Cert Guide
Learn, prepare, and practice for exam success

CISSP
Third Edition

PEARSON IT CERTIFICATION

FREE SAMPLE CHAPTER
SHARE WITH OTHERS
### Contents at a Glance

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>xlv</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 1</td>
<td>Security and Risk Management</td>
<td>2</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td>Asset Security</td>
<td>140</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td>Security Architecture and Engineering</td>
<td>178</td>
</tr>
<tr>
<td>CHAPTER 4</td>
<td>Communication and Network Security</td>
<td>334</td>
</tr>
<tr>
<td>CHAPTER 5</td>
<td>Identity and Access Management (IAM)</td>
<td>474</td>
</tr>
<tr>
<td>CHAPTER 6</td>
<td>Security Assessment and Testing</td>
<td>532</td>
</tr>
<tr>
<td>CHAPTER 7</td>
<td>Security Operations</td>
<td>564</td>
</tr>
<tr>
<td>CHAPTER 8</td>
<td>Software Development Security</td>
<td>658</td>
</tr>
<tr>
<td>CHAPTER 9</td>
<td>Final Preparation</td>
<td>712</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td>721</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>782</td>
</tr>
</tbody>
</table>

### Online Elements

<table>
<thead>
<tr>
<th>Appendix A</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPENDIX A</td>
<td>Memory Tables</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix B</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPENDIX B</td>
<td>Memory Tables Answer Key</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
</tr>
</tbody>
</table>
# Table of Contents

## Introduction  xlv

## Chapter 1  Security and Risk Management  

*Foundation Topics  5*

*Security Terms  5*

*CIA  5*

*Confidentiality  5*

*Integrity  6*

*Availability  6*

*Auditing and Accounting  6*

*Non-Repudiation  7*

*Default Security Posture  7*

*Defense in Depth  7*

*Abstraction  8*

*Data Hiding  8*

*Encryption  8*

*Security Governance Principles  8*

*Security Function Alignment  9*

*Organizational Strategies and Goals  10*

*Organizational Mission and Objectives  10*

*Business Case  10*

*Security Budget, Metrics, and Effectiveness  11*

*Resources  11*

*Organizational Processes  12*

*Acquisitions and Divestitures  12*

*Governance Committees  14*

*Organizational Roles and Responsibilities  14*

*Board of Directors  14*

*Management  14*

*Audit Committee  15*

*Data Owner  16*

*Data Custodian  16*

*System Owner  16*
System Administrator 16
Security Administrator 16
Security Analyst 17
Application Owner 17
Supervisor 17
User 17
Auditor 17
Security Control Frameworks 17
ISO/IEC 27000 Series 18
Zachman Framework 21
The Open Group Architecture Framework (TOGAF) 22
Department of Defense Architecture Framework (DoDAF) 22
British Ministry of Defence Architecture Framework (MODAF) 22
Sherwood Applied Business Security Architecture (SABSA) 22
Control Objectives for Information and Related Technology (COBIT) 23
National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series 24
HITRUST CSF 26
CIS Critical Security Controls 27
Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework 28
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) 28
Information Technology Infrastructure Library (ITIL) 28
Six Sigma 29
Capability Maturity Model Integration (CMMI) 31
CCTA Risk Analysis and Management Method (CRAMM) 31
Top-Down Versus Bottom-Up Approach 31
Security Program Life Cycle 31
Due Care and Due Diligence 32
Compliance 33
Contractual, Legal, Industry Standards, and Regulatory Compliance 34
Privacy Requirements Compliance 35
Legal and Regulatory Issues 35
Computer Crime Concepts 36
Computer-Assisted Crime 36
Computer-Targeted Crime 36
Incidental Computer Crime 36
Computer Prevalence Crime 36
Hackers Versus Crackers 37
Computer Crime Examples 37
Major Legal Systems 38
Civil Code Law 38
Common Law 38
Criminal Law 39
Civil/Tort Law 39
Administrative/Regulatory Law 39
Customary Law 39
Religious Law 40
Mixed Law 40
Licensing and Intellectual Property 40
Patent 40
Trade Secret 41
Trademark 41
Copyright 42
Software Piracy and Licensing Issues 43
Internal Protection 43
Digital Rights Managements (DRM) 43
Cyber Crimes and Data Breaches 44
Import/Export Controls 45
Trans-Border Data Flow 45
Privacy 45
Personally Identifiable Information (PII) 46
Laws and Regulations 47
Professional Ethics 52
(ISC)^2 Code of Ethics 52
Computer Ethics Institute 53
Internet Architecture Board 54
Organizational Code of Ethics 54
Security Documentation 54

Policies 55

Organizational Security Policy 56
System-Specific Security Policy 57
Issue-Specific Security Policy 57

Policy Categories 57
Processes 57
Procedures 57
Standards 57
Guidelines 58
Baselines 58

Business Continuity 58

Business Continuity and Disaster Recovery Concepts 58
Disruptions 59
Disasters 59
Disaster Recovery and the Disaster Recovery Plan (DRP) 60
Continuity Planning and the Business Continuity Plan (BCP) 60
Business Impact Analysis (BLA) 61
Contingency Plan 61
Availability 61
Reliability 61
Scope and Plan 61
Personnel Components 62
Scope 62
Business Contingency Planning 62
BIA Development 65
Identify Critical Processes and Resources 66
Identify Outage Impacts, and Estimate Downtime 66
Identify Resource Requirements 67
Identify Recovery Priorities 68

Personnel Security Policies and Procedures 68
Candidate Screening and Hiring 69
Employment Agreements and Policies 70
Employee Onboarding and Offboarding Policies 71
Vendor, Consultant, and Contractor Agreements and Controls  72
Compliance Policy Requirements  72
Privacy Policy Requirements  72
Job Rotation  73
Separation of Duties  73
Risk Management Concepts  73
Asset and Asset Valuation  73
Vulnerability  74
Threat  74
Threat Agent  74
Exploit  75
Risk  75
Exposure  75
Countermeasure  75
Risk Appetite  76
Attack  76
Breach  76
Risk Management Policy  77
Risk Management Team  77
Risk Analysis Team  77
Risk Assessment  78
Information and Asset (Tangible/Intangible) Value and Costs  78
Identity Threats and Vulnerabilities  79
Risk Assessment/Analysis  79
Countermeasure (Safeguard) Selection  81
Inherent Risk Versus Residual Risk  82
Handling Risk and Risk Response  82
Implementation  82
Control Categories  83
Compensative  83
Corrective  83
Detective  84
Deterrent  84
Directive  84
Preventive 84
Recovery 84
Control Types 84
Administrative (Management) 85
Logical (Technical) 86
Physical 87
Controls Assessment, Monitoring, and Measurement 89
Reporting and Continuous Improvement 89
Risk Frameworks 90
NIST 90
ISO/IEC 27005:2011 105
Open Source Security Testing Methodology Manual (OSSTMM) 106
COSO’s Enterprise Risk Management (ERM) Integrated Framework 107
A Risk Management Standard by the Federation of European Risk Management Associations (FERMA) 107
Geographical Threats 108
Internal Versus External Threats 108
Natural Threats 109
Hurricanes/Tropical Storms 109
Tornadoes 109
Earthquakes 109
Floods 110
Volcanoes 110
System Threats 110
Electrical 110
Communications 110
Utilities 111
Human-Caused Threats 111
Explosions 112
Fire 112
Vandalism 113
Fraud 113
Theft 113
Collusion 113
Politically Motivated Threats 114

*Strikes* 114

*Riots* 114

*Civil Disobedience* 114

*Terrorist Acts* 114

*Bombing* 115

**Threat Modeling** 115

Threat Modeling Concepts 116

Threat Modeling Methodologies 116

*STRIDE Model* 117

*Process for Attack Simulation and Threat Analysis (PASTA)* Methodology 117

*Trike Methodology* 117

*Visual, Agile, and Simple Threat (VAST) Model* 118

*NIST SP 800-154* 118

Identifying Threats 119

Potential Attacks 120

Remediation Technologies and Processes 121

**Security Risks in the Supply Chain** 121

Risks Associated with Hardware, Software, and Services 121

Third-party Assessment and Monitoring 122

*Onsite Assessment* 122

*Document Exchange/Review* 122

*Process/Policy Review* 122

*Other Third-Party Governance Issues* 123

Minimum Service-Level and Security Requirements 123

Service-Level Requirements 123

**Security Education, Training, and Awareness** 124

Levels Required 124

Methods and Techniques 125

Periodic Content Reviews 126

**Exam Preparation Tasks** 126

Review All Key Topics 126

Complete the Tables and Lists from Memory 127
Define Key Terms 128
Answer Review Questions 129
Answers and Explanations 134

Chapter 2  Asset Security 140

Foundation Topics 141
Asset Security Concepts 141
  Data Policy 141
  Roles and Responsibilities 143
  Data Owner 143
  Data Custodian 143
  Data Quality 144
  Data Documentation and Organization 145
Identify and Classify Information and Assets 146
  Data and Asset Classification 146
  Sensitivity and Criticality 146
  PII 147
  PHI 149
  Proprietary Data 151
Private Sector Classifications 151
Military and Government Classifications 152
Information Life Cycle 153
Databases 155
DBMS Architecture and Models 155
Database Interface Languages 157
Data Warehouses and Data Mining 157
Database Maintenance 158
Database Threats 158
Database Views 159
Database Locks 159
Polyinstantiation 159
OLTP ACID Test 159
Data Audit 160
Information and Asset Ownership 160
Protect Privacy 161
### Contents

- Objects and Subjects 181
- Closed Versus Open Systems 182

#### Security Model Concepts 182
- Confidentiality, Integrity, and Availability 182
- Confinement 183
- Bounds 183
- Isolation 183
- Security Modes 183
  - Dedicated Security Mode 184
  - System High Security Mode 184
  - Compartmented Security Mode 184
  - Multilevel Security Mode 184
  - Assurance and Trust 185
  - Defense in Depth 185
- Security Model Types 185
  - State Machine Models 185
  - Multilevel Lattice Models 186
  - Matrix-Based Models 186
  - Non-Interference Models 186
  - Information Flow Models 187
  - Take-Grant Model 187
  - Security Models 188
- Bell-LaPadula Model 189
- Biba Model 190
- Clark-Wilson Integrity Model 190
- Lipner Model 191
- Brewer-Nash (Chinese Wall) Model 192
- Graham-Denning Model 192
- Harrison-Ruzzo-Ullman Model 192
- Goguen-Meseguer Model 192
- Sutherland Model 192

#### System Architecture Steps 192
- ISO/IEC 42010:2011 193
- Computing Platforms 193
Mainframe/Thin Clients  194
Distributed Systems  194
Middleware  194
Embedded Systems  195
Mobile Computing  195
Virtual Computing  195
Security Services  196
Boundary Control Services  196
Access Control Services  196
Integrity Services  196
Cryptography Services  196
Auditing and Monitoring Services  196
System Components  196
CPU  197
Memory and Storage  199
Input/Output Devices  202
Input/Output Structures  202
Firmware  203
Operating Systems  204
Memory Management  205

System Security Evaluation Models  205
TCSEC  206
Rainbow Series  206
ITSEC  209
Common Criteria  211
Security Implementation Standards  213
ISO/IEC 27001  214
ISO/IEC 27002  215
Payment Card Industry Data Security Standard (PCI DSS)  216
Controls and Countermeasures  217
Certification and Accreditation  217
Control Selection Based upon Systems Security Requirements  218
Security Capabilities of Information Systems  219
Memory Protection  219
Virtualization 220
Trusted Platform Module 220
Interfaces 221
Fault Tolerance 221
Policy Mechanisms 222
Principle of Least Privilege 222
Separation of Privilege 222
Accountability 223
Encryption/Decryption 223
Security Architecture Maintenance 223
Vulnerabilities of Security Architectures, Designs, and Solution Elements 224
Client-Based Systems 224
Server-Based Systems 225
Data Flow Control 225
Database Systems 226
Inference 226
Aggregation 226
Contamination 226
Data Mining Warehouse 226
Cryptographic Systems 227
Industrial Control Systems 227
Cloud-Based Systems 230
Large-Scale Parallel Data Systems 236
Distributed Systems 237
Grid Computing 237
Peer-to-Peer Computing 237
Internet of Things 238
IoT Examples 239
Methods of Securing IoT Devices 239
NIST Framework for Cyber-Physical Systems 240
Vulnerabilities in Web-Based Systems 242
Maintenance Hooks 242
Time-of-Check/Time-of-Use Attacks 243
Web-Based Attacks 243
XML 244
SAML 244
OWASP 244
Vulnerabilities in Mobile Systems 244
  Device Security 245
  Application Security 246
  Mobile Device Concerns 246
  NIST SP 800-164 248
Vulnerabilities in Embedded Devices 250
Cryptography 250
  Cryptography Concepts 250
  Cryptography History 253
  Julius Caesar and the Caesar Cipher 253
  Vigenere Cipher 254
  Kerckhoff’s Principle 255
  World War II Enigma 255
  Lucifer by IBM 256
  Cryptosystem Features 256
  Authentication 256
  Confidentiality 257
  Integrity 257
  Authorization 257
  Non-Repudiation 257
  NIST SP 800-175A and B 257
  Cryptographic Mathematics 258
Boolean 258
  Logical Operations (And, Or, Not, Exclusive Or) 259
Modulo Function 260
One-Way Function 260
Nonce 260
Split Knowledge 260
Cryptographic Life Cycle 261
Key Management 261
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm Selection</td>
</tr>
<tr>
<td>Cryptographic Types</td>
</tr>
<tr>
<td>Running Key and Concealment Ciphers</td>
</tr>
<tr>
<td>Substitution Ciphers</td>
</tr>
<tr>
<td>One-Time Pads</td>
</tr>
<tr>
<td>Steganography</td>
</tr>
<tr>
<td>Transposition Ciphers</td>
</tr>
<tr>
<td>Symmetric Algorithms</td>
</tr>
<tr>
<td>Stream-Based Ciphers</td>
</tr>
<tr>
<td>Block Ciphers</td>
</tr>
<tr>
<td>Initialization Vectors (IVs)</td>
</tr>
<tr>
<td>Asymmetric Algorithms</td>
</tr>
<tr>
<td>Hybrid Ciphers</td>
</tr>
<tr>
<td>Symmetric Algorithms</td>
</tr>
<tr>
<td>DES and 3DES</td>
</tr>
<tr>
<td>DES Modes</td>
</tr>
<tr>
<td>3DES and Modes</td>
</tr>
<tr>
<td>AES</td>
</tr>
<tr>
<td>IDEA</td>
</tr>
<tr>
<td>Skipjack</td>
</tr>
<tr>
<td>Blowfish</td>
</tr>
<tr>
<td>Twofish</td>
</tr>
<tr>
<td>RC4/RC5/RC6/RC7</td>
</tr>
<tr>
<td>CAST</td>
</tr>
<tr>
<td>Asymmetric Algorithms</td>
</tr>
<tr>
<td>Diffie-Hellman</td>
</tr>
<tr>
<td>RSA</td>
</tr>
<tr>
<td>El Gamal</td>
</tr>
<tr>
<td>ECC</td>
</tr>
<tr>
<td>Knapsack</td>
</tr>
<tr>
<td>Zero-knowledge Proof</td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>Certification Authority and Registration Authority</td>
</tr>
<tr>
<td>Certificates</td>
</tr>
</tbody>
</table>
Certificate Life Cycle 281
Enrollment 282
Verification 282
Revocation 283
Renewal and Modification 283
Certificate Revocation List 283
OCSP 284
PKI Steps 284
Cross-Certification 285
Key Management Practices 285
Message Integrity 293
Hashing 294
One-Way Hash 294
MD2/MD4/MD5/MD6 296
SHA/SHA-2/SHA-3 296
HAVAL 297
RIPEMD-160 297
Tiger 297
Message Authentication Code 297
HMAC 298
CBC-MAC 298
CMAC 299
Salting 299
Digital Signatures 299
DSS 300
Applied Cryptography 300
Link Encryption Versus End-to-End Encryption 300
Email Security 300
Internet Security 300
Cryptanalytic Attacks 301
Ciphertext-Only Attack 302
Known Plaintext Attack 302
Chosen Plaintext Attack 302
Chosen Ciphertext Attack 302
Social Engineering 302
Brute Force 302
Differential Cryptanalysis 303
Linear Cryptanalysis 303
Algebraic Attack 303
Frequency Analysis 303
Birthday Attack 303
Dictionary Attack 303
Replay Attack 304
Analytic Attack 304
Statistical Attack 304
Factoring Attack 304
Reverse Engineering 304
Meet-in-the-Middle Attack 304
Ransomware Attack 304
Side-Channel Attack 305
Digital Rights Management 305
  Document DRM 306
  Music DRM 306
  Movie DRM 306
  Video Game DRM 306
  E-book DRM 307
Site and Facility Design 307
  Layered Defense Model 307
  CPTED 307
  Natural Access Control 308
  Natural Surveillance 308
  Natural Territories Reinforcement 308
  Physical Security Plan 308
  Deter Criminal Activity 308
  Delay Intruders 309
  Detect Intruders 309
  Assess Situation 309
  Respond to Intrusions and Disruptions 309
Facility Selection Issues 309
Visibility 309
Surrounding Area and External Entities 310
Accessibility 310
Construction 310
Internal Compartments 311
Computer and Equipment Rooms 311

Site and Facility Security Controls 312
Doors 312
Door Lock Types 312
Turnstiles and Mantraps 313
Locks 313
Biometrics 315
Glass Entries 315
Visitor Control 315
Wiring Closets/Intermediate Distribution Facilities 316
Work Areas 316
Secure Data Center 316
Restricted Work Area 316
Server Room 316
Media Storage Facilities 317
Evidence Storage 317
Environmental Security 317
Fire Protection 317
Power Supply 319
HVAC 320
Water Leakage and Flooding 320
Environmental Alarms 321
Equipment Security 321
Corporate Procedures 321
Safes, Vaults, and Locking 322

Exam Preparation Tasks 323
Review All Key Topics 323
Complete the Tables and Lists from Memory 325
Define Key Terms 325
Answer Review Questions 326
Answers and Explanations 331

Chapter 4 Communication and Network Security 334

Foundation Topics 335
Secure Network Design Principles 335
OSI Model 335
  Application Layer 336
  Presentation Layer 337
  Session Layer 337
  Transport Layer 337
  Network Layer 338
  Data Link Layer 338
  Physical Layer 338
TCP/IP Model 340
  Application Layer 340
  Transport Layer 341
  Internet Layer 343
  Link Layer 344
  Encapsulation and De-encapsulation 345
IP Networking 345
  Common TCP/UDP Ports 346
  Logical and Physical Addressing 347
IPv4 348
  IP Classes 349
  Public Versus Private IP Addresses 350
NAT 351
  MAC Addressing 352
Network Transmission 353
  Analog Versus Digital 353
  Asynchronous Versus Synchronous 354
  Broadband Versus Baseband 355
Unicast, Multicast, and Broadcast 355
  Wired Versus Wireless 356
IPv6 357
NIST SP 800-119 358
IPv6 Major Features 360
IPv4 Versus IPv6 Threat Comparison 362
IPv6 Addressing 363
Shorthand for Writing IPv6 Addresses 366
IPv6 Address Types 367
IPv6 Address Scope 368
Network Types 370
LAN 370
Intranet 370
Extranet 370
MAN 370
WAN 371
WLAN 371
SAN 371
CAN 371
PAN 372
Protocols and Services 372
ARP/RARP 372
DHCP/BOOTP 373
DNS 374
FTP, FTPS, SFTP, TFTP 374
HTTP, HTTPS, S-HTTP 375
ICMP 375
IGMP 376
IMAP 376
LDAP 376
LDP 376
NAT 376
NetBIOS 376
NFS 377
PAT 377
POP 377
Contents

CIFS/SMB 377
SMTP 377
SNMP 377
SSL/TLS 378
Multilayer Protocols 378

Converged Protocols 379
FCoE 379
MPLS 380
VoIP 381
iSCSI 381

Wireless Networks 381
FHSS, DSSS, OFDM, VOFDM, FDMA, TDMA, CDMA, OFDMA, and GSM 382
802.11 Techniques 382
Cellular or Mobile Wireless Techniques 383
Satellites 383
WLAN Structure 384
Access Point 384
SSID 384
Infrastructure Mode Versus Ad Hoc Mode 384

WLAN Standards 384
802.11 385
802.11a 385
802.11ac 385
802.11b 385
802.11g 385
802.11n 386
Bluetooth 386
Infrared 386
Near Field Communication (NFC) 386
Zigbee 387

WLAN Security 387
Open System Authentication 387
Shared Key Authentication 387
Network Access Control Devices 435
Quarantine/Remediation 436
Firewalls/Proxies 436
Endpoint Security 437
Content-Distribution Networks 438
Secure Communication Channels 438
Voice 439
Multimedia Collaboration 439
Remote Meeting Technology 440
Instant Messaging 440
Remote Access 440
Remote Connection Technologies 440
VPN Screen Scraper 449
Virtual Application/Desktop 449
Telecommuting 450
Data Communications 450
Virtualized Networks 450
SDN 450
Virtual SAN 451
Guest Operating Systems 451
Network Attacks 451
Cabling 451
Noise 452
Attenuation 452
Crosstalk 452
Eavesdropping 452
Network Component Attacks 453
Non-Blind Spoofing 453
Blind Spoofing 453
Man-in-the-Middle Attack 453
MAC Flooding Attack 454
802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack 454
Double-Encapsulated 802.1Q/Nested VLAN Attack 454
ARP Attack 454
ICMP Attacks 454
Ping of Death 455
Smurf 455
Fraggle 455
ICMP Redirect 455
Ping Scanning 456
Traceroute Exploitation 456
DNS Attacks 456
DNS Cache Poisoning 456
DoS 457
DDoS 457
DNSSEC 457
URL Hiding 458
Domain Grabbing 458
Cybersquatting 458
Email Attacks 458
Email Spoofing 458
Spear Phishing 459
Whaling 459
Spam 459
Wireless Attacks 459
Wardriving 460
Warchalking 460
Remote Attacks 460
Other Attacks 460
SYN ACK Attacks 460
Session Hijacking 461
Port Scanning 461
Teardrop 461
IP Address Spoofing 461
Zero-Day 462
Ransomware 462
Exam Preparation Tasks 462
Review All Key Topics 462
Chapter 5  Identity and Access Management (IAM)  474

Foundation Topics  475
Access Control Process  475
  Identify Resources  475
  Identify Users  476
  Identify the Relationships Between Resources and Users  476
Physical and Logical Access to Assets  477
  Access Control Administration  477
  Centralized  478
  Decentralized  478
  Information  478
  Systems  478
  Devices  479
  Facilities  479
Identification and Authentication Concepts  480
  NIST SP 800-63  480
  Five Factors for Authentication  484
    Knowledge Factors  485
    Ownership Factors  488
    Characteristic Factors  489
    Location Factors  494
    Time Factors  495
  Single-Factor Versus Multi-Factor Authentication  495
  Device Authentication  495
Identification and Authentication Implementation  496
  Separation of Duties  496
  Least Privilege/Need-to-Know  497
  Default to No Access  497
  Directory Services  498
  Single Sign-on  498
  Kerberos  499
SESAME  501
Federated Identity Management  502
Security Domains  502
Session Management  503
Registration and Proof of Identity  503
Credential Management Systems  504
Accountability  505
Auditing and Reporting  505
Identity as a Service (IDaaS) Implementation  507
Third-Party Identity Services Integration  507
Authorization Mechanisms  508
  Permissions, Rights, and Privileges  508
  Access Control Models  508
  Discretionary Access Control  509
  Mandatory Access Control  509
  Role-Based Access Control  510
  Rule-Based Access Control  510
  Attribute-Based Access Control  510
  Content-Dependent Versus Context-Dependent  513
    Access Control Matrix  513
  Access Control Policies  514
Provisioning Life Cycle  514
  Provisioning  515
  User and System Account Access Review  516
  Account Revocation  516
Access Control Threats  516
  Password Threats  517
    Dictionary Attack  517
    Brute-Force Attack  517
    Birthday Attack  518
    Rainbow Table Attack  518
    Sniffer Attack  518
  Social Engineering Threats  518
    Phishing/Pharming  518
Chapter 6  Security Assessment and Testing  532

Foundation Topics  533
Design and Validate Assessment and Testing Strategies  533
  Security Testing  534
  Security Assessments  534
  Security Auditing  535
  Internal, External, and Third-party Security Assessment, Testing, and Auditing  535
Conduct Security Control Testing  535
  Vulnerability Assessment  535
  Network Discovery Scan  536
  Network Vulnerability Scan  538
  Web Application Vulnerability Scan  539
  Penetration Testing  539
  Log Reviews  541
Chapter 7  Security Operations  564

Foundation Topics  566
Investigations  566

Forensic and Digital Investigations  566
Identification Evidence  568
Preserve and Collect Evidence  568
Examine and Analyze Evidence  569
Present Findings  569
Decide  570
Forensic Procedures 570
Reporting and Documentation 570
IOCE/SWGDE and NIST 571
Crime Scene 572
MOM 572
Chain of Custody 573
Interviewing 573
Investigative Techniques 573
Evidence Collection and Handling 574
Five Rules of Evidence 574
Types of Evidence 575
Surveillance, Search, and Seizure 576
Media Analysis 577
Software Analysis 578
Network Analysis 578
Hardware/Embedded Device Analysis 578
Digital Forensic Tools, Tactics, and Procedures 579
Investigation Types 581
Operations/Administrative 581
Criminal 582
Civil 582
Regulatory 582
Industry Standards 582
eDiscovery 585
Logging and Monitoring Activities 585
Audit and Review 585
Log Types 586
Audit Types 587
Intrusion Detection and Prevention 587
Security Information and Event Management (SIEM) 588
Continuous Monitoring 588
Egress Monitoring 588
Resource Provisioning 589
Asset Inventory and Management 590
Physical Assets  591
Virtual Assets  591
Cloud Assets  591
Applications  591
Configuration Management  592

Security Operations Concepts  593
Need to Know/Least Privilege  593
Managing Accounts, Groups, and Roles  594
Separation of Duties and Responsibilities  594
Privilege Account Management  595
Job Rotation and Mandatory Vacation  595
Two-Person Control  596
Sensitive Information Procedures  596
Record Retention  596
Information Life Cycle  596
Service-Level Agreements  597

Resource Protection  597
Protecting Tangible and Intangible Assets  597

Facilities  598
Hardware  598
Software  599
Information Assets  599
Asset Management  599
Redundancy and Fault Tolerance  600
Backup and Recovery Systems  600
Identity and Access Management  600
Media Management  601
Media History  606
Media Labeling and Storage  606
Sanitizing and Disposing of Media  606
Network and Resource Management  607

Incident Management  608
Event Versus Incident  608
Incident Response Team and Incident Investigations  609
Contents

Rules of Engagement, Authorization, and Scope  609
Incident Response Procedures  610
Incident Response Management  610
Detect  610
Respond  611
Mitigate  611
Report  611
Recover  612
Remediate  612
Lessons Learned and Review  612
Detective and Preventive Measures  612
IDS/IPS  612
Firewalls  613
Whitelisting/Blacklisting  613
Third-Party Security Services  613
Sandboxing  614
Honeypots/Honeynets  614
Anti-malware/Antivirus  614
Clipping Levels  614
Deviations from Standards  615
Unusual or Unexplained Events  615
Unscheduled Reboots  615
Unauthorized Disclosure  615
Trusted Recovery  615
Trusted Paths  616
Input/Output Controls  616
System Hardening  616
Vulnerability Management Systems  616
Patch and Vulnerability Management  617
Change Management Processes  618
Recovery Strategies  618
Create Recovery Strategies  619
Categorize Asset Recovery Priorities  619
Business Process Recovery  620
Supply and Technology Recovery  620
User Environment Recovery  623
Data Recovery  623
Training Personnel  626
Backup Storage Strategies  626
Recovery and Multiple Site Strategies  628
Hot Site  628
Cold Site  629
Warm Site  629
Tertiary Site  630
Reciprocal Agreements  630
Redundant Sites  630
Redundant Systems, Facilities, and Power  630
Fault-Tolerance Technologies  631
Insurance  631
Data Backup  632
Fire Detection and Suppression  632
High Availability  632
Quality of Service  633
System Resilience  633
Disaster Recovery  633
Response  634
Personnel  634
Damage Assessment Team  635
Legal Team  635
Media Relations Team  635
Recovery Team  635
Relocation Team  635
Restoration Team  636
Salvage Team  636
Security Team  636
Communications  636
Assessment  636
Contents

Restoration 637
Training and Awareness 637
Testing Disaster Recovery Plans 637
Read-Through Test 638
Checklist Test 638
Table-Top Exercise 638
Structured Walk-Through Test 638
Simulation Test 639
Parallel Test 639
Full- Interruption Test 639
Functional Drill 639
Evacuation Drill 639
Business Continuity Planning and Exercises 639
Physical Security 640
Perimeter Security Controls 640
Gates and Fences 640
Perimeter Intrusion Detection 642
Lighting 643
Patrol Force 644
Access Control 645
Building and Internal Security Controls 645
Personnel Safety and Security 645
Duress 646
Travel 646
Monitoring 646
Emergency Management 646
Security Training and Awareness 647
Exam Preparation Tasks 647
Review All Key Topics 647
Define Key Terms 648
Answer Review Questions 649
Answers and Explanations 653

Chapter 8 Software Development Security 658
Foundation Topics 659
Software Development Concepts 659
    Machine Languages 659
    Assembly Languages and Assemblers 660
    High-Level Languages, Compilers, and Interpreters 660
    Object-Oriented Programming 660
    Polymorphism 661
    Polyinstantiation 662
    Encapsulation 662
    Cohesion 662
    Coupling 662
    Data Structures 662
    Distributed Object-Oriented Systems 663
    CORBA 663
    COM and DCOM 663
    OLE 663
    Java 664
    SOA 664
    Mobile Code 664
    Java Applets 664
    ActiveX 664
    NIST SP 800-163 665

Security in the System and Software Development Life Cycles 668
    System Development Life Cycle 668
    Initiate 668
    Acquire/Develop 669
    Implement 669
    Operate/Maintain 669
    Dispose 670
    Software Development Life Cycle 670
    Plan/Initiate Project 671
    Gather Requirements 671
    Design 672
    Develop 672
    Test/Validate 672
Release/Maintain 673
Certify/Accredit 674
Change Management and Configuration Management/Replacement 674
Software Development Methods and Maturity Models 674
Build and Fix 675
Waterfall 676
V-Shaped 677
Prototyping 677
Modified Prototype Model (MPM) 678
Incremental 678
Spiral 678
Agile 679
Rapid Application Development (RAD) 680
Joint Analysis Development (JAD) 681
Cleanroom 681
Structured Programming Development 681
Exploratory Model 681
Computer-Aided Software Engineering (CASE) 681
Component-Based Development 682
CMMI 682
IDEAL Model 683
Operation and Maintenance 684
Integrated Product Team 685
Security Controls in Development 686
WASC 686
OWASP 687
BSI 687
ISO/IEC 27000 687
Software Environment Security 687
Source Code Analysis Tools 688
Code Repository Security 688
Software Threats 688
Malware 689
Malware Protection 693
Scanning Types 693
Security Policies 693
Software Protection Mechanisms 694
Assess Software Security Effectiveness 695
Auditing and Logging 695
Risk Analysis and Mitigation 695
Regression and Acceptance Testing 696
Security Impact of Acquired Software 696
Secure Coding Guidelines and Standards 697
Security Weaknesses and Vulnerabilities at the Source Code Level 697
Buffer Overflow 697
Escalation of Privileges 699
Backdoor 699
Rogue Programmers 699
Covert Channel 699
Object Reuse 700
Mobile Code 700
Time of Check/Time of Use (TOC/TOU) 700
Security of Application Programming Interfaces 700
Secure Coding Practices 701
Validate Input 701
Heed Compiler Warnings 701
Design for Security Policies 701
Implement Default Deny 702
Adhere to the Principle of Least Privilege, and Practice Defense in Depth 702
Sanitize Data Prior to Transmission to Other Systems 702
Exam Preparation Tasks 702
Review All Key Topics 702
Define Key Terms 703
Answer Review Questions 704
Answers and Explanations 707
About the Authors

Robin M. Abernathy has been working in the IT certification preparation industry at Kaplan IT Training for more than 18 years. Robin 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.

Troy McMillan writes practice tests, study guides, and online course materials for Kaplan IT Training, while also running his own consulting and training business.

He holds more than 30 industry certifications and also appears in training videos for Oncourse Learning and Pearson.
Dedication

For my husband, Michael, and my son, Jonas. It really is all for you! —Robin
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!

When my father and his business partner asked me to take over a retail computer store in the mid-1990s, I had no idea that a big journey was starting for me personally. Thanks, Wayne McDaniel (Dad) and Roy Green, for seeing something in me that I didn’t even see in myself and for taking a chance on a very green techie. Also, thanks to my mom, Lucille McDaniel, for supporting my career changes over the years, even if you didn’t understand them. Thanks to Mike White for sharing your knowledge and giving me a basis on which to build my expertise over the coming years. Thanks to my two Alabama Institute for Deaf and Blind (AIDB) mentors, Zackie Bosarge and Dr. Phil Wade, who gave me my first “real” jobs in the IT field.

Thanks to my husband, Michael, for supporting me, even when I had this idea to quit my wonderful job at AIDB to start working from home for this company (Kaplan) that he knew nothing about. To him and my son, Jonas, thanks for being willing to have guy time while I was hiding away writing. You are my two favorite people! Thanks for ALWAYS making me laugh!

Pearson has put together an outstanding team to help me on my journey. Thanks Michelle Newcomb, Sari Green, Chris Cleveland, Chris Crayton, and Tonya Simpson for helping me make this Third Edition the best yet!

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

—Robin
About the Technical Reviewer

Chris Crayton (MCSE) is an author, technical consultant, and trainer. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.
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 authors and editors who worked on the book.

Email: feedback@pearsonitcertification.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 9780789759696 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 broaden, 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. This requires trained professionals being 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 Systems 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 Lifecycle 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 in this section, the topics that comprise the eight domains of knowledge are covered 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
Numerous reasons exist for why a security professional would spend the time and effort required to achieve this credential:

- 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 for 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% of the exam. Topics include

- Concepts of confidentiality, integrity, and availability
- Security governance principles
- Compliance requirements
- Legal and regulatory issues
- Professional ethics
- Security policy, standards, procedures, and guidelines
- Business continuity (BC) requirements
- Personnel security policies and procedures
- Risk management concepts
- Threat modeling concepts and methodologies
- Risk-based management concepts for the supply chain
- 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% of the exam. Topics include
- Information and asset identification and classification
- Information and asset ownership
- Privacy protection
- Asset retention
- Data security controls
- Information and asset handling 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% of the exam. Topics include
- Engineering processes using secure design principles
- Fundamental concepts of security models
- Control selection based upon systems security requirements
- Security capabilities of information systems
- Vulnerabilities of security architectures, designs, and solution elements
- Vulnerabilities in web-based systems
- Vulnerabilities in mobile systems
- Vulnerabilities in embedded devices
- Cryptography
- 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 14% of the exam. The 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% 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
- Identity as a third-party service
- Authorization mechanisms
- Identity and access provisioning life cycle

Security Assessment and Testing

The Security Assessment and Testing domain, covered in Chapter 6 and comprising 12% 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% of the exam. Topics include

- Investigations and investigation types
- Logging and monitoring activities
- Resource provisioning security
- Security operations concepts
- Resource protection techniques
- Incident management
- Detective and preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes
- Disaster recovery plan testing
- Business continuity 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 10% 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.

Once 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 3–6 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 counts toward the 3–6 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 150 questions, while the linear format consists of 250 questions. As of December 2017, the CISSP exam will be in a computerized adaptive testing (CAT) format for those who take the English-language version, while all other languages only have the linear format. With the CAT format, the computer evaluates the certification candidate’s ability to get the next question right based on his or her 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 150 questions. To find out more about the CAT format, please go to https://www.isc2.org/Certifications/CISSP/CISSP-CAT#.

While 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, Third Edition**

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

**Objectives and Methods**

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

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

Providing practice exercises on the topics and the testing process via test questions on the companion website

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

- **Foundation Topics**: These are the core sections of each chapter. They explain the concepts for the topics in that chapter.

- **Exam Preparation Tasks**: After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter:
  - **Review All Key Topics**: The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
  - **Define Key Terms**: Although the CISSP exam may be unlikely to ask a question such as “Define this term,” the exam does require that you learn and know a lot of information systems security terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
  - **Review Questions**: Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.

- **Web-based practice exam**: The companion website includes the Pearson Cert Practice Test engine that allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

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

**Companion Website**

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

To access this companion website, follow the steps below:

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

**Step 2.** Enter the ISBN: **9780789759696**.

**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 at left, please visit www.pearsonITcertification.com/contact and select the **Site Problems/Comments** option. Our customer service representatives will assist you.

**Pearson Test Prep Practice Test Software**

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

**Accessing the Pearson Test Prep Software Online**

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

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

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

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

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

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

Accessing the Pearson Test Prep Software Offline

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

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

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


Step 2. Answer the challenge questions.

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

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

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

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

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

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

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

Step 10. Enter the unique access code found on the card in the sleeve in the back of your book and click the Activate button.
Step 11. Click Next and then click Finish to download the exam data to your application.

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

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

Customizing Your Exams

Once 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.
This chapter covers the following topics:

- **Design and Validate Assessment, Test, and Audit Strategies**: Explains the use of assessment, test, and audit strategies, including internal, external, and third-party strategies.

- **Conduct Security Control Testing**: Concepts discussed include the security control testing process, including vulnerability assessments, penetration testing, log reviews, synthetic transactions, code review and testing, misuse case testing, test coverage analysis, and interface testing.

- **Collect Security Process Data**: Concepts discussed include NIST SP 800-137, account management, management review and approval, key performance and risk indicators, backup verification data, training and awareness, and disaster recovery and business continuity.

- **Analyze and Report Test Outputs**: Explains the importance of analyzing and reporting test outputs, including automatic and manual reports.

- **Conduct or Facilitate Security Audits**: Describes the internal, external, and third-party auditing processes and the three types of SOC reports.

Security assessment and testing covers designing, performing, and analyzing security testing. Security professionals must understand these processes to protect their assets from attacks.
Security Assessment and Testing

Security assessment and testing requires a number of testing methods to determine an organization’s vulnerabilities and risks. It assists an organization in managing the risks in planning, deploying, operating, and maintaining systems and processes. Its goal is to identify any technical, operational, and system deficiencies early in the process, before those deficiencies are deployed. The earlier you can discover those deficiencies, the cheaper it is to fix them.

This chapter discusses assessment and testing strategies, security control testing, collection of security process data, analysis and reporting of test outputs, and internal, external, and third-party audits.

Foundation Topics

Design and Validate Assessment and Testing Strategies

Security professionals must ensure that their organization plans, designs, executes, and validates appropriate security assessment, testing, and audit strategies to ensure that risks are mitigated. Security professionals must take a lead role in helping the organization implement the appropriate security assessment, testing, and auditing strategies. The organization should rely on industry best practices, national and international standards, and vendor-recommended practices and guidelines to ensure that the strategies are planned and implemented appropriately.

Organizations will most likely establish a team that will be responsible for executing any assessment, testing, and auditing strategies. The team should consist of individuals who understand security assessment, testing, and auditing but should also include representatives from other areas of the organization. Verifying and validating security is an ongoing activity that never really stops. But security professionals should help guide an organization in terms of when a particular type of assessment or testing is best performed.
Security Testing

Security testing ensures that a control is functioning properly. Both manual and automatic security testing can be performed. Security testing should be carried out on a regular basis. Security testing should be performed on all types of devices.

When performing security testing, security professionals should understand that it will affect the performance of the devices involved in the security test. Security testing cannot always be performed during non-peak hours. Only performing this testing during non-peak hours could also result in skewed results.

Security professionals should consider the following factors when performing security testing:

- Impact
- Difficulty
- Time needed
- Changes that could affect the performance
- System risk
- System criticality
- Security test availability
- Information sensitivity level
- Likelihood of technical failure or misconfiguration

Once security tests are performed, security professionals should analyze the results and make appropriate recommendations based on those results. In addition, the security testing tools themselves can be configured to send alerts or messages based on preconfigured triggers or filters. Without proper analysis, security testing does not provide a benefit to the organization.

Security Assessments

Security assessments are the reviews of the security status and reports for a system, application, or other environment. During this assessment, a security professional will review the results of the security tests, identify any vulnerabilities, and make recommendations for remediation. Security testing leads to security assessments.

Security professionals should prepare a formal security assessment report that includes all of the identified issues and recommendations. Also, they should document the actions taken based on the recommendations.
Security Auditing

Security auditing is the process of providing the digital proof when someone who is performing certain activities needs to be identified. Like security assessment and testing, it can be performed internally, externally, and via a third party. Security auditing is covered in more detail later in this chapter and in Chapter 7, “Security Operations.”

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

Security assessment, testing, and auditing occur in three manners: internal, external, and third-party. Internal assessment, testing, and auditing are carried out by personnel within the organization. External assessment, testing, and auditing are carried out by a vendor or contractor that is engaged by the company.

Sometimes third-party assessment, testing, and auditing are performed by a party completely unrelated to the company and not previously engaged by it. This scenario often arises as a result of having to comply with some standard or regulation or when accreditation or certification is involved. Many certifying or regulating bodies may require engagement of a third party that has not had a previous relationship with the organization being assessed. In this case, the certifying body will work with the organization to engage an approved third party.

Companies should ensure that, at minimum, internal and external testing and assessments are completed on a regular basis.

Conduct Security Control Testing

Organizations must manage the security control testing that occurs to ensure that all security controls are tested thoroughly by authorized individuals. The facets of security control testing that organizations must include are vulnerability assessments, penetration testing, log reviews, synthetic transactions, code review and testing, misuse case testing, test coverage analysis, and interface testing.

Vulnerability Assessment

A vulnerability assessment helps to identify the areas of weakness in a network. It can also help to determine asset prioritization within an organization. A comprehensive vulnerability assessment is part of the risk management process. But for access control, security professionals should use vulnerability assessments that specifically target the access control mechanisms.
Vulnerability assessments usually fall into one of three categories:

- **Personnel testing:** Reviews standard practices and procedures that users follow.
- **Physical testing:** Reviews facility and perimeter protections.
- **System and network testing:** Reviews systems, devices, and network topology.

The security analyst who will be performing a vulnerability assessment must understand the systems and devices that are on the network and the jobs they perform. The analyst needs this information to be able to assess the vulnerabilities of the systems and devices based on the known and potential threats to the systems and devices.

After gaining knowledge regarding the systems and devices, the security analyst should examine existing controls in place and identify any threats against these controls. The security analyst can then use all the information gathered to determine which automated tools to use to search for vulnerabilities. After the vulnerability analysis is complete, the security analyst should verify the results to ensure that they are accurate and then report the findings to management, with suggestions for remedial action. With this information in hand, the analyst should carry out threat modeling to identify the threats that could negatively affect systems and devices and the attack methods that could be used.

Vulnerability assessment applications include Nessus, Open Vulnerability Assessment System (OpenVAS), Core Impact, Nexpose, GFI LanGuard, QualysGuard, and Microsoft Baseline Security Analyzer (MBSA). Of these applications, OpenVAS and MBSA are free.

When selecting a vulnerability assessment tool, you should research the following metrics: accuracy, reliability, scalability, and reporting. Accuracy is the most important metric. A false positive generally results in time spent researching an issue that does not exist. A false negative is more serious, as it means the scanner failed to identify an issue that poses a serious security risk.

**Network Discovery Scan**

A network discovery scan examines a range of IP addresses to determine which ports are open. This type of scan only shows a list of systems on the network and the ports in use on the network. It does not actually check for any vulnerabilities.

Topology discovery entails determining the devices in the network, their connectivity relationships to one another, and the internal IP addressing scheme in use. Any combination of these pieces of information allows a hacker to create a “map” of the network, which aids him tremendously in evaluating and interpreting the data he gathers in other parts of the hacking process. If he is completely successful, he will
end up with a diagram of the network. Your challenge as a security professional is to determine whether such a mapping process is possible, using the same tools as the attacker. Based on your findings, you should determine steps to take that make topology discovery either more difficult or, better yet, impossible.

Operating system fingerprinting is the process of using some method to determine the operating system running on a host or a server. By identifying the OS version and build number, a hacker can identify common vulnerabilities of that OS using readily available documentation from the Internet. While many of the issues will have been addressed in subsequent updates, service packs, and hotfixes, there might be zero-day weaknesses (issues that have not been widely publicized or addressed by the vendor) that the hacker can leverage in the attack. Moreover, if any of the relevant security patches have not been applied, the weaknesses the patches were intended to address will exist on the machine. Therefore, the purpose of attempting OS fingerprinting during assessment is to assess the relative ease with which it can be done and identifying methods to make it more difficult.

Operating systems have well-known vulnerabilities, and so do common services. By determining the services that are running on a system, an attacker also discovers potential vulnerabilities of the service of which he may attempt to take advantage. This is typically done with a port scan, in which all “open,” or “listening,” ports are identified. Once again, the lion’s share of these issues will have been mitigated with the proper security patches, but that is not always the case; it is not uncommon for security analysts to find that systems that are running vulnerable services are missing the relevant security patches. Consequently, when performing service discovery, check patches on systems found to have open ports. It is also advisable to close any ports not required for the system to do its job.

Network discovery tools can perform the following types of scans:

- **TCP SYN scan**: Sends a packet to each scanned port with the SYN flag set. If a response is received with the SYN and ACK flags set, the port is open.
- **TCP ACK scan**: Sends a packet to each port with the ACK flag set. If no response is received, then the port is marked as filtered. If an RST response is received, then the port is marked as unfiltered.
- **Xmas scan**: Sends a packet with the FIN, PSH, and URG flags set. If the port is open, there is no response. If the port is closed, the target responds with a RST/ACK packet.

The result of this type of scan is that security professionals can determine if ports are open, closed, or filtered. Open ports are being used by an application on the remote system. Closed ports are open ports but there is no application accepting connections on that port. Filtered ports are ports that cannot be reached.

The most widely used network discovery scanning tool is Nmap.
Network Vulnerability Scan

Network vulnerability scans perform a more complex scan of the network than network discovery scans. These scans will probe a targeted system or network to identify vulnerabilities. The tools used in this type of scan will contain a database of known vulnerabilities and will identify if a specific vulnerability exists on each device.

There are two types of vulnerability scanners:

■ **Passive vulnerability scanners**: A passive vulnerability scanner (PVS) monitors network traffic at the packet layer to determine topology, services, and vulnerabilities. It avoids the instability that can be introduced to a system by actively scanning for vulnerabilities.

PVS tools analyze the packet stream and look for vulnerabilities through direct analysis. They are deployed in much the same way as intrusion detection systems (IDSs) or packet analyzers. A PVS can pick a network session that targets a protected server and monitor it as much as needed. The biggest benefit of a PVS is its ability to do its work without impacting the monitored network. Some examples of PVSs are the Nessus Network Monitor (formerly Tenable PVS) and NetScanTools Pro.

■ **Active vulnerability scanners**: Whereas passive scanners can only gather information, active vulnerability scanners (AVSs) can take action to block an attack, such as block a dangerous IP address. They can also be used to simulate an attack to assess readiness. They operate by sending transmissions to nodes and examining the responses. Because of this, these scanners may disrupt network traffic. Examples include Nessus and Microsoft Baseline Security Analyzer (MBSA).

Regardless of whether it’s active or passive, a vulnerability scanner cannot replace the expertise of trained security personnel. Moreover, these scanners are only as effective as the signature databases on which they depend, so the databases must be updated regularly. Finally, scanners require bandwidth and potentially slow the network.

For best performance, you can place a vulnerability scanner in a subnet that needs to be protected. You can also connect a scanner through a firewall to multiple subnets; this complicates the configuration and requires opening ports on the firewall, which could be problematic and could impact the performance of the firewall.

The most popular network vulnerability scanning tools include Qualys, Nessus, and MBSA.

Vulnerability scanners can use agents that are installed on the devices, or they can be agentless. While many vendors argue that using agents is always best, there are advantages and disadvantages to both, as presented in Table 6-1.
Table 6-1  Server-Based vs. Agent-Based Scanning

<table>
<thead>
<tr>
<th>Type</th>
<th>Technology</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent-based</td>
<td>Pull technology</td>
<td>Can get information from disconnected machines or machines in the DMZ</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ideal for remote locations that have limited bandwidth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Less dependent on network connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Based on policies defined in the central console</td>
</tr>
<tr>
<td>Server-based</td>
<td>Push technology</td>
<td>Good for networks with plentiful bandwidth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dependent on network connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Central authority does all the scanning and deployment</td>
</tr>
</tbody>
</table>

Some scanners can do both agent-based and server-based scanning (also called agentless or sensor-based scanning).

**Web Application Vulnerability Scan**

Because web applications are highly used in today’s world, companies must ensure that their web applications remain secure and free of vulnerabilities. Web application vulnerability scanners are special tools that examine web applications for known vulnerabilities.

Popular web application vulnerability scanners include QualysGuard and Nexpose.

**Penetration Testing**

The goal of penetration testing, also known as ethical hacking, is to simulate an attack to identify any threats that can stem from internal or external resources planning to exploit the vulnerabilities of a system or device.

The steps in performing a penetration test are as follows:

1. Document information about the target system or device.
2. Gather information about attack methods against the target system or device. This includes performing port scans.
3. Identify the known vulnerabilities of the target system or device.
4. Execute attacks against the target system or device to gain user and privileged access.
5. Document the results of the penetration test and report the findings to management, with suggestions for remedial action.
Both internal and external tests should be performed. Internal tests occur from within the network, whereas external tests originate outside the network and target the servers and devices that are publicly visible.

Strategies for penetration testing are based on the testing objectives defined by the organization. The strategies that you should be familiar with include the following:

- **Blind test**: The testing team is provided with limited knowledge of the network systems and devices that use publicly available information. The organization’s security team knows that an attack is coming. This test requires more effort by the testing team, and the team must simulate an actual attack.

- **Double-blind test**: This test is like a blind test except the organization’s security team does not know that an attack is coming. Only a few individuals in the organization know about the attack, and they do not share this information with the security team. This test usually requires equal effort for both the testing team and the organization’s security team.

- **Target test**: Both the testing team and the organization’s security team are given maximum information about the network and the type of attack that will occur. This is the easiest test to complete but does not provide a full picture of the organization’s security.

Penetration testing is also divided into categories based on the amount of information to be provided. The main categories that you should be familiar with include the following:

- **Zero-knowledge test**: The testing team is provided with no knowledge regarding the organization’s network. The testing team can use any means available to obtain information about the organization’s network. This is also referred to as closed, or black-box, testing.

- **Partial-knowledge test**: The testing team is provided with public knowledge regarding the organization’s network. Boundaries might be set for this type of test. This is also referred to as gray-box testing.

- **Full-knowledge test**: The testing team is provided with all available knowledge regarding the organization’s network. This test is focused more on what attacks can be carried out. This is also referred to as white-box testing.

Penetration testing applications include Metasploit, Wireshark, Core Impact, Nessus, Cain & Abel, Kali Linux, and John the Ripper. When selecting a penetration testing tool, you should first determine which systems you want to test. Then research the different tools to discover which can perform the tests that you want to perform for those systems and research the tools’ methodologies for testing. In addition, the organization needs to select the correct individual to carry out the test.
Remember that penetration tests should include manual methods as well as automated methods because relying on only one of these two will not yield a thorough result.

Table 6-2 compares vulnerability assessments and penetration tests.

<table>
<thead>
<tr>
<th></th>
<th>Vulnerability Assessment</th>
<th>Penetration Test</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Identifies vulnerabilities that may result in compromise of a system.</td>
<td>Identifies ways to exploit vulnerabilities to circumvent the security features of systems.</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>After significant system changes. Schedule at least quarterly thereafter.</td>
<td>After significant system changes. Schedule at least annually thereafter.</td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>Use automated tools with manual verification of identified issues.</td>
<td>Use both automated and manual methods to provide a comprehensive report.</td>
</tr>
<tr>
<td><strong>Reports</strong></td>
<td>Potential risks posed by known vulnerabilities, ranked using base scores associated with each vulnerability. Both internal and external reports should be provided.</td>
<td>Description of each issue discovered, including specific risks the issue may pose and specifically how and to what extent it may be exploited.</td>
</tr>
<tr>
<td><strong>Duration</strong></td>
<td>Typically several seconds to several minutes per scanned host.</td>
<td>Days or weeks, depending on the scope and size of the environment to be tested. Tests may grow in duration if efforts uncover additional scope.</td>
</tr>
</tbody>
</table>

**Log Reviews**

A log is a recording of events that occur on an organizational asset, including systems, networks, devices, and facilities. Each entry in a log covers a single event that occurs on the asset. In most cases, there are separate logs for different event types, including security logs, operating system logs, and application logs. Because so many logs are generated on a single device, many organizations have trouble ensuring that the logs are reviewed in a timely manner. Log review, however, is probably one of the most important steps an organization can take to ensure that issues are detected before they become major problems.

Computer security logs are particularly important because they can help an organization identify security incidents, policy violations, and fraud. Log management ensures that computer security logs are stored in sufficient detail for an appropriate period of time so that auditing, forensic analysis, investigations, baselines, trends, and long-term problems can be identified.
The National Institute of Standards and Technology (NIST) has provided two special publications that relate to log management: NIST SP 800-92, “Guide to Computer Security Log Management,” and NIST SP 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.” While both of these special publications are primarily used by federal government agencies and organizations, other organizations may want to use them as well because of the wealth of information they provide. The following section covers NIST SP 800-92, and NIST SP 800-137 is discussed later in this chapter.

NIST SP 800-92

NIST SP 800-92 makes the following recommendations for more efficient and effective log management:

- Organizations should establish policies and procedures for log management. As part of the planning process, an organization should
  - Define its logging requirements and goals.
  - Develop policies that clearly define mandatory requirements and suggested recommendations for log management activities.
  - Ensure that related policies and procedures incorporate and support the log management requirements and recommendations.
- Management should provide the necessary support for the efforts involving log management planning, policy, and procedures development.
- Organizations should prioritize log management appropriately throughout the organization.
- Organizations should create and maintain a log management infrastructure.
- Organizations should provide proper support for all staff with log management responsibilities.
- Organizations should establish standard log management operational processes. This includes ensuring that administrators
  - Monitor the logging status of all log sources.
  - Monitor log rotation and archival processes.
  - Check for upgrades and patches to logging software and acquire, test, and deploy them.
  - Ensure that each logging host’s clock is synchronized to a common time source.
  - Reconfigure logging as needed based on policy changes, technology changes, and other factors.
  - Document and report anomalies in log settings, configurations, and processes.
According to NIST SP 800-92, common log management infrastructure components include general functions (log parsing, event filtering, and event aggregation), storage (log rotation, log archival, log reduction, log conversion, log normalization, and log file integrity checking), log analysis (event correlation, log viewing, and log reporting), and log disposal (log clearing.)

Syslog provides a simple framework for log entry generation, storage, and transfer that any operating system, security software, or application could use if designed to do so. Many log sources either use syslog as their native logging format or offer features that allow their log formats to be converted to syslog format. Each syslog message has only three parts. The first part specifies the facility and severity as numerical values. The second part of the message contains a timestamp and the hostname or IP address of the source of the log. The third part is the actual log message content.

No standard fields are defined within the message content; it is intended to be human-readable and not easily machine-parsable. This provides very high flexibility for log generators, which can place whatever information they deem important within the content field, but it makes automated analysis of the log data very challenging. A single source may use many different formats for its log message content, so an analysis program would need to be familiar with each format and be able to extract the meaning of the data within the fields of each format. This problem becomes much more challenging when log messages are generated by many sources. It might not be feasible to understand the meaning of all log messages, so analysis might be limited to keyword and pattern searches. Some organizations design their syslog infrastructures so that similar types of messages are grouped together or assigned similar codes, which can make log analysis automation easier to perform.

As log security has become a greater concern, several implementations of syslog have been created that place greater emphasis on security. Most have been based on IETF’s RFC 3195, which was designed specifically to improve the security of syslog. Implementations based on this standard can support log confidentiality, integrity, and availability through several features, including reliable log delivery, transmission confidentiality protection, and transmission integrity protection and authentication.

Security information and event management (SIEM) products allow administrators to consolidate all security information logs. This consolidation ensures that administrators can perform analysis on all logs from a single resource rather than having to analyze each log on its separate resource. Most SIEM products support two ways of collecting logs from log generators:

- **Agentless:** The SIEM server receives data from the individual hosts without needing to have any special software installed on those hosts. Some servers pull logs from the hosts, which is usually done by having the server
authenticate to each host and retrieve its logs regularly. In other cases, the hosts push their logs to the server, which usually involves each host authenticating to the server and transferring its logs regularly. Regardless of whether the logs are pushed or pulled, the server then performs event filtering and aggregation and log normalization and analysis on the collected logs.

- **Agent-based**: An agent program is installed on the host to perform event filtering and aggregation and log normalization for a particular type of log. The host then transmits the normalized log data to the SIEM server, usually on a real-time or near-real-time basis for analysis and storage. Multiple agents may need to be installed if a host has multiple types of logs of interest. Some SIEM products also offer agents for generic formats such as syslog and Simple Network Management Protocol (SNMP). A generic agent is used primarily to get log data from a source for which a format-specific agent and an agentless method are not available. Some products also allow administrators to create custom agents to handle unsupported log sources.

There are advantages and disadvantages to each method. The primary advantage of the agentless approach is that agents do not need to be installed, configured, and maintained on each logging host. The primary disadvantage is the lack of filtering and aggregation at the individual host level, which can cause significantly larger amounts of data to be transferred over networks and increase the amount of time it takes to filter and analyze the logs. Another potential disadvantage of the agentless method is that the SIEM server may need credentials for authenticating to each logging host. In some cases, only one of the two methods is feasible; for example, there might be no way to remotely collect logs from a particular host without installing an agent onto it.

SIEM products usually include support for several dozen types of log sources, such as OSs, security software, application servers (e.g., web servers, email servers), and even physical security control devices such as badge readers. For each supported log source type, except for generic formats such as syslog, the SIEM products typically know how to categorize the most important logged fields. This significantly improves the normalization, analysis, and correlation of log data over that performed by software with a less granular understanding of specific log sources and formats. Also, the SIEM software can perform event reduction by disregarding data fields that are not significant to computer security, potentially reducing the SIEM software’s network bandwidth and data storage usage.

Typically, system, network, and security administrators are responsible for managing logging on their systems, performing regular analysis of their log data, documenting and reporting the results of their log management activities, and ensuring that log data is provided to the log management infrastructure in accordance with
the organization’s policies. In addition, some of the organization’s security administrators act as log management infrastructure administrators, with responsibilities such as the following:

- Contact system-level administrators to get additional information regarding an event or to request that they investigate a particular event.
- Identify changes needed to system logging configurations (e.g., which entries and data fields are sent to the centralized log servers, what log format should be used) and inform system-level administrators of the necessary changes.
- Initiate responses to events, including incident handling and operational problems (e.g., a failure of a log management infrastructure component).
- Ensure that old log data is archived to removable media and disposed of properly once it is no longer needed.
- Cooperate with requests from legal counsel, auditors, and others.
- Monitor the status of the log management infrastructure (e.g., failures in logging software or log archival media, failures of local systems to transfer their log data) and initiate appropriate responses when problems occur.
- Test and implement upgrades and updates to the log management infrastructure’s components.
- Maintain the security of the log management infrastructure.

Organizations should develop policies that clearly define mandatory requirements and suggested recommendations for several aspects of log management, including log generation, log transmission, log storage and disposal, and log analysis. Table 6-3 gives examples of logging configuration settings that an organization can use. The types of values defined in Table 6-3 should only be applied to the hosts and host components previously specified by the organization as ones that must or should log security-related events.

<table>
<thead>
<tr>
<th>Category</th>
<th>Low-Impact Systems</th>
<th>Moderate-Impact Systems</th>
<th>High-Impact Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log retention duration</td>
<td>1–2 weeks</td>
<td>1–3 months</td>
<td>3–12 months</td>
</tr>
<tr>
<td>Log rotation</td>
<td>Optional (if performed, at least every week or every 25 MB)</td>
<td>Every 6–24 hours or every 2–5 MB</td>
<td>Every 15–60 minutes or every 0.5–1.0 MB</td>
</tr>
<tr>
<td>Log data transfer frequency (to SIEM)</td>
<td>Every 3–24 hours</td>
<td>Every 15–60 minutes</td>
<td>At least every 5 minutes</td>
</tr>
</tbody>
</table>
## Synthetic Transactions

Synthetic transaction monitoring, which is a type of proactive monitoring, is often preferred for websites and applications. It provides insight into the availability and performance of an application and warns of any potential issue before users experience any degradation in application behavior. It uses external agents to run scripted transactions against an application. For example, Microsoft’s System Center Operations Manager uses synthetic transactions to monitor databases, websites, and TCP port usage.

In contrast, real user monitoring (RUM), which is a type of passive monitoring, captures and analyzes every transaction of every application or website user. Unlike synthetic monitoring, which attempts to gain performance insights by regularly testing synthetic interactions, RUM cuts through the guesswork by seeing exactly how users are interacting with the application.

## Code Review and Testing

Code review and testing must occur throughout the entire system or application development life cycle. The goal of code review and testing is to identify bad programming patterns, security misconfigurations, functional bugs, and logic flaws.

In the planning and design phase, code review and testing include architecture security reviews and threat modeling. In the development phase, code review and testing include static source code analysis, manual code review, static binary code analysis, and manual binary review. Once an application is deployed, code review and testing involve penetration testing, vulnerability scanning, and fuzz testing.

Formal code review involves a careful and detailed process with multiple participants and multiple phases. In this type of code review, software developers attend meetings where each line of code is reviewed, usually using printed copies. Lightweight code review typically requires less overhead than formal code inspections, though it can be equally effective when done properly. Code review methods include the following:

<table>
<thead>
<tr>
<th>Category</th>
<th>Low-Impact Systems</th>
<th>Moderate-Impact Systems</th>
<th>High-Impact Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local log data analysis</td>
<td>Every 1–7 days</td>
<td>Every 12–24 hours</td>
<td>At least 6 times a day</td>
</tr>
<tr>
<td>File integrity check for rotated logs?</td>
<td>Optional</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Encrypt rotated logs?</td>
<td>Optional</td>
<td>Optional</td>
<td>Yes</td>
</tr>
<tr>
<td>Encrypt log data transfers to SIEM?</td>
<td>Optional</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>


- **Over-the-shoulder**: One developer looks over the author’s shoulder as the author walks through the code.

- **Email pass-around**: Source code is emailed to reviewers automatically after the code is checked in.

- **Pair programming**: Two authors develop code together at the same workstation.

- **Tool-assisted code review**: Authors and reviewers use tools designed for peer code review.

- **Black-box testing, or zero-knowledge testing**: The team is provided with no knowledge regarding the organization’s application. The team can use any means at its disposal to obtain information about the organization’s application. This is also referred to as closed testing.

- **White-box testing**: The team goes into the process with a deep understanding of the application or system. Using this knowledge, the team builds test cases to exercise each path, input field, and processing routine.

- **Gray-box testing**: The team is provided more information than in black-box testing, while not as much as in white-box testing. Gray-box testing has the advantage of being nonintrusive while maintaining the boundary between developer and tester. On the other hand, it may uncover some of the problems that might be discovered with white-box testing.

Table 6-4 compares black-box, gray-box, and white-box testing.

<table>
<thead>
<tr>
<th>Black Box</th>
<th>Gray Box</th>
<th>White Box</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal workings of the application are not known.</td>
<td>Internal workings of the application are somewhat known.</td>
<td>Internal workings of the application are fully known.</td>
</tr>
<tr>
<td>Also called closed-box, data-driven, and functional testing.</td>
<td>Also called translucent testing, as the tester has partial knowledge.</td>
<td>Also known as clear-box, structural, or code-based testing.</td>
</tr>
<tr>
<td>Performed by end users, testers, and developers.</td>
<td>Performed by end users, testers, and developers.</td>
<td>Performed by testers and developers.</td>
</tr>
<tr>
<td>Least time-consuming.</td>
<td>More time-consuming than black-box testing but less so than white-box testing.</td>
<td>Most exhaustive and time-consuming.</td>
</tr>
</tbody>
</table>
Other types of testing include dynamic versus static testing and manual versus automatic testing.

**Code Review Process**

Code review varies from organization to organization. Fagan inspections are the most formal code reviews that can occur and should adhere to the following process:

1. Plan
2. Overview
3. Prepare
4. Inspect
5. Rework
6. Follow-up

Most organizations do not strictly adhere to the Fagan inspection process. Each organization should adopt a code review process fitting for its business requirements. The more restrictive the environment, the more formal the code review process should be.

**Static Testing**

Static testing analyzes software security without actually running the software. This is usually provided by reviewing the source code or compiled application. Automated tools are used to detect common software flaws. Static testing tools should be available throughout the software design process.

**Dynamic Testing**

Dynamic testing analyzes software security in the runtime environment. With this testing, the tester should not have access to the application’s source code.

Dynamic testing often includes the use of synthetic transactions, which are scripted transactions that have a known result. These synthetic transactions are executed against the tested code, and the output is then compared to the expected output. Any discrepancies between the two should be investigated for possible source code flaws.

**Fuzz Testing**

Fuzz testing is a dynamic testing tool that provides input to the software to test the software’s limits and discover flaws. The input provided can be randomly generated by the tool or specially created to test for known vulnerabilities.

Fuzz testers include Untidy, Peach Fuzzer, and Microsoft SDL File/Regex Fuzzer.
Misuse Case Testing

Misuse case testing, also referred to as negative testing, tests an application to ensure that the application can handle invalid input or unexpected behavior. This testing is completed to ensure that an application will not crash and to improve the quality of an application by identifying its weak points. When misuse case testing is performed, organizations should expect to find issues. Misuse testing should include testing that looks for the following:

- Required fields must be populated.
- Fields with a defined data type can only accept data that is the required data type.
- Fields with character limits allow only the configured number of characters.
- Fields with a defined data range accept only data within that range.
- Fields accept only valid data.

Test Coverage Analysis

Test coverage analysis uses test cases that are written against the application requirements specifications. Individuals involved in this analysis do not need to see the code to write the test cases. Once a document that describes all the test cases is written, test groups refer to a percentage of the test cases that were run, that passed, that failed, and so on. The application developer usually performs test coverage analysis as a part of unit testing. Quality assurance groups use overall test coverage analysis to indicate test metrics and coverage according to the test plan.

Test coverage analysis creates additional test cases to increase coverage. It helps developers find areas of an application not exercised by a set of test cases. It helps in determining a quantitative measure of code coverage, which indirectly measures the quality of the application or product.

One disadvantage of code coverage measurement is that it measures coverage of what the code covers but cannot test what the code does not cover or what has not been written. In addition, this analysis looks at a structure or function that already exists and not those that do not yet exist.

Interface Testing

Interface testing evaluates whether an application’s systems or components correctly pass data and control to one another. It verifies whether module interactions are working properly and errors are handled correctly. Interfaces that should be tested include client interfaces, server interfaces, remote interfaces, graphical user
interfaces (GUIs), application programming interfaces (APIs), external and internal interfaces, and physical interfaces.

GUI testing involves testing a product’s GUI to ensure that it meets its specifications through the use of test cases. API testing tests APIs directly in isolation and as part of the end-to-end transactions exercised during integration testing to determine whether the APIs return the correct responses.

Collect Security Process Data

After security controls are tested, organizations must ensure that they collect the appropriate security process data. NIST SP 800-137 provides guidelines for developing an information security continuous monitoring (ISCM) program. Security professionals should ensure that security process data that is collected includes account management, management review, key performance and risk indicators, backup verification data, training and awareness, and disaster recovery and business continuity.

NIST SP 800-137

According to NIST SP 800-137, ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Organizations should take the following steps to establish, implement, and maintain ISCM:

1. Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
2. Establish an ISCM program that includes metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
3. Implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.
4. Analyze the data collected, report findings, and determine the appropriate responses. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
5. Respond to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
6. Review and update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization’s information infrastructure, and increase organizational resilience.

**Account Management**

Account management is important because it involves the addition and deletion of accounts that are granted access to systems or networks. But account management also involves changing the permissions or privileges granted to those accounts. If account management is not monitored and recorded properly, organizations may discover that accounts have been created for the sole purpose of carrying out fraudulent or malicious activities. Two-person controls should be used with account management, often involving one administrator who creates accounts and another who assigns those accounts the appropriate permissions or privileges.

*Escalation* and *revocation* are two terms that are important to security professionals. Account escalation occurs when a user account is granted more permission based on new job duties or a complete job change. Security professionals should fully analyze a user’s needs prior to changing the current permissions or privileges, making sure to grant only permissions or privileges that are needed for the new task and to remove those that are no longer needed. Without such analysis, users may be able to retain permissions that cause possible security issues because separation of duties is no longer retained. For example, suppose a user is hired in the accounts payable department to print out all vendor checks. Later this user receives a promotion to approve payment for the same accounts. If this user’s old permission to print checks is not removed, this single user would be able to both approve the checks and print them, which is a direct violation of separation of duties.

Account revocation occurs when a user account is revoked because a user is no longer with an organization. Security professionals must keep in mind that there will be objects that belong to this user. If the user account is simply deleted, access to the objects owned by the user may be lost. It may be a better plan to disable the account for a certain period. Account revocation policies should also distinguish between revoking an account for a user who resigns from an organization and revoking an account for a user who is terminated.

**Management Review and Approval**

Management review of security process data should be mandatory. No matter how much data an organization collects on its security processes, the data is useless if it is never reviewed by an administrator. Guidelines and procedures should be established to ensure that management review occurs in a timely manner. Without
Management review should include an approval process whereby management reviews any recommendations from security professionals and approves or rejects the recommendations based on the data given. If alternatives are given, management should approve the alternative that best satisfies the organizational needs. Security professionals should ensure that the reports provided to management are as comprehensive as possible so that all the data can be analyzed to ensure the most appropriate solution is selected.

**Key Performance and Risk Indicators**

By using key performance and risk indicators of security process data, organizations better identify when security risks are likely to occur. Key performance indicators (PKIs) allow organizations to determine whether levels of performance are below or above established norms. Key risk indicators (KRIs) allow organizations to identify whether certain risks are more or less likely to occur.

NIST has released the *Framework for Improving Critical Infrastructure Cybersecurity*, also known as the Cybersecurity Framework, which focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The framework consists of three parts: the Framework Core, the Framework Profiles, and the Framework Implementation Tiers.

The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational profiles. The Framework Core consists of five concurrent and continuous functions—identify, protect, detect, respond, and recover.

After each function is identified, categories and subcategories for each function are recorded. The Framework Profiles are developed based on the business needs of the categories and subcategories. Through use of the Framework Profiles, the framework helps an organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.

The Framework Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. The following tiers are used: Tier 1, partial; Tier 2, risk informed; Tier 3, repeatable; and Tier 4, adaptive.

Organizations will continue to have unique risks—different threats, different vulnerabilities, and different risk tolerances—and how they implement the practices in
the framework will vary. Ultimately, the framework is aimed at reducing and better managing cybersecurity risks and is not a one-size-fits-all approach to managing cybersecurity.

**Backup Verification Data**

Any security process data that is collected should also be backed up. Security professionals should ensure that their organization has the appropriate backup and restore guidelines in place for all security process data. If data is not backed up properly, a failure can result in vital data being lost forever. In addition, personnel should test the restore process on a regular basis to make sure it works as it should. If an organization is unable to restore a backup properly, the organization might as well not have the backup.

**Training and Awareness**

All personnel must understand any security assessment and testing strategies that an organization employs. Technical personnel may need to be trained in the details about security assessment and testing, including security control testing and collecting security process data. Other personnel, however, only need to be given more awareness training on this subject. Security professionals should help personnel understand what type of assessment and testing occurs, what is captured by this process, and why this is important to the organization. Management must fully support the security assessment and testing strategy and must communicate to all personnel and stakeholders the importance this program.

**Disaster Recovery and Business Continuity**

Any disaster recovery and business continuity plans that an organization develops must consider security assessment and testing, security control testing, and security process data collection. Often when an organization goes into disaster recovery mode, personnel do not think about these processes. As a matter of fact, ordinary security controls often fall by the wayside at such times. A security professional is responsible for ensuring that this does not happen. Security professionals involved in developing the disaster recovery and business continuity plans must cover all these areas.

**Analyze and Report Test Outputs**

Personnel should understand the automated and manual reporting that can be done as part of security assessment and testing. Output must be reported in a timely manner to management in order to ensure that they understand the value of this process. It may be necessary to provide different reports depending on the level of audience
understanding. For example, high-level management may need only a summary of findings. But technical personnel should be given details of the findings to ensure that they can implement the appropriate controls to mitigate or prevent any risks found during security assessment and testing.

Personnel may need special training on how to run manual reports and how to analyze the report outputs.

**Conduct or Facilitate Security Audits**

Organizations should conduct internal, external, and third-party audits as part of any security assessment and testing strategy. These audits should test all security controls that are currently in place. The following are some guidelines to consider as part of a good security audit plan:

- At minimum, perform annual audits to establish a security baseline.
- Determine your organization’s objectives for the audit and share them with the auditors.
- Set the ground rules for the audit, including the dates/times of the audit, before the audit starts.
- Choose auditors who have security experience.
- Involve business unit managers early in the process.
- Ensure that auditors rely on experience, not just checklists.
- Ensure that the auditor’s report reflects risks that the organization has identified.
- Ensure that the audit is conducted properly.
- Ensure that the audit covers all systems and all policies and procedures.
- Examine the report when the audit is complete.

Remember that internal audits are performed by personnel within the organization, while external or third-party audits are performed by individuals outside the organization or another company. Both types of audits should occur.

Many regulations today require that audits occur. Organizations used to rely on Statement on Auditing Standards (SAS) 70, which provided auditors information and verification about data center controls and processes related to data center users and their financial reporting. A SAS 70 audit verified that the controls and processes set in place by a data center are actually followed. The Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service
Organization, is a newer standard that verifies the controls and processes and also requires a written assertion regarding the design and operating effectiveness of the controls being reviewed.

An SSAE 16 audit results in a Service Organization Control (SOC) 1 report. This report focuses on internal controls over financial reporting. There are two types of SOC 1 reports:

- **SOC 1, Type 1 report**: Focuses on the auditors’ opinion of the accuracy and completeness of the data center management’s design of controls, system, and/or service.

- **SOC 1, Type 2 report**: Includes the Type 1 report as well as an audit of the effectiveness of controls over a certain time period, normally between six months and a year.

Two other report types are also available: SOC 2 and SOC 3. Both of these audits provide benchmarks for controls related to the security, availability, processing integrity, confidentiality, or privacy of a system and its information. A SOC 2 report includes service auditor testing and results, and a SOC 3 report provides only the system description and auditor opinion. A SOC 3 report is for general use and provides a level of certification for data center operators that assures data center users of facility security, high availability, and process integrity. Table 6-5 briefly compares the three types of SOC reports.

<table>
<thead>
<tr>
<th>What It Reports On</th>
<th>Who Uses It</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 1 Internal controls over financial reporting</td>
<td>User auditors and controller office</td>
</tr>
<tr>
<td>SOC 2 Security, availability, processing integrity, confidentiality, or privacy controls</td>
<td>Management, regulators, and others; shared under nondisclosure agreement (NDA)</td>
</tr>
<tr>
<td>SOC 3 Security, availability, processing integrity, confidentiality, or privacy controls</td>
<td>Publicly available to anyone</td>
</tr>
</tbody>
</table>

**Exam Preparation Tasks**

As mentioned in the section “About the CISSP Cert Guide, Third Edition” in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 9, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.
Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 6-6 lists a reference of these key topics and the page numbers on which each is found.

Table 6-6  Key Topics for Chapter 6

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>List</td>
<td>Three categories of vulnerability assessments</td>
<td>536</td>
</tr>
<tr>
<td>Table 6-1</td>
<td>Server-Based vs. Agent-Based Scanning</td>
<td>539</td>
</tr>
<tr>
<td>List</td>
<td>Steps in a penetration test</td>
<td>539</td>
</tr>
<tr>
<td>List</td>
<td>Strategies for penetration testing</td>
<td>540</td>
</tr>
<tr>
<td>List</td>
<td>Penetration testing categories</td>
<td>540</td>
</tr>
<tr>
<td>Table 6-2</td>
<td>Comparison of Vulnerability Assessments and Penetration Tests</td>
<td>541</td>
</tr>
<tr>
<td>List</td>
<td>NIST SP 800-92 recommendations for log management</td>
<td>542</td>
</tr>
<tr>
<td>Table 6-3</td>
<td>Examples of Logging Configuration Settings</td>
<td>545</td>
</tr>
<tr>
<td>Table 6-4</td>
<td>Black-Box, Gray-Box, and White-Box Testing</td>
<td>547</td>
</tr>
<tr>
<td>List</td>
<td>Steps to establish, implement, and maintain ISCM</td>
<td>550</td>
</tr>
<tr>
<td>List</td>
<td>Types of SOC 1 reports</td>
<td>555</td>
</tr>
<tr>
<td>Table 6-5</td>
<td>SOC Reports Comparison</td>
<td>555</td>
</tr>
</tbody>
</table>

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

account management; active vulnerability scanner (AVS); black-box testing; blind test; code review and testing; double-blind test; dynamic testing; full-knowledge test; fuzz testing; gray-box testing; information security continuous monitoring (ISCM); interface testing; log; log review; misuse case testing; negative testing; network discovery scan; network vulnerability scan; NIST SP 800-137; NIST SP 800-92; operating system fingerprinting; partial-knowledge test; passive vulnerability scanner (PVS); penetration test; real user monitoring (RUM); static testing; synthetic transaction monitoring; target test; test coverage analysis; topology discovery; vulnerability; vulnerability assessment; white-box testing; zero-knowledge test
Answer Review Questions

1. For which of the following penetration tests does the testing team know an attack is coming but have limited knowledge of the network systems and devices and only publicly available information?
   a. Target test
   b. Physical test
   c. Blind test
   d. Double-blind test

2. Which of the following is NOT a guideline according to NIST SP 800-92?
   a. Organizations should establish policies and procedures for log management.
   b. Organizations should create and maintain a log management infrastructure.
   c. Organizations should prioritize log management appropriately throughout the organization.
   d. Choose auditors with security experience.

3. According to NIST SP 800-92, which of the following are facets of log management infrastructure? (Choose all that apply.)
   a. General functions (log parsing, event filtering, and event aggregation)
   b. Storage (log rotation, log archival, log reduction, log conversion, log normalization, log file integrity checking)
   c. Log analysis (event correlation, log viewing, log reporting)
   d. Log disposal (log clearing)

4. What are the two ways of collecting logs using security information and event management (SIEM) products, according to NIST SP 800-92?
   a. Passive and active
   b. Agentless and agent-based
   c. Push and pull
   d. Throughput and rate
5. Which monitoring method captures and analyzes every transaction of every application or website user?
   a. RUM
   b. Synthetic transaction monitoring
   c. Code review and testing
   d. Misuse case testing

6. Which type of testing is also known as negative testing?
   a. RUM
   b. Synthetic transaction monitoring
   c. Code review and testing
   d. Misuse case testing

7. What is the first step of the information security continuous monitoring (ISCM) plan, according to NIST SP 800-137?
   a. Establish an ISCM program.
   b. Define the ISCM strategy.
   c. Implement an ISCM program.
   d. Analyze the data collected.

8. What is the second step of the information security continuous monitoring (ISCM) plan, according to NIST SP 800-137?
   a. Establish an ISCM program.
   b. Define the ISCM strategy.
   c. Implement an ISCM program.
   d. Analyze the data collected.

9. Which of the following is NOT a guideline for internal, external, and third-party audits?
   a. Choose auditors with security experience.
   b. Involve business unit managers early in the process.
   c. At minimum, perform bi-annual audits to establish a security baseline.
   d. Ensure that the audit covers all systems and all policies and procedures.
10. Which SOC report should be shared with the general public?
   a. SOC 1, Type 1
   b. SOC 1, Type 2
   c. SOC 2
   d. SOC 3

11. Which of the following is the last step in performing a penetration test?
   a. Document the results of the penetration test and report the findings to management, with suggestions for remedial action.
   b. Gather information about attack methods against the target system or device.
   c. Document information about the target system or device.
   d. Execute attacks against the target system or device to gain user and privileged access.

12. In which of the following does the testing team have zero knowledge of the organization’s network?
    a. Gray-box testing
    b. Black-box testing
    c. White-box testing
    d. Physical testing

13. Which of the following is defined as a dynamic testing tool that provides input to the software to test the software’s limits and discover flaws?
    a. Interface testing
    b. Static testing
    c. Test coverage analysis
    d. Fuzz testing

14. Which factors should security professionals follow when performing security testing? (Choose all that apply.)
    a. Changes that could affect the performance
    b. System risk
    c. Information sensitivity level
    d. Likelihood of technical failure or misconfiguration
15. Which of the following can a hacker use to identify common vulnerabilities in an operating system running on a host or server?
   a. Operating system fingerprinting
   b. Network discovery scan
   c. Key performance and risk indicators
   d. Third-party audits

Answers and Explanations

1. c. With a blind test, the testing team knows an attack is coming and has limited knowledge of the network systems and devices and publicly available information. A target test occurs when the testing team and the organization’s security team are given maximum information about the network and the type of attack that will occur. A physical test is not a type of penetration test. It is a type of vulnerability assessment. A double-blind test is like a blind test except that the organization’s security team does not know an attack is coming.

2. d. NIST SP 800-92 does not include any information regarding auditors. So the “Choose auditors with security experience” option is NOT a guideline according to NIST SP 800-92.

3. a, b, c, d. According to NIST SP 800-92, log management functions should include general functions (log parsing, event filtering, and event aggregation), storage (log rotation, log archival, log reduction, log conversion, log normalization, log file integrity checking), log analysis (event correlation, log viewing, log reporting), and log disposal (log clearing).

4. b. The two ways of collecting logs using security information and event management (SIEM) products, according to NIST SP 800-92, are agentless and agent-based.

5. a. Real user monitoring (RUM) captures and analyzes every transaction of every application or website user.

6. d. Misuse case testing is also known as negative testing.

7. b. The steps in an ISCM program, according to NIST SP 800-137, are
   1. Define an ISCM strategy.
   2. Establish an ISCM program.
   3. Implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting.
   4. Analyze the data collected, report findings, and determine the appropriate responses.
5. Respond to findings.
6. Review and update the monitoring program.

8. a. The steps in an ISCM program, according to NIST SP 800-137, are
   1. Define an ISCM strategy.
   2. Establish an ISCM program.
   3. Implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting.
   4. Analyze the data collected, report findings, and determine the appropriate responses.
   5. Respond to findings.
   6. Review and update the monitoring program.

9. c. The following are guidelines for internal, external, and third-party audits:
   - At minimum, perform annual audits to establish a security baseline.
   - Determine your organization’s objectives for the audit and share them with the auditors.
   - Set the ground rules for the audit, including the dates/times of the audit, before the audit starts.
   - Choose auditors who have security experience.
   - Involve business unit managers early in the process.
   - Ensure that auditors rely on experience, not just checklists.
   - Ensure that the auditor’s report reflects risks that the organization has identified.
   - Ensure that the audit is conducted properly.
   - Ensure that the audit covers all systems and all policies and procedures.
   - Examine the report when the audit is complete.

10. d. SOC 3 is the only SOC report that should be shared with the general public.

11. a. The steps in performing a penetration test are as follows:
   1. Document information about the target system or device.
   2. Gather information about attack methods against the target system or device. This includes performing port scans.
   3. Identify the known vulnerabilities of the target system or device.
4. Execute attacks against the target system or device to gain user and privileged access.

5. Document the results of the penetration test and report the findings to management, with suggestions for remedial action.

12. b. In black-box testing, or zero-knowledge testing, the testing team is provided with no knowledge regarding the organization’s network. In white-box testing the testing team goes into the testing process with a deep understanding of the application or system. In gray-box testing the testing team is provided more information than in black-box testing, while not as much as in white-box testing. Gray-box testing has the advantage of being nonintrusive while maintaining the boundary between developer and tester. Physical testing reviews facility and perimeter protections.

13. d. Fuzz testing is a dynamic testing tool that provides input to the software to test the software’s limits and discover flaws. The input provided can be randomly generated by the tool or specially created to test for known vulnerabilities. Interface testing evaluates whether an application’s systems or components correctly pass data and control to one another. It verifies whether module interactions are working properly and errors are handled correctly. Static testing analyzes software security without actually running the software. This is usually provided by reviewing the source code or compiled application. Test coverage analysis uses test cases that are written against the application requirements specifications.

14. a, b, c, d. Security professionals should consider the following factors when performing security testing:
   - Impact
   - Difficulty
   - Time needed
   - Changes that could affect the performance
   - System risk
   - System criticality
   - Security test availability
   - Information sensitivity level
   - Likelihood of technical failure or misconfiguration
15. a. Operating system fingerprinting is the process of using some method to determine the operating system running on a host or a server. By identifying the OS version and build number, a hacker can identify common vulnerabilities of that OS using readily available documentation from the Internet. A network discovery scan examines a range of IP addresses to determine which ports are open. This type of scan only shows a list of systems on the network and the ports in use on the network. It does not actually check for any vulnerabilities. By using key performance and risk indicators of security process data, organizations better identify when security risks are likely to occur. Key performance indicators allow organizations to determine whether levels of performance are below or above established norms. Key risk indicators allow organizations to identify whether certain risks are more or less likely to occur. Organizations should conduct internal, external, and third-party audits as part of any security assessment and testing strategy.
Index

ABAC (attribute-based access control), 510, 512
abstraction, 8, 661
acceptable use policy. See AUP
acceptance testing, 673, 696
access
administration, 477
aggregation, 522
asset security, 143-144
authentication, 480-507, 515-516
authorization, 508-514
control categories, 83-84
control processes, 475-476
denying, 702
IDaaS, 507
managing, 600
NAC devices, 435-436
Pearson Test Prep practice test engine, 714
physical/logical, 477-479
reviews, 516
third party, 72, 507
threats, 516-523
types, 84-87
access control, 645
matrices, 513
models, 508-510, 514
policies, 514
services, 196
access control lists. See ACLs
access points. See APs
accessibility, 310
accountability, 223, 505
accounting, 6
accounts
access reviews, 516
managing, 515-516, 551, 594
privileges, 595
revocation, 516
root, 488
accreditation, 217
Accreditation/Certification phase (SDLC), 674
ACID tests, 159
ACLs (access control lists), 346, 477-478, 514
acoustical detection systems, 643
Acquire/Develop stage (System Development Life Cycle), 669
acquired software, impact of, 696-697
acquisitions, 12, 121-123
active states, 290
active vulnerability scanners. See AVSs
ActiveX, 664-665
ACV (actual cost valuation), 631
Ad Hoc mode, 384
Address Resolution Protocol. See ARP
addresses
IP, 461
IPv4, 348
IPv6, 360, 363-372
logical, 347-353
MAC, 338, 352-353
physical, 347-353
Adleman, Leonard, 277
administration. See also managing
access, 477
passwords, 485-488
administrative controls, 85
administrative investigations, 581-582
administrative law, 39
Advanced Encryption Standard. See AES
advanced persistent threat. See APT
adware, 691
AES (Advanced Encryption Standard), 274
agent-based log reviews, 543-544
agentless log reviews, 543
agents, threats, 74, 138
aggregation, 158, 226, 362
Agile model, 679
AH (authentication header), 361
alarms, environmental, 320
ALE (annual loss expectancy), 79
algebraic attacks, 303
algorithms, 252
asymmetric, 268-269
MD2, 296
selecting, 262
SHA, 296
symmetric, 266-269, 275-276
3DES, 270-273
AES, 274
Blowfish, 275
DES, 270-273
Diffie-Hellman, 277
ECC, 278
El Gamal, 278
IDEA, 274
Knapsack, 279
RSA, 277
Skipjack, 274
Twofish, 275
zero-knowledge proof, 279
alignment, security functions, 9-11
analog signaling, 353
analysis
evidence, 569
media, 577
risk management, 73-90, 93-106, 695-696
assets, 73-74
vulnerabilities, 74
security, 553
source code tools, 688
test coverage, 549, 562
analytic attacks, 304
annual loss expectancy. See ALE, 79
antenna placements, 391
antenna types, 392
anti-malware, 437, 614, 693
antivirus applications, 614, 693
anycast addresses, IPv6, 368
APs (access points), 384, 408
APIs (application programming interfaces), 700-701
APIPA (Automatic Private IP Addressing), 352
applets, Java, 664
Application layer (Layer 7), 336-337
application programming interfaces. See APIs
applications
owners, 17
provisioning, 591
security, 246, 665-668
applied cryptography, 300

APT (advanced persistent threat), 523

architecture, 192

COBRA, 663
cryptography, 250
  features of, 256-257
  history of, 253-255
  life cycles, 261-262
  mathematics, 258-261
  NIST SP 800-175A and B, 257-258
  types, 262-269
databases, 155-156
firewalls, 403-404
ISO/IEC 42010:2011, 193
maintenance, 223
SOA, 664
system, 196-205
vulnerabilities, 224-230, 233-242

archiving, privacy, 168

ARP (Address Resolution Protocol), 343, 372, 454

AS (authentication server), 500

assemblers, 660

assembly languages, 660

assertions, 481

assessments
  controls, 89
disaster recovery, 636
effectiveness, 695-696
risk, 78. See also risk, management
security testing, 534-535
strategies, 533
vulnerabilities, 535-536

assets
  accessing, 477-479
  cloud computing, 591
costs, 78

information, 599
inventory, 590-591
managing, 599-603, 606-607
physical, 591
risk management, 73-74
security
  baselines, 169
custodians, 161
data access/sharing, 167
data classification, 146-160
data custodians, 143
data documentation, 143
data ownership, 143
data policies, 141-143
data protection methods, 171-172
data quality, 144
data retention, 164-165
data security, 166-172
data states, 166-167
  handling requirements, 172-173
  ownership, 160-161
privacy, 161-163, 168
private sector classification, 151-152
roles/responsibilities, 143-144
scoping, 170
standards selection, 170
tailoring, 170
virtual, 591

assurance, 185

asymmetric algorithms, 251, 268-269, 276
  Diffie-Hellman, 277
  ECC, 278
  El Gamal, 278
  Knapsack, 279
  RSA, 277
  zero-knowledge proof, 279
asynchronous, 251
asynchronous tokens, 488
Asynchronous Transfer Mode. See ATM
asynchronous transmissions, 354
ATM (Asynchronous Transfer Mode), 433
atomicity, 159
attacks, 76
cryptography, 301-305
networks, 451, 454-462
cabling, 451-453
components, 453-462
threat modeling, 120
time-of-check/time-of-use, 243
Web-based, 243
OWASP, 244
SAML, 244
XML, 244
attenuation, 452
attribute-based access control. See ABAC
attributes, 155, 512, 660
auditing, 6, 505, 585-587, 695
classification, 160
committees, 15
logs, 505
security, 535, 554-556, 563
services, 196
types of, 587
auditors, 17
AUP (acceptable use policy), 567
authentication, 256, 480, 486-496, 515-516
factors for, 484-493
implementing, 496-507
Kerberos, 499-500
Open System Authentication, 387
periods, 487
Shared Key Authentication, 387
authentication header. See AH
authentication server. See AS
Authenticode technology, 665
authorization, 257, 508-514, 609
autoconfiguration, IPv6, 360
Automatic Private IP Addressing. See APIPA
availability, 61, 632
avalanche effect, 252
AVSs (active vulnerability scanners), 538
awareness, 124-126, 553, 647
backdoors, 522, 699
backups
data, 624, 627, 632
hardware, 621
software, 621
storage, 626
systems, 600
types of, 625
verification data, 553
barriers, 641
base relation, 155
baseband, 355
Basel II, 49
baselines, 58, 169
BCPs (business continuity plans), 60, 62-68, 639-640
behavior, 661
behavioral systems, 491
Bell-LaPadula model, 189
best evidence, 575
best practices, software development security, 686-687
BGP (Border Gateway Protocol), 415
BIA (business impact analysis), 61, 65-68, 618
Biba model, 190
big data, 145
biometric technologies, 492-493
biometrics, 315
BIOS, 203
birthday attacks, 303, 518
bits
clocking, 354
host/networks, 349
black-box testing, 547
blacklisting, 613
blackouts, 319
blind spoofing attacks, 453
blind tests, 540
block ciphers, 267
Blowfish, 275
Bluetooth, 386
Board Briefing on IT Governance, 9
board of directors, 14
bollards, 641
bombing, 115
Boolean systems, 258
BOOP (bootstrap protocol), 373
Border Gateway Protocol. See BGP
botnets, 691
bottom-up approach, 31
boundary control services, 196
bounds, 183
breaches, 76
data, 44
Brewer-Nash (Chinese Wall) model, 192
bridges, 399
British Ministry of Defence Architecture Framework. See MODAF
broadband, 355
broadcast transmissions, 355
brownouts, 319
brute-force attacks, 302, 517
BSI (Build Security In), 687
budgets, security, 11
buffers, overflow, 520, 697
Build and Fix approach, 675
Build Security In. See BSI
building security controls, 645
bus topologies, 420
business cases, 10
business continuity plans. See BCPs
business impact analysis. See BIA
business interruption insurance, 632
business/mission ownership, 161
business process recovery, 620

C

CA (certificate authority), 279
cable communication connections, 443
cabling, 415
attacks, 451-453
coxial, 416
fiber optic, 418
twisted pair, 417-418
caching
DNS poisoning, 456
web, 404
Caesar cipher, 253
campus area networks. See CANs
CANs (campus area networks), 371
candidate keys, 156
capabilities, tables, 514
Capability Maturity Model Integration. See CMMI
capacitance detector, 643
CAPTCHA, 486
cardinality, 155
Carlisle Adams and Stafford Tavares. See CAST
Carrier Sense Multiple Access/Collision Avoidance. See CSMA/CA

Carrier Sense Multiple Access/Collision Detection. See CSMA/CD

CASE (common application service element), 337

CASE (Computer-Aided Software Engineering), 681

CAST (Carlisle Adams and Stafford Tavares), 275

categories, access control, 83-84

CBC-MAC (Cipher Block Chaining MAC), 298

CC (Common Criteria), 211-213

CCTA Risk Analysis and Management Method. See CRAMM

CCTV (closed-circuit television system), 643

CDMA (code division multiple access), 383

CDNs (content distribution networks), 438

CDP (Cisco Discovery Protocol), 413

cellular wireless, 383

Center for Internet Security. See CIS
central processing units. See CPUs
centralized access control, 478
certificate authority. See CA
certificate revocation list (CRL), 283
certificates, 280-281
certification, 217
clearing, 163, 607
chain of custody, 573
change management, 618, 674
channel service unit/data service unit. See CSU/DSU
characteristic factor authentication, 489-493
checklist tests, 638
chosen ciphertext attacks, 302
chosen plaintext attack, 302

CIA (confidentiality, integrity, and availability), 5-6, 61, 146, 182, 669

CIDR (Classless Inter-Domain Routing), 349

CIFS/SMB (Common Internet File System/Server Message Block), 377

CIP (critical infrastructure protection) plan, 64

Cipher-Based MAC (CMAC), 299

Cipher Block Chaining MAC (CBC-MAC), 298
ciphers, 263-269
ciphertext, 251
ciphertext-only attacks, 302
circuit-switching networks, 432
circumstantial evidence, 576

CIS (Center for Internet Security), 27
Cisco Discovery Protocol. See CDP
civil code law, 38
civil disobedience, 114
civil investigations, 582
civil law, 39

Clark-Wilson Integrity model, 190-191
classes, 349-350, 660
classification
    asset security, 146-160
    private sector, 151-152

Classless Inter-Domain Routing. See CIDR
Cleanroom model, 681
clearing, 163, 607
client-based system vulnerabilities, 224-225
clipping levels, 487, 614
clocking bits, 354
closed-circuit television system. See CCTV
closed systems, 182
cloud-based system vulnerabilities, 230, 233-237
laws/regulations, 34
privacy, 35
Component-Based Development method, 682, 710
Component Object Model. See COM
components, 196-205
attacks, 454-456
networks, 396, 403, 415, 424, 432
attacks, 453-462
hardware, 397-438
compromised states, 291
Computer-Aided Software Engineering. See CASE
computer crimes, 36-37, 44
Computer Ethics Institute, 52-53
Computer Fraud and Abuse Act (CFAA), 48
computer rooms, 311
Computer Security Act of 1987, 49
Computer Security Technology Planning Study, 694
computing platforms, 193-195
concealment ciphers, 263
conclusive evidence, 576
confidentiality, 148, 257
confidentiality, integrity, and availability. See CIA
configuration management, 592-593, 674
configuring
applications, 246
architecture, 196-205, 223
assets. See assets, security
auditing, 535
baselines, 169
business continuity, 58-68
capabilities, 219
capabilities.
encryption/decryption, 223
fault tolerance, 221
interfaces, 221
memory protection, 219-220
policy mechanisms, 222
TPM, 220-221
virtualization, 220
compliance, 33-34
laws/regulations, 34
privacy, 35
controls, 535-550, 562
cryptography, 267
data breaches, 44
device, 245
documentation, 54
baselines, 58
guidelines, 58
policies, 55-57
procedures, 57
processes, 57
standards, 57
domains, 502
DRM, 305-307
education, 126
e-mail, 300
endpoint, 437
engineering
closed/open systems, 182
design, 180-181
objects/subjects, 181
equipment, 321
evaluation models, 206-219
facility and site design, 307-323
geographical threats, 108-115
governance, 8-9, 94-95
control frameworks, 17-18, 21, 24-33
processes, 12-14
roles and responsibilities, 14-17
security function alignment, 9-11
import/export controls, 45, 49
Internet, 300
kernels, 694
keys, 285-293
laws/regulations, 35-43
life cycles, 31
logs, 545
message integrity, 293-296
models, 182, 188
   Bell-LaPadula model, 189
   Biba model, 190
   bounds, 183
   Brewer-Nash (Chinese Wall) model, 192
   CIA, 182
   Clark-Wilson Integrity model, 190-191
   computing platforms, 193-195
   confinement, 183
defense in depth, 185
goguen-Meseguer model, 192
   Graham-Denning model, 192
   Harrison-Ruzzo-Ullman model, 192
   ISO/IEC 42010:2011, 193
   isolation, 183
   Lipner model, 191
   modes, 183-185
   services, 196
   Sutherland model, 192
   types, 185-187
networks, 335, 382, 386, 403, 415, 424, 432, 441-443, 451, 454-462
   attacks, 451-462
   communication channels, 438-451
   components, 396-438
   converged protocols, 379-381
cryptography, 392-394
   Internet security, 394-396
   IP networking, 345-353
   IPv6, 357-369
   multilayer protocols, 378-379
   network transmission, 353-357
   OSI models, 335-338
   protocols, 372-378
   services, 376-377
   TCP/IP models, 340-345
types, 370-372
   wireless, 381-392
operations, 571-576, 579, 589-592, 595, 602, 605, 608, 611, 614, 617-619, 637
   asset management, 599-603, 606-607
   authorization, 609
   BCP, 639-640
   change management, 618
   concepts, 593
   configuration management, 592-593
   continuous monitoring, 588
detections, 612-617
disaster recovery, 633-636
eDiscovery, 585
   egress monitoring, 588-589
   forensic tools, 579-581
   IDSs, 587
incident management, 608-612
   industry standards, 582-584
   information life cycles, 596-597
   investigations, 566-579
   job rotation, 595
logging/monitoring, 585-587
   managing accounts, 594
   managing privileges, 595
   need to know/least privilege, 593
   patches, 617
   personal security, 645-647
   physical security, 640-644
   record retention, 596
   recovery strategies, 618-633
   resource protection, 597-599
resource provisioning, 589-591
sensitive information procedures, 596
separation of duties, 594
SIEM, 588
SLAs, 597
testing disaster recovery plans, 637-639
two-person controls, 596
types of investigations, 581-582
perimeters, 694
personnel, 68
compliance, 72
employee onboarding/offboarding, 71-72
employment agreements/policies, 70
biring, 69-70
job rotation, 73
privacy, 72
separation of duties, 73
third party access, 72
PKI, 279-285
policies, 693, 701
privacy, 45-52
process data, collecting, 550-551
backing up, 553
disaster recovery, 553
KRs, 552
management review, 551-552
managing accounts, 551
training, 553
professional ethics, 52-53
requirements, 123
risk management, 73-90, 93-106
assets, 73-74
vulnerabilities, 74
risks in acquisitions, 121-123
software development, 659-668, 700
API security, 700-701
coding guidelines, 697-700
impact of acquired software, 696-697
life cycles, 668-673
methods, 674-683
operation/maintenance, 684-686
secure coding, 701-702
security controls, 686-696
symmetric algorithms, 275
system architecture, 192
terms, 5
abstraction, 8
accounting, 6
auditing, 6
CLA, 5-6
data hiding, 8
default security posture, 7
defense-in-depth strategy, 7
encryption, 8
non-repudiation, 7
testing, 534-535, 553-556, 563
threat modeling, 115-121
training, 124-125, 647
trans-border data flow, 45
vulnerabilities, 224-230, 233-237
WLANs, 387-392
confusion, 252
consistency, 159
constrained data item (CDI), 191
contamination, 226
content-dependent access control, 158, 513
content distribution networks. See CDNs
contention methods, 426
context-dependent access control, 159, 513
contingency plans, 61
continuity of operations (COOP) plan, 63
continuous improvement, 89
continuous monitoring, 588
Continuous Monitoring as a Service. See CMaaS
control frameworks, NIST SP, 94-95
Control Objectives for Information and Related Technology. See COBIT
controls, 217
  access, 83-87, 475-476, 645
  assessments, 89
  asset security, 166-173
  compensative, 83
  corrective, 83
  detective, 84, 586
  deterrent, 84
  directive, 84
  import/export, 45, 49
  input/output, 616
  logical, 86
  physical, 87
  preventive, 84
security, 17-18, 21, 24-33, 562, 686, 700
  best practices, 686-687
  code repository security, 688
  environments, 687
  software effectiveness assessments, 695-696
  source code analysis tools, 688
  testing, 535-550
  threats, 688-694
selecting, 218-219
site and facility, 312-323
converged protocols, 379
  FCoE, 379
  iSCSI, 381
  MOPLS, 380
  MPLS, 381
  VoIP, 381
cookies, 396
COOP (continuity of operations), 63
copyrights, 42
corporate procedures, 321
corrective controls, 83
corroborative evidence, 576
COSO (Committee of Sponsoring Organizations), 28
costs, assets, 78
countermeasures, 75, 81, 138, 217
coupling, 662
cover channels, 694, 699
CPS (cyber-physical systems), 240
CPTED (Crime Prevention Through Environmental Design), 307
CPUs (central processing units), 197
crackers, 37
CRAMM (CCTA Risk Analysis and Management Method), 31
CRC (cyclic redundancy check), 354
credentials, 504
Crime Prevention Through Environmental Design (CPTED), 307
crime scenes, 572. See also investigations
criminal investigations, 582
criminal laws, 39
critical infrastructure protection plan, 63
criticality (data classification), 147
CRLs (certificate revocation lists), 283
cross-certification, 285
crosstalk, 452
cryptographic system vulnerabilities, 227
cryptography, 171, 250, 392
3DES, 270-273  
applied, 300  
attacks, 301-305  
email encryption, 393-394  
end-to-end encryption, 393  
features of, 256-257  
history of, 253-255  
Internet security, 394-396  
life cycles, 261-262  
link encryption, 392  
mathematics, 258-261  
NIST SP 800-175A and B, 257-258  
quantum, 394  
services, 196  
symmetric algorithms, 267  
types, 262-269  
cryptology, 252  
cryptoperiods, 287  
cryptosystem, 251  
CSF (Common Security Framework), 26  
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), 426, 429  
CSMA/CD (Carrier Sense Multiple Access/Collision Detection), 426, 428  
CSU/DSU (channel service unit/data service unit), 432  
custodians, asset security, 143, 161  
customary law, 39  
customizing exams, 715-716  
cyber crimes, 44  
cyber incident response plan, 64  
cyber-physical systems. See CPS  
Cybersecurity Framework (NIST), 552  
cybersquatting, 458  
cyclic redundancy check. See CRC  
DAC (discretionary access control), 509  
damage assessment teams, 635  
DAP (Directory Access Protocol), 498  
data  
access, 167-168  
audits, classification, 160  
backups, 624, 627, 632  
breaches, 44  
classification, asset security, 146-160  
collection, privacy, 163  
custodians, 16, 143  
databases  
architecture, 155-156  
classification, 155-159  
interface languages, 157  
locks, 159  
maintenance, 158  
threats, 158  
views, 159  
vulnerabilities, 226  
documentation, asset security, 145  
flow control, 225  
haven laws, 51  
hiding, 8, 661  
leakage, 589  
mining, 157  
owners, 16  
ownership, 143, 161  
policies, 141-143  
processors, 162  
protection methods, 171-172  
quality, 144  
recovery, 623  
remanence, 162-163  
at rest, 166
retention, 164-165
security, 166-172
states, 166-167
storage, 168
structures, 662
in transit, 167
in use, 167
warehousing, 157, 226
Data Link Layer (2), 338
DCOM (Distributed Component Object Model), 663
DDoS (distributed DoS) attacks, 457, 520
deactivated states, 291
decentralized access control, 478
decisions, evidence, 570
decoding, 252
decryption, 223, 251
dedicated security mode, 184
de-encapsulation, TCP/IP, 345
default security posture, 7
default to no access, 497
defense in depth, 7, 185, 702
degrees, 155
delaying intruders, 309
demilitarized zones (DMZs), 165
denial-of-service. See DoS attacks
denying access, 702
Department of Defense Architecture Framework. See DoDAF
deprovisioning, 516
DES (Digital Encryption Standard), 270-273
design. See also security
  accreditation/certification, 217
  applied cryptography, 300
  cryptography, 267
digital signatures, 299
DRM, 305-307
engineering, 180-181
closed/open systems, 182
objects/subjects, 181
evaluation models, 206-219
geographical threats, 108-115
keys, 285-293
message integrity, 293-299
network
  converged protocols, 379-381
  multilayer protocols, 378-379
  protocols, 375-378
  services, 376-377
  wireless, 381-392
networks, 335, 380-386, 403, 415, 424, 432, 441-462
attacks, 451-462
  communication channels, 438-451
  components, 396-438
  cryptography, 392-394
  Internet security, 394-396
  IP networking, 345-353
  IPv6, 357-369
  network transmission, 353-357
  OSI models, 335-338
  protocols, 372-375
  TCP/IP models, 340-345
  types, 370-372
policies, 165
security capabilities, 219
encryption/decryption, 223
fault tolerance, 221
interfaces, 221
memory protection, 219-220
policy mechanisms, 222
TPM, 220-221
virtualization, 220
security models, 182, 188
  Bell-LaPadula model, 189
  Biba model, 190
  bounds, 183
  Brewer–Nash (Chinese Wall) model, 192
  CIA, 182
  Clark–Wilson Integrity model, 190–191
  computing platforms, 193–195
  confinement, 183
  defense in depth, 185
  Goguen-Meseguer model, 192
  Graham-Denning model, 192
  Harrison-Ruzzo-Ullman model, 192
  ISO/IEC 42010:2011, 193
  isolation, 183
  Lipner model, 191
  modes, 183–185
  services, 196
  Sutherland model, 192
  types, 185–187
security policies, 701
symmetric algorithms, 275
system architecture, 192, 196–205
vulnerabilities, 224–230, 233–242
Design phase (SDLC), 672
destroyed phases, 291–292
destruction, 163, 173
detecting
  fires, 317
  incidents, 610–611
  intruders, 309
detective administrative control, 586
detective controls, 84
deterrent controls, 84
deterring criminal activity, 308
Develop phase (SDLC), 672
development, software, 659–668, 700
API security, 700–701
coding guidelines, 697–700
impact of acquired software, 696–697
life cycles, 668–683
operation/maintenance, 684–686
secure coding, 701–702
security controls, 686–696
deviations from standards, 615
device firmware, 204
devices
  access controls, 479
  authentication, 495–496
  firmware, 204
  hardware, 397–438
  NAC, 435–436
  security, 245
  tracking, 322
DHCP (Dynamic Host Configuration Protocol), 336, 373
dial-up connections, 441
dictionary attacks, 303, 517
differential cryptanalysis, 303
Diffie, Whitfield, 277
Diffie-Hellman algorithm, 277
diffusion, 252
digital certificates, 251, 280–281
Digital Encryption Standard. See DES
digital forensic tools, 579–581
digital identity guidelines (SP 800-63), 480
digital investigations, 566–579
Digital Rights Management. See DRM
digital signaling, 353
Digital Signature Standard. See DSS
digital signatures, 251, 299
Digital Subscriber Line. See DSL
direct evidence, 576
direct memory access. See DMA
direct sequence spread spectrum (DSSS), 382
directive controls, 84
Directory Access Protocol. See DAP
directory services, 498
disaster recovery, 58-59, 111, 553, 633-637
disaster recovery plan. See DRP
discovery, network scans, 536-537
discretionary access control. See DAC
disposal of media, 606
Dispose stage (SDLC), 670
disruptions, 59
distance vector, 413
distance vector protocols, 413
Distributed Component Object Model. See DCOM
distributed computing, 663
distributed DoS. See DDoS attacks
distributed platforms, 194
distribution facilities, 316
divestitures, 12
DMA (direct memory access), 201
DMCA (U.S. Digital Millennium Copyright Act) of 1998, 44
DMZs (demilitarized zones), 165
DNS (Domain Name System), 374
cache poisoning, 456
network attacks, 456-459
DNSSEC (Domain Name System Security Extensions), 457
documentation
asset security, 145
DRM, 306
evidence, 570
recovery, 623
reviews, 122
security, 54
disabilities, separation of, 797
Dynamic Host Configuration Protocol.
See DHCP

dynamic signature verification. See DSV
dynamic testing, 548

E

earthquakes, 109
eavesdropping, 452, 521
e-books, DRM, 307
ECC (Elliptic Curve Cryptosystem) algorithm, 278
Economic Espionage Act of 1996, 49
eDiscovery, 585
education, 124-126
effectiveness assessments, security, 11, 695-696
efficiency, transmission (IPv6), 362
egress monitoring, 588-589
eigenfaces, 491
EIGRP (Enhanced IGRP), 414
El Gamal algorithm, 278
electrical threats, 110
electromechanical systems, 642
electronic backup solutions, 625-626
Electronic Communications Privacy Act (ECPA) of 1986, 48
electronic protected health information (EPHI), 149
electronically stored information. See ESI
E-lines, 431
Elliptic Curve Cryptosystem. See ECC
email
attacks, 458
encryption, 393-394
security, 300
spoofing, 458
e-mail-pass-around code review, 547
emanations, 522
embedded devices, investigations, 578
embedded IPv4 unicast, 369
embedded systems, 195, 250
embedding, 663
emergency management, 646-647
employee onboarding/offboarding, 71-72
employees, privacy, 50
employment agreements/policies, 70
encapsulating security payload. See ESP encapsulation, 336, 345, 661-662
encoding, 252
encryption, 8, 223, 250, 321
email, 393-394
directory, 171, 300, 393
link, 392, 300
links, 171
end-to-end encryption, 171, 300, 393
endpoint authentication, 495-496
endpoint security, 437
engineering
accreditation/certification, 217
applied cryptography, 300
asymmetric algorithms. See asymmetric algorithms
cryptography, 250, 257-258, 267
features of, 256-257
history of, 253-255
life cycles, 261-262
mathematics, 258-261
types, 262-269
design, 180-181
closed/open systems, 182
objects/subjects, 181
digital signatures, 299
DRM, 305-307
evaluation models, 206-219
geographical threats, 108-115
keys, 285-293
message integrity, 293-299
PKI, 279-285
security capabilities, 219
  encryption/decryption, 223
  fault tolerance, 221
  interfaces, 221
  memory protection, 219-220
  policy mechanisms, 222
  TPM, 220-221
  virtualization, 220
security models, 182, 188
  Bell-LaPadula model, 189
  Biba model, 190
  bounds, 183
  Brewer-Nash (Chinese Wall) model, 192
  CIA, 182
  Clark-Wilson Integrity model, 190-191
  computing platforms, 193-195
  confinement, 183
  defense in depth, 185
  Goguen-Meseguer model, 192
  Graham-Denning model, 192
  Harrison-Ruzzo-Ullman model, 192
  ISO/IEC 42010:2011, 193
  isolation, 183
  Lipner model, 191
  modes, 183-185
  services, 196
  Sutherland model, 192
  types, 185-187
symmetric algorithms. See symmetric algorithms
system architecture, 192, 196-205
Enhanced IGRP. See EIGRP
Enigma machine, 255
enrollment, 282, 481
  biometrics, 492
  certificates, 282
Enterprise Risk Management. See ERM
Enterprise versions, 388
environmental alarms, 320
environmental security, 317-318
environments, software development
  security, 687
EPHI (electronic protected health information), 149
equipment rooms, 311
equipment security, 321
ERM (Enterprise Risk Management), 107
escalation, 551, 699
ESI (electronically stored information), 585
ESP (encapsulating security payload), 361
Ethernet 802.3 standard, 423
ethics, 52-53
EU (European Union) laws, 50-51
evacuation drills, 639
evaluation models
  CC, 211-213
  controls, selecting, 218-219
  controls/countermeasures, 217
  ITSEC, 209-211
  security implementation standards, 213-215
  TCSEC, 206-209
events
  managing, 608
  unusual, 615
evidence
  analyzing, 569
  best, 575
  chain of custody, 573
  circumstantial, 576
  collecting, 568-569
  collection, 574
conclusive, 576
corroborative, 576
decisions, 570
direct, 576
examining, 569
hearsay, 576
identifying, 568
opinion, 576
presenting findings, 569
preserving, 568-569
reporting, 570
secondary, 575
types of, 575
examining evidence, 569
exams
customizing, 715-716
memory tables, 717
Pearson Test Prep practice test engine, 713-715
review tools, 717
study plans, 717-718
updating, 716
exploits, 75
Exploratory Model, 681
explosions, 112
export controls, 45
exposure, 75
extended address spaces (IPv6), 360
Extensible Markup Language. See XML
extension headers, IPv6, 360
external security assessments, 535
external threats, 108-109
extranets, 370

development, 307-311
recovery, 628-629
redundancy, 631
security, 598
selection, 309
factoring attacks, 304
failover, 632
failsoft, 632
fault tolerance, 68, 221, 600, 607, 631
faults, 319
FCoE (Fibre Channel over Ethernet), 379
FDDI (Fiber Distributed Data Interface), 425
FDM (frequency division multiplexing), 355
FDMA (frequency division multiple access), 383
Federal Information Processing Standard. See FIPS
Federal Information Security Management Act (FISMA) of 2002, 49
Federal Intelligence Surveillance Act (FISA) of 1978, 48
Federal Privacy Act of 1974, 48
federated identity management, 502
federation (SP 800-63C), 481
fences, 640-642
FHSS (frequency hopping spread spectrum), 382
fiber cabling specifications, 419
Fiber Distributed Data Interface. See FDDI
fiber optic cabling, 418
Fibre Channel over Ethernet. See FCoE
File Transfer Protocol. See FTP
filters, MAC, 391
fingerprinting operating systems, 537
FIPS (Federal Information Processing Standard), 90-92
FIPS Publication 201-2, 504
fire, 112, 317-318
fire detection and suppression systems, 632
firewalls, 401, 436-438, 613
    architecture, 403-404
    rules, 346
    types, 401-403
firmware, 203-204
flooding, 110, 320
flow control, 343
foreign keys, 156
forensic investigations, 566-579
forensic procedures, 570
forensic processes, 584
forensic tools, 579-581
fraggle attacks, 455
Frame Relay, 432
Framework Core, 552
frameworks
    risk, 90, 93-106
    security controls, 17-18, 21, 24-33
fraud, 113
freeware, 43
frequency analysis, 303
frequency division multiple access. See FDMA
frequency division multiplexing. See FDM
frequency hopping spread spectrum. See FHSS
FTP (File Transfer Protocol), 374
FTPS (FTP Secure), 374
full-interruption tests, 639
full-knowledge tests, 540
functionality drills, 639
fuzz testing, 548
G

gates, 640-642
gateways, 401
Gather Requirements phase (SDLC), 671
GDPR (General Data Protection Regulation), 51-52
geographical threats, 108-115
glass entries, 315
global scope (IPv6), 369
global system for mobile communications (GSM), 383
goals, organizational, 10
Goguen-Meseguer model, 192
going dark, 44
governance
    control frameworks, 94-95
    security, 8-9
        control frameworks, 17-18, 21, 24-33
        processes, 12-14
        roles and responsibilities, 14-17
        security function alignment, 9-11
    third-party, 122-123
government, data classification, 152-153
Graham-Denning model, 192
Gramm-Leach-Bliley Act (GLBA) of 1999, 47
graphical passwords, 486
gray-box testing, 547
graylisting, 613
Green Book, 209
grid computing vulnerabilities, 237
groups, managing, 594
GSM (global system for mobile communications), 383
guaranteed delivery, 343
guest operating systems, 451
guidelines
  coding, 697-700
documentation, 58

H

hackers, 37
handling
  asset security, 172-173
evidence, 574
risk, 82. See also risk, management
hardening systems, 616
hardware, 397-438
  backups, 621
  investigations, 578-579
  redundancy, 607
  risks, 121
  security, 598
Harrison-Ruzzo-Ullman model, 192
hash, 251
hash MAC (HMAC), 298
hashing, 294
HAVAL, 297
headers
  IPv6, 360
  TCP, 341
  UDP, 341
Health Care and Education
  Reconciliation Act of 2010, 50
Health Insurance Portability and
  Accountability Act. See HIPAA
hearsay evidence, 576
heat, 320
Hellman, Martin, 277
hiding data, 661
hierarchical models, 156
hierarchical storage management. See HSM
  high availability, 632
  high cohesion, 662
  high-level languages, 660
High-Speed Serial Interface. See HSSI
higher-level recovery strategies, 619
hijacking, session, 461
HIPAA (Health Insurance Portability
  and Accountability Act), 149
hiring, 69-70
history
  media, 606
  passwords, 486
HITRUST, 26
HMAC (hash MAC), 298
honeynets, 614
honeyhops, 405, 614
hosts, bits, 349
hot sites, 628-629
HSM (hierarchical storage management), 605
HSSI (High-Speed Serial Interface), 434
HTTP (Hypertext Transfer Protocol), 336, 375
HTTPS (Hypertext Transfer Protocol Secure), 375
hubs, 398
human-caused disasters, 60
human-caused threats, 111-113
human resources, 622
humidity, 320
hurricanes, 109
HVAC, 320
hybrid ciphers, 269
hybrid protocols, 413
hybrid routing, 413
hybrid topologies, 422
Hypertext Transfer Protocol. See HTTP
Hypertext Transfer Protocol Secure. 
  See HTTPS
IAB (Internet Architecture Board), 52, 54
IAM (identity and access management)
   access control processes, 475-476
   authentication, 480-507, 515-516
   authorization, 508-514
   IDaaS, 507
   physical/logical access, 477-479
   third-party identity services, 507
   threats, 516-523
ICCs (integrated circuit cards), 489
ICMP (Internet Control Message Protocol), 343, 375
   attacks, 454
   redirects, 455
ICs (industrial control systems) vulnerabilities, 227-230
IDaaS (Identity as a Service), 507
IDEA (International Data Encryption Algorithm), 274
IDEAL model, 683
identification, implementing, 496-507.
   See also authentication
identifying
   evidence, 568
   threats, 119-120
identities
   managing, 515-516, 600
   proofing, 481
   theft, 519
identity governance and administration.
   See IGA
IDPS (intrusion detection and prevention system), 438
IDSs (intrusion detection systems), 405-407, 586-587, 612
IEC (International Electrotechnical Commission ), 18, 170
IEEE (Institute of Electrical and Electronics Engineers) standards
   802.11 standards, 382, 385
   802.11 techniques, 382
   802.11a standard, 385
   802.11ac standard, 385
   802.11b standard, 385
   802.11g standard, 385
   802.11n standard, 386
   802.11X standard, 389
IGA (identity governance and administration), 507
IGMP (Internet Group Management Protocol), 343, 376
IGRP (Interior Gateway Routing Protocol), 414
IKE (Internet Key Exchange) protocol, 361
IMAP (Internet Message Access Protocol), 376
Implement stage (System Development Life Cycle), 669
implementing
   authentication, 496-507
   authorization, 508-514
   data policies, 141-143
   IDaaS, 507
   risk management, 82
   third-party identity services, 507
import controls, 45
import/export controls, 49
incidents
   events, 608
   investigations, 609
   managing, 608, 611
   response teams, 609
Incremental model, 678
industrial control systems. See ICSs
industry standards, 34, 582-584
inference, 158, 226
information
access controls, 478
assets, 599
information flow models, 187
information life cycles, 153-154, 596-597
information security continuous monitoring. See ISCM
information security management system. See ISMS
information system contingency plan (ISCP), 64
Information Systems Audit and Control Association. See ISACA
Information Technology Infrastructure Library. See ITIL
Information Technology Security Evaluation Criteria. See ITSEC
infrared, 386
Infrastructure mode, 384
initialization vectors. See IVs
Initiate phase (System Development Life Cycle), 668-669
input validation, 699, 701
input/output (I/O), 616
devices, 202
structures, 202-203
instant messaging applications, 440
Institute of Electrical and Electronics Engineers. See IEEE
insurance, 631-632
intangible asset protection, 597-599, 602, 606
integrated circuit cards. See ICCs
Integrated Product and Process Development. See IPPD
Integrated Services Digital Networks. See ISDNs
integration testing, 673
integrity, 190, 196, 257, 293-299
integrity verification procedure (IVP), 191
intellectual property law, 40
interface-local scope (IPv6), 369
interfaces, 221
APIs, 700-701
HSSI, 434
languages, 157
testing, 549-550, 562
Interior Gateway Routing Protocol. See IGRP
Intermediate System to Intermediate System. See IS-IS
internal audits, 554-556, 563
internal protection, 43
internal security assessments, 535
internal security controls, 645
internal threats, 108-109
International Data Encryption Algorithm. See IDEA
International Electrotechnical Commission. See IEC
International Information Systems Security Certification Consortium. See ISC
International Organization on Computer Evidence. See IOCE
International Organization for Standardization. See ISO
Internet Architecture Board. See IAB
Internet Control Message Protocol. See ICMP
Internet Group Management Protocol. See IGMP
Internet Key Exchange protocol. See IKE protocol
Internet layer, 343
Internet Message Access Protocol. See IMAP
Internet of Things. See IoT
Internet Protocol. See IP
Internet security, 300, 394-396
Internet Small Computer System Interface. See iSCSI
interpreters, 660
interviewing (investigations), 573
intranets, 370
intrusion detection and prevention system. See IDPS
intrusion detection systems. See IDSs
intrusion prevention systems. See IPSs
inventories, 322, 590-591
investigations, 566, 571-572, 579
digital/forensic, 566-579
evidence, 574-576
incidents, 609
techniques, 573
types of, 581-582
IOCE (International Organization on Computer Evidence), 571
I/O (input/output)
devices, 202
structures, 202-203
IoT (Internet of Things) vulnerabilities, 238-242
IP (Internet Protocol), 343
addresses, 461
networks, 345
  addressing, 347-353, 363-369
  common TCP/UDP ports, 346
  IPv6, 357-363
  network transmission, 353-357
types, 370-372
IPPD (Integrated Product and Process Development), 685
IPS (intrusion prevention system), 407, 612
IPsec (IP security), 361
IPv4 (IP version 4) addresses, 348
threats, 362-363
IPv6 (IP version 6), 357
addressing, 363-369
major features of, 360-361
network types, 370-372
NIST Special Publication (SP) 800-119, 358-360
threats, 362-363
ISACA (Information Systems Audit and Control Association), 9
ISC (International Information Systems Security Certification Consortium), 52-53
ISCM (information security continuous monitoring), 550-551
ISCP (information system contingency plan), 64
iSCSI (Internet Small Computer System Interface), 381
ISDNs (Integrated Services Digital Networks), 441
IS-IS (Intermediate System to Intermediate System), 415
ISMS (information security management system), 19
ISO (International Organization for Standardization), 18, 335, 570
ISO 9001:2015, 682
ISO/IEC 15288:2015, 181
ISO/IEC 27000 series, 18, 687
ISO/IEC 27001:2013, 214
ISO/IEC 27002:2013, 215
ISO/IEC 27005:2011, 105
isolation, 159, 183
issue-specific security policies, 57
ITGI (IT Governance Institute), 9
ITIL (Information Technology Infrastructure Library), 9, 28
ITSEC (Information Technology Security Evaluation Criteria), 209-211
IVs (initialization vectors), 268

J

JAD (Joint Analysis Development) model, 681
Java applets, 664
Java Platform, Enterprise Edition (Java EE), 664
JDBC (Java Database Connectivity), 157
job rotation, 73, 595
Joint Analysis Development. See JAD model

K

KDC (Key Distribution Center), 500
Kerberos, 499-500
Kerckhoff’s Principle, 255
kernels, security, 694
key clustering, 251
Key Distribution Center. See KDC
key-encrypting keys, 286
key performance indicators, 552, 563
key risk indicators. See KRI
keys, 251, 261-262, 285-293
keyspace, 252
Knapsack algorithm, 279
knowledge factor authentication, 485-489, 515
known plaintext attacks, 302
KRI (key risk indicators), 552

L

Label Distribution Protocol. See LDP
labeling, 172, 606
LANs (local area networks), 351, 370
languages
- assembly, 660
- high-level, 660
- machine, 659
- very-high-level, 660
large-scale parallel data systems vulnerabilities, 236-237
laws, 34-35
- computer crimes, 36-37
- EU, 50-51
- major legal systems, 38-43
- privacy, 47-51
Layer 3 switches, 400
Layer 4 switches, 400
layered defense models, 307
layers
- Data Link (2), 338
- Network (3), 338
- Physical (1), 339
- Presentation (6), 337
- Session (5), 337
- TCP/IP, 341-345
- Transport (4), 337
LDAP (Lightweight Directory Access Protocol), 376
LDP (Label Distribution Protocol), 376
least privilege principle, 497, 593, 702
legal teams, 635
legally permissible, 574
length of passwords, 487
licenses, 43
licensing law, 40
life cycles, 481
certificates, 281
cryptography, 261-262
information, 153-154, 596-597
passwords, 486
provisioning, 514-515
managing

security, 31
software development, 668-673

lighting
security, 643
types of, 644

Lightweight Directory Access Protocol. See LDAP

limiting data collection, 163-164
linear cryptanalysis, 303
link encryption, 392-393, 300
Link layer, TCP/IP models, 345
link-local scope (IPv6), 369
link state, 413
link state protocols, 413
linking, 663
links, encryption, 171
Linux, password storage, 488
Lipner model, 191
LLC (logical link control), 338
load balancing, 633
local area networks. See LANs
location factor authentication, 494
locks, 313-315, 323
databases, 159
doors, 312
logging, 585, 695
audits/reviews, 585-587
continuous monitoring, 588
egress monitoring, 588-589
IDSs, 587
SIEM, 588
types of logs, 586
logic bombs, 691
logical access to assets, 477-479
logical addressing, 347-353
logical controls, 86
logical link control. See LLC
logical operations, 259-260
logs, 541
audit, 505
configuring, 545
NIST SP 800-92, 542-545, 556
low humidity, 320
Lucifer project, 256

M

MAC (mandatory access control), 509
MAC (media access control)
addresses, 338, 352-353
filters, 391
flooding attacks, 454
MAC (Message Authentication Code), 297
machine languages, 659
mainframe/thin client platforms, 194
maintenance
architecture, 223
databases, 158
hooks, 242
software development, 684-686
major legal systems, 38-43
malware, 521, 614, 689, 693
MAN (metropolitan area network), 370
man-in-the-middle (MITM) attacks, 454
managing
access, 475-523
accounts, 515-516, 551, 594
assets, 145, 590-591, 599-603, 606-607
change management, 618, 674
configuration management, 592-593
controls, 85
credentials, 504
data policies, 141-143
identities, 515-516
incidents, 608, 611
authorization, 609
events, 608
investigations, 609
mitigation, 611
recovery, 612
remediation, 612
reporting, 611
responses, 610-611
reviewing, 612
keys, 261-262, 285-293
lifecycles, 481
media, 601
memory, 205
networks, 607
passwords, 485-488
patch management, 617
privileges, 595
reviews, 551-552
risk, 73-90, 93-106
assets, 73-74
vulnerabilities, 74
responsibilities, 14
security
abstraction, 8
baselines, 58
business continuity, 58-68
compliance, 33-35, 72
control framework, 17-18, 21, 24-33
data breaches, 44
data hiding, 8
default security posture, 7
defense-in-depth strategy, 7
documentation, 54-57
employee onboarding/offboarding, 71-72
employment agreements/policies, 70
encryption, 8
governance, 8-11
guidelines, 58
import/export controls, 45
job rotation, 73
laws/regulations, 35-43
personnel, 68-70
privacy, 45-52, 72
procedures, 57
processes, 12-14, 57
professional ethics, 52-53
roles and responsibilities, 14-17
separation of duties, 73
standards, 57
terms, 5-7
third party access, 72
trans-border data flow, 45
sessions, 503
vulnerabilities, 616
mandatory access control. See MAC
mantraps, 313
marking, 172
masking passwords, 487
massive multiple input multiple output (MIMO), 383
mathematics, cryptography, 258-261
matrix-based models, 186
maturity methods, 674-683
MD2 message digest algorithms, 296
mean time between failure. See MTBF
mean time to repair. See MTTR
measurements, 89
media
analysis, 577
disposal, 606
history, 606
labeling/storage, 606
management, 601
sanitizing, 606
storage facilities, 317
media access control. See MAC, addresses
meet-in-the-middle attacks, 304
memorized secrets, 481, 484
memory, 199-201
    cards, 489
    managing, 205
    protection, 219-220
    tables (exams), 717
memory cards, 489
mesh topologies, 421
Message Authentication Code. See MAC
message integrity, 293-299
methods, 156, 661
    contention, 426
    data protection, 171-172
    maturity, 675
    software development, 674-683
metrics, security, 11
metropolitan area networks. See MANs
MFA (multi-factor authentication), 481
middleware, 194
military, data classification, 152-153
MIME (Multipurpose Internet Mail Extension), 394
MIMO (massive multiple input multiple output), 383
MIPv6 (Mobile IPv6), 361
mirrored sites, 630
missions, organizational, 10
misuse case testing, 549
mitigation, 523, 611, 695
MITM (man-in-the-middle) attacks, 454
mixed law, 40
MLD (Multicast Listener Discovery), 359
mobile application security, 665-668
mobile code, 438, 520, 664, 700
mobile computing, 195
mobile devices, 408, 412
Mobile IPv6. See MIPv6
mobile system vulnerabilities, 244-248
    application security, 246
    device security, 245
    NIST SP 800-164, 248-249
mobile wireless, 383
MODAF (British Ministry of Defence Architecture Framework), 22
models
access control, 508-510, 514
COM, 663
databases, 155-156
DCOM, 663
evaluation, 206-219
layered defense, 307
OSI, 335-338
security, 182, 188
    Bell-LaPadula model, 189
    Biba model, 190
    bounds, 183
    Breuer-Nash (Chinese Wall) model, 192
    CLA, 182
    Clark-Wilson Integrity model, 190-191
    computing platforms, 190-191
    confinement, 183
    defense in depth, 185
    Goguen-Meseguer model, 192
    Graham-Denning model, 192
    Harrison-Ruzzo-Ullman model, 192
    ISO/IEC 42010:2011, 193
    isolation, 183
    Lipner model, 191
    modes, 183-185
    services, 196
    Sutherland model, 192
    types, 183-187
STRIDE, 117
TCP/IP, 340-345
threats, 115-121
VAST, 118

modes, 183-185, 715-716

Modified Prototype Model. See MPM

modifying, 283

applications, 246
architecture, 196-205, 223
assets. See assets, security
auditing, 535
baselines, 169
business continuity, 58-68
capabilities, 219
capabilities. See encryption/decryption, 223
capabilities. See fault tolerance, 221
capabilities. See interfaces, 221
capabilities. See memory protection, 219-220
capabilities. See policy mechanisms, 222
capabilities. See TPM, 220-221
capabilities. See virtualization, 220
capabilities. See compliance, 33-34
capabilities. See laws/regulations, 34
capabilities. See privacy, 35
capabilities. See controls, 535-550, 562
capabilities. See cryptography, 267
capabilities. See data breaches, 44
capabilities. See device, 245
capabilities. See documentation, 54
capabilities. See baselines, 58
capabilities. See guidelines, 58
capabilities. See policies, 55-57
capabilities. See procedures, 57
capabilities. See processes, 57
capabilities. See standards, 57
domains, 502
DRM, 305-307
education, 126
e-mail, 300
data breaches, 44
devices, 245
documentation, 54
documentation. See baselines, 58
documentation. See guidelines, 58
documentation. See policies, 55-57
documentation. See procedures, 57
documentation. See processes, 57
documentation. See standards, 57
domains, 502
DRM, 305-307
isolation, 183
Lipner model, 191
modes, 183-185
services, 196
Sutherland model, 192
types, 185-187
networks, 335, 382, 386, 403, 415, 424, 432, 441-443, 451, 454-462
attacks, 451-462
communication channels, 438-451
components, 396-438
converged protocols, 379-381
cryptography, 392-394
Internet security, 394-396
IP networking, 345-353
IPv6, 357-369
multilayer protocols, 378-379
network transmission, 353-357
OSI models, 335-338
protocols, 372-378
services, 376-377
TCP/IP models, 340-345
types, 370-372
wireless, 381-392
operations, 571-576, 579, 589-592, 595, 602, 605, 608, 611, 614, 617-619, 637
asset management, 599-603, 606-607
authorization, 609
BCP, 639-640
change management, 618
concepts, 593
configuration management, 592-593
continuous monitoring, 588
detections, 612-617
disaster recovery, 633-636
eDiscovery, 585
egress monitoring, 588-589
forensic tools, 579-581
IDSs, 587
incident management, 608-612
industry standards, 582-584
information life cycles, 596-597
investigations, 566-579
job rotation, 595
logging/monitoring, 585-587
managing accounts, 594
managing privileges, 595
need to know/least privilege, 593
patches, 617
personal security, 645-647
physical security, 640-644
record retention, 596
recovery strategies, 618-633
resource protection, 597-599
resource provisioning, 589-591
sensitive information procedures, 596
separation of duties, 594
SIEM, 588
SLAs, 597
testing disaster recovery plans, 637-639
two-person controls, 596
types of investigations, 581-582
perimeters, 694
personnel, 68
compliance, 72
employee onboarding/offboarding, 71-72
employment agreements/policies, 70
hiring, 69-70
job rotation, 73
privacy, 72
separation of duties, 73
third party access, 72
PKI, 279-285
policies, 693, 701
privacy, 45-52
process data, collecting, 550-551
  backing up, 553
  disaster recovery, 553
  KPIs, 552
  management review, 551-552
  managing accounts, 551
  training, 553
professional ethics, 52-53
requirements, 123
risk management, 73-90, 93-106
  assets, 73-74
  vulnerabilities, 74
risks in acquisitions, 121-123
software development, 659-668, 700
  API security, 700-701
  coding guidelines, 697-700
  impact of acquired software, 696-697
  life cycles, 668-673
  methods, 674-683
  operation/maintenance, 684-686
  secure coding, 701-702
  security controls, 686-696
symmetric algorithms, 275
system architecture, 192
terms, 5
  abstraction, 8
  accounting, 6
  auditing, 6
  CA, 5-6
  data hiding, 8
  default security posture, 7
  defense-in-depth strategy, 7
  encryption, 8
  non-repudiation, 7
testing, 534-535, 553-556, 563
threat modeling, 115-121
training, 124-125, 647
trans-border data flow, 45
vulnerabilities, 224-230, 233-237
WLANs, 387-392
modulo function, 260
MOM (motive, opportunity, and means), 572
monitoring, 89, 585
  accountability, 505
  audits/reviews, 585-587
  continuous, 588
  egress, 588-589
  IDSs, 587
  ISCM, 550
  personnel, 646
  services, 196
  SIEM, 588
  special privileges, 595
  synthetic transactions, 546
motive, opportunity, and means. See MOM
movies, DRM, 306
MPLS (Multiprotocol Label Switching), 380
MPM (Modified Prototype Model), 678
MTBF (mean time between failure), 608
MTTR (mean time to repair), 608
multicast addresses, IPv6, 368
Multicast Listener Discovery. See MLD
multicast transmissions, 355
multi-factor authentication. See MFA
multilayer protocols, 378-379
multilevel lattice models, 186
multilevel security mode, 184
multimedia collaboration, 439
multiprocessing, 199
Multitopic Control Switching. See MPLS
Multipurpose Internet Mail Extension. See MIME
multi-state systems, 199
multitasking, 198
music, DRM, 306

N

NAC (network access control) devices, 435-436
NAS (network-attached storage), 605
NAT (network address translation), 351, 376
National Information Assurance Certification and Accreditation Process. See NIACAP
National Institute of Standards and Technology. See NIST
natural access control, 308
natural disasters, 60
natural territories reinforcement, 308
natural threats, 109
near field communication. See NFC
Neighbor Discovery, 361
Nessus, 538
NetBIOS (Network Basic Input/Output System), 376
network access control devices. See NAC devices
network address translation. See NAT
network-attached storage. See NAS
Network Basic Input/Output System. See NetBIOS
network discovery scans, 536-537
Network File System. See NFS
Network Layer (3), 338
network models, 156
networks
design, 335, 380-382, 386, 403, 415, 424, 432, 441-443, 451, 454-462
attacks, 451-462
communication channels, 438-451
components, 396-438
converged protocols, 379-381
cryptography, 392-394
Internet security, 394-396
IP networking, 345-353
IPv6, 357-369
multilayer protocols, 378-379
network transmission, 353-357
OSI models, 335-338
protocols, 372-378
services, 376-377
TCP/IP models, 340-345
types, 370-372
wireless, 381-392
investigations, 578
managing, 607
routing, 412-413
technologies, 423-424, 432
testing, 536
vulnerability scans, 538
NFC (near field communication), 386
NFS (Network File System), 377
NIACAP (National Information Assurance Certification and Accreditation Process), 217
NIST Framework for Improving Critical Infrastructure Cybersecurity, 103-105
NIST Interagency Report (NISTIR) 7924, 281
NIST (National Institute of Standards and Technology), 9, 90, 147, 170, 570-571
SP (Special Publication), 94-95
SP 800-2, 504
SP 800-12 Rev. 1, 24
SP 800-16 Rev. 1, 24
SP 800-18 Rev. 1, 24
SP 800-30 Rev. 1, 24, 101
SP 800-34 Rev. 1, 24, 62-63, 618
SP 800-35, 24
SP 800-36, 24
SP 800-37, 90, 99-101
SP 800-37 Rev. 1, 24
SP 800-39, 24, 102
SP 800-50, 24
SP 800-53 Rev. 4, 24, 90, 149
SP 800-53A Rev. 4, 24, 90
SP 800-55 Rev. 1, 24
SP 800-57, 285
SP 800-60, 90, 93
SP 800-60 Vol. 1 Rev. 1, 24, 94
SP 800-61 Rev. 2, 25
SP 800-63, 481-482
  authentication, 480
  passwords, 482-484, 487
SP 800-66
  Risk Management Framework (RMF), 151
  Security Rule, 151
SP 800-82 Rev. 2, 25, 228
SP 800-84, 25
SP 800-86, 25, 583-584
SP 800-88 Rev. 1, 25
SP 800-92, 25, 542-556
SP 800-101 Rev. 1, 25
SP 800-115, 25
SP 800-119, 358-360
SP 800-122, 25, 147, 149
SP 800-123, 25
SP 800-124 Rev, 25, 408
SP 800-137, 25, 90, 550-551
SP 800-144, 25, 234
SP 800-145, 25, 231
SP 800-146, 25
  benefits of IaaS deployments, 236
  benefits of PaaS deployments, 236
  benefits of SaaS deployments, 235
  cloud computing, 235
  concerns of SaaS deployments, 236
SP 800-150, 25
SP 800-153, 25
SP 800-154, 25, 118
SP 800-160, 25, 90, 96-98, 181
SP 800-161, 25
SP 800-162
  ABAC, 511-512
  subject attributes, 512
SP 800-163, 26, 665, 667-668
SP 800-164, 26
SP 800-167, 26
SP 800-175A and B, 26, 257-258
SP 800-181, 26
SP 800-183, 26
  no access, defaults to, 497
  noise, 452
  non-blind spoofing attacks, 453
  nonce, 260
  non-interference models, 186
  non-repudiation, 7, 257
  no-operation instructions. See NOPs
  NOPs (no-operation instructions), 697
  normalization, 156-157
  numeric passwords, 486

Object Linking and Embedding.
  See OLE

object-oriented models, 156
object-oriented programming. See OOP
object-relational models, 157
objectives, organizational, 10
objects, 181, 660, 700
occupant emergency plan (OEP), 64
OCSP (Online Certificate Status Protocol), 284
OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), 28
ODBC (Open Database Connectivity), 157
OEP (occupant emergency plan), 64
OFDM (orthogonal frequency division multiplexing), 382
OFDMA (orthogonal frequency division multiple access), 383
offline, accessing Pearson Test Prep practice test engine, 714
OLE (Object Linking and Embedding), 663
OLE DB (Object Linking and Embedding Database), 157
OLTP (Online Transaction Processing), 159
one-time pads, 264
one-way function, 252, 260
one-way hash, 294
online, accessing Pearson Test Prep practice test engine, 714
Online Certificate Status Protocol. See OCSP
Online Transaction Processing. See OLTP
onsite assessments, 122
on-time passwords, 486
OOP (object-oriented programming), 660-661
Open Database Connectivity. See ODBC
Open Group Architecture Framework. See TOGAF
Open Group Security Forum, 498
Open Shortest Path First. See OSPF
Open Source Security Testing Methodology Manual. See OSSTMM
Open System Authentication, 387
open systems, 182
Open Systems Interconnection models. See OSI models
Open Web Application Security Project. See OWASP
Operate/Maintain stage (System Development Life Cycle), 669
operating systems, 204
fingerprinting, 537
guest, 451
operational phases, 292
Operationally Critical Threat, Asset and Vulnerability Evaluation. See OCTAVE
operations
concepts, 593-595
information life cycles, 596-597
job rotation, 595
managing accounts, 594
managing privileges, 595
need to know/least privilege, 593
record retention, 596
sensitive information procedures, 596
separation of duties, 594
SLAs, 597
two-person control, 596
disaster recovery, 633-637
eDiscovery, 585
industry standards, 582-584
investigations, 566, 571-576, 579
civil, 582
criminal, 582
digital/forensic, 566-579
forensic tools, 579-581
operations/administrative, 581-582
regulatory, 582
types of, 581-582
logging/monitoring, 585
   audits/reviews, 585-587
   continuous monitoring, 588
   egress monitoring, 588-589
   IDSs, 587
   SIEM, 588
personal security, 645-647
physical security, 640-644
recovery
   BCP, 639-640
   strategies, 618-633
   testing plans, 637-639
resource provisioning, 589-592
   asset inventory, 590-591
   configuration management, 592-593
resources, 602, 605, 608, 611, 614, 617
   asset management, 599-603, 606-607
   change management, 618
   incident management, 608-612
   patch management, 617
   protection, 597-599
   threat prevention, 612-617
software development, 684-686
operators, 259-260
opinion evidence, 576
optimizing, 89
Orange Book, 206, 615, 694
organizational code of ethics, 54
organizational security policies, 56
organizational strategies, 10
orthogonal frequency division multiple access (OFDMA), 383
orthogonal frequency division multiplexing (OFDM), 382
OSI (Open Systems Interconnection) models, 335-338
OSPF (Open Shortest Path First), 414
OSSTMM (Open Source Security Testing Methodology Manual), 106
outages, 66, 319
over-the-shoulder code review, 547
overflow buffers, 520, 697
OWASP (Open Web Application Security Project), 244, 687
ownership
   asset security, 143, 160-161
   factor authentication, 488-489

P

packet creation, 336
packet-switching networks, 432
pair programming code review, 547
PAN (personal area network), 372
parallel tests, 639
paraphrase passwords, 486
parity information, 602
partial-knowledge tests, 540
passing tokens, 430
passive infrared (PIR) systems, 642
passive vulnerability scanners. See PVSs
passwords
   managing, 485-488
   NIST Special Publication (SP) 800-63, 481-484, 487
   threats, 517
PASTA methodology, 117
PAT (port address translation), 351, 377
patch management, 617
patch panels, 397
patent law, 40
Path Maximum Transmission Unit Discovery. See PMTUD
paths, trusted, 616
patrol force, 644
PBX (private branch exchange), 405, 434
PCI DSS Version 3.2, 216
Pearson Test Prep practice test engine, 713-715
customizing, 715
memory tables, 717
review tools, 717
study plans, 717-718
updating, 716
peer-to-peer computing vulnerabilities, 237
penetration testing, 539-545
perimeter intrusion detection, 642
perimeter security, 640, 694
periodic reviews, 126
permissions, 508
personal area networks. See PAN
personal firewalls, 438
Personal Information Protection and Electronic Documents Act (PIPEDA), 49
personal security, 645-647
Personal versions, 388
Personally identifiable information. See PII
personnel, 68
compliance, 72
disaster recovery, 634
employee onboarding/offboarding, 71-72
employment agreements/policies, 70
hiring, 69-70
job rotation, 73
monitoring, 646
personal security, 646-647
privacy, 72
separation of duties, 73
third party access, 72
personnel components (business continuity), 62
personnel testing, 536
PGP (Pretty Good Privacy), 393
pharming, 518-519
PHI (protected health information), 149-151
phishing, 459, 518-519
photoelectric systems, 643
photometric systems, 643
physical access to assets, 477-479
physical addressing, 347-353
physical assets, 591
physical controls, 87
Physical layer (1), 339
physical security, 308, 640-644
physical testing, 536
physiological systems, 490
PII (Personally Identifiable Information), 46, 147
ping of death, 455
ping scanning, 456
pipe systems, 318
PIR (passive infrared) systems, 642
piracy, 43
PKI (public key infrastructure), 279-285
plain old telephone service. See POTS
plaintext, 251
Plan/Initiate Project phase (SDLC), 671
planning
BCP, 639-640
business contingency, 62-65
recovery, 637-639
study plans, 717-718
PMTUD (Path Maximum Transmission Unit Discovery), 362
Point-to-Point-Protocol. See PPP
policies
access control, 514
AUP, 567
compliance, 72
data, 141-143
design, 165
employee onboarding/offboarding, 71-72
employment, 70
mechanisms, 222
privacy, 72
provisioning, 515
reviews, 122
risk management, 77
security, 55-57, 693, 701
third party, 72
politically motivated threats, 114-115
polling, 430
polyinstantiation, 159, 662
polymorphism, 661
POP (Post Office Protocol), 377
port address translation. See PAT
portable media devices, 322
ports
  common TCP/UDP, 346
  scanning, 461
Post Office Protocol. See POP
post-operational phases, 292
potential attacks, 120
POTS (plain old telephone service), 434
power
  conditioners, 320
  levels, 391
  redundancy, 631
  supplies, 319
PPP (Point-to-Point-Protocol), 433
pre-activation states, 290-291
Presentation Layer (6), 337
presenting findings (evidence), 569
preservation, 574
preserving evidence, 568-569
Pretty Good Privacy. See PGP
preventing
  access control threats, 523
  threats, 612-617
  unauthorized access, 587
preventive controls, 84
preventive measures against threats, 614
primary keys, 156
primary memory, 201
principles
  of least privilege, 222
  security governance, 94-95
privacy, 45-52
  asset security, 161-163, 168
  cloud-based systems, 234
  compliance, 35
  import/export controls, 49
  personnel, 72
private authorization keys, 287
private branch exchange. See PBX
private ephemeral key-agreement keys, 287
private IP addresses, 350
private key-transport keys, 286
private keys, 285-286
private sector classification, 151-152
private static key-agreement keys, 287
privileges, 508
procedures
  documentation, 57
  forensic, 570, 579-581
  incident responses, 610-611
process data (security), collecting, 550
  backing up, 553
  disaster recovery, 553
  KRI, 552
  management review, 551-552
  managing accounts, 551
NIST SP 800-13, 550-551
training, 553
processes
access, 475-476
critical, 66
documentation, 57
forensic, 584
remediation, 121
review, 122
security, 12-14
states, 199
processors, privacy, 162
professional ethics, 52-53
programming languages, 659
proof of identity processes, 503
properly identified, 574
proprietary data, 151
protected health information. See PHI
protecting resources, 597-599, 602, 605, 608
protection domains, 503
protocols, 336, 372
ARP, 343, 372, 454
BGP, 415
BOOTP, 373
CDP, 412
CIFS/SMB, 377
converged, 379
FCoE, 379
iSCSI, 381
MPLS, 380-381
VoIP, 381
DAP, 498
DHCP, 336, 373
DNS, 374, 456
FTP, 374
FTPS, 374
HTTP, 336, 375
HTTPS, 375
ICMP, 343, 375, 454-455
IGMP, 343, 376
IGRP, 414
IKE, 361
IMAP, 376
IP, 343-353
IPv4, 362-363
IPv6, 357
addressing, 363-369
major features of, 360-361
network types, 370-372
NIST Special Publication (SP) 800-119, 358-360
threats, 362-363
Kerberos, 499-500
LDAP, 376
LDP, 376
multilayer, 378-379
POP, 377
PPP, 433
RARP, 372
remote authentication, 448
RIP, 414
SFTP, 374
S-HTTP, 375
SMTP, 377, 498
SNMP, 377, 544
SSL, 378
TCP, 341
TCP/IP, 340-345
TFTP, 374
TLS, 378
UDP, 341
VRRP, 414
prototyping, 677

provisioning
- account revocation, 516
- life cycles, 514-515
- resources, 589-592
  - asset inventory, 590-591
  - configuration management, 592-593

proxy servers, 404, 436

PSTN (public switched telephone network), 434

public authorization keys, 287

public ephemeral key-agreement keys, 287

public IP addresses, 350

public key infrastructure. See PKI

public key-transport keys, 286

public keys, 285-286

public static key-agreement keys, 287

public switched telephone network. See PSTN

purging data, 163, 607

PVSs (passive vulnerability scanners), 538

Q

QoS (Quality of Service), 361, 633

qualitative risk management, 80

quality of asset security, 144

Quality of Service. See QoS

Qualys, 538

quantitative risk analysis, 79

quantum cryptography, 394

quarantines, 436

R

RA (registration authority), 279

RAD (Rapid Application Development) model, 680

RADIUS (Remote Authentication Dial-In User Service), 447

RAID (Redundant Array of Inexpensive Discs), 601-603, 632

Rainbow Series, 206

rainbow table attacks, 518

random access devices, 202

ransomware, 304, 462, 521, 692

Rapid Application Development. See RAD model

RARP (Reverse ARP), 372

RBAC (role-based access control), 510, 512


RDBMSs (relational database management systems, 155

read-through tests, 638

real user monitoring. See RUM

reboots, 615

reciprocal agreements, 630

records, 155, 596

recoverability, 68

recovery
  - BCP, 639-640
  - controls, 84
  - data, 623
  - disaster, 633-637
  - incidents, 612
  - priorities, 68
  - strategies, 618-633
  - systems, 600
  - teams, 635
  - testing, 637-639
  - trusted, 615

recovery point objective. See RPO

recovery time object. See RTO

Red Book, 206
redundancy, 600, 607
sites, 630
systems, 630
reference monitors, 694
referential integrity, 156
registration, 503
registration authority. See RA
regression testing, 673, 696
regulations, 34-35
computer crimes, 36-37
major legal systems, 38-43
privacy, 47-51
regulatory investigations, 582
regulatory law, 39
relational database management systems (RDBMSs), 155
relational models, 155
Release/Maintenance phase (SDLC), 673
reliability, 61, 574
religious law, 40
relocation teams, 635
remanence, 162-163, 607
remediation, 121, 436, 612
remote access, 440-451
remote access applications, 395, 440
Remote Authentication Dial-In User Service. See RADIUS
remote authentication protocols, 448
remote connection technologies, 440
remote meeting technology, 440
remote network attacks, 460
renewal of certificates, 283
repeaters, 398
replay attacks, 304
reporting, 89, 505
evidence, 570
incidents, 611
reports, SOC, 555
requirements
asset handling, 172-173
security, 123
services, 123
residual risk, 82
resilience, 633
resources
access control, 475
critical, 66
managing, 607
protecting, 597-599, 602, 605, 608
provisioning, 589-592
 asset inventory, 590-591
 configuration management, 592-593
relationship between users and, 476
requirements, 67
security, 11
responding
responses
to disasters, 634
to incidents, 610-611
responsibilities
asset security, 143-144
security governance, 14-17
restoration processes, 637
restoration teams, 636
restricted work areas, 316
retention (data), asset security, 164-165
reuse of objects, 700
Reverse ARP. See RARP
reverse engineering, 304
review tools (exams), 717
reviews, 585-587
 access, 516
code, 546-548
incidents, 612
log, 542-545, 556
management, 551-552
periodic, 126
revocation, 551
accounts, 516
certificates, 283
rights, 508
Rijndael design, 274
ring structures, 205
ring topologies, 419
riots, 114
RIP (Routing Information Protocol), 414
RIPEMD, 160, 297
risk
in acquisitions, 121-123
analysis, 695-696
appetite, 76
definition of, 75
management, 73-90, 93-106
assets, 73-74
vulnerabilities, 74
terms, 5-6
abstraction, 8
accounting, 6
auditing, 6
CIA, 5-7
data hiding, 8
default security posture, 7
defense-in-depth strategy, 7
encryption, 8
non-repudiation, 7
Rivest, Ron, 277
rogue programmers, 699
role-based access control. See RBAC
rules
asset security, 143-144
managing, 594
security governance, 14-17
separation of, 594
root accounts, 488
rootkits, 692
routers, 400-401
routes, aggregation (IPv6), 362
routing
hybrid, 413
networks, 412-413
Routing Information Protocol. See RIP
RPO (recovery point objective), 619
RSA algorithm, 277
RTO (recovery time object), 619
rule-based access control, 510
rules
firewalls, 346
of engagement, 609
of evidence, 574
RUM (real user monitoring), 546
running key ciphers, 263
safe harbor laws, 51
safeguards, 81
safes, 323
sags, 319
salting, 299
salvage teams, 636
SAM (Security Accounts Manager), 488
SAML (Security Assertion Markup Language), 244, 502
SAN (storage area network), 371, 604, 632
sandboxing, 614, 664
sanitization, 163
data, 702
media, 606
Sarbanes-Oxley (SOX) Act, 47
SASE (specific application service element), 337
satellites, 383
scanning
    network discovery, 536-537
    network vulnerability, 538
    ports, 461
types, 693
schemas, 155
Scientific Working Group on Digital Evidence. See SWGDE
scope
    for incident response teams, 609
    of business continuity, 62
    of IP addresses, 368-369
scoping, 170
screening, 69-70
scrubbing, 506
SDLC (Software Development Life Cycle), 670-673
    Accreditation/Certification phase, 674
    Design phase, 672
    Develop phase, 672
    Dispose stage, 670
    Gather Requirements phase, 671
    Plan/Initiate Project phase, 671
    Release/Maintenance phase, 673
    Test/Validate phase, 672
SDN (software-defined networking), 450
searching (investigations), 576-577
secondary evidence, 575
secure data centers, 316
Secure Electronic Transaction. See SET
Secure European System for Applications in a Multi-vendor Environment. See SESAME
Secure Hash Algorithm. See SHA
Secure-HTTP. See S-HTTP
Secure MIME. See S/MIME
Secure Shell. See SSH
Secure Sockets Layer. See SSL
security
    applications, 246
    architecture, 196-205, 223
    assets. See assets, security
    auditing, 535
    baselines, 169
    business continuity, 58-68
capabilities, 219
    encryption/decryption, 223
    fault tolerance, 221
    interfaces, 221
    memory protection, 219-220
    policy mechanisms, 222
    TPM, 220-221
    virtualization, 220
compliance, 33-34
    laws/regulations, 34
    privacy, 35
controls, 535-550, 562
cryptography, 267
data breaches, 44
device, 245
documentation, 54
    baselines, 58
    guidelines, 58
    policies, 55-57
    procedures, 57
    processes, 57
    standards, 57
domains, 502
DRM, 305-307
education, 126
email, 300
endpoint, 437
ingenring
    closed/open systems, 182
- design, 180-181
- objects/subjects, 181
- equipment, 321
- evaluation models, 206-219
- facility and site design, 307-323
- geographical threats, 108-115
- governance, 8-9, 94-95
  - control frameworks, 17-18, 21, 24-33
  - processes, 12-14
  - roles and responsibilities, 14-17
  - security function alignment, 9-11
- import/export controls, 45, 49
- Internet, 300
- kernels, 694
- keys, 285-293
- laws/regulations, 35-43
- life cycles, 31
- message integrity, 293-296
- models, 182, 188
  - Bell-LaPadula model, 189
  - Biba model, 190
  - bounds, 183
  - Brewer-Nash (Chinese Wall) model, 192
  - CIA, 182
  - Clark-Wilson Integrity model, 190-191
  - computing platforms, 193-195
  - confinement, 183
  - defense in depth, 185
  - Goguen-Meseguer model, 192
  - Graham-Denning model, 192
  - Harrison-Ruzzo-Ullman model, 192
  - ISO/IEC 42010:2011, 193
  - isolation, 183
  - Lipner model, 191
  - modes, 183-185
  - services, 196
- Sutherland model, 192
  - types, 185-187
- networks, 335, 382, 386, 403, 415, 424, 432, 441-443, 451, 454-462
  - attacks, 451-462
  - communication channels, 438-451
  - components, 396-438
  - converged protocols, 379-381
  - cryptography, 392-394
  - Internet security, 394-396
  - IP networking, 345-353
  - IPv6, 357-369
  - multilayer protocols, 378-379
  - network transmission, 353-357
  - OSI models, 335-338
  - protocols, 372-378
  - services, 376-377
  - TCP/IP models, 340-345
  - types, 370-372
  - wireless, 381-392
- operations, 571-576, 579, 589-592, 595, 602, 605, 608, 611, 614, 617-619, 637
  - asset management, 599-603, 606-607
  - authorization, 609
  - BCP, 639-640
  - change management, 618
  - concepts, 593
  - configuration management, 592-593
  - continuous monitoring, 588
  - detections, 612-617
  - disaster recovery, 633-636
  - eDiscovery, 585
  - egress monitoring, 588-589
  - forensic tools, 579-581
  - IDSs, 587
  - incident management, 608-612
  - industry standards, 582-584
information life cycles, 596-597
investigations, 566-579
job rotation, 595
logging/monitoring, 585-587
managing accounts, 594
managing privileges, 595
need to know/least privilege, 593
patches, 617
personal security, 645-647
physical security, 640-644
record retention, 596
recovery strategies, 618-633
resource protection, 597-599
resource provisioning, 589-591
sensitive information procedures, 596
separation of duties, 594
SIEM, 588
SLAs, 597
two-person controls, 596
types of investigations, 581-582
perimeters, 694
personnel, 68
compliance, 72
employee onboarding/offboarding, 71-72
employment agreements/policies, 70
hiring, 69-70
job rotation, 73
privacy, 72
separation of duties, 73
third party access, 72
PKI, 279-285
policies, 693, 701
privacy, 45-52
process data, collecting, 550-551
backing up, 553
disaster recovery, 553
KRI, 552
management review, 551-552
managing accounts, 551
training, 553
professional ethics, 52-53
requirements, 123
risk management, 73-90, 93-106
assets, 73-74
vulnerabilities, 74
risks in acquisitions, 121-123
software development, 659-668, 700
API security, 700-701
coding guidelines, 697-700
impact of acquired software, 696-697
defense-in-depth strategy, 7
life cycles, 668-673
methods, 674-683
operation/maintenance, 684-686
secure coding, 701-702
security controls, 686-696
symmetric algorithms, 275
system architecture, 192
terms, 5
abstraction, 8
accounting, 6
auditing, 6
CLA, 5-6
data hiding, 8
default security posture, 7
defense-in-depth strategy, 7
equity, 8
non-repudiation, 7
testing, 534-535, 553-556, 563
threat modeling, 115-121
training, 124-125, 647
trans-border data flow, 45
vulnerabilities, 224-230, 233-237
WLANs, 387-392
Security Accounts Manager. See SAM
security administrators, 16
security analysts, 17
Security Assertion Markup Language. See SAML
security information and event management. See SIEM
security teams, 636
segmenting data, 146
seizure (investigations), 576-577
selecting standards, 170
sensitive information procedures, 596
sensitivity, data classification, 146-151
separation of duties, 73, 496, 594
separation of privilege, 222
sequencing, 343
server-based system vulnerabilities, 225-226
server rooms, 316
servers, proxy, 404
service-level agreements. See SLAs
Service Organization Control. See SOC
service-oriented architect. See SOA
service set identifiers. See SSIDs
services, 372
directory, 498
IDaaS, 507
NAT, 376
NetBIOS, 376
NFS, 377
PAT, 377
requirements, 123
risks, 121
security, 196
third-party identity, 507
SESAME (Secure European System for Applications in a Multi-vendor Environment), 501
Session layer (5), 337
sessions
hijacking attacks, 461
managing, 503
SET (Secure Electronic Transaction), 395
SFTP (SSH File Transfer Protocol), 374
SHA (Secure Hash Algorithm), 296
Shamir, Adi, 277
Shared Key Authentication, 387
shareware, 43
sharing data, 167-168
Sherwood Applied Business Security Architecture (SABSA), 22
shoulder surfing, 519
S-HTTP (Secure-HTTP), 375
side-channel attacks, 305
SIEM (security information and event management), 543-544, 588
signaling, analog/digital, 353
signatures, digital, 299
Simple Mail Transfer Protocol. See SMTP
Simple Network Management Protocol. See SNMP, 377
simple passwords, 485
simple security rule, 189
simulation tests, 639
single-factor authentication, 495
single loss expectancy. See SLE
single point of failure. See SPOF
single sign-on. See SSO
single-state systems, 199
site design, 307-323
site-local scope (IPv6), 369
site surveys, 391
Six Sigma, 29
skills, security training, 124-125
Skipjack, 274
SLAs (service-level agreements), 597, 607
SLE (single loss expectancy), 79
smart cards, 489
SMDS (Switched Multimegabit Data Service), 433
S/MIME (Secure MIME), 394
SMTP (Simple Mail Transfer Protocol), 377, 498
smurf attacks, 455
SNAT (Stateful NAT), 351
sniffer attacks, 518, 521
SNMP (Simple Network Management Protocol), 377, 544
SOA (service-oriented architecture), 664
SOC (Service Organization Control), 555
social engineering attacks, 302, 518
sockets, 346
software
analyzing, 578
backups, 621
development, 659-668, 700
  API security, 700-701
coding guidelines, 697-700
impact of acquired software, 696-697
life cycles, 668-683
operation/maintenance, 684-686
secure coding, 701-702
security controls, 686-696
patches, 617
risks, 121
security, 599
threats, 688-694
software-defined networking. See SDN
Software Development Life Cycle. See SDLC
software piracy, 43
SONET (Synchronous Optical Networking), 431
source code
  analysis tools, 688
  issues, 697
SPs (Special Publications [NIST]), 94-95
  SP 800-2, 504
  SP 800-12 Rev. 1, 24
  SP 800-16 Rev. 1, 24
  SP 800-18 Rev. 1, 24
  SP 800-30 Rev. 1, 24, 101
  SP 800-34 Rev. 1, 24, 62-63, 618
  SP 800-35, 24
  SP 800-36, 24
  SP 800-37, 90, 99-101
  SP 800-37 Rev. 1, 24
  SP 800-39, 24, 102
  SP 800-50, 24
  SP 800-53A Rev. 4, 24, 90
  SP 800-53 Rev. 4, 24, 90, 149
  SP 800-55 Rev. 1, 24
  SP 800-57, 285
  SP 800-60, 90, 93
  SP 800-60 Vol. 1 Rev. 1, 24, 94
  SP 800-61 Rev. 2, 25
  SP 800-63, 481-482
    authentication, 480
    passwords, 482-484, 487
  SP 800-66
    Risk Management Framework (RMF), 151
    Security Rule, 151
  SP 800-82 Rev. 2, 25, 228
  SP 800-84, 25
  SP 800-86, 25, 583-584
  SP 800-88 Rev. 1, 25
  SP 800-92, 25, 542-545, 556
SP 800-101 Rev. 1, 25
SP 800-115, 25
SP 800-119, 358-360
SP 800-122, 25, 147, 149
SP 800-123, 25
SP 800-124 Rev, 25, 408
SP 800-137, 25, 90, 550-551
SP 800-144, 25, 234
SP 800-145, 25, 231
SP 800-146, 25

benefits of IaaS deployments, 236
benefits of PaaS deployments, 236
benefits of SaaS deployments, 235
cloud computing, 235
concerns of SaaS deployments, 236

SP 800-150, 25
SP 800-153, 25
SP 800-154, 25, 118
SP 800-160, 25, 90, 96-98, 181
SP 800-161, 25
SP 800-162

ABAC, 511-512
subject attributes, 512
SP 800-163, 26, 665, 667-668
SP 800-164, 26
SP 800-167, 26
SP 800-175A and B, 26, 257-258
SP 800-181, 26
SP 800-183, 26

spam, 459
spear phishing, 519
special privileges, monitoring, 595
specific application service element. See SASE

Spiral model, 678
split knowledge, 260
SPOF (single point of failure), 608
spoofing, 461, 521
spyware, 521, 691
SSAE (Statements on Standards for Attestation Engagement), 554
SSH (Secure Shell), 396
SSH File Transfer Protocol. See SFTP
SSID (service set identifiers), 384, 390
SSL (Secure Sockets Layer), 378
SSO (single sign-on), 498, 507
stacks, 336
standard word passwords, 485

standards
802.11, 382
coding, 697-700
deviations, 615
documentation, 57
industry, 34, 582-584
security implementation, 213-215
selecting, 170
WLANs, 384-386
star (*) property rule, 189
star topologies, 421
state machine models, 185
Stateful NAT. See SNAT
Statements on Standards for Attestation Engagement. See SSAE
states, data, 166-167
static passwords, 485
static testing, 548
statistical attacks, 304
steganography, 265
storage, 172, 199-201
backup, 626. See also backup
media, 606
privacy, 168
storage area networks. See SAN
strategies
assessment, 533-535
recovery, 618-633
testing, 533-535
stream-based ciphers, 267
STRIDE model, 117
strikes, 114
strong star property rule, 189
Structured Programming Development model, 681
structured walk-through test, 638
study plans, 717-718
subject attributes, 512
subjects, 181
substitution, 252
substitution ciphers, 263
supervisors, 17
supply recovery, 620
surges, 319
surveillance, 308, 576-577
suspended states, 291
Sutherland model, 192
SWGDE (Scientific Working Group on Digital Evidence), 571
Switched Multimegabit Data Service. See SMDS
switches, 399
symmetric, 251
symmetric algorithms, 266-269
AES, 274
Blowfish, 275
CAST, 275
DES, 270-273
IDEA, 274
Skipjack, 274
Twofish, 275
symmetric authorization keys, 287
symmetric data-encryption keys, 286
symmetric key-agreement keys, 287
symmetric-key algorithms, 286
symmetric key-wrapping key, 286
symmetric master keys, 286
synonymous random number generation keys, 286
SYN ACK attacks, 460
synchronous, 251
Synchronous Optical Networking. See SONET
synchronous tokens, 488
synchronous transmissions, 354
synthetic transaction monitoring, 546
system administrators, 16
system architecture, 192, 196-205
System Development Life Cycle, 668
Acquire/Develop stage, 669
Dispose stage, 670
Initiate phase, 668-669
Operate/Maintain stage, 669
system evaluation models
CC, 211-213
controls/countermeasures, 217
ITSEC, 209-211
security implementation standards, 213-215
selecting controls, 218-219
TCSEC, 206-209
system hardening, 616
system high security mode, 184
system-level recovery strategies, 619
system resilience, 633
system-specific security policies, 57
system threats, 110-111
systems
access controls, 478-479
access reviews, 516
certification, 217
client-based vulnerabilities, 224-225
cloud-based systems vulnerabilities, 230, 233-237
cryptographic vulnerabilities, 227
custodians, 161
database vulnerabilities, 226
embedded vulnerabilities, 250
grid computing vulnerabilities, 237
ICSs vulnerabilities, 227-230
IoT vulnerabilities, 238-242
large-scale parallel data vulnerabilities, 236-237
mobile vulnerabilities, 244-249
operating CPUs, 204
ownership, 161
peer-to-peer computing vulnerabilities, 237
server-based vulnerabilities, 225-226
testing, 536
Web-based vulnerabilities, 242-244
systems owners, 16

TCP/IP (Transmission Control Protocol/Internet Protocol) models, 340-345
TCSEC (Trusted Computer System Evaluation Criteria), 206-209
TDM (Time Division Multiplexing), 355
TDMA (time division multiple access), 383
teams
  risk analysis, 77
  risk management, 77
tear drop attacks, 461
technical controls, 86
technological disasters, 59
technologies
  networks, 423-424, 432
  recovery, 620
  WANs, 430
telco concentrators, 397
telecommuting, 450
telnets, 448
TEMPEST program, 522
Terminal Access Controller Access-Control System Plus. See TACACS+
terrorism, 114
tertiary sites, 630
test coverage analysis, 549, 562
test data method, 672
Test/Validate phase (SDLC), 672
testing
  acceptance, 696
code, 546-548
dynamic, 548
fuzz, 548
interfaces, 549-550, 562
misuse case, 549
penetration, 539-545
recovery plans, 637-639
regression, 696
testing, training, and exercises. See TT&E
TFTP (Trivial FTP), 374
theft, 113, 519
third party
access, 72
audits, 554-556, 563
governance, 122-123
identity services, 507
security assessments, 535
security services, 613
threats, 74, 79
access control, 516-522
agents, 74, 138
APT, 523
databases, 158
geographical, 108-115
identifying, 119-120
IPv4, 362-363
IPv6, 362-363
mitigating, 523
modeling, 115-119
passwords, 517
potential attacks, 120
prevention, 612-617
preventive measures against, 614
remediation, 121
software, 688-694
Tiger, 297
Time division multiple access (TDMA), 383
Time Division Multiplexing. See TDM
time factor authentication, 495

Time of Check/Time of Use. See TOC/TOU
T-lines, 430
TLS (Transport Layer Security), 378
TOC/TOU (Time of Check/Time of Use), 243, 700
TOGAF (Open Group Architecture Framework), 22
Token Ring 802.5 standard, 424
tokens, 430, 488
tool-assisted, 547
tools
digital forensic, 579-581
network discovery, 537
Pearson Test Prep practice test engine, 713-715
review (exams), 717
source code analysis, 688
top-down approach, 31
tornadoes, 109
tort law, 39
total risk, 82
TPM (Trusted Platform Module), 220-221
Traceroute exploitation, 456
tracking devices, 322
trademarks, 41-42
trade secrets, 41
trails, audit, 506
training, 126, 553, 626
disaster recovery, 637
security, 124-125, 647
trans-border data flow, 45
transformation procedure (TP), 191
transmission
IPv6, 362
networks, 353-357
sanitizing data, 702
transmission media, 415, 424, 432
Transport layer (4), 337
Transport Layer Security. See TLS
transposition ciphers, 252, 265
trapdoors, 252, 522, 699
travel, security, 646
Treadway Commission Framework, 28
Trike, 117
Trivial FTP. See TFTP
Trojan horses, 521, 691
tropical storms, 109
trust, 185
transposition ciphers, 252, 265
trapdoors, 252, 522, 699
travel, security, 646
Treadway Commission Framework, 28
Trike, 117
Trivial FTP. See TFTP
Trojan horses, 521, 691
tropical storms, 109
trust, 185
transposition ciphers, 252, 265
trapdoors, 252, 522, 699
travel, security, 646
Treadway Commission Framework, 28
Trike, 117
Trivial FTP. See TFTP
Trojan horses, 521, 691
tropical storms, 109
trust, 185
trusted computer base. See TCB
Trusted Computer System Evaluation
Criteria. See TCSEC
tested paths, 616
Trusted Platform Module. See TPM, 220
TT&E (testing, training, and exercises), 65
tuples, 155
turnstiles, 313
twisted pair cabling, 417-418
two-person control, 596
Twofish, 275
types
of access control, 84-87
of antennas, 392
of audits, 587
of backups, 625
of cryptography, 262-269
of doors, 312
of evidence, 575-576
of firewalls, 401-403
of glass, 315
of investigations, 581
civil, 582
criminal, 582
of IP networks, 370-372
of IPv6 addresses, 367-368
of lighting, 644
of locks, 313
of logs, 586
of memory, 200
of outages, 319
of passwords, 485-488
of security models, 185-187
of viruses, 689
U
UDP (User Datagram Protocol)
headers, 341
ports, 346
ULAs (unique local addresses), 369
unauthorized disclosure of information, 615
unconstrained data item (UDI), 191
unicast addresses, 368
unicast transmissions, 355
uninterruptible power supplies (UPSs), 320
unique local addresses. See ULAs
unit testing, 673
United States Federal Sentencing
Guidelines of 1991, 49
unscheduled reboots, 615
updating exams, 716
URFI (Unified Extensible Firmware
Interface), 203
URL hiding, 458
USA Freedom Act of 2015, 50
USA PATRIOT Act of 2001, 50
U.S. Digital Millennium Copyright Act.
See DMCA
users, 17
  access control, 476
  access reviews, 516
  environment recovery, 623
  relationship between resources and, 476
utility threats, 111

V
vacations, 595
validation testing, 673
values, 661
vandalism, 113
VAST model, 118
vaults, 323
vectored orthogonal frequency division multiplexing (VOFDM), 383
verification, 282, 673
verification data, backing up, 553
Vernam, Gilbert, 264
very-high-level languages, 660
video games, DRM, 306
views, 155, 159
Vigenere cipher, 254
virtual computing, 195
virtual local area networks. See VLANs
virtual private networks. See VPNs
Virtual Router Redundancy Protocol. See VRRP
virtual storage area networks. See VSANs
virtualization, 220, 449
virtualized networks, 450-451
viruses, 521, 689-690, 693
visibility (of building), 309
visitor control, 315
VLANs (virtual local area networks), 400
VOFDM (vectored orthogonal frequency division multiplexing), 383
voice, 439
VoIP (Voice over Internet Protocol), 381, 434-435
volcanoes, 110
VPNs (virtual private networks), 443-445
  concentrator, 398
  screen scraper, 449
VRRP (Virtual Router Redundancy Protocol), 414
VSANs (virtual storage area network), 451
V-shaped model, 677
vulnerabilities, 79, 224
architecture
  client-based systems, 224-225
  cloud-based systems, 230, 233-235, 237
  cryptographic systems, 227
  database systems, 226
  grid computing, 237
  ICSs, 227-230
  IoT, 238-242
  large-scale parallel data systems, 236-237
  peer-to-peer computing, 237
  server-based systems, 225-226
assessments, 535-536
embedded systems, 250
management systems, 616
managing, 617
mobile systems, 244-248
  application security, 246
  device security, 245
  NIST SP 800-164, 248-249
network scans, 538
risk management, 74
source code, 697
Web-based systems, 242
attacks, 243-244
maintenance hooks, 242
time-of-check/time-of-use attacks, 243

walls, 642
WANs (wide area networks), 371, 430
warchalking, 460
wardriving, 460
warm sites, 629
WASC (Web Application Security Consortium), 686
water leakage, 320
Waterfall model, 676
wave motion detectors, 643
Web Application Security Consortium. See WASC
Web-based systems vulnerabilities, 242
attacks, 243-244
maintenance hooks, 242
time-of-check/time-of-use attacks, 243
web caching, 404
WEP (Wired Equivalent Privacy), 387
whaling, 459
white-box testing, 547
whitelisting, 613
wide area networks. See WANs
Wi-Fi Protected Access. See WPA
Wired Equivalent Privacy. See WEP
wired transmissions, 356-357
wireless local area networks. See WLANs
wireless networks, 381
802.11 techniques, 382
attacks, 459
cellular or mobile, 383
satellites, 383
WLANs, 384-392

wireless transmisions, 356-357
wiring controls, 316
WLANs (wireless local area networks), 356, 371, 384-386
802.11 techniques, 382
security, 387-392
standards, 384
work areas, 316
work factor, 252
work function, 252
work recovery time. See WRT
worms, 521, 690
WPA (Wi-Fi Protected Access), 388
WRT (work recovery time), 619

X.25, 433
XML (Extensible Markup Language)
attacks, 244
data storage, 157

Zachman Framework, 21
zero-day attacks, 462
zero-knowledge
proof algorithm, 279
testing, 540, 547
Zigbee, 387
zombies, 691