Contents at a Glance

Introduction 3
Chapter 1 Security and Risk Management 14
Chapter 2 Asset Security 113
Chapter 3 Security Engineering 157
Chapter 4 Communication and Network Security 293
Chapter 5 Identity and Access Management 409
Chapter 6 Security Assessment and Testing 455
Chapter 7 Security Operations 480
Chapter 8 Software Development Security 565
Glossary 613
Appendix A Memory Tables 671
Appendix B Memory Tables Answer Key 683
Index 782
# Table of Contents

**Introduction**  
The Goals of the CISSP Certification  
Sponsoring Bodies  
Stated Goals  

The Value of the CISSP Certification  
To the Security Professional  
To the Enterprise  

The Common Body of Knowledge  
Security and Risk Management (e.g. Security, Risk, Compliance, Law, Regulations, Business Continuity)  
Asset Security (Protecting Security of Assets)  
Security Engineering (Engineering and Management of Security)  
Communication and Network Security (Designing and Protecting Network Security)  
Identity and Access Management (Controlling Access and Managing Identity)  
Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)  
Security Operations (e.g. Foundational Concepts, Investigations, Incident Management, Disaster Recovery)  
Software Development Security (Understanding, Applying, and Enforcing Software Security)  

Steps to Becoming a CISSP  
Qualifying for the Exam  
Signing Up for the Exam  
About the CISSP Exam  

**Chapter 1 Security and Risk Management**  
Security Terms  
CIA  
*Confidentiality*  
*Integrity*  
*Availability*  
Default Stance  
Defense in Depth  
Job Rotation  
Separation of Duties
Security Governance Principles 17
Security Function Alignment 18
Organizational Strategy and Goals 19
Organizational Mission and Objectives 19
Business Case 19
Security Budget, Metrics, and Effectiveness 20
Resources 20
Organizational Processes 21
Acquisitions and Divestitures 21
Governance Committees 23
Security Roles and Responsibilities 23
Board of Directors 23
Management 24
Audit Committee 25
Data Owner 25
Data Custodian 25
System Owner 25
System Administrator 25
Security Administrator 26
Security Analyst 26
Application Owner 26
Supervisor 26
User 26
Auditor 26
Control Frameworks 27
ISO/IEC 27000 Series 27
Zachman Framework 30
The Open Group Architecture Framework (TOGAF) 31
Department of Defense Architecture Framework (DoDAF) 31
British Ministry of Defence Architecture Framework (MODAF) 31
Sherwood Applied Business Security Architecture (SABSA) 31
Control Objectives for Information and Related Technology (CobiT) 32
National Institute of Standards and Technology (NIST) Special Publication (SP) 33
Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework 34
Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) 34
Import/Export Controls 51
Trans-Border Data Flow 52
Privacy 52
Personally Identifiable Information (PII) 52
Laws and Regulations 53
Data Breaches 58
Professional Ethics 59
(ISC)^2 Code of Ethics 59
Computer Ethics Institute 59
Internet Architecture Board 60
Organizational Ethics 60
Security Documentation 60
Policies 61
Organizational Security Policy 62
System-Specific Security Policy 63
Issue-Specific Security Policy 63
Policy Categories 63
Standards 64
Baselines 64
Guidelines 64
Procedures 64
Business Continuity 64
Business Continuity and Disaster Recovery Concepts 65
Disruptions 65
Disasters 66
Disaster Recovery and the Disaster Recovery Plan (DRP) 67
Continuity Planning and the Business Continuity Plan (BCP) 67
Business Impact Analysis (BIA) 67
Contingency Plan 67
Availability 68
Reliability 68
Project Scope and Plan 68
Personnel Components 68
Project Scope 69
Business Continuity Steps 69
Business Impact Analysis Development 70
Identify Critical Processes and Resources 71
Identify Outage Impacts, and Estimate Downtime 71
Identify Resource Requirements  72
Identify Recovery Priorities  72
Recoverability  73
Fault Tolerance  73
Personnel Security Policies  73
  Employment Candidate Screening  73
  Employment Agreement and Policies  75
  Employment Termination Policies  75
  Vendor, Consultant, and Contractor Controls  76
  Compliance  76
  Privacy  76
Risk Management Concepts  77
  Vulnerability  77
  Threat  77
  Threat Agent  77
  Risk  77
  Exposure  77
  Countermeasure  78
  Risk Management Policy  78
  Risk Management Team  79
  Risk Analysis Team  79
  Risk Assessment  79
Information and Asset (Tangible/Intangible) Value and Costs  81
Identify Threats and Vulnerabilities  82
Risk Assessment/Analysis  82
Countermeasure (Safeguard) Selection  84
Total Risk Versus Residual Risk  85
Handling Risk  85
Implementation  86
Access Control Categories  86
Compensative  87
Corrective  87
Detective  87
Deterrent  87
Directive  87
Preventive  87
Recovery  88
Contents

Access Control Types  88

Administrative (Management) Controls  88
Logical (Technical) Controls  90
Physical Controls  91

Control Assessment, Monitoring, and Measurement  92
Reporting and Continuous Improvement  92

Risk Frameworks  93

Threat Modeling  93
Identifying Threats  94
Potential Attacks  96
Remediation Technologies and Processes  96

Security Risks in Acquisitions  97
Hardware, Software, and Services  97
Third-Party Governance  97
Onsite Assessment  98
Document Exchange/Review  98
Process/Policy Review  98
Other Third-Party Governance Issues  98

Minimum Security Requirements  98
Minimum Service-Level Requirements  99

Security Education, Training, and Awareness  100
Levels Required  100
Periodic Review  101

Exam Preparation Tasks  101
Review All Key Topics  101
Complete the Tables and Lists from Memory  102
Define Key Terms  102
Answer Review Questions  103
Answers and Explanations  107

Chapter 2  Asset Security  113

Asset Security Concepts  114
Data Policy  114
Roles and Responsibilities  115
Data Owner  116
Data Custodian  116
Data Quality  116
Data Documentation and Organization  117
Classify Information and Assets 118
  Sensitivity and Criticality 119
  Commercial Business Classifications 119
  Military and Government Classifications 120
Information Life Cycle 121
Databases 122
  DBMS Architecture and Models 122
  Database Interface Languages 124
  Data Warehouses and Data Mining 125
Database Maintenance 126
Database Threats 126
Data Audit 127
Asset Ownership 128
  Data Owners 128
  System Owners 129
  Business/Mission Owners 129
Asset Management 129
  Redundancy and Fault Tolerance 130
  Backup and Recovery Systems 130
  Identity and Access Management 130
  RAID 131
  SAN 135
  NAS 135
  HSM 135
Network and Resource Management 136
Asset Privacy 137
  Data Processors 137
  Data Storage and Archiving 137
  Data Remanence 138
  Collection Limitation 139
Data Retention 140
Data Security and Controls 141
  Data Security 141
  Data at Rest 141
  Data in Transit 141
  Data Access and Sharing 142
Baselines 142
Scoping and Tailoring 143
Standards Selection 144
Cryptography 146
Link Encryption 147
End-to-End Encryption 147
Asset Handling Requirements 147
Marking, Labeling, and Storing 148
Destruction 148
Exam Preparation Tasks 148
Review All Key Topics 148
Complete the Tables and Lists from Memory 149
Define Key Terms 149
Answers and Explanations 152

Chapter 3 Security Engineering 157
Engineering Using Secure Design Principles 158
Security Model Concepts 161
Confidentiality, Integrity, and Availability 161
Dedicated Security Mode 162
System High Security Mode 162
Compartmented Security Mode 162
Multilevel Security Mode 162
Assurance 163
Defense in Depth 163
Security Model Types 163
Security Model Types 163
State Machine Models 164
Multilevel Lattice Models 164
Matrix-Based Models 164
Non-inference Models 165
Information Flow Models 165
Security Models 165
Bell-LaPadula Model 166
Biba Model 167
Clark-Wilson Integrity Model 168
Lipner Model 169
Brewer-Nash (Chinese Wall) Model 169
Security Capabilities of Information Systems 191
  Memory Protection 191
  Virtualization 191
  Trusted Platform Module (TPM) 192
  Interfaces 193
  Fault Tolerance 193
Certification and Accreditation 193
Security Architecture Maintenance 194
Vulnerabilities of Security Architectures, Designs, and Solution Elements 194
  Client-Based 195
  Server-Based 196
  Data Flow Control 196
  Database Security 196
  Inference 197
  Aggregation 197
  Contamination 197
  Data Mining Warehouse 197
  Distributed Systems 197
  Cloud Computing 198
  Grid Computing 199
  Peer-to-Peer Computing 199
  Large-Scale Parallel Data Systems 201
  Cryptographic Systems 201
  Industrial Control Systems 202
Vulnerabilities in Web-Based Systems 203
  Maintenance Hooks 203
  Time-of-Check/Time-of-Use Attacks 204
  Web-Based Attacks 204
  XML 204
  SAML 204
  OWASP 205
Vulnerabilities in Mobile Systems 205
Vulnerabilities in Embedded Devices and Cyber-Physical Systems 208
Cryptography 209
  Cryptography Concepts 209
  Cryptographic Life Cycle 211
Asymmetric Algorithms  231
  Diffie-Hellman  231
  RSA  232
  El Gamal  233
  ECC  233
  Knapsack  233
  Zero Knowledge Proof  233
Public Key Infrastructure  234
  Certification Authority (CA) and Registration Authority (RA)  234
  OCSP  235
  Certificates  235
  Certificate Revocation List (CRL)  236
  PKI Steps  236
  Cross-Certification  236
Key Management Practices  237
Digital Signatures  245
Digital Rights Management (DRM)  246
Message Integrity  246
  Hashing  247
  One-Way Hash  248
  MD2/MD4/MD5/MD6  249
  SHA/SHA-2/SHA-3  250
  HAVAL  250
  RIPEMD-160  251
  Tiger  251
  Message Authentication Code  251
  HMAC  251
  CBC-MAC  252
  CMAC  252
  Salting  252
Cryptanalytic Attacks  253
  Ciphertext-Only Attack  254
  Known Plaintext Attack  254
  Chosen Plaintext Attack  254
  Chosen Ciphertext Attack  254
  Social Engineering  255
  Brute Force  255
Differential Cryptanalysis  255
Linear Cryptanalysis  255
Algebraic Attack  255
Frequency Analysis  255
Birthday Attack  256
Dictionary Attack  256
Replay Attack  256
Analytic Attack  256
Statistical Attack  256
Factoring Attack  257
Reverse Engineering  257
Meet-in-the-Middle Attack  257

Geographical Threats  257
Internal Versus External Threats  257
Natural Threats  257
Hurricanes/Tropical Storms  258
Tornadoes  258
Earthquakes  258
Floods  258
System Threats  259
Electrical  259
Communications  259
Utilities  260
Human-Caused Threats  260
Explosions  261
Fire  261
Vandalism  262
Fraud  262
Theft  262
Collusion  262
Politically Motivated Threats  262
Strikes  263
Riots  263
Civil Disobedience  263
Terrorist Acts  263
Bombing  264
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site and Facility Design</td>
<td>264</td>
</tr>
<tr>
<td>Layered Defense Model</td>
<td>264</td>
</tr>
<tr>
<td>CPTED</td>
<td>264</td>
</tr>
<tr>
<td>Natural Access Control</td>
<td>264</td>
</tr>
<tr>
<td>Natural Surveillance</td>
<td>265</td>
</tr>
<tr>
<td>Natural Territorial Reinforcement</td>
<td>265</td>
</tr>
<tr>
<td>Physical Security Plan</td>
<td>265</td>
</tr>
<tr>
<td>Deter Criminal Activity</td>
<td>265</td>
</tr>
<tr>
<td>Delay Intruders</td>
<td>266</td>
</tr>
<tr>
<td>Detect Intruders</td>
<td>266</td>
</tr>
<tr>
<td>Assess Situation</td>
<td>266</td>
</tr>
<tr>
<td>Respond to Intrusions and Disruptions</td>
<td>266</td>
</tr>
<tr>
<td>Facility Selection Issues</td>
<td>266</td>
</tr>
<tr>
<td>Visibility</td>
<td>266</td>
</tr>
<tr>
<td>Surrounding Area and External Entities</td>
<td>267</td>
</tr>
<tr>
<td>Accessibility</td>
<td>267</td>
</tr>
<tr>
<td>Construction</td>
<td>267</td>
</tr>
<tr>
<td>Internal Compartments</td>
<td>268</td>
</tr>
<tr>
<td>Computer and Equipment Rooms</td>
<td>268</td>
</tr>
<tr>
<td>Building and Internal Security</td>
<td>269</td>
</tr>
<tr>
<td>Doors</td>
<td>269</td>
</tr>
<tr>
<td>Door Lock Types</td>
<td>269</td>
</tr>
<tr>
<td>Turnstiles and Mantraps</td>
<td>270</td>
</tr>
<tr>
<td>Locks</td>
<td>270</td>
</tr>
<tr>
<td>Biometrics</td>
<td>271</td>
</tr>
<tr>
<td>Glass Entries</td>
<td>272</td>
</tr>
<tr>
<td>Visitor Control</td>
<td>272</td>
</tr>
<tr>
<td>Equipment Rooms</td>
<td>273</td>
</tr>
<tr>
<td>Work Areas</td>
<td>273</td>
</tr>
<tr>
<td>Secure Data Center</td>
<td>273</td>
</tr>
<tr>
<td>Restricted Work Area</td>
<td>273</td>
</tr>
<tr>
<td>Media Storage Facilities</td>
<td>274</td>
</tr>
<tr>
<td>Evidence Storage</td>
<td>274</td>
</tr>
<tr>
<td>Environmental Security</td>
<td>274</td>
</tr>
<tr>
<td>Fire Protection</td>
<td>274</td>
</tr>
<tr>
<td>Fire Detection</td>
<td>274</td>
</tr>
<tr>
<td>Fire Suppression</td>
<td>275</td>
</tr>
</tbody>
</table>
Power Supply 276
Types of Outages 276
Preventive Measures 277
HVAC 277
Water Leakage and Flooding 278
Environmental Alarms 278
Equipment Security 278
Corporate Procedures 278
Tamper Protection 278
Encryption 279
Inventory 279
Physical Protection of Security Devices 279
Tracking Devices 279
Portable Media Procedures 280
Safes, Vaults, and Locking 280
Exam Preparation Tasks 280
Review All Key Topics 280
Complete the Tables and Lists from Memory 282
Define Key Terms 282
Answer Review Questions 283
Answers and Explanations 288

Chapter 4 Communication and Network Security 293
Secure Network Design Principles 294
OSI Model 294
Application Layer 295
Presentation Layer 295
Session Layer 296
Transport Layer 296
Network Layer 296
Data Link Layer 297
Physical Layer 297
TCP/IP Model 298
Application Layer 299
Transport Layer 300
Internet Layer 302
Link Layer 304
Encapsulation 304
SNMP 322
Multi-Layer Protocols 322
Converged Protocols 323
  FCoE 324
  MPLS 324
  VoIP 325
  iSCSI 325
Wireless Networks 326
  FHSS, DSSS, OFDM, VOFDM, FDMA, TDMA, CDMA, OFDMA, and
    GSM 326
  802.11 Techniques 326
  Cellular or Mobile Wireless Techniques 327
  Satellites 327
  WLAN Structure 328
  Access Point 328
  SSID 328
Infrastructure Mode Versus Ad Hoc Mode 328
WLAN Standards 329
  802.11 329
  802.11a 329
  802.11ac 329
  802.11b 329
  802.11f 329
  802.11g 330
  802.11n 330
  Bluetooth 330
  Infrared 330
Near Field Communication (NFC) 331
WLAN Security 331
  Open System Authentication 331
  Shared Key Authentication 331
  WEP 331
  WPA 332
  WPA2 332
Personal Versus Enterprise 332
SSID Broadcast 333
  MAC Filter 333
Communications Cryptography 333
   Link Encryption 333
   End-to-End Encryption 334
   Email Security 334
   PGP 335
   MIME and S/MIME 335
   Quantum Cryptography 336
   Internet Security 336
   Remote Access 336
   SSL/TLS 337
   HTTP, HTTPS, and S-HTTP 337
   SET 337
   Cookies 338
   SSH 338
   IPsec 338

Secure Network Components 339
   Hardware 339
   Network Devices 340
   Network Routing 351
   Transmission Media 354
   Cabling 354
   Network Topologies 358
   Network Technologies 362
   WAN Technologies 369
   Network Access Control Devices 374
   Quarantine/Remediation 376
   Firewalls/Praxies 376
   Endpoint Security 376
   Content Distribution Networks 377

Secure Communication Channels 377
   Voice 377
   Multimedia Collaboration 377
   Remote Meeting Technology 378
   Instant Messaging 378
   Remote Access 379
   Remote Connection Technologies 379
   VPN Screen Scraper 388
Virtual Application/Desktop 388
Telecommuting 388
Virtualized Networks 389
SDN 389
Virtual SAN 389
Guest Operating Systems 390

Network Attacks 390
    Cabling 390
    Noise 390
    Attenuation 391
    Crosstalk 391
    Eavesdropping 391
    Network Component Attacks 391
    Non-Blind Spoofing 392
    Blind Spoofing 392
    Man-in-the-Middle Attack 392
    MAC Flooding Attack 392
    802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack 393
    Double-Encapsulated 802.1Q/Nested VLAN Attack 393
    ARP Attack 393
    ICMP Attacks 393
    Ping of Death 394
    Smurf 394
    Fraggle 394
    ICMP Redirect 394
    Ping Scanning 395
    Traceroute Exploitation 395
    DNS Attacks 395
    DNS Cache Poisoning 395
    DoS 396
    DDoS 396
    DNSSEC 396
    URL Hiding 397
    Domain Grabbing 397
    Cybersquatting 397
Chapter 5  Identity and Access Management  409

Access Control Process  410
   Identify Resources  410
   Identify Users  410
   Identify the Relationships Between Resources and Users  411

Physical and Logical Access to Assets  411
   Access Control Administration  412
      Centralized  412
      Decentralized  412

Provisioning Life Cycle  413
   Information  413
   Systems  413
   Devices  414
   Facilities  414

Identification and Authentication Concepts  415
   Five Factors for Authentication  415
      Knowledge Factors  416
      Ownership Factors  420
Characteristic Factors 422
Location Factors 427
Time Factors 427
Identification and Authentication Implementation 427
Separation of Duties 427
Least Privilege/Need-to-Know 428
Default to No Access 429
Directory Services 429
Single Sign-on 430
Kerberos 431
SESAME 433
Federated Identity Management 433
Security Domains 434
Session Management 434
Registration and Proof of Identity 434
Credential Management Systems 435
Accountability 436
Auditing and Reporting 437
Identity as a Service (IDaaS) Implementation 438
Third-Party Identity Services Implementation 439
Authorization Mechanisms 439
Access Control Models 439
Discretionary Access Control 440
Mandatory Access Control 440
Role-Based Access Control 440
Rule-Based Access Control 441
Content-Dependent Versus Context-Dependent 441
Access Control Matrix 442
Access Control Policies 442
Access Control Threats 443
Password Threats 443
Dictionary Attack 443
Brute-Force Attack 444
Social Engineering Threats 444
Phishing/Pharming 444
Shoulder Surfing 445
Identity Theft 445
Dumpster Diving 445
DoS/DDoS 445
Buffer Overflow 446
Mobile Code 446
Malicious Software 446
Spoofing 447
Sniffing and Eavesdropping 447
Emanating 447
Backdoor/Trapdoor 448
Prevent or Mitigate Access Control Threats 448
Exam Preparation Tasks 449
Review All Key Topics 449
Define Key Terms 449
Review Questions 450
Answers and Explanations 452

Chapter 6 Security Assessment and Testing 455
Assessment and Testing Strategies 456
Security Control Testing 456
Vulnerability Assessment 456
Penetration Testing 457
Log Reviews 459
NIST SP 800-92 460
Synthetic Transactions 464
Code Review and Testing 464
Misuse Case Testing 465
Test Coverage Analysis 466
Interface Testing 466
Collect Security Process Data 466
NIST SP 800-137 467
Account Management 467
Management Review 468
Key Performance and Risk Indicators 468
Backup Verification Data 469
Training and Awareness 469
Disaster Recovery and Business Continuity 470
Chapter 7  Security Operations  480

Investigations  481

Forensic and Digital Investigations  481
Identify Evidence  482
Preserve and Collect Evidence  483
Examine and Analyze Evidence  484
Present Findings  484
Decide  484
IOCE/SWGDE and NIST  484
Crime Scene  485
MOM  486
Chain of Custody  486
Interviewing  487
Evidence  487
Five Rules of Evidence  488
Types of Evidence  488
Surveillance, Search, and Seizure  490
Media Analysis  491
Software Analysis  491
Network Analysis  492
Hardware/Embedded Device Analysis  492

Investigation Types  493
Operations  493
Criminal  493
Civil  493
Regulatory  494
eDiscovery  494

Logging and Monitoring Activities  494
Audit and Review  494
Intrusion Detection and Prevention  495
Contents  xxvii

Security Information and Event Management (SIEM)  496
Continuous Monitoring  496
Egress Monitoring  496
Resource Provisioning  497
Asset Inventory  497
Configuration Management  498
Physical Assets  500
Virtual Assets  500
Cloud Assets  501
Applications  501
Security Operations Concepts  501
Need to Know/Least Privilege  501
Managing Accounts, Groups, and Roles  501
Separation of Duties  502
Job Rotation  503
Sensitive Information Procedures  503
Record Retention  504
Monitor Special Privileges  504
Information Life Cycle  504
Service-Level Agreements  505
Resource Protection  505
Protecting Tangible and Intangible Assets  505
Facilities  505
Hardware  506
Software  506
Information Assets  507
Asset Management  507
Redundancy and Fault Tolerance  507
Backup and Recovery Systems  508
Identity and Access Management  508
Media Management  509
Media History  513
Media Labeling and Storage  514
Sanitizing and Disposing of Media  514
Network and Resource Management  515
Incident Management  516
Event Versus Incident  516
Incident Response Team and Incident Investigations  516
Rules of Engagement, Authorization, and Scope 517
Incident Response Procedures 517
Incident Response Management 518
Detect 518
Respond 518
Mitigate 519
Report 519
Recover 519
Remediate 520
Lessons Learned and Review 520
Preventive Measures 520
Clipping Levels 520
Deviations from Standards 520
Unusual or Unexplained Events 521
Unscheduled Reboots 521
Unauthorized Disclosure 521
Trusted Recovery 521
Trusted Paths 521
Input/Output Controls 522
System Hardening 522
Vulnerability Management Systems 522
IDS/IPS 523
Firewalls 523
Whitelisting/Blacklisting 523
Third-Party Security Services 523
Sandboxing 524
Honeypots/Honeynets 524
Anti-malware/Antivirus 524
Patch Management 524
Change Management Processes 525
Recovery Strategies 526
Redundant Systems, Facilities, and Power 526
Fault-Tolerance Technologies 526
Insurance 527
Data Backup 527
Fire Detection and Suppression 527
High Availability 528
Contents

Quality of Service 528
System Resilience 529
Create Recovery Strategies 529
Categorize Asset Recovery Priorities 530
Business Process Recovery 530
Facility Recovery 531
Supply and Technology Recovery 534
User Environment Recovery 537
Data Recovery 537
Training Personnel 541
Disaster Recovery 541
Response 542
Personnel 542
Damage Assessment Team 543
Legal Team 543
Media Relations Team 543
Recovery Team 543
Relocation Team 543
Restoration Team 544
Salvage Team 544
Security Team 544
Communications 544
Assessment 544
Restoration 545
Training and Awareness 545
Testing Recovery Plans 545
Read-Through Test 546
Checklist Test 546
Table-Top Exercise 546
Structured Walk-Through Test 547
Simulation Test 547
Parallel Test 547
Full- Interruption Test 547
Functional Drill 547
Evacuation Drill 547
Business Continuity Planning and Exercises 547
Physical Security  548
   Perimeter Security  548
   Gates and Fences  549
   Perimeter Intrusion Detection  550
   Lighting  552
   Patrol Force  553
   Access Control  553
   Building and Internal Security  554
Personnel Privacy and Safety  554
   Duress  554
   Travel  555
   Monitoring  555
Exam Preparation Tasks  555
Review All Key Topics  555
Define Key Terms  556
Answer Review Questions  557
Answers and Explanations  560

Chapter 8  Software Development Security  565
Software Development Concepts  566
   Machine Languages  566
   Assembly Languages and Assemblers  566
   High-Level Languages, Compilers, and Interpreters  566
   Object-Oriented Programming  567
   Polymorphism  568
   Polymorphism  568
   Encapsulation  568
   Cohesion  569
   Coupling  569
   Data Structures  569
   Distributed Object-Oriented Systems  569
   CORBA  569
   COM and DCOM  570
   OLE  570
   Java  570
   SOA  571
   Mobile Code  571
   Java Applets  571
   ActiveX  571
Security in the System and Software Development Life Cycle 572

System Development Life Cycle 572

Initiate 572
Acquire/Develop 573
Implement 573
Operate/Maintain 573
Dispose 574

Software Development Life Cycle 574

Plan/Initiate Project 575
Gather Requirements 575
Design 576
Develop 576
Test/Validate 576
Release/Maintain 577
Certify/Accredit 578

Change Management and Configuration Management/Replacement 578

Software Development Methods and Maturity Models 578

Build and Fix 579
Waterfall 580
V-Shaped 580
Prototyping 582
Modified Prototype Model (MPM) 582
Incremental 582
Spiral 583
Agile 583

Rapid Application Development (RAD) 584
Joint Analysis Development (JAD) 585
Cleanroom 585
Structured Programming Development 585
Exploratory Model 586

Computer-Aided Software Engineering (CASE) 586
Component-Based Development 586
CMMI 586
Integrated Product Team 588

Security Controls in Development 589

Software Development Security Best Practices 589
WASC 590
OWASP 590
BSI 590
ISO/IEC 27000 590
Software Environment Security 591
Source Code Issues 591
Buffer Overflow 591
Escalation of Privileges 593
Backdoor 593
Rogue Programmers 594
Covert Channel 594
Object Reuse 594
Mobile Code 594
Time of Check/Time of Use (TOC/TOU) 595
Source Code Analysis Tools 595
Code Repository Security 595
Application Programming Interface Security 596
Software Threats 596
Malware 596
Malware Protection 600
Scanning Types 601
Security Policies 601
Software Protection Mechanisms 601
Assess Software Security Effectiveness 602
Auditing and Logging 603
Risk Analysis and Mitigation 603
Regression and Acceptance Testing 604
Security Impact of Acquired Software 604
Exam Preparation Tasks 605
Review All Key Topics 605
Define Key Terms 605
Answer Review Questions 606
Answers and Explanations 609

Glossary 613
Appendix A Memory Tables 671
Appendix B Memory Tables Answer Key 683
Index 782
About the Author

Robin M. Abernathy has been working in the IT certification preparation industry at Kaplan IT Certification Preparation, the owners of the Transcender and Self Test brands, for more than a decade. Robin has written and edited certification preparation materials for many (ISC)², Microsoft, CompTIA, PMI, Cisco, and ITIL 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 couple years, she has ventured into the traditional publishing industry by technically editing several publications and co-authoring Pearson’s CASP Cert Guide. She presents at technical conferences and hosts webinars on IT certification topics.

Dedication

For my husband, Michael, and my son, Jonas. You are everything!
Acknowledgments

I would be remiss if I did not first of all mention my gratitude to God for blessing me throughout my life. I do nothing on my own. It is only through Him that I have the strength and wisdom to accomplish my goals.

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 just starting. So thanks, Wayne McDaniel (a.k.a. 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 Zackie Bosarge, a great mentor, who gave me my first “real” job in the IT field at Alabama Institute for the Deaf and Blind.

Thanks also to my little family, my husband, Michael, and my son, Jonas. Thanks for being willing to have Friday night fun nights without me while I spent my extra time knee-deep in security topics. Thanks to Michael for always making sure I knew that everything was easier on a Mac. Thanks to Jonas for keeping mom humble by making sure she understood that you couldn’t see why someone was paying mom to write a book where Percy Jackson or Harry Potter was NOT the main character. I love you both immensely!

Pearson has put together an outstanding team to help me on my journey. Thanks to everyone at Pearson for polishing my work so brilliantly. Thanks especially to Chris Crayton and Troy McMillan for completing such thorough reviews of my work and even managing to make some great suggestions!

It is my wish that you, the reader, succeed in your IT certification and career goals. I wish you the very best.
About the Technical Reviewers

**Chris Crayton**, MCSE, is an author, technical consultant, and trainer. Formerly, he 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.

**Troy McMillan** writes practice tests, study guides, and online course materials for Kaplan IT Cert Prep, while also running his own consulting and training business. He holds over 30 industry certifications and also appears in training videos for OnCourse Learning and Pearson Press. Troy can be reached at mcmillantroy@hotmail.com.
We Want to Hear from You!

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

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

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

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

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
      ATTN: Reader Feedback
      800 East 96th Street
      Indianapolis, IN 46240 USA

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 9780789755186 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
Book Features and Exam Preparation 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. Therefore, this book does not try to help you pass the exams only by memorization but by truly learning and understanding the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it, but do not study it any further, you probably will not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you don’t know, and be well prepared for the exam. These tools include

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

- **Exam Preparation Tasks**: These sections list a series of study activities that should be done after reading the Foundation Topics section. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include

  - **Key Topics Review**: The Key Topic icon appears next to the most important items in the Foundation Topics section of the chapter. The Key Topics Review activity lists the key topics from the chapter and 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. Review these topics carefully.

  - **Definition of Key Terms**: Although certification exams might be unlikely to ask a question such as “Define this term,” the CISSP exam requires you to learn and know a lot of terminology. This section lists some of the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary.

  - **End of Chapter Review Questions**: Confirm that you understand the content that you just covered.

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 author 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 exclusive discounts on future editions of this product or related products. To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780789755186
3. Answer the challenge question as proof of purchase.
4. Click on 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.

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 these steps, visit www.pearsonITcertification.com/contact and select the Site Problems/Comments option. Our customer service representatives will assist you.

Pearson IT Certification Practice Test Engine and Questions

The companion website includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions. You can also serve up questions in a Flash Card Mode, which displays just the question and no answer, challenging you to state the answer in your own words before checking the actual answer to verify your work.

The installation process requires two major steps: installing the software and then activating the exam. The website has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam (the database of exam questions) is not on this site.

NOTE The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activation code. Also included on the paper is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.
Install the Software

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows virtual machine, but it was built specifically for the PC platform. The minimum system requirements are as follows:

- Windows 10, Windows 8.1, Windows 7, or Windows 8
- Microsoft .NET Framework 4.0 Client
- Pentium-class 1 GHz processor (or equivalent)
- 512 MB RAM
- 650 MB disk space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

The software installation process is routine as compared with other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the cardboard sleeve.

The following steps outline the installation process:

1. Download the exam practice test engine from the companion site.
2. Respond to Windows prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the cardboard sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

Once the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the My Products or Tools tab, click the Activate Exam button.
3. At the next screen, enter the activation key from the paper inside the cardboard sleeve in the back of the book. Once entered, click the **Activate** button.

4. The activation process downloads the practice exam. Click **Next**, and then click **Finish**.

When the activation process completes, the My Products tab should list your new exam. If you do not see the exam, make sure that you have selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam you have already activated and downloaded, display the **Tools** tab and click the **Update Products** button. Updating your exams ensures that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Certification Practice Test exam engine software, display the **Tools** tab and click the **Update Application** button. You can then ensure that you are running the latest version of the software engine.

**Activating Other Exams**

The exam software installation process and the registration process, only have to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another Pearson IT Certification Cert Guide, extract the activation code from the cardboard sleeve in the back of that book; you do not even need the exam engine at this point. From there, all you have to do is start the exam engine (if not still up and running) and perform steps 2 through 4 from the previous list.

**Assessing Exam Readiness**

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

**Premium Edition eBook and Practice Tests**

This book also includes an exclusive offer for 70% off the Premium Edition eBook and Practice Tests edition of this title. See the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.
This page intentionally left blank
This Introduction covers the following subjects:

- **The Goals of the CISSP Certification**: Describes the sponsoring bodies and the stated goals of the certification.

- **The Value of the CISSP Certification**: Examines the career and business drivers that comprise the value of the certification.

- **The Common Body of Knowledge**: Lists the eight domains of information that make up the topics covered in the certification.

- **Steps to Becoming a CISSP**: Describes the process involved in achieving CISSP certification.

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.
The CISSP Certification

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 Authorization Professional (CAP)
- Certified Secure Software Lifecycle Professional (CSSLP)
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 certification, 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 that the candidate 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 (e.g. Security, Risk, Compliance, Law, Regulations, Business Continuity)

The security and risk management domain covers a broad spectrum of general information security and risk management topics. Topics include:

- Concepts of confidentiality, integrity, and availability
- Security governance principles, including organizational processes and control frameworks
- Compliance with laws, regulations, and privacy requirements
- Professional ethics
- Security policies, standards, procedures, and guidelines
- Business continuity requirements
- Personnel security policies
- Risk management concepts
- Threat modeling
- Security risk considerations during acquisitions
- Information security education, training, and awareness

**Asset Security (Protecting Security of Assets)**

The asset security domain focuses on the collection, handling, and protection of information throughout its life cycle. Topics include:

- Information and supporting asset classification
- Asset ownership
- Privacy protection
- Asset retention
- Security controls
- Handling requirements

**Security Engineering (Engineering and Management of Security)**

The security engineering domain addresses the practice of building information systems and related architecture that deliver the required functionality when threats occur. Topics include:

- Engineering processes using secure design principles
- Security model concepts
- Control and countermeasure selection
- 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 and cyber-physical systems
- Cryptography
- Site and facility design
- Physical security
Communication and Network Security (Designing and Protecting Network Security)

The communication and network security domain focuses on protecting data in transit and securing the underlying networks over which the data travels. The topics include:

- Network architecture secure design principles
- Network components security
- Secure communication channels
- Network attacks

Identity and Access Management (Controlling Access and Managing Identity)

The identity and access management domain 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 asset access
- Identification and authentication of people and devices
- Identity as a Service integration
- Third-party identity service integration
- Authorization mechanisms
- Access control attacks
- Identity and access provisioning life cycle

Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

The security assessment and testing domain covers 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 areas, 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 and test strategies design and validation
- Security control testing
- Security process data collection
- Test output analysis and reporting
- Internal and third-party audits

**Security Operations (e.g. Foundational Concepts, Investigations, Incident Management, Disaster Recovery)**

The operations security domain surveys the execution of security measures and maintenance of proper security posture. Topics include:

- Investigations and investigation types
- Logging and monitoring activities
- Resource provisioning security
- Security operations concepts
- Resource protection techniques
- Incident management
- Preventive measures
- Patch and vulnerability management
- Change management process
- Recovery strategies
- Disaster recovery processes
- Disaster recovery plan testing
- Business continuity planning and testing
- Physical security
- Personnel safety concerns

**Software Development Security (Understanding, Applying, and Enforcing Software Security)**

The software development security domain explores the software development life cycle and development best practices. Topics include:

- System and software development life cycle
- Security controls in development environments
Steps to Becoming a CISSP

To become a CISSP, certain prerequisites must be met and procedures followed. This final section covers those topics.

Qualifying for the Exam

Candidates must have a minimum of five years of direct 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:

- Create a Pearson Vue account and schedule your exam.
- 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.
- Review the Candidate Background Questions.
- 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.
About the CISSP Exam

The CISSP exam is a computer-based test that the candidate can spend up to 6 hours completing. 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 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 test consists of 250 items with 4 choices per item. Some of the items will not be scored and are for research, and these are not identified to the candidate. The passing grade is 700 out of a possible 1,000. 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.
This page intentionally left blank
This chapter covers the following topics:

- **Security terms**: Concepts discussed include confidentiality, integrity, and availability (CIA); default stance; defense in depth; job rotation; and separation of duties.

- **Security governance principles**: Concepts discussed include security function alignment, organizational processes, security roles and responsibilities, control frameworks, due care, and due diligence.

- **Compliance**: Concepts discussed include legislative and regulatory compliance and privacy requirements compliance.

- **Legal and regulatory issues**: Concepts discussed include computer crime concepts, major legal systems, licensing and intellectual property, import/export controls, trans-border data flow, privacy, and data breaches.

- **Professional ethics**: Ethics discussed include (ISC)² Code of Ethics, Computer Ethics Institute, Internet Architecture Board, and organizational ethics.

- **Security documentation**: Documentation types include policies, standards, baselines, guidelines, and procedures.

- **Business continuity**: Concepts discussed include business continuity and disaster recovery concepts, project scope and plan, and business impact analysis.

- **Personnel security policies**: Policies discussed include employment candidate screening; employment agreement and policies; employment termination policies; vendor, consultant, and contractor controls; compliance; and privacy.

- **Risk management concepts**: Concepts discussed include vulnerability, threat, threat agent, risk, exposure, countermeasure, risk management policy, risk management team, risk analysis team, risk assessment, implementation, access control categories, access control types, control assessment, monitoring, measurement, reporting and continuous improvement, and risk frameworks.
- **Threat modeling**: Concepts discussed include identifying threats, potential attacks, and remediation technologies and processes.

- **Security risks in acquisitions**: Concepts discussed include hardware, software, and services; third-party governance; minimum security requirements; and minimum service-level requirements.

- **Security education, training, and awareness**: Concepts discussed include levels required and periodic review.

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

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

Business continuity and disaster recovery ensures that the organization can recover from any attack or disaster that affects operations. Using the results from the risks assessment, security professionals should ensure that the appropriate business continuity and disaster recovery plans are created, tested, and revised at appropriate intervals.
This chapter covers the following topics:

- **Access Control Process**: Concepts discussed include the steps of the access control process.
- **Physical and Logical Access to Assets**: Concepts discussed include access control administration, information access, systems access, device access, and facility access.
- **Identification and Authentication Concepts**: Concepts discussed include knowledge factors, ownership factors, characteristics factors, and time factors.
- **Identification and Authentication Implementation**: Concepts discussed include separation of duties, least privilege/need-to-know, default to no access, directory services, single sign-on, session management, registration and proof of identity, credential management systems, and accountability.
- **Identity as a Service (IDaaS) Implementation**: Describes the considerations when implementing IDaaS.
- **Third-Party Identity Services Implementation**: Details how to integrate third-party identity services in an enterprise.
- **Authorization Mechanisms**: Covers access control models and access control policies.
- **Access Control Threats**: Concepts discussed include password threats, social engineering threats, DoS/DDoS, buffer overflow, mobile code, malicious software, spoofing, sniffing and eavesdropping, emanating, and backdoor/trapdoor.
- **Prevent or Mitigate Access Control Threats**: Describes ways to prevent or mitigate access control threats.

Identity and Access Management is mainly concerned with controlling access to assets and managing identities. These assets include computers, equipment, networks, and applications. Security professionals must understand how to control physical and logical access to the assets and manage identification, authentication, and authorization systems. Finally, the access control threats must be addressed.
Identity and Access Management

Identity and access management involve how access management works, why identity and access management (IAM) are important, and how IAM components and devices work together in an enterprise. Access control allows only authorized users, applications, devices, and systems to access enterprise resources and information. It includes facilities, support systems, information systems, network devices, and personnel. Security professionals use access controls to specify which users can access a resource, which resources can be accessed, which operations can be performed, and which actions will be monitored. Once again, the CIA triad is important in providing enterprise IAM.
Foundation Topics

Access Control Process

Although many approaches to implementing access controls have been designed, all the approaches generally involve the following steps:

1. Identify resources.
2. Identify users.
3. Identify the relationships between the resources and users.

Identify Resources

This first step in the access control process involves defining all resources in the IT infrastructure by deciding which entities need to be protected. When defining these resources, you must also consider how the resources will be accessed. The following questions can be used as a starting point during resource identification:

- Will this information be accessed by members of the general public?
- Should access to this information be restricted to employees only?
- Should access to this information be restricted to a smaller subset of employees?

Keep in mind that data, applications, services, servers, and network devices are all considered resources. Resources are any organizational asset that users can access. In access control, resources are often referred to as objects.

Identify Users

After identifying the resources, an organization should identify the users who need access to the resources. A typical security professional must manage multiple levels of users who require access to organizational resources. During this step, only identifying the users is important. The level of access these users will be given will be analyzed further in the next step.

As part of this step, you must analyze and understand the users’ needs and then measure the validity of those needs against organizational needs, policies, legal issues, data sensitivity, and risk.

Remember that any access control strategy and the system deployed to enforce it should avoid complexity. The more complex an access control system is, the harder
that system is to manage. In addition, anticipating security issues that could occur in more complex systems is much harder. As security professionals, we must balance the organization’s security needs and policies with the needs of the users. If a security mechanism that we implement causes too much difficulty for the user, the user might engage in practices that subvert the mechanisms that we implement. For example, if you implement a password policy that requires a very long, complex password, users might find remembering their passwords to be difficult. Users might then write their passwords on sticky notes that are attached to their monitor or keyboard.

**Identify the Relationships Between Resources and Users**

The final step in the access control process is to define the access control levels that need to be in place for each resource and the relationships between the resources and users. For example, if an organization has defined a web server as a resource, general employees might need a less restrictive level of access to the resource than the public and a more restrictive level of access to the resource than the web development staff. Access controls should be designed to support the business functionality of the resources that are being protected. Controlling the actions that can be performed for a specific resource based on a user’s role is vital.

**Physical and Logical Access to Assets**

Access control is all about using physical or logical controls to control who has access to a network, system, or device. It also involves what type of access is given to the network, system, or device. Access control is primarily provided using physical and logical controls.

**NOTE** Physical and logical access controls are covered in more depth in Chapter 1, “Security and Risk Management.”

Physical access focuses on controlling access to a network, system, or device. In most cases, physical access involves using access control to prevent users from being able to touch network components (including wiring), systems, or devices. While locks are the most popular physical access control method to preventing access to devices in a data center, other physical controls, such as guards and biometrics, should also be considered, depending on the needs of the organization and the value of the asset being protected.

Logical controls limit the access a user has through software or hardware components. Authentication and encryption are examples of logical controls.
When installing an access control system, security professionals should understand who needs access to the asset being protected and how those users need to access the asset. When multiple users need access to an asset, the organization should set up a multi-layer access control system. For example, users wanting access to the building may only need to sign in with a security guard. However, to access the locked data center within the same building, users would need a smart card. Both of these would be physical access controls. To protect data on a single server within the building (but not in the data center), the organization would need to deploy such mechanisms as authentication, encryption, and access control lists (ACLs) as logical access controls but could also place the server in a locked server room to provide physical access control.

When deploying physical and logical access controls, security professionals must understand the access control administration methods and the different assets that must be protected and their possible access controls.

**Access Control Administration**

Access control administration occurs in two basic manners: centralized and decentralized.

**Centralized**

In centralized access control, a central department or personnel oversees the access for all organizational resources. This administration method ensures that user access is controlled in a consistent manner across the entire enterprise. However, this method can be slow because all access requests are processed by the central entity.

**Decentralized**

In decentralized access control, personnel closest to the resources, such as department managers and data owners, oversee the access control for individual resources. This administration method ensures that those who know the data control the access rights to it. However, this method can be hard to manage because not just one entity is responsible for configuring access rights, thereby losing the uniformity and fairness of security.

Some companies may implement a hybrid approach that includes both centralized and decentralized access control. In this deployment model, centralized administration is used for basic access, but granular access to individual assets, such as data on a departmental server, is handled by the data owner.
Provisioning Life Cycle

Organizations should create a formal process for creating, changing, and removing users, which is the provisioning life cycle. This process includes user approval, user creation, user creation standards, and authorization. Users should sign a written statement that explains the access conditions, including user responsibilities. Finally, access modification and removal procedures should be documented.

User provision policies should be integrated as part of human resource management. Human resource policies should include procedures whereby the human resource department formally requests the creation or deletion of a user account when new personnel are hired or terminated.

Information

To fully protect information that is stored on an organization’s network, servers, or other devices, security professionals must provide both physical and logical access controls. The physical access controls, such as placing devices in a locked room, protect the devices on which the information resides. The logical access controls—such as deploying data or drive encryption, transport encryption, ACLs, and firewalls—protect the data from unauthorized access.

The value of the information being protected will likely determine the controls that an organization is willing to deploy. For example, regular correspondence on a client computer will likely not require the same controls as financial data stored on a server. For the client computer, the organization may simply deploy a local software firewall and appropriate ACL permissions on the local folders and files. For the server, the organization may need to deploy more complex measures, including drive encryption, transport encryption, ACLs, and other measures.

Systems

To fully protect the systems used by the organization, including client and server computers, security professionals may rely on both physical and logical access controls. However, some systems, like client computers, may be deployed in such a manner that only minimal physical controls are used. If a user is granted access to a building, he or she may find client computers being used in non-secure cubicles throughout the building. For these systems, a security professional must ensure that the appropriate authentication mechanisms are deployed. If confidential information is stored on the client computers, encryption should also be deployed. But only the organization can best determine which controls to deploy on individual client computers.
When it comes to servers, determining which access controls to deploy is usually a more complicated process. Security professionals should work with the server owner, whether it is a department head or an IT professional, to determine the value of the asset and the needed protection. Of course, most servers should be placed in a locked room. In many cases, this will be a data center or server room. However, servers can be deployed in regular locked offices if necessary. In addition, other controls should be deployed to ensure that the system is fully protected. The access control needs of a file server are different from those of a web server or database server. It is vital that the organization perform a thorough assessment of the data that is being processed and stored on the system before determining which access controls to deploy. If limited resources are available, security professionals must ensure that their most important systems have more access controls than other systems.

**Devices**

As with systems, physical access to devices is best provided by placing the devices in a secure room. Logical access to devices is provided by implementing the appropriate ACL or rule list, authentication, and encryption, as well as securing any remote interfaces that are used to manage the device. In addition, security professionals should ensure that the default accounts and passwords are changed or disabled on the device.

For any IT professionals that need to access the device, a user account should be configured for the professional with the appropriate level of access needed. If a remote interface is used, make sure to enable encryption, such as SSL, to ensure that communication via the remote interface is not intercepted and read. Security professionals should closely monitor vendor announcements for any devices to ensure that the devices are kept up to date with the latest security patches and firmware updates.

**Facilities**

With facilities, the primary concern is physical access, which can be provided using locks, fencing, bollards, guards, and closed-circuit television (CCTV). Many organizations think that such measures are enough. But with today’s advanced industrial control systems and the Internet of Things (IoT), organizations must also consider any devices involved in facility security. If an organization has an alarm/security system that allows remote viewing access from the Internet, the appropriate logical controls must be in place to prevent a malicious user from accessing the system and changing its settings or from using the system to gain inside information about the facility layout and day-to-day operations. If the organization uses an industrial control system (ICS), logical controls should also be a priority. Security professionals
must work with organizations to ensure that physical and logical controls are implemented appropriately to ensure that the entire facility is protected.

**Identification and Authentication Concepts**

To be able to access a resource, a user must profess his identity, provide the necessary credentials, and have the appropriate rights to perform the tasks he is completing. The first step in this process is called identification, which is the act of a user professing an identity to an access control system.

Authentication, the second part of the process, is the act of validating a user with a unique identifier by providing the appropriate credentials. When trying to differentiate between the two, security professionals should know that identification identifies the user and authentication verifies that the identity provided by the user is valid. Authentication is usually implemented through a user password provided at logon. When a user logs in to a system, the login process should validate the login after the user supplies all the input data.

After a user is authenticated, the user must be granted the rights and permissions to resources. The process is referred to as authorization.

The most popular forms of user identification include user IDs or user accounts, account numbers, and personal identification numbers (PINs).

**Five Factors for Authentication**

After establishing the user identification method, an organization must decide which authentication method to use.

Authentication methods are divided into five broad categories:

- **Knowledge factor authentication**: Something a person knows
- **Ownership factor authentication**: Something a person has or possesses
- **Characteristic factor authentication**: Something a person is
- **Location factor authentication**: Somewhere a person is
- **Time factor authentication**: The time a person is authenticating

Authentication usually ensures that a user provide at least one factor from these categories, which is referred to as single-factor authentication. An example of this would be providing a username and password at login. Two-factor authentication ensures that the user provides two of the five factors. An example of two-factor authentication would be providing a username, password, and smart card at login. Three-factor authentication ensures that a user provides three factors. An example
of three-factor authentication would be providing a username, password, smart card, and fingerprint at login. For authentication to be considered strong authentication, a user must provide factors from at least two different categories. (Note that the username is the identification factor, not an authentication factor.)

**NOTE** Originally there were three factors (something you know, something you have, and something you are). They were referred to as Type I, Type II, and Type III factors, respectively. However, modern technology has forced the security field to recently recognize two additional factors: somewhere you are and the time of authentication.

You should understand that providing multiple authentication factors from the same category is still considered single-factor authentication. For example, if a user provides a username, password, and the user’s mother’s maiden name, single-factor authentication is being used. In this example, the user is still only providing factors that are something a person knows.

**Knowledge Factors**

As briefly described in the preceding section, *knowledge factor* authentication is authentication that is provided based on something that a person knows. Although the most popular form of authentication used by this category is password authentication, other knowledge factors can be used, including date of birth, mother’s maiden name, key combination, or PIN.

**Identity and Account Management**

Identity and account management is vital to any authentication process. As a security professional, you must ensure that your organization has a formal procedure to control the creation and allocation of access credentials or identities. If invalid accounts are allowed to be created and are not disabled, security breaches will occur. Most organizations implement a method to review the identification and authentication process to ensure that user accounts are current. Questions that are likely to help in the process include:

- Is a current list of authorized users and their access maintained and approved?
- Are passwords changed at least every 90 days or earlier if needed?
- Are inactive user accounts disabled after a specified period of time?
Any identity management procedure must include processes for creating (provisioning), changing and monitoring (reviewing), and removing users from the access control system (revoking). This is referred to as the provisioning life cycle. When initially establishing a user account, new users should be required to provide valid photo identification and should sign a statement regarding password confidentiality. User accounts must be unique. Policies should be in place that standardize the structure of user accounts. For example, all user accounts should be firstname.lastname or some other structure. This ensures that users within an organization will be able to determine a new user’s identification, mainly for communication purposes.

After creation, user accounts should be monitored to ensure that they remain active. Inactive accounts should be automatically disabled after a certain period of inactivity based on business requirements. In addition, any termination policy should include formal procedures to ensure that all user accounts are disabled or deleted. Elements of proper account management include the following:

- Establish a formal process for establishing, issuing, and closing user accounts.
- Periodically review user accounts.
- Implement a process for tracking access authorization.
- Periodically rescreen personnel in sensitive positions.
- Periodically verify the legitimacy of user accounts.

User account reviews are a vital part of account management. User accounts should be reviewed for conformity with the principle of least privilege. (The principle of least privilege is explained later in this chapter.) User account reviews can be performed on an enterprise-wide, system-wide, or application-by-application basis. The size of the organization will greatly affect which of these methods to use. As part of user account reviews, organizations should determine whether all user accounts are active.

Password Types and Management

As mentioned earlier, password authentication is the most popular authentication method implemented today. However, password types can vary from system to system. Understanding all the types of passwords that can be used is vital.

The types of passwords that you should be familiar with include:

- **Standard word or simple passwords**: As the name implies, these passwords consist of single words that often include a mixture of upper- and lowercase letters and numbers. The advantage of this password type is that it is easy to
remember. A disadvantage of this password type is that it is easy for attackers to crack or break, resulting in a compromised account.

- **Combination passwords**: This password type uses a mix of dictionary words, usually two unrelated words. These are also referred to as composition passwords. Like standard word passwords, they can include upper- and lowercase letters and numbers. An advantage of this password is that it is harder to break than simple passwords. A disadvantage is that it can be hard to remember.

- **Static passwords**: This password type is the same for each login. It provides a minimum level of security because the password never changes. It is most often seen in peer-to-peer networks.

- **Complex passwords**: This password type forces a user to include a mixture of upper- and lowercase letters, numbers, and special characters. For many organizations today, this type of password is enforced as part of the organization’s password policy. An advantage of this password type is that it is very hard to crack. A disadvantage is that it is harder to remember and can often be much harder to enter correctly than standard or combination passwords.

- **Passphrase passwords**: This password type requires that a long phrase be used. Because of the password’s length, it is easier to remember but much harder to attack, both of which are definite advantages. Incorporating upper- and lowercase letters, numbers, and special characters in this type of password can significantly increase authentication security.

- **Cognitive passwords**: This password type is a piece of information that can be used to verify an individual’s identity. This information is provided to the system by answering a series of questions based on the user’s life, such as favorite color, pet’s name, mother’s maiden name, and so on. An advantage to this type is that users can usually easily remember this information. The disadvantage is that someone who has intimate knowledge of the person’s life (spouse, child, sibling, and so on) might be able to provide this information as well.

- **One-time passwords**: Also called a dynamic password, this type of password is only used once to log in to the access control system. This password type provides the highest level of security because passwords are discarded when they are used.

- **Graphical passwords**: Also called CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, passwords, this type of password uses graphics as part of the authentication mechanism. One popular implementation requires a user to enter a series of characters in the graphic displayed. This implementation ensures that a human
is entering the password, not a robot. Another popular implementation requires the user to select the appropriate graphic for his account from a list of graphics given.

- **Numeric passwords**: This type of password includes only numbers. Keep in mind that the choices of a password are limited by the number of digits allowed. For example, if all passwords are 4 digits, then the maximum number of password possibilities is 10,000, from 0000 through 9999. After an attacker realizes that only numbers are used, cracking user passwords would be much easier because the possibilities would be known.

Passwords are considered weaker than passphrases, one-time passwords, token devices, and login phrases. After an organization has decided which type of password to use, the organization must establish its password management policies. Password management considerations include, but might not be limited to:

- **Password life**: How long the password will be valid. For most organizations, passwords are valid for 60 to 90 days.
- **Password history**: How long before a password can be reused. Password policies usually remember a certain number of previously used passwords.
- **Authentication period**: How long a user can remain logged in. If a user remains logged in for the period without activity, the user will be automatically logged out.
- **Password complexity**: How the password will be structured. Most organizations require upper- and lowercase letters, numbers, and special characters.
- **Password length**: How long the password must be. Most organizations require 8–12 characters.
- **Password masking**: Prevents a password from being learned through shoulder surfing by obscuring the characters entered except for the last one.

As part of password management, organizations should establish a procedure for changing passwords. Most organizations implement a service that allows users to automatically reset their password before the password expires. In addition, most organizations should consider establishing a password reset policy in cases where users have forgotten their password or passwords have been compromised. A self-service password reset approach allows users to reset their own passwords without the assistance of help desk employees. An assisted password reset approach requires that users contact help desk personnel for help in changing their passwords.

Password reset policies can also be affected by other organizational policies, such as account lockout policies. Account lockout policies are security policies that organizations
implement to protect against attacks that are carried out against passwords. Organizations often configure account lockout policies so that user accounts are locked after a certain number of unsuccessful login attempts. If an account is locked out, the system administrator might need to unlock or re-enable the user account. Security professionals should also consider encouraging organizations to require users to reset their password if their account has been locked or after a password has been used for a certain amount of time (90 days for most organizations). For most organizations, all the password policies, including account lockout policies, are implemented at the enterprise level on the servers that manage the network. Account lockout policies are most often used to protect against brute-force or dictionary attacks.

**NOTE** An older term that you might need to be familiar with is *clipping level*. A clipping level is a configured baseline threshold above which violations will be recorded. For example, an organization might want to start recording any unsuccessful login attempts after the first one, with account lockout occurring after five failed attempts.

Depending on which servers are used to manage the enterprise, security professionals must be aware of the security issues that affect user account and password management. Two popular server operating systems are Linux and Windows.

For Linux, passwords are stored in the `/etc/passwd` and `/etc/shadow` file. Because the `/etc/passwd` file is a text file that can be easily accessed, you should ensure that any Linux servers use the `/etc/shadow` file where the passwords in the file can be protected using a hash. The root user in Linux is a default account that is given administrative-level access to the entire server. If the root account is compromised, all passwords should be changed. Access to the root account should be limited only to systems administrators, and root login should only be allowed via a local system console, not remotely.

For Windows computers that are in workgroups, the Security Accounts Manager (SAM) stores user passwords in a hashed format. However, known security issues exist with a SAM, including the ability to dump the password hashes directly from the registry. You should take all Microsoft-recommended security measures to protect this file. If you manage a Windows network, you should change the name of the default Administrator account or disable it. If this account is retained, make sure that you assign it a password. The default Administrator account might have full access to a Windows server.

**Ownership Factors**

*Ownership factor authentication* is authentication that is provided based on something that a person has. Ownership factors can include token devices, memory cards, and smart cards.
Synchronous and Asynchronous Token

The token device (often referred to as a password generator) is a handheld device that presents the authentication server with the one-time password. If the authentication method requires a token device, the user must be in physical possession of the device to authenticate. So although the token device provides a password to the authentication server, the token device is considered an ownership authentication factor because its use requires ownership of the device.

Two basic token device authentication methods are used: synchronous or asynchronous. A synchronous token generates a unique password at fixed time intervals with the authentication server. An asynchronous token generates the password based on a challenge/response technique with the authentication server, with the token device providing the correct answer to the authentication server’s challenge.

A token device is usually only implemented in very secure environments because of the cost of deploying the token device. In addition, token-based solutions can experience problems because of the battery lifespan of the token device.

Memory Cards

A memory card is a swipe card that is issued to valid users. The card contains user authentication information. When the card is swiped through a card reader, the information stored on the card is compared to the information that the user enters. If the information matches, the authentication server approves the login. If it does not match, authentication is denied.

Because the card must be read by a card reader, each computer or access device must have its own card reader. In addition, the cards must be created and programmed. Both of these steps add complexity and cost to the authentication process. However, it is often worth the extra complexity and cost for the added security it provides, which is a definite benefit of this system. However, the data on the memory cards is not protected, a weakness that organizations should consider before implementing this type of system. Memory-only cards are very easy to counterfeit.

Smart Cards

Similar to a memory card, a smart card accepts, stores, and sends data but can hold more data than a memory card. Smart cards, often known as integrated circuit cards (ICCs), contain memory like a memory card but also contain an embedded chip like bank or credit cards. Smart cards use card readers. However, the data on the smart card is used by the authentication server without user input. To protect against lost or stolen smart cards, most implementations require the user to input a secret
PIN, meaning the user is actually providing both a knowledge (PIN) and ownership (smart card) authentication factor.

Two basic types of smart cards are used: contact cards and contactless cards. Contact cards require physical contact with the card reader, usually by swiping. Contactless cards, also referred to as proximity cards, simply need to be in close proximity to the reader. Hybrid cards are available that allow a card to be used in both contact and contactless systems.

For comparative purposes, security professionals should remember that smart cards have processing power due to the embedded chips. Memory cards do not have processing power. Smart card systems are much more reliable than memory card systems.

Smart cards are even more expensive to implement than memory cards. Many organizations prefer smart cards over memory cards because they are harder to counterfeit and the data on them can be protected using encryption.

**Characteristic Factors**

*Characteristic factor authentication* is authentication that is provided based on something that a person is. Biometric technology is the technology that allows users to be authenticated based on physiological or behavioral characteristics. Physiological characteristics include any unique physical attribute of the user, including iris, retina, and fingerprints. Behavioral characteristics measure a person’s actions in a situation, including voice patterns and data entry characteristics.

Biometric technologies are now starting to creep into some of the most popular operating systems. Examples include Windows Hello and Apple’s Touch ID technology. As a security professional, you need to be aware of such new technologies as they are deployed to provide added security. Educating users on these technologies should also be a priority to ensure that users adopt these technologies as they are deployed.

**Physiological Characteristics**

Physiological systems use a biometric scanning device to measure certain information about a physiological characteristic. You should understand the following physiological biometric systems:

- Fingerprint
- Finger scan
- Hand geometry
- Hand topography
- Palm or hand scans
- Facial scans
- Retina scans
- Iris scans
- Vascular scans

A fingerprint scan usually scans the ridges of a finger for matching. A special type of fingerprint scan called minutiae matching is more microscopic in that it records the bifurcations and other detailed characteristics. Minutiae matching requires more authentication server space and more processing time than ridge fingerprint scans. Fingerprint scanning systems have a lower user acceptance rate than many systems because users are concerned with how the fingerprint information will be used and shared.

A finger scan extracts only certain features from a fingerprint. Because a limited amount of the fingerprint information is needed, finger scans require less server space or processing time than any type of fingerprint scan.

A hand geometry scan usually obtains size, shape, or other layout attributes of a user’s hand but can also measure bone length or finger length. Two categories of hand geometry systems are mechanical and image-edge detective systems. Regardless of which category is used, hand geometry scanners require less server space and processing time than fingerprint or finger scans.

A hand topography scan records the peaks and valleys of the hand and its shape. This system is usually implemented in conjunction with hand geometry scans because hand topography scans are not unique enough if used alone.

A palm or hand scan combines fingerprint and hand geometry technologies. It records fingerprint information from every finger as well as hand geometry information.

A facial scan records facial characteristics, including bone structure, eye width, and forehead size. This biometric method uses eigenfeatures or eigenfaces. Neither of these methods actually captures a picture of a face. With eigenfeatures, the distance between facial features are measured and recorded. With eigenfaces, measurements of facial components are gathered and compared to a set of standard eigenfaces. For example, a person’s face might be composed of the average face plus 21% from eigenface 1, 83% from eigenface 2, and –18% from eigenface 3. Many facial scan biometric devices will use a combination of eigenfeatures and eigenfaces.
A retina scan scans the retina’s blood vessel pattern. A retina scan is considered more intrusive than an iris scan.

An iris scan scans the colored portion of the eye, including all rifts, coronas, and furrows. Iris scans have a higher accuracy than any other biometric scan.

A vascular scan scans the pattern of veins in the user’s hand or face. Although this method can be a good choice because it is not very intrusive, physical injuries to the hand or face, depending on which the system uses, could cause false rejections.

Behavioral Characteristics

Behavioral systems use a biometric scanning device to measure a person’s actions. You should understand the following behavioral biometric systems:

- Signature dynamics
- Keystroke dynamics
- Voice pattern or print

Signature dynamics measure stroke speed, pen pressure, and acceleration and deceleration while the user writes his signature. Dynamic Signature Verification (DSV) analyzes signature features and specific features of the signing process.

Keystroke dynamics measure the typing pattern that a user uses when inputting a password or other predetermined phrase. In this case, even if the correct password or phrase is entered but the entry pattern on the keyboard is different, the user will be denied access. Flight time, a term associated with keystroke dynamics, is the amount of time it takes to switch between keys. Dwell time is the amount of time you hold down a key.

Voice pattern or print measures the sound pattern of a user stating a certain word. When the user attempts to authenticate, he will be asked to repeat those words in different orders. If the pattern matches, authentication is allowed.

Biometric Considerations

When considering biometric technologies, security professionals should understand the following terms:

- **Enrollment time**: The process of obtaining the sample that is used by the biometric system. This process requires actions that must be repeated several times.

- **Feature extraction**: The approach to obtaining biometric information from a collected sample of a user’s physiological or behavioral characteristics.
- **Accuracy**: The most important characteristic of biometric systems. It is how correct the overall readings will be.

- **Throughput rate**: The rate at which the biometric system will be able to scan characteristics and complete the analysis to permit or deny access. The acceptable rate is 6–10 subjects per minute. A single user should be able to complete the process in 5–10 seconds.

- **Acceptability**: Describes the likelihood that users will accept and follow the system.

- **False rejection rate (FRR)**: A measurement of valid users that will be falsely rejected by the system. This is called a Type I error.

- **False acceptance rate (FAR)**: A measurement of the percentage of invalid users that will be falsely accepted by the system. This is called a Type II error. Type II errors are more dangerous than Type I errors.

- **Crossover error rate (CER)**: The point at which FRR equals FAR. Expressed as a percentage, this is the most important metric.

When analyzing biometric systems, security professionals often refer to a Zephyr chart that illustrates the comparative strengths and weaknesses of biometric systems. However, you should also consider how effective each biometric system is and its level of user acceptance. The following is a list of the more popular biometric methods ranked by effectiveness, with the most effective being first:

1. Iris scan
2. Retina scan
3. Fingerprint
4. Hand print
5. Hand geometry
6. Voice pattern
7. Keystroke pattern
8. Signature dynamics

The following is a list of the more popular biometric methods ranked by user acceptance, with the methods that are ranked more popular by users being first:

1. Voice pattern
2. Keystroke pattern
3. Signature dynamics
4. Hand geometry
5. Hand print
6. Fingerprint
7. Iris scan
8. Retina scan

When considering FAR, FRR, and CER, smaller values are better. FAR errors are more dangerous than FRR errors. Security professionals can use the CER rate for comparative analysis when helping their organization decide which system to implement. For example, voice print systems usually have higher CERs than iris scans, hand geometry, or fingerprints.

Figure 5-1 shows the biometric enrollment and authentication process.
Location Factors

*Location factor authentication* provides a means of authenticating the user based on the location from which the user is authenticating. This could include the computer or device the person is using or his or her geographic location based on GPS coordinates. The primary appeal to this type of authentication is that it limits the user to logging in from those certain locations only. This is particularly useful in large manufacturing environments for users who should only log in to certain terminals in the facility.

Geo-fencing is one example of the use of location factors. With geo-fencing, devices only operate correctly within the geo-fence boundaries. If a device enters or exits the geo-fenced area, an alert is generated and sent to the operator.

Time Factors

*Time factor authentication* authenticates a user based on the time and/or date the user is authenticating. For example, if certain users work only a set schedule, you can configure their accounts to only allow them to log in during those set work hours. However, keep in mind that such a limitation could cause administrative issues if overtime hours are allowed. Some organizations implement this effectively by padding the allowed hours with an hour or two leeway for the start and end times. Credit cards use this feature effectively to protect their customers. If transactions take place in a short timeframe from geographically dispersed locations, credit cards will often block the second transaction.

Identification and Authentication Implementation

Identification and authentication are necessary steps to providing authorization. Authorization is the point after identification and authentication at which a user is granted the rights and permissions to resources. The next sections cover important components in authorization: separation of duties, least privilege/need-to-know, default to no access, directory services, single sign-on (including Kerberos, SESAME, Federated Identity Management, and security domains), session management, registration and proof of identity, credential management systems, and accountability.

Separation of Duties

Separation of duties is an important concept to keep in mind when designing an organization’s authentication and authorization policies. Separation of duties prevents fraud by distributing tasks and their associated rights and privileges between more than one user. This helps deter fraud and collusion because any fraudulent act can occur only if there is collusion. A good example of separation of duties is
authorizing one person to manage backup procedures and another to manage re-
store procedures.

Separation of duties is associated with dual controls and split knowledge. With dual 
controls, two or more users are authorized and required to perform certain func-
tions. For example, a retail establishment might require two managers to open the 
safe. Split knowledge ensures that no single user has all the information to perform a 
particular task. An example of a split control is the military’s requiring two individu-
als to each enter a unique combination to authorize missile firing.

**Least Privilege/Need-to-Know**

The principle of least privilege requires that a user or process is given only the 
minimum access privilege needed to perform a particular task. Its main purpose is 
to ensure that users only have access to the resources they need and are authorized 
to perform only the tasks they need to perform. To properly implement the least 
privilege principle, organizations must identify all users’ jobs and restrict users only 
to the identified privileges.

The need-to-know principle is closely associated with the concept of least privilege.
Although least privilege seeks to reduce access to a minimum, the need-to-know 
principle actually defines what the minimums for each job or business function are.
Excessive privileges become a problem when a user has more rights, privileges, and 
permissions than he needs to do his job. Excessive privileges are hard to control in 
large environments.

A common implementation of the least privilege and need-to-know principles is 
when a systems administrator is issued both an administrative-level account and 
a normal user account. In most day-to-day functions, the administrator should use 
his normal user account. When the systems administrator needs to perform 
administrative-level tasks, he should use the administrative-level account. If the 
administrator uses his administrative-level account while performing routine tasks, 
he risks compromising the security of the system and user accountability.

Organizational rules that support the principle of least privilege include the 
following:

- Keep the number of administrative accounts to a minimum.
- Administrators should use normal user accounts when performing routine 
operations.
- Permissions on tools that are likely to be used by attackers should be as restric-
tive as possible.
To more easily support the least privilege and need-to-know principles, users should be divided into groups to facilitate the confinement of information to a single group or area. This process is referred to as compartmentalization.

**Default to No Access**

During the authorization process, you should configure an organization’s access control mechanisms so that the default level of security is to default to *no access*. This means that if nothing has been specifically allowed for a user or group, then the user or group will not be able to access the resource. The best security approach is to start with no access and add rights based on a user’s need to know and least privilege needed to accomplish his daily tasks.

**Directory Services**

A directory service is a database designed to centralize data management regarding network subjects and objects. A typical directory contains a hierarchy that includes users, groups, systems, servers, client workstations, and so on. Because the directory service contains data about users and other network entities, it can be used by many applications that require access to that information.

The most common directory service standards are

- X.500
- Lightweight Directory Access Protocol (LDAP)
- X.400
- Active Directory Domain Services (AD DS)

X.500 uses the directory access protocol (DAP). In X.500, the distinguished name (DN) provides the full path in the X.500 database where the entry is found. The relative distinguished name (RDN) in X.500 is an entry’s name without the full path.

Based on X.500’s DAP, LDAP is simpler than X.500. LDAP supports DN and RDN, but includes more attributes such as the common name (CN), domain component (DC), and organizational unit (OU) attributes. Using a client/server architecture, LDAP uses TCP port 389 to communicate. If advanced security is needed, LDAP over SSL communicates via TCP port 636.

X.400 is mainly for message transfer and storage. It uses elements to create a series of name/value pairs separated by semicolons. X.400 has gradually been replaced by Simple Mail Transfer Protocol (SMTP) implementations.

Microsoft’s implementation of LDAP is Active Directory Domain Services (AD DS), which stores and organizes directory data into trees and forests. It also manages
logon processes and authentication between users and domains and allows administrators to logically group users and devices into organizational units.

**Single Sign-on**

In a single sign-on (SSO) environment, a user enters his login credentials once and can access all resources in the network. The Open Group Security Forum has defined many objectives for an SSO. Some of the objectives for the user sign-on interface and user account management include the following:

- The interface should be independent of the type of authentication information handled.
- The creation, deletion, and modification of user accounts should be supported.
- Support should be provided for a user to establish a default user profile.
- They should be independent of any platform or operating system.

**NOTE** To obtain more information about the Open Group’s Single Sign-On Standard, you should access the website at www.opengroup.org/security/sso_scope.htm.

SSO provides many advantages and disadvantages when it is implemented.

**Key Topic**

**Advantages of an SSO system include:**

- Users are able to use stronger passwords.
- User and password administration is simplified.
- Resource access is much faster.
- User login is more efficient.
- Users only need to remember the login credentials for a single system.

**Disadvantages of an SSO system include:**

- After a user obtains system access through the initial SSO login, the user is able to access all resources to which he is granted access. Although this is also an advantage for the user (only one login needed), it is also considered a disadvantage because only one sign-on can compromise all the systems that participate in the SSO network.
- If a user’s credentials are compromised, attackers will have access to all resources to which the user has access.
Although the discussion on SSO so far has been mainly on how it is used for networks and domains, SSO can also be implemented in web-based systems. Enterprise Access Management (EAM) provides access control management for web-based enterprise systems. Its functions include accommodation of a variety of authentication methods and role-based access control.

SSO can be implemented in Kerberos and Secure European System for Applications in a Multi-vendor Environment (SESAME) environments.

**Kerberos**

Kerberos is an authentication protocol that uses a client/server model developed by MIT’s Project Athena. It is the default authentication model in the recent editions of Windows Server and is also used in Apple, Sun, and Linux operating systems. Kerberos is an SSO system that uses symmetric key cryptography. Kerberos provides confidentiality and integrity.

Kerberos assumes that messaging, cabling, and client computers are not secure and are easily accessible. In a Kerberos exchange involving a message with an authenticator, the authenticator contains the client ID and a timestamp. Because a Kerberos ticket is valid for a certain time, the timestamp ensures the validity of the request.

In a Kerberos environment, the Key Distribution Center (KDC) is the repository for all user and service secret keys. The client sends a request to the authentication server (AS), which might or might not be the KDC. The AS forwards the client credentials to the KDC. The KDC authenticates clients to other entities on a network and facilitates communication using session keys. The KDC provides security to clients or principals, which are users, network services, and software. Each principal must have an account on the KDC. The KDC issues a ticket-granting ticket (TGT) to the principal. The principal will send the TGT to the ticket-granting service (TGS) when the principal needs to connect to another entity. The TGS then transmits a ticket and session keys to the principal. The set of principles for which a single KDC is responsible is referred to as a realm.

Some advantages of implementing Kerberos include the following:

- User passwords do NOT need to be sent over the network.
- Both the client and server authenticate each other.
- The tickets passed between the server and client are time stamped and include lifetime information.
- The Kerberos protocol uses open Internet standards and is not limited to proprietary codes or authentication mechanisms.
Some disadvantages of implementing Kerberos include:

- KDC redundancy is required if providing fault tolerance is a requirement. The KDC is a single point of failure.

- The KDC must be scalable to ensure that performance of the system does not degrade.

- Session keys on the client machines can be compromised.

- Kerberos traffic needs to be encrypted to protect the information over the network.

- All systems participating in the Kerberos process must have synchronized clocks.

- Kerberos systems are susceptible to password-guessing attacks.

Figure 5-2 shows the ticket-issuing process for Kerberos.
SESAME

The Secure European System for Applications in a Multi-vendor Environment (SESAME) project extended Kerberos’ functionality to fix Kerberos’ weaknesses. SESAME uses both symmetric and asymmetric cryptography to protect interchanged data. SESAME uses a trusted authentication server at each host.

SESAME uses Privileged Attribute Certificates (PACs) instead of tickets. It incorporates two certificates: one for authentication and one for defining access privileges. The trusted authentication server is referred to as the Privileged Attribute Server (PAS), which performs roles similar to the KDC in Kerberos. SESAME can be integrated into a Kerberos system.

Federated Identity Management

A federated identity is a portable identity that can be used across businesses and domains. In federated identity management, each organization that joins the federation agrees to enforce a common set of policies and standards. These policies and standards define how to provision and manage user identification, authentication, and authorization. Federated identity management uses two basic models for linking organizations within the federation: cross certification and trusted third-party or bridge model.

In the cross-certification model, each organization certifies that every other organization is trusted. This trust is established when the organizations review each other’s standards. Each organization must verify and certify through due diligence that the other organizations meet or exceed standards. One disadvantage of cross certification is that the number of trust relationships that must be managed can become a problem. In addition, verifying the trustworthiness of other organizations can be time-consuming and resource intensive.

In the trusted third-party or bridge model, each organization subscribes to the standards of a third party. The third party manages verification, certification, and due diligence for all organizations. This is usually the best model if an organization needs to establish federated identity management relationships with a large number of organizations.

Security Assertion Markup Language (SAML) 2.0 is an SAML standard that exchanges authentication and authorization data between organizations or security domains. It uses an XML-based protocol to pass information about a principal between an SAML authority and a web service via security tokens. In SAML 2.0, there are three roles: the principal or user, the identity provider, and the service provider. The service provider requests identity verification from the identity provider. SAML is very flexible because it is based on XML. If an organization implements
enterprise SAML identity federation, the organization can select which identity attributes to share with another organization.

Security Domains

A domain is a set of resources that are available to a subject over a network. Subjects that access a domain include users, processes, and applications. A security domain is a set of resources that follows the same security policies and are available to a subject. The domains are usually arranged in a hierarchical structure of parent and child domains.

NOTE Do not confuse the term security domain with protection domain. Although a security domain usually encompasses a network, a protection domain resides within a single resource. A protection domain is a group of processes that share access to the same resource.

Session Management

Session management ensures that any instance of identification and authentication to a resource is managed properly. This includes managing desktop sessions and remote sessions.

Desktop sessions should be managed through a variety of mechanisms. Screensavers allow computers to be locked if left idle for a certain period of time. To reactivate a computer, the user must log back in. Screensavers are a timeout mechanism, and other timeout features may also be used, such as shutting down or placing a computer in hibernation after a certain period. Session or logon limitations allow organizations to configure how many concurrent sessions a user can have. Schedule limitations allow organizations to configure the time during which a user can access a computer.

Remote sessions usually incorporate some of the same mechanisms as desktop sessions. However, remote sessions do not occur at the computer itself. Rather, they are carried out over a network connection. Remote sessions should always use secure connection protocols. In addition, if users will only be remotely connecting from certain computers, the organization may want to implement some type of rule-based access that allows only certain connections.

Registration and Proof of Identity

A proof of identity process involves collecting and verifying information about an individual to prove that the person who has a valid account is who he or she claims
to be. The most basic method of proof of identity is providing a driver’s license, passport, or some other government-issued identification. Proof of identity is performed before user account creation. Once proof of identity is completed, the user is issued a credential, and authentication factors are determined and recorded. From that point forward, authentication occurs each time the user logs in using the issued credential.

The National Institute of Standards and Technology (NIST) has issued documents that provide guidance on proof of identity:

- **FIPS Publication 201.2, Personal Identity Verification (PIV) of Federal Employees and Contractors**: This document specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. This publication includes identification, security, and privacy requirements and personal identity verification system guidelines.

- **NIST 800-79-2, Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)**: This document includes preparation guidelines, issuer control implementation guidelines, and issuer control life cycle guidelines.

Both of these NIST publications are intended to guide federal government agencies in their proof of identity efforts and can also be used by private organizations to aid in the development of their own systems.

**Credential Management Systems**

Users are often required to remember usernames, passwords, and other authentication information for a variety of organizations. They often use the same authentication credentials across multiple platforms, which makes online identity theft and fraud easier to commit. Once a set of credentials has been discovered on one online system, attackers often use the same set of credentials on another organization’s systems to see if they can gain access. Along with this problem comes an organization’s own internal issue for maintaining different credentials for users needing access to multiple systems with different credentialing systems. Factor in the increasing use of mobile devices, and you have a recipe for disaster.

Credential management systems allow organizations to establish an enterprise-wide user authentication and authorization framework. Organizations should employ security professionals to design, deploy, and manage secure credential management systems. The business requirements for a credential management system should include individual privacy protection guidelines, automated identity solutions,
security, and innovation. Some of the guidelines of a credential management system include the following:

- Use strong passwords.
- Automatically generate complex passwords.
- Implement password history.
- Use access control mechanisms, including the who, what, how, and when of access.
- Implement auditing.
- Implement backup and restore mechanisms for data integrity.
- Implement redundant systems within the credential management systems to ensure 24/7/365 access.
- Implement credential management group policies or other mechanisms offered by operating systems.

When an organization implements a credential management system, separation of duties becomes even more important because the centralized credential management system can be used to commit fraud. Security professionals should provide guidance on how the separation should occur to best protect the organization and its assets.

Accountability

Accountability is an organization’s ability to hold users responsible for the actions they perform. To ensure that users are accountable for their actions, organizations must implement auditing and other accountability mechanisms.

To ensure that users are accountable for their actions, organizations could implement any combination of the following components:

- **Strong identification**: Each user should have his or her own account. Group or role accounts cannot be traced back to a single individual.
- **Strong authentication**: Multi-factor authentication is best. At minimum, two-factor authentication should be implemented.
- **Monitoring**: User actions should be monitored, including login, privilege use, and other actions. Users should be warned as part of a no expectation of privacy statement that all actions can be monitored.
- **Audit Logs**: Audit logs should be maintained and stored according to organizational security policies. Administrators should periodically review these logs.
Although organizations should internally implement these accountability mechanisms, they should also periodically have a third party perform audits and tests. This is important because the outside third party can provide objectivity that internal personnel often cannot provide.

**Auditing and Reporting**

Auditing and reporting ensure that users are held accountable for their actions, but an auditing mechanism can only report on events that it is configured to monitor. You should monitor network events, system events, application events, user events, and keystroke activity. Keep in mind that any auditing activity will impact the performance of the system being monitored. Organizations must find a balance between auditing important events and activities and ensuring that device performance is maintained at an acceptable level. Also, organizations must ensure that any monitoring that occurs is in compliance with all applicable laws.

When designing an auditing mechanism, security professionals should remember the following guidelines:

- Develop an audit log management plan that includes mechanisms to control the log size, backup processes, and periodic review plans.
- Ensure that the ability to delete an audit log is a two-man control that requires the cooperation of at least two administrators. This ensures that a single administrator is not able to delete logs that might hold incriminating evidence.
- Monitor all high-privilege accounts (including all root users and administrative-level accounts).
- Ensure that the audit trail includes who processed the transaction, when the transaction occurred (date and time), where the transaction occurred (which system), and whether the transaction was successful or not.
- Ensure that deleting the log and deleting data within the logs cannot occur unless the user has the appropriate administrative-level permissions.

**NOTE** Scrubbing is the act of deleting incriminating data within an audit log.

Audit trails detect computer penetrations and reveal actions that identify misuse. As a security professional, you should use the audit trails to review patterns of access to individual objects. To identify abnormal patterns of behavior, you should first identify normal patterns of behavior. Also, you should establish the clipping level, which is a baseline of user errors above which violations will be recorded. For example,
your organization might choose to ignore the first invalid login attempt, knowing that initial failed login attempts are often due to user error. Any invalid login after the first would be recorded because it could be a sign of an attack. A common clipping level that is used is three failed login attempts. Any failed login attempt above the limit of three would be considered malicious. In most cases, a lockout policy would lock out a user’s account after this clipping level is reached.

Audit trails deter attacker attempts to bypass the protection mechanisms that are configured on a system or device. As a security professional, you should specifically configure the audit trails to track system/device rights or privileges being granted to a user and data additions, deletions, or modifications.

Finally, audit trails must be monitored, and automatic notifications should be configured. If no one monitors the audit trail, then the data recorded in the audit trail is useless. Certain actions should be configured to trigger automatic notifications. For example, you might want to configure an email alert to occur after a certain number of invalid login attempts because invalid login attempts might be a sign that a brute-force password attack is occurring.

Identity as a Service (IDaaS) Implementation

Identity as a Service (IDaaS) provides a set of identity and access management functions to target systems on customers’ premises and/or in the cloud. IDaaS includes identity governance and administration (IGA), which provides the ability to provision identities held by the service to target applications. It includes user authentication, single sign-on (SSO), and authorization enforcement. IDaaS services are divided into two categories: web access software for cloud-based applications and cloud-delivered legacy identity management services. Web IDaaS applications do not work with on-premises applications. Most IDaaS deployments offer SSO authentication, federated identities, remote administration, and internal directory service integration. IDaaS is different from identity and access management (IAM) solutions, which are operated from within the organization’s own network via bundled software and hardware. IAM solutions may use Active Directory and Lightweight Directory Access Protocol (LDAP).

If organizations consider IDaaS deployment, they should primarily be concerned with service availability, identity data protection, and trusting a third party with a critical business function. They should also be concerned with regulatory compliance. Moving identity management to the cloud brings up a whole host of questions for the organization regarding auditing, ensuring compliance of regulations, and what happens if disclosures occur.
An organization should perform a comprehensive risk analysis prior to deploying any IDaaS service. After performing the risk analysis, the organization should determine which identities should be placed on the IDaaS solution.

**Third-Party Identity Services Implementation**

If an organization decides to deploy a third-party identity service, including cloud computing solutions, security practitioners must be involved in the integration of that implementation with internal services and resources. This integration can be complex, especially if the provider solution is not fully compatible with existing internal systems. Most third-party identity services provide cloud identity, directory synchronization, and federated identity. Examples of these services include Amazon Web Services (AWS) Identity and Access Management (IAM) service and Oracle Identity Management.

**Authorization Mechanisms**

Authorization mechanisms are systems an organization deploys to control which systems a user or device can access. Authorization mechanisms include access control models and access control policies.

**Access Control Models**

An access control model is a formal description of an organization’s security policy. Access control models are implemented to simplify access control administration by grouping objects and subjects. Subjects are entities that request access to an object or data within an object. Users, programs, and processes are subjects. Objects are entities that contain information or functionality. Computers, databases, files, programs, directories, and fields are objects. A secure access control model must ensure that secure objects cannot flow to a less secure subject.

The access control models and concepts that you need to understand include the following:

- Discretionary access control
- Mandatory access control
- Role-based access control
- Rule-based access control
- Content-dependent versus context-dependent access control
- Access control matrix
Discretionary Access Control

In discretionary access control (DAC), the owner of the object specifies which subjects can access the resource. DAC is typically used in local, dynamic situations. The access is based on the subject’s identity, profile, or role. DAC is considered to be a need-to-know control.

DAC can be an administrative burden because the data custodian or owner grants access privileges to the users. Under DAC, a subject’s rights must be terminated when the subject leaves the organization. Identity-based access control is a subset of DAC and is based on user identity or group membership.

Non-discretionary access control is the opposite of DAC. In non-discretionary access control, access controls are configured by a security administrator or other authority. The central authority decides which subjects have access to objects based on the organization’s policy. In non-discretionary access control, the system compares the subject’s identity with the objects’ ACL.

Mandatory Access Control

In mandatory access control (MAC), subject authorization is based on security labels. MAC is often described as prohibitive because it is based on a security label system. Under MAC, all that is not expressly permitted is forbidden. Only administrators can change the category of a resource.

MAC is more secure than DAC. DAC is more flexible and scalable than MAC. Because of the importance of security in MAC, labeling is required. Data classification reflects the data’s sensitivity. In a MAC system, a clearance is a subject’s privilege. Each subject and object is given a security or sensitivity label. The security labels are hierarchical. For commercial organizations, the levels of security labels could be confidential, proprietary, corporate, sensitive, and public. For government or military institutions, the levels of security labels could be top secret, secret, confidential, and unclassified.

In MAC, the system makes access decisions when it compares the subject’s clearance level with the object’s security label.

Role-Based Access Control

In role-based access control (RBAC), each subject is assigned to one or more roles. Roles are hierarchical. Access control is defined based on the roles. RBAC can be
used to easily enforce minimum privileges for subjects. An example of RBAC is implementing one access control policy for bank tellers and another policy for loan officers.

RBAC is not as secure as the previously mentioned access control models because security is based on roles. RBAC usually has a much lower cost to implement than the other models and is popular in commercial applications. It is an excellent choice for organizations with high employee turnover. RBAC can effectively replace DAC and MAC because it allows you to specify and enforce enterprise security policies in a way that maps to the organization’s structure.

RBAC is managed in four ways. In non-RBAC, no roles are used. In limited RBAC, users are mapped to single application roles, but some applications do not use RBAC and require identity-based access. In hybrid RBAC, each user is mapped to a single role, which gives them access to multiple systems, but each user can be mapped to other roles that have access to single systems. In full RBAC, users are mapped to a single role as defined by the organization’s security policy, and access to the systems is managed through the organizational roles.

**Rule-Based Access Control**

Rule-based access control facilitates frequent changes to data permissions and is defined in RFC 2828. Using this method, a security policy is based on global rules imposed for all users. Profiles are used to control access. Many routers and firewalls use this type of access control and define which packet types are allowed on a network. Rules can be written allowing or denying access based on packet type, port number used, MAC address, and other parameters.

**Content-Dependent Versus Context-Dependent**

Content-dependent access control makes access decisions based on the data contained within the object. With this access control, the data that a user sees might change based on the policy and access rules that are applied.

Context-dependent access control is based on subject or object attributes or environmental characteristics. These characteristics can include location or time of day. An example of this is if administrators implement a security policy that ensures that a user only logs in from a particular workstation during certain hours of the day.

Security experts consider a constrained user interface as another method of access control. An example of a constrained user interface is a shell, which is a software interface to an operating system that implements access control by limiting the system commands that are available. Another example is database views that are filtered based on user or system criteria. Constrained user interfaces can be content- or context-dependent based on how the administrator constrains the interface.
Access Control Matrix

An access control matrix is a table that consists of a list of subjects, a list of objects, and a list of the actions that a subject can take upon each object. The rows in the matrix are the subjects, and the columns in the matrix are the objects. Common implementations of an access control matrix include a capabilities table and an ACL.

Capabilities Table

A capability corresponds to a subject’s row from an access control matrix. A capability table lists the access rights that a particular subject has to objects. A capability table is about the subject.

ACL

An ACL corresponds to an object’s column from an access control matrix. An ACL lists all the access rights that subjects have to a particular object. An ACL is about the object.

Figure 5-3 shows an access control matrix and how a capability and ACL are part of it.

<table>
<thead>
<tr>
<th>Subject</th>
<th>File 1</th>
<th>File 2</th>
<th>Printer 1</th>
<th>Printer 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>Read</td>
<td>Read, Write</td>
<td>Print</td>
<td>Full Control</td>
</tr>
<tr>
<td>Sally</td>
<td>Full Control</td>
<td>Read</td>
<td>Full Control</td>
<td>Print</td>
</tr>
<tr>
<td>George</td>
<td>No Access</td>
<td>Full Control</td>
<td>No Access</td>
<td>Print</td>
</tr>
</tbody>
</table>

Figure 5-3  Access Control Matrix

Access Control Policies

An access control policy defines the method for identifying and authenticating users and the level of access that is granted to users. Organizations should put access control policies in place to ensure that access control decisions for users are based on formal guidelines. If an access control policy is not adopted, organizations will have trouble assigning, managing, and administering access management.
Access Control Threats

Access control threats directly impact the confidentiality, integrity, and availability of organizational assets. The purpose of most access control threats is to cause harm to an organization. Because harming an organization is easier to do from within its network, outsiders usually first attempt to attack any access controls that are in place.

Access control threats that you should understand include:

- Password threats
- Social engineering threats
- DoS/DDoS
- Buffer overflow
- Mobile code
- Malicious software
- Spoofing
- Sniffing and eavesdropping
- Emanating
- Backdoor/trapdoor

Password Threats

A password threat is any attack that attempts to discover user passwords. The two most popular password threats are dictionary attacks and brute-force attacks.

The best countermeasures against password threats are to implement complex password policies, require users to change passwords on a regular basis, employ account lockout policies, encrypt password files, and use password-cracking tools to discover weak passwords.

Dictionary Attack

A dictionary attack occurs when attackers use a dictionary of common words to discover passwords. An automated program uses the hash of the dictionary word and compares this hash value to entries in the system password file. Although the program comes with a dictionary, attackers also use extra dictionaries that are found on the Internet.
You should implement a security rule that says that a password must NOT be a word found in the dictionary to protect against these attacks. You can also implement an account lockout policy so that an account is locked out after a certain number of invalid login attempts.

**Brute-Force Attack**

Brute-force attacks are more difficult to carry out because they work through all possible combinations of numbers and characters. A brute-force attack is also referred to as an exhaustive attack. It carries out password searches until a correct password is found. These attacks are also very time consuming.

**Social Engineering Threats**

Social engineering attacks occur when attackers use believable language and user gullibility to obtain user credentials or some other confidential information. Social engineering threats that you should understand include phishing/pharming, shoulder surfing, identity theft, and dumpster diving.

The best countermeasure against social engineering threats is to provide user security awareness training. This training should be required and must occur on a regular basis because social engineering techniques evolve constantly.

**Phishing/Pharming**

Phishing is a social engineering attack in which attackers try to learn personal information, including credit card information and financial data. This type of attack is usually carried out by implementing a fake website that very closely resembles a legitimate website. Users enter data, including credentials on the fake website, allowing the attackers to capture any information entered. Spear phishing is a phishing attack carried out against a specific target by learning about the target’s habits and likes. Spear phishing attacks take longer to carry out than phishing attacks because of the information that must be gathered. Whaling is a type of phishing that specifically targets high-level executives or other high-profile individuals. Vishing is a type of phishing that uses a phone system or VoIP technologies. The user initially receives a call, text, or email that says to call a specific number and provide personal information such as name, birth date, Social Security number, and credit card information.

Pharming is similar to phishing, but it actually pollutes the contents of a computer’s DNS cache so that requests to a legitimate site are actually routed to an alternate site.
Caution users against using any links embedded in email messages, even if the message appears to have come from a legitimate entity. Users should also review the address bar any time they access a site where their personal information is required to ensure that the site is correct and that SSL is being used, which is indicated by an HTTPS designation at the beginning of the URL address.

Shoulder Surfing

Shoulder surfing occurs when an attacker watches when a user enters login or other confidential data. Encourage users to always be aware of who is observing their actions. Implementing privacy screens helps to ensure that data entry cannot be recorded.

Identity Theft

Identity theft occurs when someone obtains personal information, including driver’s license number, bank account number, and Social Security number, and uses that information to assume an identity of the individual whose information was stolen. After the identity is assumed, the attack can go in any direction. In most cases, attackers open financial accounts in the user’s name. Attackers also can gain access to the user’s valid accounts.

Dumpster Diving

Dumpster diving occurs when attackers examine garbage contents to obtain confidential information. This includes personnel information, account login information, network diagrams, and organizational financial data.

Organizations should implement policies for shredding documents that contain this information.

DoS/DDoS

A denial-of-service (DoS) attack occurs when attackers flood a device with enough requests to degrade the performance of the targeted device. Some popular DoS attacks include SYN floods and teardrop attacks.

A distributed DoS (DDoS) attack is a DoS attack that is carried out from multiple attack locations. Vulnerable devices are infected with software agents, called zombies. This turns the vulnerable devices into botnets, which then carry out the attack. Because of the distributed nature of the attack, identifying all the attacking botnets is virtually impossible. The botnets also help to hide the original source of the attack.
Buffer Overflow

Buffers are portions of system memory that are used to store information. A buffer overflow occurs when the amount of data that is submitted to the application is larger than the buffer can handle. Typically, this type of attack is possible because of poorly written application or operating system code. This can result in an injection of malicious code.

To protect against this issue, organizations should ensure that all operating systems and applications are updated with the latest service packs, updates, and patches. In addition, programmers should properly test all applications to check for overflow conditions. Finally, programmers should use input validation to ensure that the data submitted is not too large for the buffer.

Mobile Code

Mobile code is any software that is transmitted across a network to be executed on a local system. Examples of mobile code include Java applets, Java script code, and ActiveX controls. Mobile code includes security controls, Java sandboxes, and ActiveX digital code signatures. Malicious mobile code can be used to bypass access controls.

Organizations should ensure that users understand the security concerns of malicious mobile code. Users should only download mobile code from legitimate sites and vendors.

NOTE For more information about mobile code, see the section, “Mobile Code,” in Chapter 8, “Software Development Security.”

Malicious Software

Malicious software, also called malware, is any software that is designed to perform malicious acts.

The following are the five classes of malware you should understand:

- **Virus**: Any malware that attaches itself to another application to replicate or distribute itself.
- **Worm**: Any malware that replicates itself, meaning that it does not need another application or human interaction to propagate.
- **Trojan horse**: Any malware that disguises itself as a needed application while carrying out malicious actions.
- Spyware: Any malware that collects private user data, including browsing history or keyboard input.

- Ransomware: Any malware that prevents or limits a user’s access to his or her system or device. Usually it forces victims to pay the ransom for the return of system access.

The best defense against malicious software is to implement anti-virus and anti-malware software. Today most vendors package these two types of software in the same package. Keeping anti-virus and anti-malware software up to date is vital. This includes ensuring that the latest virus and malware definitions are installed.

Spoofing

Spoofing, also referred to as masquerading, occurs when communication from an attacker appears to come from trusted sources. Spoofing examples include IP spoofing and hyperlink spoofing. The goal of this type of attack is to obtain access to credentials or other personal information.

A man-in-the-middle attack uses spoofing as part of the attack. Some security professionals consider phishing attacks as a type of spoofing attack.

Sniffing and Eavesdropping

Sniffing, also referred to as eavesdropping, occurs when an attacker inserts a device or software into the communication medium that collects all the information transmitted over the medium. Network sniffers are used by both legitimate security professionals and attackers.

Organizations should monitor and limit the use of sniffers. To protect against their use, you should encrypt all traffic on the network.

Emanating

Emanations are electromagnetic signals that are emitted by an electronic device. Attackers can target certain devices or transmission mediums to eavesdrop on communication without having physical access to the device or medium.

The TEMPEST program, initiated by the United States and UK, researches ways to limit emanations and standardizes the technologies used. Any equipment that meets TEMPEST standards suppresses signal emanations using shielding material. Devices that meet TEMPEST standards usually implement an outer barrier or coating, called a Faraday cage or Faraday shield. TEMPEST devices are most often used in government, military, or law enforcement.
Backdoor/Trapdoor

A backdoor or trapdoor is a mechanism implemented in many devices or applications that gives the user who uses the backdoor unlimited access to the device or application. Privileged backdoor accounts are the most common method of backdoor that you will see today.

Most established vendors no longer release devices or applications with this security issue. You should be aware of any known backdoors in the devices or applications you manage.

Prevent or Mitigate Access Control Threats

Because access control threats are so widespread, organizations must do all they can to protect their access control systems, including deploying anti-malware, firewalls, intrusion detection and prevention, and other defense tools. Security professionals should encourage their organizations to deploy the following measures to prevent or mitigate access control threats:

- Deploy physical access controls for all systems and devices.
- Control and monitor access to password files.
- Encrypt password files.
- Deploy an enterprise-wide strong password policy.
- Deploy password masking on all operating systems and applications.
- Deploy multi-factor authentication.
- Deploy account lockout.
- Deploy auditing for access controls.
- Deploy a user account management policy to ensure that user accounts are created and removed as necessary.
- Provide user security awareness training that specifically focuses on access control.
Exam Preparation Tasks

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 5-1 lists a reference of these key topics and the page numbers on which each is found.

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paragraph</td>
<td>Access control process</td>
<td>410</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Provisioning life cycle</td>
<td>413</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Five factors of authentication</td>
<td>415</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Password types</td>
<td>417</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Password management considerations</td>
<td>419</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Physiological characteristics</td>
<td>422</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Behavioral characteristics</td>
<td>424</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Biometric considerations</td>
<td>424</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Advantages and disadvantages of SSO</td>
<td>430</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Advantages and disadvantages of Kerberos</td>
<td>431</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Auditing mechanism guidelines</td>
<td>437</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Classes of malware</td>
<td>446</td>
</tr>
</tbody>
</table>

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:
access control, access control list (ACL), access control matrix, access control policy, authentication, authorization, backdoor, biometric acceptability, biometric accuracy, biometric throughput, brute-force attack, buffer overflow, capability table, centralized access control, characteristic factors, context-dependent access control, cross-certification federated identity model, crossover error rate, decentralized access control, Dictionary attack, discretionary access control (DAC), dumpster diving, false acceptance rate (FAR), false rejection rate (FRR), federated identity, identification, Identity as a Service (IDaaS), Kerberos, knowledge factors, least privilege,
Lightweight Directory Access Protocol (LDAP), location factors, logical control, mandatory access control (MAC), multi-factor authentication, need-to-know, ownership factors, password masking, pharming, phishing, physical control, provisioning life cycle, ransomware, role-based access control (RBAC), rule-based access control, Secure European System for Applications in a Multi-vendor Environment (SESAME), Security Assertion Markup Language (SAML), security domain, separation of duties, shoulder surfing, single-factor authentication, single sign-on (SSO), spyware, trapdoor, Trojan horse, trusted third-party federated identity model, virus, vishing, whaling, worm

**Review Questions**

1. Which of the following is NOT an example of a knowledge authentication factor?
   a. password
   b. mother’s maiden name
   c. city of birth
   d. smart card

2. Which of the following statements about memory cards and smart cards is false?
   a. A memory card is a swipe card that contains user authentication information.
   b. Memory cards are also known as integrated circuit cards (ICCs).
   c. Smart cards contain memory and an embedded chip.
   d. Smart card systems are more reliable than memory card systems.

3. Which biometric method is most effective?
   a. iris scan
   b. retina scan
   c. fingerprint
   d. hand print

4. What is a Type I error in a biometric system?
   a. crossover error rate (CER)
   b. false rejection rate (FRR)
   c. false acceptance rate (FAR)
   d. throughput rate
5. Which access control model is most often used by routers and firewalls to control access to networks?
   a. discretionary access control
   b. mandatory access control
   c. role-based access control
   d. rule-based access control

6. Which threat is NOT considered a social engineering threat?
   a. phishing
   b. pharming
   c. DoS attack
   d. dumpster diving

7. Which of the following statements best describes an IDaaS implementation?
   a. Ensures that any instance of identification and authentication to a resource is managed properly.
   b. Collects and verifies information about an individual to prove that the person who has a valid account is who he or she claims to be.
   c. Provides a set of identity and access management functions to target systems on customers’ premises and/or in the cloud.
   d. It is an SAML standard that exchanges authentication and authorization data between organizations or security domains.

8. Which of the following is an example of multi-factor authentication?
   a. username and password
   b. username, retina scan, and smart card
   c. retina scan and finger scan
   d. smart card and security token

9. You decide to implement an access control policy that requires that users logon from certain workstations within your enterprise. Which type of authentication factor are you implementing?
   a. knowledge factor
   b. location factor
   c. ownership factor
   d. characteristic factor
10. Which threat is considered a password threat?
   a. buffer overflow
   b. sniffing
   c. spoofing
   d. brute-force attack

11. Which session management mechanisms are often used to manage desktop sessions?
   a. screensavers and timeouts
   b. FIPS 201.2 and NIST SP 800-79-2
   c. Bollards and locks
   d. KDC, TGT, and TGS

12. Which of the following is a major disadvantage of implementing an SSO system?
   a. Users are able to use stronger passwords.
   b. Users need to remember the login credentials for a single system.
   c. User and password administration are simplified.
   d. If a user’s credentials are compromised, attacker can access all resources.

13. Which type of attack is carried out from multiple locations using zombies and botnets?
   a. TEMPEST
   b. DDoS
   c. Backdoor
   d. Emanating

**Answers and Explanations**

1. **d**. Knowledge factors are something a person knows, including passwords, mother’s maiden name, city of birth, and date of birth. Ownership factors are something a person has, including a smart card.

2. **b**. Memory cards are NOT also known as integrated circuit cards (ICCs). Smart cards are also known as ICCs.

3. **a**. Iris scans are considered more effective than retina scans, fingerprints, and hand prints.

4. **b**. A Type I error in a biometric system is false rejection rate (FRR). A Type II error in a biometric system is false acceptance rate (FAR). Crossover error rate
(CER) is the point at which FRR equals FAR. Throughput rate is the rate at which users are authenticated.

5. **d.** Rule-based access control is most often used by routers and firewalls to control access to networks. The other three types of access control models are not usually implemented by routers and firewalls.

6. **c.** A denial-of-service (DoS) attack is not considered a social engineering threat. The other three options are considered to be social engineering threats.

7. **c.** An Identity as a Service (IDaaS) implementation provides a set of identity and access management functions to target systems on customers’ premises and/or in the cloud. Session management ensures that any instance of identification and authentication to a resource is managed properly. A proof of identity process collects and verifies information about an individual to prove that the person who has a valid account is who he or she claims to be.

8. **b.** Using username, retina scan, and a smart card is an example of multi-factor authentication. The username is something you know, the retina scan is something you are, and the smart card is something you have.

9. **b.** You are implementing location factors, which are based on where a person is located when logging in.

10. **d.** A brute-force attack is considered a password threat.

11. **a.** Desktop sessions can be managed through screensavers, timeouts, logon, and schedule limitations. Federal Information Processing Standards (FIPS) Publication 201.2 and NIST Special Publication 800-79-2 are documents that provide guidance on proof of identity. Physical access to facilities can be provided securely using locks, fencing, bollards, guards, and closed-circuit television (CCTV). In Kerberos, the key distribution center (KDC) issues a ticket-granting ticket (TGT) to the principal. The principal sends the TGT to the ticket-granting service (TGS) when the principal needs to connect to another entity.

12. **d.** If a user’s credentials are compromised in a single sign-on (SSO) environment, attackers have access to all resources to which the user has access. All other choices are advantages to implementing an SSO system.

13. **b.** A distributed DoS (DDoS) attack is a DoS attack that is carried out from multiple attack locations. Vulnerable devices are infected with software agents, called zombies. This turns the vulnerable devices into botnets, which then carry out the attack. Devices that meet TEMPEST standards implement an outer barrier or coating, called a Faraday cage or Faraday shield. A backdoor or trapdoor is a mechanism implemented in many devices or applications that gives the user who uses the backdoor unlimited access to the device or application. Emanations are electromagnetic signals that are emitted by an electronic device. Attackers can target certain devices or transmission mediums to eavesdrop on communication without having physical access to the device or medium.
Index

Numerics

3DES (Triple DES), 225-228
802.11 standard, 326, 329
802.11a standard, 329
802.11ac standard, 329
802.11b standard, 329
802.11f standard, 329
802.11g standard, 330
802.11n standard, 330
IDaaS, 438
integrity, 16
job rotation, 17
managing, 130
NAC devices, 374-376
natural access control, 264
physical/logical, 411-414
separation of duties, 17
third-party identity services, 439
threats, 443-448
types, 88-91
access controls lists. See ACLs
access points. See APs
accountability, 436
accounts, managing, 417-416, 467
accreditation, 193-194
Accreditation/Certification phase (SDLC), 578
ACID tests, 127
ACLs (access control lists), 16, 412, 442
acoustical systems, 551
Acquire/Develop stage (SDLC), 573
acquired software, impact of, 604
acquisitions, 21, 97-98
active states, 242
ActiveX, 571
actual cost valuation. See ACV
ACV (actual cost valuation), 527
Ad Hoc mode, 328
Address Resolution Protocol. See ARP
addresses
IP, 401
common TCP/UDP ports, 305
logical/physical addressing, 307-311
spoofing, 401
IPv4, 307, 310
IPv6, 310
logical, 307-311
MAC, 311, 333, 392
physical, 307-311
administration. See also managing
access, 412
passwords, 417-420
administrative controls, 88
administrative/regulatory law, 46
Advanced Encryption Standard. See AES
adware, 599
AES (Advanced Encryption Standard), 228
agent-based log reviews, 462
agentless log reviews, 462
agents, threats, 77
aggregation, 126, 197
Agile model, 583
agreements
employment, 75
processes, 158
alarms, environmental, 278
algebraic attacks, 255
algorithms
asymmetric, 221-222, 231
Diffie-Hellman, 231
ECC, 233
El Gamal, 233
Knapsack, 233
RSA, 232
Zero Knowledge Proof, 233
SHA, 250
symmetric, 219-221, 224
AES, 228
Blowfish, 229
CAST, 230
DES/3DES, 225-228
IDEA, 229
RC4/RC5/RC6, 230
Skipjack, 229
Twofish, 230
alignment, security functions, 18
allow-by-default stance, 16
analog signaling, 311
analysis
BIA, 70-73
evidence, 484
risk, 603
risk management, 77-92
security, testing, 470
source code tools, 595
test coverage, 466
analytic attacks, 256
anti-malware software, 524, 601
antivirus applications, 524, 600
APIs (application programming interfaces), 596
applets (Java), 571
Application layer, TCP/IP models, 299
application programming interfaces. See APIs
applications
ownership roles, 26
provisioning, 501
APs (access points), 328, 351
architecture
COBRA, 569
databases, 122-124
firewalls, 346-347
maintenance, 194
OSI models, 294
SOA, 571
system, 170
components, 174-177
computing platforms, 171-172
input/output devices, 177-180
ISO/IEC 42010:2011, 170
security services, 173-174
vulnerabilities, 194
client-based, 195
cryptographic systems, 201
databases, 196-197
distributed systems, 197-200
ICSs, 202
large-scale parallel data systems, 201
server-based, 196
archiving privacy, 137-138
ARP (Address Resolution Protocol), 303, 317, 393
assemblers, 566
assembly languages, 566
assessments
controls, 92
disaster recovery, 544
effectiveness, 602-603
risk, 79. See also risks, management strategies, 456
vulnerabilities, 456-457
assets
accessing, 411-414
classification, 118
commercial businesses, 120
databases, 122-127
government/military, 120-121
information life cycles, 121-122
sensitivity, 119
cloud computing, 501
data
custodians, 116
documentation, 117-118
ownership, 116
policies, 114
quality, 116
retention, 140-141
security, 141-147
handling requirements, 147-148
information, 507
inventories, 497
managing, 129, 507
access/identities, 130
backup/recovery systems, 130
fault tolerance
redundancy, 130
fault tolerance/redundancy, 130
HSM, 135
NAS, 135
networks/resources, 136
RAID, 131, 134, 675, 687
SANs, 135
ownership, 128
business/mission, 129
data, 128
systems, 129
physical security, 500
privacy, 137
collection limitation, 139
data processors, 137
data remanence, 138-139
data storage, 137-138oles/responsibilities, 115
virtual, 500
assurance, 163
asymmetric algorithms, 221-222, 231
Diffie-Hellman, 231
ECC, 233
El Gamal, 233
Knapsack, 233
RSA, 232
Zero Knowledge Proof, 233
asynchronous tokens, 421
Asynchronous Transfer Mode. See ATM
asynchronous transmissions, 312
ATM (Asynchronous Transfer Mode), 372
attacks
cryptanalytic, 253-257
networks, 390, 400-401
cabling, 390
components, 391-395
DNS, 395-398
remote, 399
wireless, 399
threat modeling, 96
time-of-check/time-of-use, 204
web-based, 204
attenuation, 391
attributes, 123, 567
auditing, 437, 494-495, 603
classification, 127-128
roles/responsibilities, 25
security, testing, 470-472
services, 174
auditors, roles/responsibilities, 26
authentication, 215, 415-427
implementing, 427-437
Kerberos, 431
MAC, 251-253
Open System Authentication, 331
periods, 419
Shared Key Authentication, 331
Authenticode technology, 571
authorization, 216, 440-442, 439
availability, 16
Disaster recovery, 68
awareness, 100-101, 469
board of directors, roles/responsibilities, 23
bollards, 549
bombing, 264
Border Gateway Protocol. See BGP
botnets, 599
bottom-up approaches, 38
boundary control services, 173
breaches (data), 58
Brewer-Nash (Chinese Wall) model, 169
bridges, 341
British Ministry of Defense Architecture Framework. See MODAF
broadband, 313
broadcast transmissions, 314
brute-force attacks, 255, 444
BSI (Build Security In), 590
budgets, 20
buffers, overflow, 446, 591
Build and Fix approach, 579
Build Security In. See BSI
building security, 269-278
business cases, 19
business continuity, 64
BIA, 70-73
disaster recovery, 65-67
business continuity plan.
See BCPs
business impact analysis.
See BIA
business interruption insurance, 527
business/mission ownership, 129
business process recovery, 530
bus topologies, 359

CA (certification authority), 234
cabling, 354
connecting, 381
coil, 355
fiber optic, 357
network attacks, 390
twisted pair, 356-357
Caesar cipher-encrypted messages, 212
Caesar, Julius, 212
CANC (Cipher-Based MAC), 252
candidate keys, 123
capabilities of information systems, 191
fault tolerance, 193
interfaces, 193
memory protection, 191
TPM, 192
virtualization, 191
tables, 442

Capability Maturity Model Integration. See CMMI

backdoors, 448, 593
backing up
backups, 130
data, 527, 537-540
hardware, 534
software, 535
verification data, 469
barriers, 549
base relation, 123
baseband, 313
Basel II, 56
baselines, 142
documentation, 64
BCPs (business continuity plans), 67, 470, 548
behavior, 567
behavioral systems, 424
Bell-LaPadula model, 166
best evidence, 488
BGP (Border Gateway Protocol), 354
BIA (business impact analysis), 67, 70-73
Biba model, 167
big data, 118
biometrics
security, 271
technologies, 424-425
birthday attacks, 256
blacklisting, 523
blind spoofing attacks, 392
blind tests, 458
block ciphers, 221
Blowfish, 229
Bluetooth, 330

business continuity plan.
See BCPs
business impact analysis.
See BIA
business interruption insurance, 527
business/mission ownership, 129
business process recovery, 530
bus topologies, 359
capacitance detectors, 551
cardinality, 123
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 (Computer-Aided Software Engineering), 586
CAST (Carlisle Adams and Stafford Tavares), 230
categories
access control, 86-88
security policies, 63
CBC-MAC (Cipher Block Chaining MAC), 252
CCTA Risk Analysis and Management Method. See CRAMM
CCTV (closed-circuit television system), 552
CDNs (content distribution networks), 377
centralized access control, 412
central processing units. See CPUs
certificate revocation list. See CRL
certificates, 235
certification, 193-194
cross-certification, 236
certification authority. See CA
chain of custody, 486
change management, 525, 578
channel service unit/data service unit. See CSU/DSU
characteristic factor authentication, 422-425
checklist tests, 546
chosen ciphertext attacks, 254
chosen plaintext attacks, 254
CIA (confidentiality, integrity, and availability), 15, 161, 215
availability, 16
confidentiality, 15
integrity, 16
CIFS (Common Internet File System), 322
Cipher Block Chaining MAC. See CBC-MAC
ciphers
block, 221
hybrid, 222-223
running, 217
stream-based, 220
substitution, 218, 222-224
transposition, 219
chosen ciphertext-only attacks, 254
circuit-switching networks, 371
circumstantial evidence, 489
civil code law, 45
civil disobedience, 263
civil investigations, 493
civil/tort law, 46
Clark-Wilson Integrity model, 168
classes, 567
IP, 308-309
classification, asset security, 118
audits, 127-128
commercial businesses, 120
databases, 122-127
government/military, 120-121
information life cycles, 121-122
sensitivity, 119
Cleanroom model, 585
clearing, 138
clients
thin, 171
vulnerabilities, 195
clipping levels, 520
closed-circuit television system. See CCTV
cloud computing, 198
assets, 501
clustering, 528
CMaaS, 496
CMMI (Capability Maturity Model Integration), 37, 586
coxial cabling, 355
CobiT (Control Objectives for Information and Related Technology), 32-33
COBRA (Common Object Request Broker Architecture), 569
code
mobile, 571, 594
repository security, 595
reviews, 464
source code analysis
tools, 595
cognitive passwords, 418
cohesion, 569
cold sites, 532
collecting
data
privacy, 139
security process data,
466, 469
evidence, 483
collision domains, 366
collusion, 262
combination passwords,
418
COM (Component
Object Model), 570
commercial businesses,
data classification, 120
commercial software, 50
Committee of
Sponsoring
Organizations. See
COSO
committees
audit, 25
governance, 23
Common Internet File
System. See CIFS
Common Criteria, 186-187
common law, 46
Common Object
Request Broker
Architecture. See
COBRA
common TCP/UDP
ports, 305
communication channels,
377-389
virtualized networks,
389-390
communications
disaster recovery, 544
networks, 311-315
Communications
Assistance for Law
Enforcement Act
(CALEA) of 1994, 56
communications threats,
259
comparing
asynchronous/
synchronous
transmissions, 312
broadband/baseband,
313
IPv4/IPv6, 310
wired/wireless
transmissions, 315
compartmented security
mode, 162
compensative controls,
87
compilers, 566
complex passwords, 418
compliance, 40
legislative/regulatory, 41
personnel security
policies, 76
privacy, 42
Component-Based
Development method,
586
Component Object
Model. See COM
components, 174-177
network attacks, 391-395
networks, 339
CDNs, 377
endpoint security, 376
hardware, 339-341,
344-353
NAC devices, 374-376
transmission media,
354, 358-359,
362-366, 369-373
compromised states, 243
Computer-Aided
Software Engineering,
See CASE
computer crime
concepts, 42-44
Computer Ethics
Institute, 59
Computer Fraud and
Abuse Act (CFAA), 54
Computer Security Act of
1987, 55
Computer Security
Technology Planning
Study, 601
computing platforms,
171-172
concealment ciphers, 217
conclusive evidence, 489
confidentiality, 15, 215
confidentiality, integrity,
and availability. See CIA
configuration
management, 498-499,
578
configuring
accreditation/
certification, 193-194
architecture
maintenance, 194
vulnerabilities, 194-202
asymmetric algorithms, 231
  Diffie-Hellman, 231
  ECC, 233
  El Gamal, 233
  Knapsack, 233
  RSA, 232
  Zero Knowledge Proof, 233
building/internal security, 269-278
cryptanalytic attacks, 253-257
cryptography, 209-211
  asymmetric algorithms, 221-222
c ryptosystem features, 215-216
  history of, 211-215
  hybrid ciphers, 222-223
  key management, 216-217
  life cycles, 211
  running ciphers, 217
  substitution ciphers, 218, 223-224
  symmetric algorithms, 219-221
  transposition ciphers, 219
  types, 217
  cyber-physical system vulnerabilities, 208
digital signatures, 245
  DRM, 246
  embedded system vulnerabilities, 208
  equipment security, 278-280
evaluation models, 180
  Common Criteria, 186-187
  controls/countermeasures, 190
  ITSEC, 184-186
  security implementation standards, 187-190
  TCSEC, 181-184
geographical threats, 257-264
information systems, 191
  fault tolerance, 193
  interfaces, 193
  memory protection, 191
  TPM, 192
  virtualization, 191
keys, managing, 237-245
logs, 463
  MAC, 251-253
message integrity, 246-251
mobile system vulnerabilities, 205-207
networks, 294
  attacks, 390-401
  communications, 311-315, 377-390
  converged protocols, 323-325
  cryptography, 333-339
  IP, 305-311
  OSI models, 294-297
  protocols, 317-323
TCP/IP models, 298-304
  types of, 315-317
  wireless, 326-333
PKI, 234-237
  principles, 158-160
  security models, 161
  Bell-LaPadula model, 166
  Biba model, 167
  Breuer-Nash (Chinese Wall) model, 169
  CIA, 161
  Clark-Wilson Integrity model, 168
  Graham-Denning model, 169
  Harrison-Ruzzo-Ullman model, 169
  Lipner model, 169
  modes, 161-163
  types, 163-165
site and facility, 264-269
symmetric algorithms, 224
  AES, 228
  Blowfish, 229
  CAST, 230
  IDEA, 229
  Skipjack, 229
  Twofish, 230
system architecture, 170
  components, 174-177
  computing platforms, 171-172
  input/output devices, 177-180
  security services, 173-174
web-based vulnerabilities, 203
attacks, 204
maintenance books, 203
OWASP, 205
SAML, 204
time-of-check/time-of-use attacks, 204
XML, 204
consultant controls, 76
contamination, 197
content-dependent access control, 126, 441
content distribution networks. See CDNs
contention methods, 365
context-dependent access control, 126, 441
contingency plans, 67
continuity (business), 64. See also BCP
disaster recovery, 65-67
continuous improvement, 92
contractor controls, 76
Control Objectives for Information and Related Technology. See CobiT
controls
access, 87-88
managing, 410-411
types, 88-91
assessments, 92
asset security, 141-148
data flow, 196
evaluation models, 190
frameworks, 27
CMMI, 37
CobiT, 32-33
COSO, 34
CRAMM, 37
DoDAF, 31
ISO/IEC 27000 Series, 28-30
ITIL, 34
MODAF, 31
NIST SP, 33-34
OCTAVE, 34
SABSA, 31
security program life cycles, 38
Six Sigma, 36
TOGAF, 31
top-down/bottom-down approaches, 38
Zachman framework, 30
import/export, 51-58
input/output, 522
security
software development, 589-602
testing, 456-466
vendor, 76
converged protocols, 323
FCoE, 324
iSCSI, 325
MPLS, 324-325
VoIP, 325
cookies, 338
copyrights, 49
corrective controls, 87
corroborative evidence, 489
COSO (Committee of Sponsoring Organizations), 34
countermeasures, 78, 84
evaluation models, 190
coupling, 569
cryptographic attacks, 253-257
cryptography, 146, 201, 209-211, 333
asymmetric algorithms, 221-222
ciphers
running, 217
substitution, 218
transposition, 219
deny-by-default stance  703

cryptosystem features, 215-216
email encryption, 334-335
end-to-end encryption, 334
history of, 211-215
hybrid ciphers, 222-223
Internet security, 336-339
key management, 216-217
life cycles, 211
link encryption, 333-334
services, 174
substitution ciphers, 223-224
symmetric algorithms, 219-221
types, 217
cryptoperiods, 239
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), 365, 368
CSMA/CD (Carrier Sense Multiple Access/Collision Detection), 365-367
CSU/DSU (channel service unit/data service unit), 371
custodians, asset security, 116
custodial, 25
damage assessment teams, 543
data access, 142
asset security, 118
audits, 127-128
commercial businesses, 120
databases, 122-127
government/military, 120-121
information life cycles, 121-122
sensitivity, 119
audits, classification, 127-128
backups, 527, 537-540
breaches, 58
custodians
asset security, 116
roles/responsibilities, 25
data center security, 273
documentation, 117-118
flow
trans-border, 52
control, 196
hiding, 567
mining, 125, 197
ownership, 25, 128
roles/responsibilities, 25
asset security, 116
policies, 114
privacy, 139
processors, privacy, 137
quality, 116
recovery, 537
remanence, privacy, 138-139
at rest, 141
retention, 140-141
security, 141-147
storage, privacy, 137-138
structures, 569
in transit, 141
warehousing, 125, 197
Data Link layer (2), 297
databases
architecture, 122-124
classification, 122-127
interface languages, 124
locks, 127
maintenance, 126
threats, 126
views, 126
vulnerabilities, 196-197
DCOM (Distributed Component Object Model), 570
DDoS (Distributed DOS) attacks, 396, 445
dead, 243
dedicated access control, 412
dedicated security modes, 162
default stance, 16
default to no access, 429
defense-in-depth strategies, 16, 163
degrees, 123
denial-of-service. See DoS attacks
deny-by-default stance, 16
Department of Defense Architecture Framework. See DoDAF

DES (Digital Encryption Standard), 225-228
design

accreditation/certification, 193-194
architecture

  maintenance, 194
  vulnerabilities, 194-202
asymmetric algorithms, 231

  Diffie-Hellman, 231
  ECC, 233
  El Gamal, 233
  Knapsack, 233
  RSA, 232

  Zero Knowledge Proof, 233

building/internal security, 269-278
cryptanalytic attacks, 253-257

cryptography, 209-211

  asymmetric algorithms, 221-222
cryptosystem features, 215-216

  history of, 211-215
  hybrid ciphers, 222-223
  key management, 216-217
  life cycles, 211
  running ciphers, 217
  substitution ciphers, 218, 223-224

  symmetric algorithms, 219-221
  transposition ciphers, 219
types, 217
cyber-physical system vulnerabilities, 208
digital signatures, 245

  DRM, 246
embedded system vulnerabilities, 208
equipment security, 278-280
evaluation models, 180

  Common Criteria, 186-187
  controls/countermeasures, 190
ITSEC, 184-186
security implementation standards, 187-190

  TCSEC, 181-184
geographical threats, 257-264

information systems, 191

  fault tolerance, 193
  interfaces, 193
  memory protection, 191
  TPM, 192
virtualization, 191
keys, managing, 237-245
MAC, 251-253
message integrity, 246-251
mobile system vulnerabilities, 205-207

networks, 294
attacks, 390-401
communications, 311-315, 377-390

  converged protocols, 323-325
cryptography, 333-339

  IP, 305-311
  OSI models, 294-297
  protocols, 317-323
  TCP/IP models, 298-304
types of, 315-317
wireless, 326-333

PKI, 234-237

principles, 158-160
security models, 161

  Bell-LaPadula model, 166
  Biba model, 167
  Brewer-Nash (Chinese Wall) model, 169
  CIA, 161
  Clark-Wilson Integrity model, 168
defense-in-depth, 163

  Graham-Denning model, 169
  Harrison-Ruzzo-Ullman model, 169

Lipner model, 169
modes, 161-163
types, 163-165

site and facility, 264-269

symmetric algorithms, 224

  AES, 228
  Blowfish, 229
Domain Name System Security Extensions.  
See DNSSEC  
domains, 123  
collisions, 366  
grabbing, 397  
security, 434  
doors, security, 269  
DoS (denial-of-service) attacks, 396, 445  
double-blind tests, 458  
downtime estimates, 71  
DRM (Digital Rights Management), 51, 246  
DRPs (disaster recovery plans), 67, 528  
DSL (digital subscriber line) connections, 380  
due care, 39  
due diligence, 39  
dumpster diving, 445  
duties, separation of, 427  

earthquakes, 258  
eavesdropping, 391, 447  
ECC (Elliptic Curve Cryptosystem) algorithm, 233  
Economic Espionage Act of 1996, 56  
eDiscovery investigations, 494  
education, 100-101  
effectiveness, 20  
effectiveness assessments, 602-603  
egress monitoring, 496  
EIGRP (Enhanced IGRP), 353  
electrical threats, 259  
electromechanical systems, 551  
Electronic Communications Privacy Act (ECPA) of 1986, 55  
El Gamal algorithm, 233  
E-lines, 370  
Elliptic Curve Cryptosystem.  See ECC  
email attacks, 397  
encryption, 334-335  
spoofering, 397  
emanations, 447  
embedded devices, investigations, 492  
embedded systems, 172, 208  
employment agreements, 75  
screening, 73-75  
termination, 75-76  
encapsulation, 295, 567-568  
TCP/IP, 304  
encryption, 279  
email, 334-335  
end-to-end, 147, 334  
links, 147, 333-334  
endpoint security, 376  
end-to-end encryption, 147, 334  
engineering accreditation/certification, 193-194  
arctecture maintenance, 194  
vulnerabilities, 194-202  
asymmetric algorithms, 231  
Diffie-Hellman, 231  
ECC, 233  
El Gamal, 233  
Knapsack, 233  
RSA, 232  
Zero Knowledge Proof, 233  
building/internal security, 269-278  
cryptanalytic attacks, 253-257  
cryptography, 209-211  
asymmetric algorithms, 221-222  
cryptosystem features, 215-216  
history of, 211-215  
hybrid ciphers, 222-223  
key management, 216-217  
life cycles, 211  
running ciphers, 217  
substitution ciphers, 218, 223-224  
symmetric algorithms, 219-221  
transposition ciphers, 219  
types, 217  
cyber-physical system vulnerabilities, 208  
design principles, 158-160  
digital signatures, 245  
DRM, 246  
embedded system vulnerabilities, 208  
equipment security, 278-280
evaluation models, 180
Common Criteria, 186-187
controls/countermeasures, 190
ITSEC, 184-186
security implementation standards, 187-190
TCSEC, 181-184
geographical threats, 257-264
information systems, 191
fault tolerance, 193
interfaces, 193
memory protection, 191
TPM, 192
virtualization, 191
keys, managing, 237-245
MAC, 251-253
message integrity, 246-251
mobile system vulnerabilities, 205-207
PKI, 234-237
security models, 161
Bell-LaPadula model, 166
Biba model, 167
Brewer-Nash (Chinese Wall) model, 169
CLA, 161
Clark-Wilson Integrity model, 168
defense-in-depth, 163
Graham-Denning model, 169
Harrison-Ruzzo-Ullman model, 169
Lipner model, 169
modes, 161-163
types, 163-165
site and facility design, 264-269
symmetric algorithms, 224
AES, 228
Blowfish, 229
CAST, 230
DES/3DES, 225-228
IDEA, 229
RC4/RC5/RC6, 230
Skipjack, 229
Twofish, 230
system architecture, 170
components, 174-177
computing platforms, 171-172
input/output devices, 177-180
ISO/IEC 27001:2005, 170
security services, 173-174
web-based vulnerabilities, 203
attacks, 204
maintenance books, 205
OWASP, 205
SAML, 204
time-of-check/time-of-use attacks, 204
XML, 204
Enhanced IGRP. See EIGRP
Enigma machine, 214
Enterprise versions, 332
environmental alarms, 278
environmental security, 274
evironments, software, 591
equipment rooms, security, 273
equipment security, 278-280
escalation, 467, 593
estimates, downtime, 71
Ethernet 802.3 standard, 362
ethics, 59
Computer Ethics Institute, 59
IAB, 60
ISC Code of Ethics, 59
organizational, 60
EU (European Union) laws, 58
evacuation drills, 547
evaluation models, 180
Common Criteria, 186-187
controls/countermeasures, 190
ITSEC, 184-186
security implementation standards, 187-190
TCSEC, 181-184
events, 516, 521
evidence, 487-490
analyzing, 484
chain of custody, 486
collecting, 483
examining, 484
identifying, 482
preserving, 483
storage, 274
Exploratory Model, 586
explosions, 261
exposure, 77
Extensible Markup Language. See XML
external threats, 257
extranets, 316

F
facilities
  access controls, 414
design, 264-269
recovery, 531-532
redundancy, 526
security, 505
factoring attacks, 257
failover, 528
failsoft, 528
fault tolerance, 73, 130, 136
information systems, 193
FCoE (Fibre Channel over Ethernet), 324
FDDI (Fiber Distributed Data Interface), 364
Federal Information Security Management Act (FISMA) of 2002, 56
Federal Intelligence Surveillance Act (FISA) of 1978, 55
Federal Privacy Act of 1974, 55
federated identity management, 433
fences, 549
fencing, 550
Fiber Distributed Data Interface. See FDDI
fiber optic cabling, 357
Fibre Channel over Ethernet. See FCoE
filters, MAC, 333
fire, 261
detection and suppression systems, 527
extinguishers, 275
protection, 274-275
firewalls, 344, 376
architecture, 346-347
types, 344-346
floods, 258, 278
flow control, 302
foreign keys, 123
forensic investigations, 481-486
fraggle attacks, 394
Frame Relay, 371
Framework Core, 469
frameworks, risk, 93
fraud, 262
freeware, 50
frequency analysis, 255
FTP (File Transfer Protocol), 319
FTPS (FTP Secure), 319
full-interruption tests, 547
full-knowledge tests, 458
functionality drills, 547
gates, 549-550
gateway, 344
Gather Requirements phase (SDLC), 575
government, data classification, 120-121
Graham-Denning model, 169
Gramm-Leach-Bliley Act (GLBA) of 1999, 54
graphical passwords, 418
grid computing, 199
groups, managing, 501
guest operating systems, 390
guidelines, documentation of, 64
glass entries, security, 272-274
goals, organizational strategies and, 19
governance (security), 17
  budgets, 20
  business case, 19
  committees, 23
  control frameworks, 27-38
  due care, 39
  due diligence, 39
  effectiveness, 20
  metrics, 20
organizations
  missions/objectives, 19
  processes, 21-23
  strategies/goals, 19
resources, 20-21
roles/responsibilities, 23-25
security function alignment, 18
third-party, 97-98
H

hackers, 44
handling
asset security, 147-148
risk, 85. See also risks, management
hardening systems, 522
hardware, 339-341, 344-353
backups, 534
investigations, 492
risks, 97
security, 506
Harrison-Ruzzo-Ullman model, 169
hash MAC. See HMAC
hashing, 247-248
HAVAL, 250
Health Care and Education
Reconciliation Act of 2010, 57
Health Insurance Portability and Accountability Act (HIPAA), 54
hearsay evidence, 490
heat, 277
hiding data, 567
hierarchical models, 124
hierarchical storage management. See HSM
high availability, 528
high cohesion, 569
high-level languages, 566
higher-level recovery strategies, 529
High-Speed Serial Interface. See HSSI
hijacking, session, 400
history
media, 514
of cryptography, 211-215
passwords, 419
HMAC (hash MAC), 251
honeynets, 524
honeypots, 348
hooks, maintenance, 203
hot sites, 532
HSM (hierarchical storage management), 135, 513
HSSI (High-Speed Serial Interface), 373
HTTP (Hypertext Transfer Protocol), 320, 337
HTTPS (HTTP Secure), 320, 337
hubs, 341
human-caused threats, 260-262
human resources, 535
humidity, 277
hurricanes, 258
HVAC, security, 277
hybrid ciphers, 222-223
hybrid protocols, 352
hybrid topologies, 361
Hypertext Transfer Protocol. See HTTP
Hypertext Transfer Protocol Secure. See HTTPS
IAM (identity and access management)
access control processes, 410-411
authentication, 415-437
authorization, 439-442
IDaaS, 438
physical/logical access, 411-414
third-party identity services, 439
threats, 443-447, 448
ICMP (Internet Control Message Protocol), 302, 320
attacks, 393
redirects, 394
ICSs (industrial control systems), 202
IDaaS (Identity as a Service), 438
IDEA (International Data Encryption Algorithm), 229
identification
evidence, 482
implementing, 427-437
identifying threats, 94-95
identities, managing, 130, 416-417, 445, 508
identity and access management. See IAM
IDSs (intrusion detection systems), 349-350, 495, 523
IEC (International Electrotechnical Commission), 27, 146
IGMP (Internet Group Management Protocol), 303
IGRP (Interior Gateway Routing Protocol), 353
IMAP (Internet Message Access Protocol), 321
Implement stage (SDLC), 573
implementing
authentication, 427-437
authorization, 439-442
data policies, 114
IDaaS, 438
risk management, 86
security implementation standards, 187-190
third-party identity services, 439
import/export controls, 51-58
incidents
managing, 516-520
response teams, 516
Incremental model, 582
Industrial control systems. See ICSs
inference, 126, 197
information
access controls, 413
assets, 507
flow models, 165
life cycles, 121-122
systems, 17, 191
fault tolerance, 193
interfaces, 193
memory protection, 191
TPM, 192
virtualization, 191
information security continuous monitoring. See ISCM
Information Technology Infrastructure Library. See ITIL
Information Technology Security Evaluation Criteria. See ITSEC
infrared systems, 551
Infrastructure mode, 328
initialization vectors. See IVs
Initiate phase (SDLC), 572
input/output controls, 522
devices, 177-180
validation, 593
instant messaging applications, 378
insurance, 527
intangible asset protection, 505-509, 512-514
Integrated Product and Process Development. See IPPD
Integrated Services Digital Networks, See ISDNs
integrity, 16, 216
messages, 246-251
services, 174
intellectual property law, 47
copyrights, 49
DRM, 51
international protection, 51
patents, 47-48
software piracy, 50
trademarks, 49
trade secrets, 48
interfaces
APIs, 596
HSSI, 373
information systems, 193
languages, 124
testing, 466
Interior Gateway Routing Protocol. See IGRP
Intermediate System to Intermediate System. See IS-IS
internal audits, 470-472
internal security, 269-278
internal threats, 257
International Data Encryption Algorithm. See IDEA
International Electrotechnical Commission. See IEC
International Organization for Standardization. See ISO
International Organization on Computer Evidence. See IOCE
international protection, intellectual property, 51
Internet Architecture Board. See IAB
Internet Control Message Protocol. See ICMP
Internet Group Management Protocol. See IGMP
Internet layer, TCP/IP models, 302-303
Internet Protocol. See IP
Internet Protocol Security. See IPsec
Internet security, 336-339
Internet Small Computer System Interface. See iSCSI
interpreters, 566
interviewing, investigation skills, 487
intranets, 316
intruders, delaying, 266
intrusion detection systems. See IDSs
intrusion prevention systems. See IPSs
intrusion responses, 266
inventories
  assets, 497
  security, 279
investigations, 481, 487-492, 516
digital/forensic, 481-486
evidence, 487-491
incidents, 516
types, 493-494
IOCE (International Organization on Computer Evidence), 484-485
IP (Internet Protocol), 302
  addresses, spoofing, 401
  networks, 305
    common TCP/UDP ports, 305
    logical/physical addressing, 307-311
IPPD (Integrated Product and Process Development), 588-589
IPsec (Internet Protocol Security), 338
IPSs (intrusion prevention system), 350, 523
IPv4 (IP version 4)
  addresses, 307
  IPv6, comparing to, 310
IPv6 (IP version 6), 310
ISC (Internet Systems Consortium) Code of Ethics, 59
ISCM (information security continuous monitoring), 466
iSCSI (Internet Small Computer System Interface), 325
ISDNs (Integrated Services Digital Networks), 380
IS-IS (Intermediate System to Intermediate System), 354
ISO (International Organization for Standardization), 27
  ISO 9001:2015, 587
  ISO/IEC 27000 series, 590
  ISO/IEC 27000 Series, 27-30
  ISO/IEC 27001:2013, 188-189
  ISO/IEC 27002:2013, 189
  ISO/IEC 42010:2011, 170
ISs (information systems). See information
issue-specific security policies, 63
ITGI (IT Governance Institute), 18
IT Governance Institute. See ITGI
ITIL (Information Technology Infrastructure Library), 18, 34
ITSEC (Information Technology Security Evaluation Criteria), 184-186
IVs (initialization vectors), 221

J

JAD (Joint Analysis Development) models, 585
Java applets, 571
Java Database Connectivity. See JDBC
Java Platform, Enterprise Edition (Java EE), 570
JDBC (Java Database Connectivity), 125
job rotation, 17
Joint Analysis Development. See JAD models

K

Kerberos, 431
Kerckhoff’s principle, 214
key-encrypting keys, 238
key performance indicators, 468
key risk indicators, 468
keys
  managing, 216-217, 237-245
  PKI, 234-237
Knapsack, 233
knowledge factor
authentication, 416-422
known plaintext attacks, 254

L
labeling, 148, 514
languages
assembly, 566
high-level, 566
machine, 566
very-high-level, 566
LANs (local area
networks), 315
large-scale parallel
data systems,
vulnerabilities, 201
laws
administrative/
regulatory, 46
civil code, 45
civil/tort, 46
common, 46
criminal, 46
custumary, 47
EU, 58
intellectual property, 47
copyrights, 49
DRM, 51
international
protection, 51
patents, 47-48
software piracy, 50
trademarks, 49
trade secrets, 48
mixed, 47
privacy, 53-58
religious, 47
layer 3 switches, 343
layer 4 switches, 343
layered defense models, 264
layers
Data Link (2), 297
Network (3), 296
OSI models, 295-297
Physical (1), 297
Presentation (6), 295
Session (5), 296
TCP/IP models, 299
  Application, 300
  Internet, 302-303
  Link, 304
  Transport, 300
Transport (4), 296
LDAP (Lightweight
Directory Access
Protocol), 321
least privilege principle, 428-429, 501
legal systems, 42-45. See also laws
copyrights, 49
DRM, 51
international
protection, 51
patents, 47-48
software piracy, 50
trademarks, 49
trade secrets, 48
mixed, 47
privacy, 53-58
religious, 47
provisioning, 413
security, 38
software development, 572-589
lighting, 552-553
linear cryptanalysis, 255
Link layer, TCP/IP
models, 304
link state protocols, 352
links, encryption, 147, 333-334
Lipner model, 169
development, 572-589
lighting, 552-553
linear cryptanalysis, 255
Link layer, TCP/IP
models, 304
link state protocols, 352
links, encryption, 147, 333-334
Lipner model, 169
load balancing, 528
local area network. See
LANs
location factor
authentication, 427
locks, 280
databases, 127
security, 270
logging, 494-497, 603
logical access to assets, 411-414
logical addressing,
307-311
logical controls, 90
gle logic bombs, 598
logs, 459
configuring, 463
NIST SP 800-92,
460-463
Lucifer project, 215

M
MAC (mandatory access
control), 440
MAC (media access
control) addresses, 311
filters, 333
flooding attacks, 392
MAC (message authentication code), 251-253
machine languages, 566
mainframes, 171
maintenance
architecture, 194
databases, 126
hooks, 203
major legal systems, 45.
See also laws
administrative/regulatory, 46
civil code law, 45
civil/tort law, 46
common law, 46
criminal law, 46
customary, 47
mixed, 47
religious, 47
malware, 446, 596, 600
anti-malware software, 524
managing
access
authentication, 415-427
authorization, 439-442
control processes, 410-411
IDaaS, 438
implementing
authentication, 427-437
mitigating threats, 448
physical/logical, 411-414
third-party identity services, 439
threats, 443-447
accounts, 416-417, 467
asset security, 129, 507
access/identities, 130
backup/recovery systems, 130
documentation, 117-118
fault tolerance/redundancy, 130
HSM, 135
NAS, 135
networks/resources, 136
RAID, 131, 134, 675, 687
SANs, 135
change management, 525
configuration management, 498-499
controls, 88
data policies, 114
digital signatures, 245
DRM, 246
identities, 416-417
incidents, 516-520
keys, 216-217, 237-245
media, 509
memory, 180
networks, 515
passwords, 417-420
patch management, 524-525
risk, 77-92
reviews, 468
roles/responsibilities, 24
sessions, 434
vulnerabilities, 522
mandatory access control. See MAC
man-in-the-middle (MITM) attacks, 392
MANs (metropolitan area networks), 316
mantraps, 270
marking, 148
masking passwords, 419
matrix-based models, 164
maturity methods, 578-580, 583-587
MD4/MD5/MD6 messages, 249
mean time between failure. See MTBF
mean time to repair. See MTTR
measurements, 92
media
analysis, 491
disposal, 514
history, 514
labeling/storage, 514
management, 509
relations teams, 543
sanitizing, 514
storage facilities, 274
media access control addresses. See MAC addresses
meet-in-the-middle attacks, 257
memory, 175-176
managing, 180
protection, 191
memory cards, 421
mesh topologies, 361
message authentication code. See MAC
messages
integrity, 246-251
MAC, 251-253
methods, 124, 567
contention, 365
maturity, 578-580, 583-587
software development, 578-580, 583-587
metrics, 20
metropolitan area networks. See MANs
middleware, 172
military, data classification, 120-121
MIME (Multipurpose Internet Mail Extension), 335
mirrored sites, 534
missions, organizational, 19
misuse case testing, 465
mitigating, 603
access control threats, 448
incidents, 519
MITM (man-in-the-middle) attacks, 392
mixed law, 47
mobile code, 446, 571, 594
mobile computing, 172
mobile devices, 351
mobile system vulnerabilities, 205-207
MODAF (British Ministry of Defense Architecture Framework), 31
modeling threats, 93
identifying, 94-95
potential attacks, 96
remediation, 96
models
access control, 439-442
COM, 570
databases, 122-124
DCOM, 570
evaluation, 180
Common Criteria, 186-187
countermeasures, 190
ITSEC, 184-186
security implementation standards, 187-190
TCSEC, 181-184
OSI, 294-297
security, 161
Bell-LaPadula model, 166
Biba model, 167
Brewer-Nash (Chinese Wall) model, 169
CLA, 161
Clark-Wilson Integrity model, 168
defense-in-depth, 163
Graham-Denning model, 169
Harrison-Ruzzo-Ullman model, 169
Lipner model, 169
modes, 161-163
types, 163-165
TCP/IP, 298-304
modes, security, 161-163
Modified Prototype Model. See MPM
MOM (motive, opportunity, and means), 486
monitoring, 494-496
employees, 555
ISCM, 466
services, 174
special privileges, 504
synthetic transactions, 504
motive, opportunity, and means. See MOM
MPLS (Multiprotocol Label Switching), 324-325
MPM (Modified Prototype Model), 582
MTBF (mean time between failure), 136
MTTR (mean time to repair), 137
multicast transmissions, 314
multilayer protocols, 322-323
multilevel lattice models, 164
multilevel security mode, 162
multimedia collaboration, 377
multiplexers, 340
multiprocessing, 174
Multiprotocol Label Switching. See MPLS
Multipurpose Internet Mail Extension. See MIME
multitasking, 179

N

NAC (network access control) devices, 374-376
NAS (network-attached storage), 135, 513
NAT (network address translation), 310, 321
National Institute of Standards and Technology. See NIST
natural access control, 264
natural surveillance, 265
natural territorials reinforcement, 265
natural threats, 257-258
near field communication. See NFC
need-to-know principle, 428-429, 501
NetBIOS, 321
Network access control devices. See NAC devices
network address translation. See NAT
network-attached storage. See NAS
Network layer (3), 296
networks, 124
design, 294
attacks, 390-401
communication channels, 377-390
communications, 311-315
converged protocols, 323-325
cryptography, 333-339
IP, 305-311
OSI models, 294-297
protocols, 317-323
TCP/IP models, 298-304
types of networks, 315-317
wireless, 326-333
investigations, 492
managing, 136
routings, 351
technologies, 362-366, 369-373
testing, 457
topologies, 359
NFC (near field communication), 331
NFS (Network File System), 321
NIST (National Institute of Standards and Technology), 17, 143
NIST SP 800-86, 485
NIST SP 800-92, 460-463
NIST SP 800-137, 466
SP (Special Publication), 33-34
noise, 390
non-blind spoofing attacks, 392
non-inference models, 165
non-repudiation, 216
NOPs (no-operation instructions), 591
normalization, 124
numeric passwords, 419

Object Linking and Embedding. See OLE
object-oriented programming. See also OOP
object-relational models, 124
objectives, organizational, 19
objects, 567, 594
OCSP (Online Certificate Status Protocol), 235
OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), 34
ODBC (Open Database Connectivity), 125
OLE (Object Linking and Embedding), 570
OLE DB (Object Linking and Embedding Database), 125
OLTP (Online Transaction Processing), 127
on-time passwords, 418
one-time pads, 223
one-way hashing, 248
Online Certificate Status Protocol. See OCSP
Online Transaction Processing. See OLTP
OOP (object-oriented programming), 567
Open Database Connectivity. See ODBC
Open Shortest Path First. See OSPF
Open System Authentication, 331
Open Web Application Security Project. See OWASP

Operate/Maintain stage (SDLC), 573

operating systems, 178, 390

Operationally Critical Threat, Asset and Vulnerability Evaluation. See OCTAVE

operations

concepts, 501-504
disaster recovery, 541-545
investigations, 481, 487-494, 493
digital/forensic, 481-486
evidence, 487-491
personnel privacy/safety, 554-555
phases, 244
physical security, 548-554
recovery
testing, 545-547
strategies, 526-541
resources
change management, 525
incident management, 516-520
patch management, 524-525
preventive measures, 520-524
protecting, 505-510, 513-515
provisioning, 497-501

opinion evidence, 490
optimizing, 92
Orange Book, 181-184, 521, 601
organizational ethics, 60
organizational missions/objectives, 19
organizational processes, 21-23
organizational project-enabling processes, 158
organizational security policy, 62
organizational strategies/goals, 19
OSI (the Open Systems Interconnection) models, 130, 294-297
OSPF (Open Shortest Path First), 353
outage impacts, 71
overflow buffers, 446, 591
OWASP (Open Web Application Security Project), 590
vulnerabilities, 205
ownership, asset security, 116, 128
business/mission, 129
data, 128
factor authentication, 420-422
systems, 129

P

packet creation, 295
packet-switching networks, 371
parallel tests, 547
paraphrase passwords, 418
parity information, 509
partial-knowledge tests, 458
passing tokens, 369
passwords
managing, 417-420
threats, 443
PAT (Port Address Translation), 321
patches
management, 524-525
panels, 340
patents, 47-48
paths, trusted, 521
patrol forces, 553
Payment Card Industry Data Security Standard. See PCI-DSS
PBX (private branch exchange), 348, 374
PCI-DSS (Payment Card Industry Data Security Standard), 190
peer-to-peer computing, 199
penetration testing, 457-459
perimeter intrusion detection systems, 551
perimeter security, 548
periodic reviews, 101
Personal Information Protection and Electronic Documents Act (PIPEDA), 56
Personal versions, 332
Personally Identifiable Information. See PII
personnel
disaster recovery, 542
privacy/safety, 554-555
security policies, 73
employment agreements, 75
disaster recovery, 542
employment screening, 73-75
employment termination, 75-76
privacy, 76
vendor controls, 76
planning
business contingency, 68-70
business continuity, 67
recovery testing, 545-547
Point-to-Point-Protocol. See PPP
policies, 61-63
access control, 442
data, asset security, 114
personnel security, 73
compliance, 76
employment agreements, 75
employment screening, 73-75
employment termination, 75-76
privacy, 76
vendor controls, 76
physical access to assets, 411-414
physical addressing, 307-311
physical assets, 500
physical controls, 91
Physical layer (1), 297
physical security plans, 265-266, 548-554
physical testing, 457
physiological systems, 422
PII (Personally Identifiable Information), 52
ping
of death, 394
scanning, 395
piracy, software, 50
PKI (public key infrastructure), 234-237
plain old telephone service. See POTS
Plan/Initiate Project phase (SDLC), 575
post-operational phases, 244
potential attacks, 96
POTS (plain old telephone service), 373
power
conditioners, 277
redundancy, 526
supplies, security, 276-277
PPP (Point-to-Point-Protocol), 373
pre-activation states, 242-243
Presentation layer (6), 295
preserving evidence, 483
Pretty Good Privacy. See PGP
preventing
access control threats, 448
static electricity, 277
unauthorized access, 495
preventive controls, 87
preventive measures against threats, 520-524
primary keys, 123
principles
design, 158-160
security governance, 17
budgets, 20
business case, 19
control frameworks, 27-38
due care, 39
due diligence, 39
effectiveness, 20
metrics, 20
principles

organizational missions/objectives, 19
organizational processes, 21-23
organizational strategies/goals, 19
resources, 20-21
roles/responsibilities, 23-25
security function alignment, 18
priorities, recovery, 72
privacy
asset security, 137
collection limitation, 139
data processors, 137
data remanence, 138-139
data storage, 137-138
compliance, 42
import/export controls, 52-58
personnel, 554-555
personnel security policies, 76
private authorization keys, 239
private branch exchange. See PBX
private ephemeral key-agreement keys, 239
private IP addresses, 309
private key-transport keys, 238
private keys, 237-238
private static key-agreement keys, 239
procedure documentation, 64
process data (security), collecting, 466, 469
processes
access, managing, 410-411
critical, 71
design, 158
organizational, 21-23
remediation, 96
processors, privacy, 137
professional ethics, 59
Computer Ethics Institute, 59
IAB, 60
ISC Code of Ethics, 59
organizational, 60
project scope, 68-70
proof of identity processes, 434
protecting
memory, 191
resources, 505-510, 513-515
protocols, 294, 317
ARP, 303, 317
BGP, 354
converged, 323
FCoE, 324
iSCSI, 325
MPLS, 324-325
VoIP, 325
DHCP, 318
FTP, 319
FTPS, 319
HTTP, 320, 337
HTTPS, 320, 337
ICMP, 302, 320
IGMP, 303
IGRP, 353
IMAP, 321
IP, 302
IPsec, 338
Kerberos, 431
LDAP, 321
multilayer, 322-323
OCSP, 235
POP, 322
PPP, 373
RIP, 353
SFTP, 319
SHHTTP, 320, 337
SNMP, 322
VRRP, 354
prototyping, 582
provisioning
life cycles, 413
resources, 497-501
proxies, 376
proxy servers, 347
PSTN (public switched telephone network), 373
public authorization keys, 239
Public ephemeral key-agreement keys, 239
public IP addresses, 309
public key infrastructure. See PKI
public key-transport keys, 238
public keys, 237-238
public static key-agreement keys, 239
public switched telephone network. See PSTN
purging, 139
QoS (Quality of Service), 528
qualitative risk management, 84
quality, asset security, 116
quantum cryptography, 336
quarantines, 376

RA (registration authority), 234
RAD (Rapid Application Development) models, 584
RADIUS (Remote Authentication Dial-In User Service), 385
RAID (Redundant Array of Independent Disks), 130-131, 134, 675, 687
ransomware, 44, 447, 600
Rapid Application Development. See RAD models
RBAC (role-based access control), 440
read-through tests, 546
real user monitoring. See RUM
reboots, 521
reciprocal agreements, 533
records, 123, 504
recoverability, 73

recovery controls, 88
data, 537
disaster, 541-545
incidents, 519
priorities, 72
strategies, 526-541
systems, 130
teams, 543
testing, 545-547
trusted, 521
Red Book, 184
redundancy, 130, 136
sites, 534
systems, 526
Redundant Array of Independent Disks. See RAID
referential integrity, 123
registration, 435
registration authority. See RA
regression testing, 604
regulations, 42
compliance, 41
computer crime concepts, 42-44
investigations, 494
privacy, 53-58
relational models, 123
Release/Maintenance phase (SDLC), 577
reliability, disaster recovery, 68
religious law, 47
relocation teams, 543
remediation, 96, 376, 520
remanence, privacy, 138-139
remote access applications, 336, 379
Remote Authentication Dial-In User Service. See RADIUS
remote authentication protocols, 386
remote connection technologies, 379
remote meeting technology, 378
remote networks, attacks, 399
repeaters, 341
replay attacks, 256
reporting, 92, 437, 519
reports, SOC, 471
requirements
asset handling, 147-148
resources, 72
security, 98-99
services, 99
residual risk, 85
resilience, 529
resources, 20-21
access control, 410
critical, 71
managing, 136
protecting, 505-510, 513-515
provisioning, 497-501
relationship between users and, 411
requirements, 72
responding to disasters, 542
to incidents, 518
responsibilities
asset security, 115
security, 23-25
restoration processes, 545
teams, 544
restricted work areas, 273
retention (data), asset security, 140-141
reuse of objects, 594
reverse engineering, 257
reviews, 494-495
code, 464
incidents, 520
log, 459
management, 468
NIST SP 800-92, 460-463
periodic, 101
revocation, 467
rights (DRM), 246
ring topologies, 359
riots, 263
RIPEMD-160, 251
RIP (Routing Information Protocol), 353
risks
analysis, 603
in acquisitions, 97-98
definition of, 77
management, 77-92
Rivest, Ron, 230
rogue programmers, 594
role-based access control. See RBAC
roles
asset security, 115
managing, 501
security, 23-25
rootkits, 600
routers, 343
routing networks, 351
Routing Information Protocol. See RIP
RSA algorithms, 232
rule-based access control, 441
rules
of engagement, 517
of evidence, 488
RUM (real user monitoring), 464
running ciphers, 217
S
SABSA (Sherwood Applied Business Security Architecture), 31
safes, 280
safety, personnel, 554-555
salting, 252-253
salvage teams, 544
SAML (Security Assertion Markup Language)
vulnerabilities, 204
sandboxing, 524, 571
sanitization, 139, 514
SANs (storage area networks), 135, 512, 528
Sarbanes-Oxley (SOX) Act, 54
satellites, 327
SCADA (supervisory control and data acquisition), 202
scanning
ports, 400
types, 601
scareware, 44
schemas, 123
Scientific Working Group on Digital Evidence. See SWGDE
scope, 143
for incident response teams, 517
projects, 68-70
screening, employment, 73-75
scrubbing, 437
scytale cipher, 212
SDLC (System Development Life Cycle), 572
Accreditation/Certification phase, 578
Acquire/Develop stage, 573
Design phase, 576
Develop phase, 576
Dispose stage, 574
Gather Requirements phase, 575
Implement stage, 573
Initiate phase, 572
Operate/Maintain stage, 573
Plan/Initiate Project phase, 575
Release/Maintenance phase, 577
Test/Validate phase, 576
SDN (software-defined networking), 389
searching, investigations, 490
secondary evidence, 489
Secure Electronic Transaction. See SET
Secure European System for Applications in a Multi-vendor Environment. See SESAME
Secure HTTP. See SHTTP
Secure Shell. See SSH
Secure Sockets Layer. See SSL
security
accreditation/certification, 193-194
architecture, 170
components, 174-177
computing platforms, 171-172
input/output devices, 177-180
ISO/IEC 42010:2011, 170
maintenance, 194
security services, 173-174
vulnerabilities, 194-202
asymmetric algorithms, 231
DES/3DES, 225-228
Diffie-Hellman, 231
ECC, 233
El Gamal, 233
Knapsack, 233
RC4/RC5/RC6, 230
RSA, 232
Zero Knowledge Proof, 233
business continuity, 64
BLA, 70-73
disaster recovery, 65-67
project scope/plans, 68-70
compliance, 40
legislative/regulatory, 41
privacy, 42
controls, testing, 456-466
cryptanalytic attacks, 253-257
cryptography, 209-211
asymmetric algorithms, 221-222
cryptosystem features, 215-216
history of, 211-215
hybrid ciphers, 222-223
key management, 216-217
life cycles, 211
running ciphers, 217
substitution ciphers, 218, 223-224
symmetric algorithms, 219-221
transposition ciphers, 219
types, 217
cyber-physical system vulnerabilities, 208
data breaches, 58
digital signatures, 245
documentation, 60-61
baselines, 64
policies, 61-63
procedures, 64
standards, 64
domains, 434
DRM, 246
education, 100-101
embedded system vulnerabilities, 208
endpoint, 376
engineering. See engineering
equipment security, 278-280
evaluation models, 180
Common Criteria, 186-187
controls/countermeasures, 190
ITSEC, 184-186
security implementation standards, 187-190
TCSEC, 181-184
geographical threats, 257-264
governance, 17
budgets, 20
business case, 19
due diligence, 39
effectiveness, 20
metrics, 20
organizational missions/objectives, 19
organizational processes, 21-23
organizational strategies/goals, 19
resources, 20-21
roles/responsibilities, 23-25
security function alignment, 18
implementation standards, 187-190
import/export controls, 51-58
information systems, 191
fault tolerance, 193
interfaces, 193
memory protection, 191
TPM, 192
virtualization, 191
intellectual property law, 47
copyrights, 49
DRM, 51
international protection, 51
patents, 47-48
software piracy, 50
trademarks, 49
trade secrets, 48
keys, managing, 237-245
legal/regulatory issues, 42-44
MAC, 251-253
major legal systems, 45
administrative/regulatory law, 46
civil code law, 45
civil/tort law, 46
common law, 46
criminal law, 46
customary, 47
mixed, 47
religious, 47
message integrity, 246-251
mobile system vulnerabilities, 205-207
models, 161
Bell-LaPadula model, 166
Biba model, 167
Brewer-Nash (Chinese Wall) model, 169
CLA, 161
Clark-Wilson Integrity model, 168
defense-in-depth, 163
Graham-Denning model, 169
Harrison-Ruzzo-Ullman model, 169
Lipner model, 169
modes, 161-163
types, 163-165
networks, 294
attacks, 390-401
communications, 311-315, 377-390
converged protocols, 323-325
cryptography, 333-339
IP, 305-311
OSI models, 294-297
protocols, 317-323
TCP/IP models, 298-304
types of, 315-317
wireless, 326-333
operations
change management, 525
concepts, 501-504
disaster recovery, 541-545
incident management, 516-520
investigations, 481-494
logging/monitoring, 494-497
patch management, 524-525
personnel privacy/safety, 554-555
physical security, 548-554
preventive measures, 520-524
protecting resources, 505-510, 513-515
recovery strategies, 526-541
resource provisioning, 497-501
testing recovery plans, 545-547
personnel security policies, 73
compliance, 76
employment agreements, 75
employment screening, 73-75
employment termination, 75-76
privacy, 76
vendor controls, 76
PKI, 234-237
policies, 601
process data, collecting, 466, 469
professional ethics, 59
Computer Ethics Institute, 59
IAB, 60
ISC Code of Ethics, 59
organizational, 60
requirements, 98-99
risk
acquisitions, 97-98
management, 77-92
services, 173-174
site and facility design, 264-269
software development
acquired software, 604
controls, 589-602
effectiveness assessments, 602-603
life cycles, 572-589
teams, 544
terms, 15
CIA, 15-16
default stance, 16
defense-in-depth strategy, 16
job rotation, 17
separation of duties, 17
testing
analyzing, 470
auditing, 470-472
threat modeling, 93
identifying, 94-95
potential attacks, 96
remediation, 96
web-based vulnerabilities, 203
attacks, 204
maintenance hooks, 203
OWASP, 205
SAML, 204
time-of-check/time-of-use attacks, 204
XML, 204
Security Assertion Markup Language. See SAML
security information and event management. See SIEM
seizure, investigations, 490
selecting
facilities, 266-269
standards, 144-146
sensitive information procedures, 503
sensitivity, data classification, 119
separation of duties, 17, 427
sequencing, 302
servers
proxy, 347
vulnerabilities, 196
service-level agreements. See SLAs
Service Organization Control. See SOC
service-oriented architect. See SOA
service set identifiers. See SSIDs
services, 317
directory, 429
DNS, 319
IDaaS, 438
NAT, 321
NETBIOS, 321
requirements, 99
risks, 97
security, 173-174
third-party identity, 439
SESAME (Secure European System for Applications in a Multi-vendor Environment), 433
Session layer (5), 296
sessions
hijacking, 400
managing, 434
SET (Secure Electronic Transaction), 337
SFTP (Secure FTP), 319
Shared Key Authentication, 331
shareware, 50
sharing data, 142
SHA (Secure Hash Algorithm), 250
Sherwood Applied Business Security Architecture. See SABSA
shoulder surfing, 445
SHTTP (Secure HTTP), 320, 337
SIEM (security information and event management), 462, 496
signaling, analog/digital, 311
signatures (digital), 245
simple passwords, 417
simulation tests, 547
single point of failure. See SPOF
single sign-on. See SSO
site design, 264-269
Six Sigma, 36
Skipjack, 229
SLAs (service-level agreements), 136, 505
smart cards, 421-422
SMB (Server Message Block), 322
SMDS (Switched Multimegabit Data Service), 372
smurf attacks, 394
sniffing, 447
SNMP, 322
SOA (service-oriented architecture), 571
social engineering, 255, 444
SOC (Service Organization Control), 471
software
analyzing, 491
backups, 535
development, 566-571
acquired software, 604
effectiveness assessments, 602-603
life cycles, 572-589
security controls, 589-602
patches, managing, 524-525
piracy, 50
risks, 97
Software-defined networking. See SDN
solution elements, vulnerabilities, 194
client-based, 195
cryptographic systems, 201
databases, 196-197
distributed systems, 197-200
large-scale parallel data systems, 201
server-based, 196
SONET (Synchronous Optical Networking), 370
source code
analysis tools, 595
issues, 591
spam, 398
spear phishing, 444
special privileges, monitoring, 504
Spiral model, 583
SPOF (single point of failure), 137
spoofing, 401, 447
spyware, 447, 599
SSAE (Statements on Standards for Attestation Engagement), 471
SSH (Secure Shell), 338
SSID (service set identifiers), 328, 333
SSL (Secure Sockets Layer), 337
SSO (single sign-on), 430-431
stacks, 295
standard word passwords, 417
standards
802.11a standard, 329
802.11ac standard, 329
802.11b standard, 329
802.11f standard, 329
802.11g standard, 330
802.11n standard, 330
802.11 standard, 326, 329
deviations, 520
documentation, 64
ISO/IEC 27000 Series, 27-30
security implementation, 187-190
selecting, 144-146
WLANs, 329-330
star topologies, 360
state machine models, 164
Statements on Standards for Attestation Engagement. See SSAE
static passwords, 418
statistical attacks, 256
steganography, 224
storage, 148, 175-176
evidence, 274
media, 514
privacy, 137-138
storage-area networks. See SANs
strategies
assessment, 456
defense-in-depth, 16
organizational strategies/goals, 19
recovery, 526-541
testing, 456
stream-based ciphers, 220
strikes, 263
Structured Programming Development model, 585
structured walk-through tests, 547
Stuxnet virus, 202
substitution ciphers, 218, 223-224
supervisors, roles/responsibilities, 26
supervisory control and data acquisition. See SCADA
supplies, recovery, 534-536
surveillance, 265
suspended states, 242
SWGDE (Scientific Working Group on Digital Evidence), 484-485
Switched Multimegabit Data Service. See SMDS
switches, 342
symmetric algorithms, 219-221, 224
AES, 228
Blowfish, 229
CAST, 230
DES/3DES, 225-228
IDEA, 229
RC4/RC5/RC6, 230
Skipjack, 229
Twofish, 230
symmetric authorization keys, 239
symmetric data-encryption keys, 238
symmetric key-agreement keys, 239
symmetric-key algorithms, 238
symmetric key-wrapping key, 238
symmetric master keys, 238
symmetric random number generation keys, 238
SYN ACK attacks, 400
Synchronous Optical Networking. See SONET
synchronous tokens, 421
synchronous transmissions, 312
synthetic transaction monitoring, 464
system administrators, roles/responsibilities, 25-26
system analysts, roles/responsibilities, 26
system architecture, 170
components, 174-177
computing platforms, 171-172
input/output devices, 177-180
ISO/IEC 42010:2011, 170
security services, 173-174
System Development Life Cycle. See SDLC
system evaluation models, 180
Common Criteria, 186-187
controls/countermeasures, 190
ITSEC, 184-186
security implementation standards, 187-190
TCSEC, 181-184
system high security modes, 162
system-level recovery strategies, 529
system owners, roles/responsibilities, 25
system-specific security policies, 63
systems
access controls, 413
hardening, 522
ownership, 129
resilience, 529
testing, 457
threats, 259-260
table-top exercises, 546
tables, capabilities, 442
TACACS+ (Terminal Access Controller Access-Control System Plus), 385
tagging attacks, 393
tailoring, 143
tampering, 278	
tangible asset protection, 505-509, 512-514
target tests, 458
TCP (Transmission Control Protocol) ports, 305
TCP/IP (Transmission Control Protocol/Internet Protocol), 298-304
TACACS+ (Terminal Access Controller Access-Control System Plus), 385
tagging attacks, 393
tailoring, 143
tampering, 278
tangible asset protection, 505-509, 512-514
target tests, 458
TCP (Transmission Control Protocol) ports, 305
TCP/IP (Transmission Control Protocol/Internet Protocol), 298-304
TCSEC (Trusted Computer System Evaluation Criteria), 181-184
teams
risk analysis, 79
risk management, 79
teadrop attacks, 401
technical controls, 90
technical management processes, 158
technical processes, 158
technologies
networks, 362-366, 369-373
recovery, 534
WANs, 369
telco concentrators, 340
telecommuting, 388
telnets, 387
TEMPEST program, 447
Terminal Access Controller Access-Control System Plus. See TACACS+
termination of employment, 75-76
terms (security), 15
availability, 16
confidentiality, 15
default stance, 16
defense-in-depth strategy, 16
integrity, 16
job rotation, 17
separation of duties, 17
terrorism, 263
tertiary sites, 533
test coverage analysis, 466
Test/Validate phase (SDLC), 576
testing
code, 464
interfaces, 466
misuse case, 465
penetration, 457-459
recovery plans, 545-547
security
analyzing, 470
auditing, 470-472
controls, 456-466
strategies, 456
theft, 262, 445
The Open Group Architecture Framework. See TOGAF
thin clients, 171
third-party
audits, 470-472
governance, 97-98
identity services, 439
security services, 523
threats, 77, 82. See also vulnerabilities
access control, 443-447
agents, 77
databases, 126
geographical, 257-264
identifying, 94-95
mitigating, 448
modeling, 93
passwords, 443
potential attacks, 96
preventive measures against, 520-524
remediation, 96
software, 596
Tiger, 251
time factor
authentication, 427
time-of-check/time-of-use attacks, 204
Time of Check/Time of Use. See TOC/TOU
T-lines, 369
TLS (Transport Layer Security), 337
TOC/TOU: Time of Check/Time of Use, 595
TOGAF (The Open Group Architecture Frame), 31
Token Ring 802.5 standard, 364
tokens, 421
passing, 369
tools, source code analysis, 595
top-down approaches, 38
topologies, networks, 359
tornadoes, 258
total risk, 85
TPM (Trusted Platform Module), 192
Traceroute, 395
tracking devices, 279
trade secrets, 48
trademarks, 49
training, 100-101, 469
disaster recovery, 545
trans-border data flow, 52
transmission
media, 354, 358-373
networks, 311-315
Transport layer (4), 296, 300
Transport Layer Security. See TLS
transposition ciphers, 219
trapdoors, 448, 593
turkey, employees, 555
Transport Layer Security. See TLS
transposition ciphers, 219
trapdoors, 448, 593
turkey, employees, 555
Treadway Commission Framework, 34
Triple DES (3DES), 225-228
Trojan horses, 446, 598
tropical storms, 258
Trusted Computer System Evaluation Criteria. See TCSEC
trusted paths, 521
Trusted Platform Module. See TPM
terrestrial recovery, 521
tuples, 123
turnstiles, 270
twisted pair cabling, 356-357
Twofish, 230
types
of access control, 88-91
cryptographic, 217
of doors, 269
of evidence, 488-491
of investigations, 493-494
of firewalls, 344-346
of locks, 270
of memory, 176
of networks, 315
extranets, 316
intranets, 316
LANs, 315
MANs, 316
WANs, 317

of passwords, 417-420
of power outages, 276
security outages, 276
security models, 163-165

U
unauthorized disclosure of information, 521
unicast transmissions, 314
uninterruptible power supplies. See UPSs
unscheduled reboots, 521
UPSs (Uninterruptible power supplies), 277
URL (uniform resource locator) hiding, 397
USA PATRIOT Act of 2001, 57
users
access control, 410
environment recovery, 537
relationship between resources and, 411
roles/responsibilities, 26
utility threats, 260

V
values, 567
vandalism, 262
vaults, 280
vendor controls, 76
verification data, backing up, 469
Vernam, Gilbert, 223
very-high-level languages, 566
views, 123, 126
Vigenere cipher, 213
virtual computing, 172
virtual local area networks. See VLANs
Virtual Router Redundancy Protocol. See VRRP
virtual storage area networks. See VSANs
virtualization, 191, 388
virtualized networks, 389-390
viruses, 446, 597
antivirus software, 600
visitor control, security, 272
VLANs (virtual local area networks), 343
voice, 377
VoIP (Voice over Internet Protocol), 325, 374
VPNs (virtual private networks), 382-384
concentrator, 340
screen scraper, 388
VRRP (Virtual Router Redundancy Protocol), 354
VSANs (virtual storage area network), 389
V-shaped model, 580
vulnerabilities, 77, 82
architecture, 194
cryptographic systems, 201
databases, 196-197
**distributed systems,** 197-200
**ICSs,** 202
**large-scale parallel data systems,** 201
**server-based,** 196
**assessments,** 456-457
**attacks,** 204
**cyber-physical system,** 208
**embedded system,** 208
**management systems,** 522
**mobile system,** 205-207
**OWASP,** 205
**SAML,** 204
**web-based,** 203
**maintenance books,** 203
**time-of-check/time-of-use attacks,** 204
**XML,** 204

**W**

**walls,** 550
**WANs** (wide area networks), 317, 369
**war Alexandria,** 399
**wardriver,** 399
**warm sites,** 532

**WASC** (Web Application Security Consortium), 590
**water leakage,** 278
**Waterfall model,** 580
**wave motion detectors,** 551
**Web Application Security Consortium. See WASC
web-based vulnerabilities,** 203
**attacks,** 204
**maintenance hooks,** 203
**OWASP,** 205
**SAML,** 204
**time-of-check/time-of-use attacks,** 204
**XML,** 204

**WEP** (Wired Equivalent Privacy), 331
**whaling,** 398
**whitelisting,** 523
**wide area networks. See WANs
Wi-Fi Protected Access. See WPA
Wired Equivalent Privacy. See WEP
**wireless transmissions,** 315

**X**

**X.25,** 372
**XML** (Extensible Markup Language)
**data storage,** 125
**vulnerabilities,** 204

**Z**

**Zachman framework,** 30
**Zero Knowledge Proof,** 233
**zero-knowledge tests,** 458