulnerabilities, 275
- serverless systems, 294–295
- service account, 617–618, 703
- services, access control, 567–568
- SESAME (Secure European System for Applications in a Multi-vendor Environment), 597
- session hijacking, 544
- Session layer, OSI (Open Systems Interconnection) model, 394
- session management, 599
- SET (Secure Electronic Transaction), 471–472
- SFTP (SSH File Transfer Protocol), 439
- SHA (Secure Hash Algorithm), 350–351
- Shared Key Authentication, 463
- shared responsibility, 229
- shorthand for writing IPv6 addresses, 426–427
- shoulder surfing, 621
- side-channel attack, 359
- SIEM (security information and event management), 648–649, 693
- signal
 - analog, 413
 - digital, 413–414
- silicon root of trust, 152

- simulation test, 753
- Singapore, PDPA (Personal Data Protection Act), 59
- single-factor authentication, 584
- single-state system, 248
- SIP (Session Initiation Protocol), 393
- site survey, wireless network, 467
- Six Sigma, 35–36
- Skipjack, 330
- SLA (service-level agreement), 81, 152–153, 706–707, 718
- smart cards, 578
- smartphone, 700
- SMB (Server Message Block), 441
- SMDS (Switched Multimegabit Data Service), 514
- SME (subject matter expert), 14
- S/MIME (Secure MIME), 470
- SMTP (Simple Mail Transfer Protocol), 441
- smurf attack, 537
- SNAT (Stateful NAT), 411–412
- sniffer attack, 620
- SNMP (Simple Network Management Protocol), 441–442
- SNR (signal-to-noise ratio), 503–504
- SOA (service-oriented architecture), 779
- SOAR (security orchestration and automated response), 693–694
- SOC (Service Organization Control) report, 660–661
- social engineering, 44, 357, 620
- Social Security information verification, 91
- socket, 404
- SOCKS (Socket Secure) firewall, 482
- SoD (separation of duties), 227
- software, 708–709. *See also* malware
 - acquired, security impact, 817–819
 - analysis, 686
 - automation, 702
 - backup, 733
 - DLP (data loss prevention), 695–696
 - patch management, 729
 - piracy, 50–51
 - protection mechanisms, 814–815
 - risks, 148–150
- software development
 - Agile model, 797–798
 - API security, 823
 - auditing and logging, 816
 - build and fix model, 793–794
 - CASE (computer-aided software engineering), 801
 - CD (continuous delivery), 799
 - CI (continuous integration), 799
 - Cleanroom model, 800
 - code repository security, 808
 - Component-Based, 801
 - Exploratory model, 801
 - IDEAL model, 803–804
 - Incremental model, 796
 - IPT (integrated product team), 804–806
 - JAD (Joint Analysis Development) model, 800
 - library, 807
 - life cycle, 786
 - certify/accredit, 789
 - change management and configuration management/replacement, 789–790
 - CMMI (Capability Maturity Model Integration), 801–802
 - design, 787
 - develop, 788
 - gather requirements, 787
 - plan/initiate project, 786–787
 - release/maintenance, 789
 - test/validate, 788–789
 - modified Waterfall model, 795
 - MPM (Modified Prototype Model), 796
 - operation and maintenance, 804
 - prototyping, 795–796
 - RAD (Rapid Application Development), 800
 - regression and acceptance testing, 817

- risk analysis and mitigation, 816–817
- SAFe (Scaled Agile Framework), 798–799
- SDLC (system development life cycle), 783–784
 - acquire/develop, 784–785
 - dispose/decommission, 785
 - implement, 785
 - initiate, 784
 - operate/maintain, 785
- secure coding practices, 823–825
- security best practices
 - BSI (Build Security In), 807
 - ISO/IEC 27000 Series, 807
 - OWASP (Open Web Application Security Project), 807
 - WASC (Web Application Security Consortium), 806
- security controls, 806
- software environment security, 807
- source code analysis tools, 808
- source code security weaknesses and vulnerabilities
 - backdoors and trapdoors, 821–822
 - buffer overflow, 819–821
 - covert channel, 822
 - mobile code, 822–823
 - object reuse, 822
 - privilege escalation, 821
 - rogue programmers, 822
 - TOC (time of check)/TOU (time of use), 823
- Spiral model, 797
- Structured Programming Development Model, 801
- V-shaped model, 795
- Waterfall model, 794
- SONET (Synchronous Optical Networking), 512
- source code analysis tools, 808
- SOX (Sarbanes-Oxley Act), 55
- SP (Special Publication) 800 Series, 28–31
- spam, 543
- spear phishing, 542
- SPF (Sender Policy Framework), 541
- Spiral model, 797
- split knowledge, 315
- SPOF (single point of failure), 719
- spyware, 811
- SSH (Secure Shell), 472
- SSID (Service Set Identifier), 458
- SSL (Secure Sockets Layer), 442, 530–531
- SSO (single sign-on), 298, 451, 594–595
- standards, 21, 76
 - compliance, 40–42
 - deviations from, 726
 - digital forensics, 67–68
 - industry, 67–69
 - ISO/IEC 27000 Series, 22–25, 264–266
 - PCI DSS (Payment Card Industry Data Security Standard), 37–38, 266–267
 - selection, 207–208
 - Six Sigma, 35–36
 - TLS (Transport Layer Security), 442
- star topology, 502
- state machine model, 234
- stateful firewall, 481
- static NAT, 412
- static testing, 653
- statistical attack, 359
- statutory law, 46
- steganography, 320
- storage
 - backup, 738–739
 - cloud computing, 282
 - data, 205–206
 - evidence, 373
 - media, 717
 - password, 576–577
- STP (shielded twisted pair), 498
- strategy/ies
 - backup, 738–739
 - contingency, 85
 - organizational security, 12–13
 - recovery, 729–731

- stream-based cipher, 322
- STRIDE, 143–144
- Structured Programming Development Model, 801
- structured walk-through test, 752
- subjects, 225
- subnet, 406
- subnet mask, 406
- substance-abuse testing, 91
- substitution cipher, 307, 318–319
- sudo command, 616–617
- superscalar architecture, 254
- supervisor, 21
- supply chain
 - interdependencies, 149
 - monitoring, 151–153
 - risks, 148
- surveillance, 681
 - natural, 364
 - physical, 685
- Sutherland model, 241
- switch, 477–478
 - Layer 3, 478
 - Layer 4, 478
- symmetric algorithm, 321–322, 325
 - 3DES, 329
 - AES (Advanced Encryption Standard), 329–330
 - Blowfish, 330
 - CAST, 331–332
 - DES (Digital Encryption Standard), 325–329
 - IDEA (International Data Encryption Algorithm), 330
 - RC, 331
 - Skipjack, 330
 - Twofish, 331
- SYN ACK attack, 544
- synchronous transmission, 414
- synthetic transaction monitoring, 650
- syslog, 647
- system administrator, 20
- system high security mode, 233
- system/s, 223–224. *See also* computer/
 - computing; information systems; operating system
- access control, 565–566
- accreditation, 267–268
- architecture, 241–242
 - access control services, 245
 - auditing and monitoring services, 245–246
 - boundary control services, 245
 - computing platforms, 242–245. *See also* computing platforms
 - cryptography services, 245
 - integrity services, 245
- biometric, 579–580, 581–583
- certification, 267–268
- client-based, vulnerabilities, 273–274
- closed, 225
- cryptographic
 - features, 311
 - NIST guidelines, 312–313
 - vulnerabilities, 276–277
- custodian, 196
- database, vulnerabilities, 275–276
- edge computing, 296
- embedded, 243, 304
- engineering, 223–224
- hardening, 728
- High Performance Computing, 295
- ICS (Industrial Control Systems), 277–281
- image, 676–677
- integrity, 7
- large-scale parallel data, 287–288
- multistate/single-state, 248
- open, 225
- owner, 20, 195
- redundant, 744
- resilience, 746
- secure design principles. *See also* secure design principles
 - closed versus open systems, 225
 - defense-in-depth, 226

- fail securely, 227
 - least privilege, 225–226
 - objects and subjects, 225
 - secure defaults, 226–227
 - threat modeling, 225
 - server-based, vulnerabilities, 275
 - serverless, 294–295
 - specific security policy, 75
 - threats, 135, 136
 - virtualized, 296
- T**
- T lines, 510–511
 - tabletop exercise, 752
 - TACACS+ (Terminal Access Controller Access-Control System Plus), 528–529, 601
 - tagging attack, 536
 - Take-Grant model, 236
 - tangible assets, 96
 - facilities, 707–708
 - hardware, 708
 - software, 708–709
 - target test, 644
 - TCB (trusted computer base), 814–815
 - TCP (Transmission Control Protocol), 398–399, 400
 - common port numbers, 403–405
 - three-way handshake, 399–400
 - TCP/IP model, 397
 - Application layer, 397–398
 - Internet layer, 400–402
 - Link layer, 402
 - Transport layer, 398–400
 - TDM (time-division multiplexing), 415
 - TDMA (time-division multiple access), 449
 - team
 - damage assessment, 748
 - incident response, 720
 - integrated product, 804–806
 - legal, 748
 - media relations, 748
 - recovery, 749
 - restoration, 749
 - salvage, 749
 - security, 749
 - teardrop attack, 545
 - technological disaster, 78
 - telco concentrator, 476
 - telecommuting/telework, 531
 - Telnet, 530
 - tertiary site, 742
 - test/ing
 - acceptance, 789, 817
 - code, 651–653
 - coverage analysis, 654
 - disaster recovery plans, 751–754
 - dynamic application security, 790–791
 - fuzz, 653
 - integration, 789
 - interface, 654
 - misuse case, 653–654
 - penetration, 637–638, 643–645
 - regression, 789, 817
 - security, 636–637
 - static application security, 790
 - unit, 788
 - validation, 788
 - verification, 788
 - TFTP (Trivial FTP), 439
 - theft, 139
 - thicknet, 497
 - thinnet, 497
 - third-party
 - assessment and monitoring, 150–151
 - connectivity, 451–452
 - identity services, 602
 - security services, 725
 - thread, 254
 - threat/s, 5, 97. *See also* malware
 - access control. *See* access control, threats
 - advanced persistent, 624

- agent, 97
- database, 192–193
- employee, 16
- human-caused, 137
 - collusion, 139–140
 - explosions, 137–138
 - fire, 138–139
 - fraud, 139
 - theft, 139
 - vandalism, 139
- hunting, 697
- identifying, 101–102, 146–147
- intelligence, 697
- internal versus external, 134
- IPv6, 423
- modeling, 142–143, 225
 - methodology comparison, 145
 - PASTA methodology, 144
 - STRIDE model, 143–144
 - Trike methodology, 144
 - VAST model, 144–145
- natural, 134–135
- politically motivated, 140–141
- system, 135
 - communications, 136–137
 - electrical, 136
 - utilities, 137
- three-legged firewall, 484
- three-way handshake, TCP (Transmission Control Protocol), 399–400
- throughput, 503–504, 581
- Tiger, 351
- time factor authentication, 584
- time-of-check/time-of-use attack, 297–298
- timing attack, 360
- TLS (Transport Layer Security), 442, 530–531
- ToE (Target of Evaluation), 262–263
- TOGAF (The Open Group Architecture Framework), 26
- token device, 577
- token passing, 510
- Token Ring, 505–506
- tools
 - final preparation, exam, 835–837
 - machine learning and AI, 728
 - network discovery, 641
 - rootkit, 812
 - SCA (software composition analysis), 791–792
 - SIEM (security information and event management), 693
 - source code analysis, 808
 - tuning, 694–695
- topology, network
 - bus topology, 501
 - discovery, 640–641
 - hybrid, 503
 - mesh, 502
 - ring, 500
 - star, 502
- tort law, 46–47
- TPM (Trusted Platform Module), 270
- traceroute, exploitation, 538
- trade secret, 48–49
- trademark, 49
- traffic shaping, 473–474
- training
 - disaster recovery, 750–751
 - investigator, 689
 - personnel, 738
 - security awareness, 16, 153–155
- transaction log backup, 737
- trans-border data flow, 53
- transmission
 - analog signal, 413
 - asynchronous, 414
 - baseband, 415
 - broadband, 415
 - broadcast, 416
 - cabling, noise, 495–496
 - digital signal, 413–414
 - multicast, 416

- satellite, 454
- synchronous, 414
- unicast, 416
- wired, 416
- wireless, 416–417
- Transport layer
 - OSI (Open Systems Interconnection)
 - model, 394
 - TCP/IP model, 398–400
- transposition cipher, 320–321
- trapdoor, 624, 821–822
- Trike methodology, 144
- Trojan horse, 811
- trust but verify, 229
- trusted path, 727
- trusted recovery, 727
- TSCEC (Trusted Computer System
 - Evaluation Criteria), 256, 260–261
- TT&E (testing, training, and
 - exercises), 85
- tuning, 694–695
- turnstiles and mantraps, 368–369
- twisted pair cable, 498–499
- Twofish, 331
- two-person control, 705
- Type I error, 582
- Type II error, 582

U

- UDP (User Datagram Protocol), 398–400, 403–405
- UEBA (user and entity behavior analytics), 697
- UEFI (Unified Extensible Firmware Interface), 253–254
- unauthorized disclosure, 727
- unicast, 416, 428
- unit test, 788
- United States
 - Digital Millenium Copyright Act (DMCA, 1998), 51

- Health Insurance Portability and Accountability Act (HIPAA), 55
- Sarbanes-Oxley Act (SOX, 2002), 55
- unscheduled reboot, 727
- unusual or unexplained events, 726
- UPS (uninterruptible power supply), 136
- URL hiding, 540
- US Federal Sentencing Guidelines of 1991, 57
- USA Freedom Act of 2015, 61
- USA PATRIOT Act of 2001, 60–61
- user, 21
 - behavior analytics, 697
 - environment recovery, 734–735
 - orientation, 93
 - principle of least privilege, 225–226
 - provisioning, 93
- UTM (unified threat management), 482–483
- UTP (unshielded twisted pair), 498

V

- validation testing, 788
- vandalism, 139
- vascular scan, 580
- VAST (Visual, Agile, and Simple Threat)
 - model, 144–145
- vendor, compliance policy requirements, 94. *See also* employee
- verification testing, 788
- vertical privilege escalation, 616
- very-high level languages, 774–775
- vetting process, app, 780–782
- video game DRM, 362
- Vigenere cipher, 308–309
- virtual application/desktop, 531
- virtual assets, 701
- virtual computing, 244
- virtualized systems, 296
- virus, 809–810
- visibility, 365

- visitor control, 371
- VLAN (virtual local-area network), 479
- VM (virtual machine), 244
- voice communication, 520
- voice pattern, authentication, 581
- VoIP (Voice over Internet Protocol), 447, 515
- VPC (virtual private cloud), 533–534
- VPN (virtual private network), 525–528
 - concentrator, 476
 - screen scraper, 531
- VRRP (Virtual Router Redundancy Protocol), 494–495
- VSAN (virtual storage-area network), 534
- V-shaped model, 795
- vulnerability/ies, 96
 - assessment, 639–640
 - client-based systems, 273–274
 - database systems, 275–276
 - embedded system, 304
 - identifying, 101–102
 - management, 729
 - management system, 728
 - mobile system, 299–300
- scan
 - network, 642–643
 - web application, 643
- server-based system, 275
- web-based system
 - maintenance hooks, 297
 - time-of-check/time-of-use attack, 297–298

W

- walls, 756
- WAN (wide area network), 433–434
 - ATM (Asynchronous Transfer Mode), 513
 - circuit switching versus packet switching, 512–513
- CSU/DSU, 512

- E lines, 511
- Frame Relay, 513
- HSSI (High-Speed Serial Interface), 514
- PPP (Point-to-Point Protocol), 514
- PSTN (public switched telephone network), 514–515
- SMDS (Switched Multimegabit Data Service), 514
- SONET (Synchronous Optical Networking), 512
- T lines, 510–511
- X.25, 513
- warchalking, 543
- wardriving, 543
- warm site, 741
- warrant, 681
- WASC (Web Application Security Consortium), 806
- water leakage and flooding, 376–377
- Waterfall model, 794
- WAVE (wireless access in vehicle environments), 451
- wave motion detector, 757
- web application vulnerability scan, 643
- web caching, 484
- web-based system, vulnerabilities
 - maintenance hooks, 297
 - time-of-check/time-of-use attack, 297–298
- WEP (Wired Equivalent Privacy), 463
- whaling, 542, 620
- white hat, 44
- white-box testing, 652, 790
- whitelisting, 725
- Windows, SAM (Security Accounts Manager), 577
- WIPO (World Intellectual Property Organization), 50
- wireless networks and communication, 416–417, 448. *See also* mobile communication
- 5G, 450

- CUPS (Control and User Plane Separation), 450–451
- D2D (device-to-device communication), 451
- MEC (multi-access Edge Computing), 450–451
- voice over, 451
- 0802.11 standards, 458–461
- ad hoc mode, 458
- antenna placement and signal power levels, 467–468
- AP (access point), 457–458
- Bluetooth, 461
- CDMA (code-division multiple access), 449
- DSSS (direct-sequence spread spectrum), 449
- FDMA (frequency-division multiple access), 449
- FHSS (frequency hopping spread spectrum), 448
- hardware support, 456–457
- infrared, 462
- infrastructure mode, 458
- NFC (Near Field Communication), 462
- OFDM (orthogonal frequency-division multiplexing), 449
- OFDMA (orthogonal frequency-division multiple access), 449
- security
 - 0802.1X, 464–466
 - MAC filter, 466
 - Open System Authentication, 462
 - Shared Key Authentication, 463
 - WEP (Wired Equivalent Privacy), 463

- WPA (Wi-Fi Protected Access), 463
- WPA2, 463–464
- WPA3, 464
- site survey, 467
- SSID (Service Set Identifier), 458
- TDMA (time-division multiple access), 449
- third-party connectivity, 451–452
- VOFDM (vectored orthogonal frequency-division multiplexing), 449
- Zigbee, 462
- WLAN (wireless local-area network), 434
- World Wide Web, 470
- worm, 810
- WPA (Wi-Fi Protected Access), 463
- WPA2, 463–464
- WPA3, 464
- WRT (work recovery time), 87

X

- X.25, 513
- X.400, 593
- X.500, 593
- X.509, 335
- XML (eXtensible Markup Language), 191, 298

Y-Z

- Zachman Framework, 26
- Zephyr chart, 582
- zero trust, 228
- zero-day exploit, 545
- zero-knowledge proof, 335
- zero-knowledge test, 644–645
- Zigbee, 462