Cert Guide
Learn, prepare, and practice for exam success

CompTIA®
Advanced Security Practitioner
(CASP)
CAS-003

Save 10% on Exam Voucher
See Inside

FREE SAMPLE CHAPTER
SHARE WITH OTHERS
CompTIA® Advanced Security Practitioner (CASP) CAS-003 Cert Guide

Robin Abernathy
Troy McMillan
Contents at a Glance

INTRODUCTION The CASP Exam 2

CHAPTER 1 Business and Industry Influences and Associated Security Risks 38

CHAPTER 2 Security, Privacy Policies, and Procedures 64

CHAPTER 3 Risk Mitigation Strategies and Controls 96

CHAPTER 4 Risk Metric Scenarios to Secure the Enterprise 174

CHAPTER 5 Network and Security Components, Concepts, and Architectures 192

CHAPTER 6 Security Controls for Host Devices 286

CHAPTER 7 Security Controls for Mobile and Small Form Factor Devices 328

CHAPTER 8 Software Vulnerability Security Controls 354

CHAPTER 9 Security Assessments 382

CHAPTER 10 Select the Appropriate Security Assessment Tool 410

CHAPTER 11 Incident Response and Recovery 448

CHAPTER 12 Host, Storage, Network, and Application Integration 486

CHAPTER 13 Cloud and Virtualization Technology Integration 512

CHAPTER 14 Authentication and Authorization Technology Integration 536

CHAPTER 15 Cryptographic Techniques 570

CHAPTER 16 Secure Communication and Collaboration 616

CHAPTER 17 Industry Trends and Their Impact to the Enterprise 638

CHAPTER 18 Security Activities Across the Technology Life Cycle 664

CHAPTER 19 Business Unit Interaction 716

APPENDIX A Answers 732

Glossary 754

Index 798

Online-only Elements:

Appendix B Memory Tables

Appendix C Memory Table Answers

Appendix D Study Planner
# Table of Contents

**Introduction**  
The CASP Exam  2

- The Goals of the CASP Certification  3
- Sponsoring Bodies  3
- Other Security Exams  4
- Stated Goals  4

The Value of the CASP Certification  5

- To the Security Professional  5
- Department of Defense Directive 8140 and 8570 (DoDD 8140 and 8570)  5
- To the Enterprise  6

**CASP Exam Objectives**  7

1.0 Risk Management  7

- 1.1 Summarize business and industry influences and associated security risks.  7
- 1.2 Compare and contrast security, privacy policies and procedures based on organizational requirements.  8
- 1.3 Given a scenario, execute risk mitigation strategies and controls.  9
- 1.4 Analyze risk metric scenarios to secure the enterprise.  11

2.0 Enterprise Security Architecture  12

- 2.1 Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.  12
- 2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements.  14
- 2.3 Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.  17
- 2.4 Given software vulnerability scenarios, select appropriate security controls.  19

3.0 Enterprise Security Operations  21

- 3.1 Given a scenario, conduct a security assessment using the appropriate methods.  21
- 3.2 Analyze a scenario or output, and select the appropriate tool for a security assessment.  22
- 3.3 Given a scenario, implement incident response and recovery procedures.  23
Chapter 1  Business and Industry Influences and Associated Security Risks  38


New or Changing Business Models/Strategies  40

Partnerships  40
Outsourcing  41
Cloud  41
Acquisition/Merger and Divestiture/Demerger  42
Data Ownership  43
Data Reclassification  44

Security Concerns of Integrating Diverse Industries  44
Rules  44
Policies  45
Regulations 45
Export Controls 45
Legal Requirements 46
Geography 50
Data Sovereignty 50
Jurisdictions 51
Internal and External Influences 52
  Competitors 52
  Auditors/Audit Findings 52
  Regulatory Entities 53
  Internal and External Client Requirements 53
  Top-Level Management 54
Impact of De-perimeterization (e.g., Constantly Changing Network Boundary) 54
  Telecommuting 55
  Cloud 55
  Mobile 55
  BYOD 56
  Outsourcing 58
  Ensuring Third-Party Providers Have Requisite Levels of Information Security 58
Exam Preparation Tasks 60
Review All Key Topics 60
Define Key Terms 60
Review Questions 61

Chapter 2 Security, Privacy Policies, and Procedures 64
Policy and Process Life Cycle Management 65
  New Business 68
  New Technologies 68
  Environmental Changes 69
  Regulatory Requirements 69
  Emerging Risks 70
Support Legal Compliance and Advocacy 70
Common Business Documents to Support Security 71
Risk Assessment (RA) 71
Business Impact Analysis (BIA) 72
Interoperability Agreement (IA) 72
Interconnection Security Agreement (ISA) 72
Memorandum of Understanding (MOU) 73
Service-Level Agreement (SLA) 73
Operating-Level Agreement (OLA) 73
Non-Disclosure Agreement (NDA) 74
Business Partnership Agreement (BPA) 74
Master Service Agreement (MSA) 75
Security Requirements for Contracts 75
Request for Proposal (RFP) 76
Request for Quote (RFQ) 76
Request for Information (RFI) 76
Agreement or Contract 77
General Privacy Principles for Sensitive Information 77
Support the Development of Policies Containing Standard Security Practices 78
Separation of Duties 78
Job Rotation 79
Mandatory Vacation 80
Least Privilege 80
Incident Response 81
Events Versus Incidents 83
Rules of Engagement, Authorization, and Scope 83
Forensic Tasks 84
Employment and Termination Procedures 85
Continuous Monitoring 86
Training and Awareness for Users 86
Auditing Requirements and Frequency 88
Information Classification and Life Cycle 89
Commercial Business Classifications 89
Military and Government Classifications 90
Information Life Cycle 90
Exam Preparation Tasks  91
Review All Key Topics  91
Define Key Terms  92
Review Questions  92

Chapter 3 Risk Mitigation Strategies and Controls  96
Categorize Data Types by Impact Levels Based on CIA  98
Incorporate Stakeholder Input into CIA Impact-Level Decisions  100
Determine the Aggregate CIA Score  101
Determine Minimum Required Security Controls Based on Aggregate Score  102
Select and Implement Controls Based on CIA Requirements and Organizational Policies  102
  Access Control Categories  102
    Compensative  103
    Corrective  103
    Detective  103
    Deterrent  103
    Directive  103
    Preventive  104
    Recovery  104
  Access Control Types  104
    Administrative (Management) Controls  104
    Logical (Technical) Controls  106
    Physical Controls  107
Security Requirements Traceability Matrix (SRTM)  108
Security Control Frameworks  109
ISO/IEC 27000 Series  110
Zachman Framework™  112
The Open Group Architecture Framework (TOGAF)  113
Department of Defense Architecture Framework (DoDAF)  113
British Ministry of Defence Architecture Framework (MODAF)  113
Sherwood Applied Business Security Architecture (SABSA)  113
Control Objectives for Information and Related Technology (COBIT)  114
National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series  115
HITRUST CSF 118

CIS Critical Security Controls 118

Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework 119

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) 120

Information Technology Infrastructure Library (ITIL) 120

Six Sigma 121

Capability Maturity Model Integration (CMMI) 123

CCTA Risk Analysis and Management Method (CRAMM) 123

Extreme Scenario Planning/Worst-Case Scenario 123

Conduct System-Specific Risk Analysis 125

Make Risk Determination Based upon Known Metrics 126

Qualitative Risk Analysis 126

Quantitative Risk Analysis 127

Magnitude of Impact Based on ALE and SLE 128

SLE 128

ALE 128

Likelihood of Threat 129

Motivation 129

Source 130

ARO 130

Trend Analysis 130

Return on Investment (ROI) 131

Payback 132

Net Present Value (NPV) 132

Total Cost of Ownership 133

Translate Technical Risks in Business Terms 134

Recommend Which Strategy Should Be Applied Based on Risk Appetite 135

Avoid 135

Transfer 136

Mitigate 136

Accept 137
Risk Management Processes  137
  Information and Asset (Tangible/Intangible) Value and Costs  138
  Vulnerabilities and Threats Identification  139
  Exemptions  139
  Deterrence  140
  Inherent  140
  Residual  140

Continuous Improvement/Monitoring  141

Business Continuity Planning  141
  Business Continuity Scope and Plan  141
  Personnel Components  142
  Project Scope  142
  Business Continuity Steps  142
  Develop Contingency Planning Policy  144
  Conduct the BLA  145
  Identify Preventive Controls  147
  Create Contingency Strategies  148
  Plan Testing, Training, and Exercises (TT&E)  148
  Maintain the Plan  148

IT Governance  148
  Adherence to Risk Management Frameworks  149
  NIST  149
  Organizational Governance Components  164
  Policies  165
  Processes  167
  Procedures  167
  Standards  167
  Guidelines  167
  Baselines  167

Enterprise Resilience  168

Exam Preparation Tasks  170
  Review All Key Topics  170
  Define Key Terms  171
  Review Questions  171
Chapter 4  Risk Metric Scenarios to Secure the Enterprise  174

Review Effectiveness of Existing Security Controls  175
  Gap Analysis  176
  Lessons Learned and After-Action Reports  177
Reverse Engineer/Deconstruct Existing Solutions  177
Creation, Collection, and Analysis of Metrics  177
  KPIs  179
  KRIs  180
Prototype and Test Multiple Solutions  180
Create Benchmarks and Compare to Baselines  181
Analyze and Interpret Trend Data to Anticipate Cyber Defense Needs  182
Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs  183
  Performance  183
  Latency  184
  Scalability  184
  Capability  185
  Usability  185
  Maintainability  185
  Availability  185
  Recoverability  186
  Cost/Benefit Analysis  186
  ROI  186
  TCO  186
Use Judgment to Solve Problems Where the Most Secure Solution Is Not Feasible  187
Exam Preparation Tasks  187
  Review All Key Topics  187
  Define Key Terms  188
  Review Questions  189

Chapter 5  Network and Security Components, Concepts, and Architectures  192

Physical and Virtual Network and Security Devices  194
  UTM  194
  IDS/IPS  195
HIDS/HIPS 197
NIPS 197
NIDS 198
INE 198
NAC 199
SIEM 199
Switch 201
Firewall 202
Types of Firewalls 202
NGFWs 205
Firewall Architecture 205
Wireless Controller 208
Router 210
Proxy 210
Load Balancer 211
HSM 211
MicroSD HSM 212
Application and Protocol-Aware Technologies 212
WAF 212
Firewall 213
Passive Vulnerability Scanners 213
Active Vulnerability Scanners 214
DAM 214
Advanced Network Design (Wired/Wireless) 215
Remote Access 215
VPN 215
SSH 220
RDP 220
VNC 221
VDI 221
Reverse Proxy 222
IPv4 and IPv6 Transitional Technologies 222
Network Authentication Methods 224
802.1x 226
Mesh Networks 228

Application of Solutions 229

Placement of Hardware, Applications, and Fixed/Mobile Devices 230

Complex Network Security Solutions for Data Flow 241

  DLP 241
  Deep Packet Inspection 242
  Data-Flow Enforcement 243
  Network Flow (S/flow) 244
  Network Flow Data 244
  Data Flow Diagram 245

Secure Configuration and Baselining of Networking and Security Components 246

  ACLs 246
  Creating Rule Sets 246
  Change Monitoring 247
  Configuration Lockdown 248
  Availability Controls 248

Software-Defined Networking 254

Network Management and Monitoring Tools 255

  Alert Definitions and Rule Writing 259
  Tuning Alert Thresholds 259
  Alert Fatigue 260

Advanced Configuration of Routers, Switches, and Other Network Devices 260

  Transport Security 260
  Trunking Security 260
  Port Security 262
  Limiting MAC Addresses 263
  Implementing Sticky Mac Ports 263
  Ports 264
  Route Protection 266
  DDoS Protection 266
  Remotely Triggered Black Hole 267
Security Zones 268
  DMZ 268
  Separation of Critical Assets 268
  Network Segmentation 269
Network Access Control 269
  Quarantine/Remediation 270
  Persistent/Volatile or Non-persistent Agent 270
  Agent vs. Agentless 271
Network-Enabled Devices 271
  System on a Chip (SoC) 271
  Secure Booting 271
  Secured Memory 272
  Runtime Data Integrity Check 273
  Central Security Breach Response 274
Building/Home Automation Systems 274
IP Video 275
HVAC Controllers 276
Sensors 277
Physical Access Control Systems 277
A/V Systems 278
  Scientific/Industrial Equipment 279
Critical Infrastructure 279
Exam Preparation Tasks 280
Review All Key Topics 280
Define Key Terms 282
Review Questions 282

Chapter 6 Security Controls for Host Devices 286
  Trusted OS (e.g., How and When to Use It) 287
    SELinux 289
    SEAndroid 289
    TrustedSolaris 290
    Least Functionality 290
Chapter 7  Security Controls for Mobile and Small Form Factor Devices  328

Enterprise Mobility Management  329
   Containerization  329
   Configuration Profiles and Payloads  329
   Personally Owned, Corporate-Enabled  330
   Application Wrapping  330
   Remote Assistance Access  330
   VNC  330

Screen Mirroring  330
   Application, Content, and Data Management  331
   Over-the-Air Updates (Software/Firmware)  331
   Remote Wiping  332
   SCEP  332
   BYOD  332
   COPE  332
   VPN  333
Application Permissions 333
Side Loading 334
Unsigned Apps/System Apps 334
Context-Aware Management 334
Geolocation/Geofencing 335
User Behavior 335
Security Restrictions 336
Time-Based Restrictions 336
Frequency 336
Security Implications/Privacy Concerns 336
Data Storage 336
Non-Removable Storage 337
Removable Storage 337
Cloud Storage 337
Transfer/Backup Data to Uncontrolled Storage 338
USB OTG 338
Device Loss/Theft 338
Hardware Anti-Tamper 338
eFuse 338
TPM 339
Rooting/Jailbreaking 339
Push Notification Services 339
Geotagging 339
Encrypted Instant Messaging Apps 340
Tokenization 340
OEM/Carrier Android Fragmentation 340
Mobile Payment 340
NFC-Enabled 340
Inductance-Enabled 341
Mobile Wallet 341
Peripheral-Enabled Payments (Credit Card Reader) 341
Tethering 341
USB 342
Spectrum Management 342
Bluetooth 3.0 vs. 4.1 342
Authentication 342

Swype Pattern 343

Gesture 343

PIN Code 343

Biometric 343

Malware 344

Unauthorized Domain Bridging 344

Baseband Radio/SOC 345

Augmented Reality 345

SMS/MMS/Messaging 345

Wearable Technology 345

Devices 346

Cameras 346

Watches 346

Fitness Devices 347

Glasses 347

Medical Sensors/Devices 348

Headsets 348

Security Implications 349

Unauthorized Remote Activation/Deactivation of Devices or Features 349

Encrypted and Unencrypted Communication Concerns 349

Physical Reconnaissance 349

Personal Data Theft 350

Health Privacy 350

Digital Forensics on Collected Data 350

Exam Preparation Tasks 350

Review All Key Topics 350

Define Key Terms 351

Review Questions 351

Chapter 8 Software Vulnerability Security Controls 354

Application Security Design Considerations 355

Secure: By Design, By Default, By Deployment 355

Specific Application Issues 356

Unsecure Direct Object References 356

XSS 356
Cross-Site Request Forgery (CSRF) 357
Click-Jacking 358
Session Management 359
Input Validation 360
SQL Injection 360
Improper Error and Exception Handling 362
Privilege Escalation 362
Improper Storage of Sensitive Data 362
Fuzzing/Fault Injection 363
Secure Cookie Storage and Transmission 364
Buffer Overflow 364
Memory Leaks 367
Integer Overflows 367
Race Conditions 367
Time of Check/Time of Use 367
Resource Exhaustion 368
Geotagging 368
Data Remnants 369
Use of Third-Party Libraries 369
Code Reuse 370
Application Sandboxing 370
Secure Encrypted Enclaves 371
Database Activity Monitor 371
Web Application Firewalls 371
Client-Side Processing vs. Server-Side Processing 371
JSON/REST 372
Browser Extensions 373
ActiveX 373
Java Applets 373
HTML5 374
AJAX 374
SOAP 376
State Management 376
JavaScript 376
Chapter 9  Security Assessments  382

Methods  383

Malware Sandboxing  383
Memory Dumping, Runtime Debugging  384
Reconnaissance  385
Fingerprinting  385
Code Review  387
Social Engineering  388

Phishing/Pharming  388
Shoulder Surfing  389
Identity Theft  389
Dumpster Diving  389
Pivoting  389
Open Source Intelligence  390

Social Media  390
Whois  391
Routing Tables  392
DNS Records  394
Search Engines  397

Test Types  398

Penetration Test  398
Black Box  400
White Box  400
Gray Box  400
Vulnerability Assessment  401
Self-Assessment  402

Tabletop Exercises  403
Chapter 10  Select the Appropriate Security Assessment Tool  410

Network Tool Types  411
  Port Scanners  411
  Network Vulnerability Scanners  413
  Protocol Analyzer  414

Wired  414

Wireless  415

SCAP Scanner  416

Permissions and Access  418

Execute Scanning  419

Network Enumerator  420

Fuzzer  421

HTTP Interceptor  422

Exploitation Tools/Frameworks  422

Visualization Tools  424

Log Reduction and Analysis Tools  425

Host Tool Types  427

Password Cracker  427

Host Vulnerability Scanners  428

Command Line Tools  429

netstat  429

ping  431

tracert/traceroute  433

ipconfig/ifconfig  434

nslookup/dig  435

Sysinternals  435

OpenSSL  436

Local Exploitation Tools/Frameworks  436
SCAP Tool 437
File Integrity Monitoring 437
Log Analysis Tools 438
Antivirus 439
Reverse Engineering Tools 440
Physical Security Tools 441
Lock Picks 441
Locks 442
RFID Tools 444
IR Camera 444
Exam Preparation Tasks 444
Review All Key Topics 444
Define Key Terms 445
Review Questions 446

Chapter 11 Incident Response and Recovery 448
E-Discovery 449
Electronic Inventory and Asset Control 450
Data Retention Policies 451
Data Recovery and Storage 451
Data Ownership 452
Data Handling 453
Legal Holds 454
Data Breach 454
Detection and Collection 455
Data Analytics 455
Mitigation 456
Minimize 456
Isolate 456
Recovery/Reconstitution 456
Response 457
Disclosure 457
Facilitate Incident Detection and Response 457
Internal and External Violations 458
Privacy Policy Violations 458
Criminal Actions 459
Insider Threats 459
Non-malicious Threats/Misconfigurations 459
Hunt Teaming 460
Heuristics/Behavioral Analytics 460
Establish and Review System, Audit and Security Logs 461

Incident and Emergency Response 461
Chain of Custody 461
Evidence 462
Surveillance, Search, and Seizure 463
Forensic Analysis of Compromised System 463
Media Analysis 464
Software Analysis 464
Network Analysis 464
Hardware/Embedded Device Analysis 465
Continuity of Operations 465
Disaster Recovery 465
Data Backup Types and Schemes 465
Electronic Backup 469
Incident Response Team 469
Order of Volatility 470

Incident Response Support Tools 471
dd 471
tcpdump 472
nbtstat 473
netstat 474
nc (Netcat) 475
memcopy 476
tshark 476
foremost 477

Severity of Incident or Breach 478
Scope 478
Impact 478
System Process Criticality 479
Cost 479
Downtime 479
Legal Ramifications 480
Post-incident Response 480
Root-Cause Analysis 480
Lessons Learned 480
After-Action Report 481
Change Control Process 481
Update Incident Response Plan 481
Exam Preparation Tasks 481
Review All Key Topics 481
Define Key Terms 482
Review Questions 483

Chapter 12 Host, Storage, Network, and Application Integration 486
Adapt Data Flow Security to Meet Changing Business Needs 487
Standards 489
Open Standards 489
Adherence to Standards 489
Competing Standards 490
Lack of Standards 490
De Facto Standards 490
Interoperability Issues 491
Legacy Systems and Software/Current Systems 491
Application Requirements 492
Software Types 492
In-house Developed 493
Commercial 493
Tailored Commercial 493
Open Source 493
Standard Data Formats 493
Protocols and APIs 494
Resilience Issues 494
Use of Heterogeneous Components 494
Course of Action Automation/Orchestration 495
Distribution of Critical Assets 495
Persistence and Non-persistence of Data 495
Chapter 13  Cloud and Virtualization Technology Integration  512

Technical Deployment Models (Outsourcing/Insourcing/Managed Services/Partnership)  513
  Cloud and Virtualization Considerations and Hosting Options  513
    Public  514
    Private  514
    Hybrid  514
    Community  514
    Multitenancy  515
    Single Tenancy  515
  On-Premise vs. Hosted  515
Cloud Service Models  516

Security Advantages and Disadvantages of Virtualization  518
  Type 1 vs. Type 2 Hypervisors  519
    Type 1 Hypervisor  519
    Type 2 Hypervisor  519
  Container-Based  520
    vTPM  520
  Hyperconverged Infrastructure  521
  Virtual Desktop Infrastructure  521
  Secure Enclaves and Volumes  521
Cloud Augmented Security Services  521
  Hash Matching  522
  Anti-malware  522
  Vulnerability Scanning  523
  Sandboxing  525
  Content Filtering  525
  Cloud Security Broker  526
  Security as a Service  527
  Managed Security Service Providers  527

Vulnerabilities Associated with Comingling of Hosts with Different Security Requirements  527
  VM Escape  527
  Privilege Elevation  528
Chapter 14 Authentication and Authorization Technology Integration  536

Authentication  537
  Authentication Factors  538  
  Knowledge Factors  538
  Ownership Factors  538
  Characteristic Factors  539
  Additional Authentication Concepts  540
  Identity and Account Management  540
  Password Types and Management  541
  Physiological Characteristics  544
  Behavioral Characteristics  545
  Biometric Considerations  546
  Dual-Factor and Multi-Factor Authentication  547
  Certificate-Based Authentication  548
  Single Sign-on  548
  802.1x  549
  Context-Aware Authentication  550
  Push-Based Authentication  550

Authorization  550
  Access Control Models  550
  Discretionary Access Control  551
  Mandatory Access Control  551
Role-Based Access Control 551
Rule-Based Access Control 552
Content-Dependent Access Control 552
Access Control Matrix 552
ACLs 553
Access Control Policies 553
Default to No Access 553
OAuth 553
XACML 555
SPML 556
Attestation 557
Identity Proofing 558
Identity Propagation 558
Federation 559
SAML 560
OpenID 561
Shibboleth 561
WAYF 563
Trust Models 563
RADIUS Configurations 563
LDAP 564
AD 565
Exam Preparation Tasks 566
Review All Key Topics 566
Define Key Terms 567
Review Questions 567

Chapter 15 Cryptographic Techniques 570
Techniques 572
Key Stretching 572
Hashing 572
MD2/MD4/MD5/MD6 574
SHA/SHA-2/SHA-3 575
HAVAL 576
RIPEMD-160 576
Digital Signature 576
Message Authentication 577
Code Signing 578
Pseudo-Random Number Generation 578
Perfect Forward Secrecy 578
Data-in-Transit Encryption 579
SSL/TLS 579
HTTP/HTTPS/SHTTP 579
SET and 3-D Secure 580
IPsec 580
Data-in-Memory/Processing 581
Data-at-Rest Encryption 581
Symmetric Algorithms 582
Asymmetric Algorithms 585
Hybrid Ciphers 588
Disk-Level Encryption 588
Block-Level Encryption 589
File-Level Encryption 589
Record-Level Encryption 589
Port-Level Encryption 591
Steganography 591
Implementations 592
Crypto Modules 592
Crypto Processors 593
Cryptographic Service Providers 593
DRM 593
Watermarking 594
GNU Privacy Guard (GPG) 594
SSL/TLS 595
Secure Shell (SSH) 595
S/MIME 596
Cryptographic Applications and Proper/Improper Implementations 596
Strength Versus Performance Versus Feasibility to Implement Versus Interoperability 596
Feasibility to Implement 597
Interoperability 597
Stream vs. Block 597
Stream Ciphers 597
Block Ciphers 598
Modes 598
Known Flaws/Weaknesses 602
PKI 603
Wildcard 603
OCSP vs. CRL 604
Issuance to Entities 604
Key Escrow 606
Certificate 606
Tokens 607
Stapling 608
Pinning 608
Cryptocurrency/Blockchain 609
Mobile Device Encryption Considerations 610
Elliptic Curve Cryptography 610
P256 vs. P384 vs. P512 610
Exam Preparation Tasks 611
Review All Key Topics 611
Define Key Terms 612
Review Questions 613

Chapter 16 Secure Communication and Collaboration 616
Remote Access 617
Dial-up 617
VPN 618
SSL 618
Remote Administration 618
Resource and Services 618
Desktop and Application Sharing 619
Remote Assistance 620
Unified Collaboration Tools 621
   Web Conferencing 621
   Video Conferencing 622
   Audio Conferencing 623
Storage and Document Collaboration Tools 624
Unified Communication 625
Instant Messaging 625
Presence 626
Email 627
IMAP 627
POP 627
SMTP 628
Email Spoofing 628
Spear Phishing 628
Whaling 629
Spam 629
Captured Messages 629
Disclosure of Information 630
Malware 630
Telephony and VoIP Integration 630
Collaboration Sites 632
Social Media 632
Cloud-Based Collaboration 633
Exam Preparation Tasks 634
   Review All Key Topics 634
Define Key Terms 635
Review Questions 635

Chapter 17 Industry Trends and Their Impact to the Enterprise 638
Perform Ongoing Research 639
   Best Practices 640
New Technologies, Security Systems and Services 641
Technology Evolution (e.g., RFCs, ISO) 642
Threat Intelligence 643
   Latest Attacks 644
Knowledge of Current Vulnerabilities and Threats 646
Zero-Day Mitigation Controls and Remediation 647
Threat Model 648
Research Security Implications of Emerging Business Tools 649
   Evolving Social Media Platforms 650
   End-User Cloud Storage 650
   Integration Within the Business 651
   Big Data 652
   AI/Machine Learning 653
Global IA Industry/Community 653
   Computer Emergency Response Team (CERT) 654
   Conventions/Conferences 654
   Research Consultants/Vendors 655
   Threat Actor Activities 655
   Topology Discovery 656
   OS Fingerprinting 657
   Service Discovery 657
   Packet Capture 657
   Log Review 658
   Router/Firewall ACLs Review 658
   Email Harvesting 658
   Social Media Profiling 659
   Social Engineering 659
   Phishing 659
   Emerging Threat Sources 660
Exam Preparation Tasks 660
   Review All Key Topics 660
   Define Key Terms 661
   Review Questions 661

Chapter 18 Security Activities Across the Technology Life Cycle 664
Systems Development Life Cycle 665
   Requirements 667
   Acquisition 668
   Test and Evaluation 668
Commissioning/Decommissioning 668
Operational Activities 669
Monitoring 669
Maintenance 670
Configuration and Change Management 671
Asset Disposal 672
Asset/Object Reuse 673
Software Development Life Cycle 673
Plan/Initiate Project 674
Gather Requirements 674
Design 675
Develop 675
Test/Validate 676
Release/Maintain 676
Certify/Accredit 676
Change Management and Configuration Management/
Replacement 677
Application Security Frameworks 677
Software Assurance 677
Auditing and Logging 677
Risk Analysis and Mitigation 678
Regression and Acceptance Testing 678
Security Impact of Acquired Software 679
Standard Libraries 679
Industry-Accepted Approaches 680
Web Services Security (WS-Security) 681
Forbidden Coding Techniques 681
NX/XN Bit Use 682
ASLR Use 682
Code Quality 683
Code Analyzers 683
Development Approaches 688
Build and Fix 689
Waterfall 689
V-Shaped 690
Prototyping 691
Incremental 691
Spiral 692
Rapid Application Development (RAD) 692
Agile 694
JAD 694
Cleanroom 695
DevOps 695
Security Implications of Agile, Waterfall, and Spiral Software Development Methodologies 696
Continuous Integration 698
Versioning 698
Secure Coding Standards 700
Documentation 700
Security Requirements Traceability Matrix (SRTM) 700
Requirements Definition 701
System Design Document 701
Testing Plans 702
Validation and Acceptance Testing 704
Unit Testing 704
Adapt Solutions 706
Address Emerging Threats 706
Address Disruptive Technologies 707
Address Security Trends 708
Asset Management (Inventory Control) 709
Device-Tracking Technologies 709
Geolocation/GPS Location 709
Object Tracking and Containment Technologies 709
Geotagging/Geofencing 710
RFID 710
Exam Preparation Tasks 711
Review All Key Topics 711
Define Key Terms 712
Review Questions 713
Chapter 19  Business Unit Interaction  716

Interpreting Security Requirements and Goals to Communicate with Stakeholders from Other Disciplines  717
  Sales Staff  717
  Programmer  718
  Database Administrator  719
  Network Administrator  720
  Management/Executive Management  720
  Financial  722
  Human Resources  722
  Emergency Response Team  723
  Facilities Manager  723
  Physical Security Manager  723
  Legal Counsel  724

Provide Objective Guidance and Impartial Recommendations to Staff and Senior Management on Security Processes and Controls  724

Establish Effective Collaboration Within Teams to Implement Secure Solutions  725

Governance, Risk, and Compliance Committee  726

Exam Preparation Tasks  727
  Review All Key Topics  727
  Define Key Terms  728
  Review Questions  729

Appendix A  Answers  732

Glossary  754

Index  798

Online-only Elements:
  Appendix B Memory Tables
  Appendix C Memory Table Answers
  Appendix D Study Planner
About the Authors

Robin Abernathy, CASP, is a product developer and technical editor for Kaplan IT training. She has developed and reviewed certification preparation materials in a variety of product lines, including Microsoft, CompTIA, Cisco, ITIL, (ISC)², and PMI, and holds multiple certifications from these vendors. Her work with Kaplan IT Training includes practice tests and study guides for the Transcender brands.

Robin most recently co-authored Pearson’s CISSP Cert Guide with Troy McMillan and Sari Green and authored Pearson’s Project+ Cert Guide. She provides training on computer hardware, software, networking, security, and project management. Robin also presents at technical conferences and hosts webinars on IT certification topics. More recently, Robin has recorded videos for CyberVista’s IT certification training courses.

Troy McMillan, CASP, is a product developer and technical editor for Kaplan IT Training as well as a full-time trainer. He became a professional trainer more than 15 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. His recent work includes:

- Contributing subject matter expert for CCNA Cisco Certified Network Associate Certification Exam Preparation Guide (Kaplan)
- Prep test question writer for Network+ Study Guide (Sybex)
- Technical editor for Windows 7 Study Guide (Sybex)
- Contributing author for CCNA-Wireless Study Guide (Sybex)
- Technical editor for CCNA Study Guide, Revision 7 (Sybex)
- Author of VCP VMware Certified Professional on vSphere 4 Review Guide: Exam VCP-410 and associated instructional materials (Sybex)
- Author of Cisco Essentials (Sybex)
- Co-author of CISSP Cert Guide (Pearson)
- Prep test question writer for CCNA Wireless 640-722 (Cisco Press)

He also has appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND 1; ICND 2; and Cloud+.

He now creates certification practice tests and study guides for the Transcender brands. Troy lives in both Sugarloaf Key, Florida, and Pfafftown, North Carolina, with his wife, Heike.
Dedication

For my husband, Michael, and my son, Jonas. I love you both!
—Robin

I dedicate this book to my wife, who worked tirelessly recovering us from Hurricane Irma. I love you, honey!
—Troy
Acknowledgments

First, I once again thank my heavenly Father for blessing me throughout my life. I would also like to thank all my family members, many of whom wondered where their acknowledgement was in the CISSP Cert Guide. To my siblings, Libby McDaniel Loggins and Kenneth McDaniel: Thanks for putting up with my differences and loving me anyway. To their spouses, Dave Loggins and Michelle Duncan McDaniel, thanks for choosing my siblings and deciding to still stay with them, even when you realized I was part of the package. LOL! To my husband’s family, I thank you for accepting me into your family. James and Sandra Abernathy, thanks for raising such a wonderful man. Cathy Abernathy Bonds and Tony Abernathy, thanks for helping to shape him into the man he is. Tony, you are missed more than you will ever know!

I must thank my wonderful husband, Michael, and son, Jonas, for once again being willing to do “guy things” while I was locked away in the world of CASP. You are my world! What a wonderful ride we are on!!!

Thanks to all at Pearson for once again assembling a wonderful team to help Troy and me get through this CASP journey.

To you, the reader, I wish you success in your IT certification goals!

—Robin Abernathy

I must thank my coworkers at Kaplan IT Training, who have helped me to grow over the past 15 years. Thank you, Ann, George, John, Josh, Robin, and Shahara. I also must as always thank my beautiful wife, who has supported me through the lean years and continues to do so. Finally, I have to acknowledge all the help and guidance from the Pearson team.

—Troy McMillan
About the Reviewer

**Chris Crayton**, MCSE, is an author, a technical consultant, and a 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.
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 CompTIA Advanced Security Practitioner (CASP) CAS-003 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 9780789759443 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.
About the Book

The CompTIA Advanced Security Practitioner (CASP) certification is a popular certification for those in the security field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA CASP certification is unique in that it is vendor neutral. The CompTIA CASP certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by ISC².

In the CompTIA CASP exam, the topics are mostly generic in that they can apply to many security devices and technologies, regardless of vendor. Although the CompTIA CASP is vendor neutral, devices and technologies are implemented by multiple independent vendors. In that light, several of the examples associated with this book include using particular vendors’ configurations and technologies. More detailed training regarding a specific vendor’s software and hardware can be found in books and training specific to that vendor.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the CASP CAS-003 blueprint from CompTIA. This book also helps you demonstrate your knowledge by passing the CAS-003 version of the CompTIA CASP exam.

To aid you in mastering and understanding the CASP + certification objectives, this book provides the following tools:

- **Opening topics list:** This list defines the topics that are covered in the chapter.

- **Key Topics icons:** These icons indicate important figures, tables, and lists of information that you need to know for the exam. They are sprinkled throughout each chapter and are summarized in table format at the end of each chapter.

- **Memory tables:** These can be found on the companion website and in Appendix B, “Memory Tables,” and Appendix C, “Memory Tables Answer Key.” Use them to help memorize important information.

- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the Glossary.

For current information about the CompTIA CASP certification exam, visit https://certification.comptia.org/certifications/comptia-advanced-security-practitioner.
Who Should Read This Book?

Readers of this book will range from people who are attempting to attain a position in the IT security field to people who want to keep their skills sharp or perhaps retain their job when a company policy mandates that they take the new exams.

This book is also for readers who want to acquire additional certifications beyond the CASP certification (for example, the CISSP certification and beyond). The book is designed in such a way to offer easy transition to future certification studies.

Strategies for Exam Preparation

Read the chapters in this book, jotting down notes with key concepts or configurations on a separate notepad.

Download the current list of exam objectives by submitting a form at http://certification.comptia.org/examobjectives.aspx.

Use the practice exam, which is included on this book’s companion website. As you work through the practice exam, note the areas where you lack confidence and review those concepts. After you review these areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through a practice exam, the more familiar the questions become, and the practice exam becomes a less accurate indicator of your skills.

After you work through a practice exam a second time and feel confident with your skills, schedule the real CompTIA CASP exam (CAS-003). The following website provides information about registering for the exam: www.pearsonvue.com/comptia/.

CompTIA CASP Exam Topics

Table 1 lists general exam topics (objectives) and specific topics under each general topic (subobjectives) for the CompTIA CASP CAS-003 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters.
<table>
<thead>
<tr>
<th>Chapter</th>
<th>CAS-003 Exam Objective</th>
<th>CAS-003 Exam Subobjective</th>
</tr>
</thead>
</table>
| 1       | Business and Industry Influences and Associated Security Risks | 1.1 Summarize business and industry influences and associated security risks. | - Risk management of new products, new technologies and user behaviors  
- New or changing business models/strategies  
- Security concerns of integrating diverse industries  
- Internal and external influences  
- Impact of de-perimeterization (e.g., constantly changing network boundary) |
| 2       | Security, Privacy Policies, and Procedures | 1.2 Compare and contrast security, privacy policies and procedures based on organizational requirements. | - Policy and process life cycle management  
- Support legal compliance and advocacy by partnering with human resources, legal, management and other entities  
- Understand common business documents to support security  
- Research security requirements for contracts  
- Understand general privacy principles for sensitive information  
- Support the development of policies containing standard security practices |
| 3       | Risk Mitigation Strategies and Controls | 1.3 Given a scenario, execute risk mitigation strategies and controls. | - Categorize data types by impact levels based on CIA  
- Incorporate stakeholder input into CIA impact-level decisions  
- Determine minimum-required security controls based on aggregate score  
- Select and implement controls based on CIA requirements and organizational policies  
- Extreme scenario planning/worst-case scenario  
- Conduct system-specific risk analysis  
- Make risk determination based upon known metrics  
- Translate technical risks in business terms  
- Recommend which strategy should be applied based on risk appetite  
- Risk management processes  
- Continuous improvement/monitoring  
- Business continuity planning  
- IT governance  
- Enterprise resilience |
<table>
<thead>
<tr>
<th>Chapter</th>
<th>CAS-003 Exam Objective</th>
<th>CAS-003 Exam Subobjective</th>
</tr>
</thead>
</table>
| 4       | 1.4 Analyze risk metric scenarios to secure the enterprise. | ■ Review effectiveness of existing security controls  
■ Reverse engineer/deconstruct existing solutions  
■ Creation, collection and analysis of metrics  
■ Prototype and test multiple solutions  
■ Create benchmarks and compare to baselines  
■ Analyze and interpret trend data to anticipate cyber defense needs  
■ Analyze security solution metrics and attributes to ensure they meet business needs  
■ Use judgment to solve problems where the most secure solution is not feasible |
| 5       | 2.1 Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements. | ■ Physical and virtual network and security devices  
■ Application and protocol-aware technologies  
■ Advanced network design (wired/wireless)  
■ Complex network security solutions for data flow  
■ Secure configuration and baselining of networking and security components  
■ Software-defined networking  
■ Network management and monitoring tools  
■ Advanced configuration of routers, switches and other network devices  
■ Security zones  
■ Network access control  
■ Network-enabled devices  
■ Critical infrastructure |
| 6       | 2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements. | ■ Trusted OS (e.g., how and when to use it)  
■ Endpoint security software  
■ Host hardening  
■ Boot loader protections  
■ Vulnerabilities associated with hardware  
■ Terminal services/application delivery services |
<table>
<thead>
<tr>
<th>Chapter</th>
<th>CAS-003 Exam Objective</th>
<th>CAS-003 Exam Subobjective</th>
</tr>
</thead>
</table>
| 7       | 2.3 Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements. | ▪ Enterprise mobility management  
▪ Security implications/privacy concerns  
▪ Wearable technology |
| 8       | 2.4 Given software vulnerability scenarios, select appropriate security controls. | ▪ Application security design considerations  
▪ Specific application issues  
▪ Application sandboxing  
▪ Secure encrypted enclaves  
▪ Database activity monitor  
▪ Web application firewalls  
▪ Client-side processing vs. server-side processing  
▪ Operating system vulnerabilities  
▪ Firmware vulnerabilities |
| 9       | 3.1 Given a scenario, conduct a security assessment using the appropriate methods. | ▪ Methods  
▪ Types |
| 10      | 3.2 Analyze a scenario or output, and select the appropriate tool for a security assessment. | ▪ Network tool types  
▪ Host tool types  
▪ Physical security tools |
| 11      | 3.3 Given a scenario, implement incident response and recovery procedures. | ▪ E-discovery  
▪ Data breach  
▪ Facilitate incident detection and response  
▪ Incident and emergency response  
▪ Incident response support tools  
▪ Severity of incident or breach  
▪ Post-incident response |
<table>
<thead>
<tr>
<th>Chapter</th>
<th>CAS-003 Exam Objective</th>
<th>CAS-003 Exam Subobjective</th>
</tr>
</thead>
</table>
| 12      | 4.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture. | ■ Adapt data flow security to meet changing business needs  
■ Standards  
■ Interoperability issues  
■ Resilience issues  
■ Data security considerations  
■ Resources provisioning and deprovisioning  
■ Design considerations during mergers, acquisitions and demergers/divestitures  
■ Network secure segmentation and delegation  
■ Logical deployment diagram and corresponding physical deployment diagram of all relevant devices  
■ Security and privacy considerations of storage integration  
■ Security implications of integrating enterprise applications |
| 13      | 4.2 Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture. | ■ Technical deployment models (outsourcing/insourcing/managed services/partnership)  
■ Security advantages and disadvantages of virtualization  
■ Cloud augmented security services  
■ Vulnerabilities associated with comingling of hosts with different security requirements  
■ Data security considerations  
■ Resources provisioning and deprovisioning |
| 14      | 4.3 Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives. | ■ Authentication  
■ Authorization  
■ Attestation  
■ Identity proofing  
■ Identity propagation  
■ Federation  
■ Trust models |
<table>
<thead>
<tr>
<th>Chapter</th>
<th>CAS-003 Exam Objective</th>
<th>CAS-003 Exam Subobjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Cryptographic Techniques</td>
<td>4.4 Given a scenario, implement cryptographic techniques.</td>
<td>■ Techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Implementations</td>
</tr>
<tr>
<td>16 Secure Communication and Collaboration</td>
<td>4.5 Given a scenario, select the appropriate control to secure communications and collaboration solutions.</td>
<td>■ Remote access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Unified collaboration tools</td>
</tr>
<tr>
<td>17 Industry Trends and Their Impact to the Enterprise</td>
<td>5.1 Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.</td>
<td>■ Perform ongoing research</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Threat intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Research security implications of emerging business tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Global IA industry/community</td>
</tr>
<tr>
<td>18 Security Activities Across the Technology Life Cycle</td>
<td>5.2 Given a scenario, implement security activities across the technology life cycle.</td>
<td>■ Systems development life cycle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Software development life cycle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Adapt solutions to address: emerging threats, disruptive technologies, and security trends</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Asset management (inventory control)</td>
</tr>
<tr>
<td>19 Business Unit Interaction</td>
<td>5.3 Explain the importance of interaction across diverse business units to achieve security goals.</td>
<td>■ Interpreting security requirements and goals to communicate with stakeholders from other disciplines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Establish effective collaboration within teams to implement secure solutions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Governance, risk and compliance committee</td>
</tr>
</tbody>
</table>
How This Book Is Organized

Although this book could be read cover-to-cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use.

In addition to the 19 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The companion website also includes a practice test and memory tables that you can work through to verify your knowledge of the subject matter.

Companion Website

Register this book to get access to the Pearson Test Prep practice test software 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 updates and 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: 9780789759443.
3. Answer the challenge question as proof of purchase.
4. Click the Access Bonus Content link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

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

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

Pearson Test Prep Practice Test Software

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

NOTE The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

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

2. Select Pearson IT Certification as your product group.
3. Enter the email/password for your account. If you don’t have an account on PearsonITCertification.com or CiscoPress.com, you need to establish one by going to PearsonITCertification.com/join.
4. In the My Products tab, click the Activate New Product button.
5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is now listed in your My Products page.
6. Click the Exams button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book’s companion website, or you can just enter this link in your browser: http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip.

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

2. Respond to the challenge questions.

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

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

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

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

7. Double-click the application file to start the installation and follow the on-screen instructions to complete the registration.

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

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

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

11. Click Next and then the Finish button to download the exam data to your application.

12. You can now start using the practice exams by selecting the product and clicking the Open Exam button to open the exam settings screen.

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

**Customizing Your Exams**

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

- **Study Mode**
- **Practice Exam Mode**
- **Flash Card Mode**

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

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

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

**Updating Your Exams**

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

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and select the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the **Tools** tab and select the **Update Application** button. This will ensure you are running the latest version of the software engine.
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. The best way to determine your readiness is to work through the chapter questions at the end of each chapter and to review the foundation and key topics. 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. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.
This page intentionally left blank
This chapter covers the following topics:

- **The Goals of the CASP Certification**: This section describes CASP’s sponsoring bodies and the stated goals of the certification.

- **The Value of the CASP Certification**: This section examines the career and business drivers for the CASP certification.

- **CASP Exam Objectives**: This section lists the official objectives covered on the CASP exam.

- **Steps to Becoming a CASP**: This section explains the process involved in achieving the CASP certification.

- **CompTIA Authorized Materials Use Policy**: This section provides information on the CompTIA Certification Exam Policies web page.
The CASP Exam

The CompTIA Certified Advanced Security Practitioner (CASP) exam is designed to identify IT professionals with advanced-level competency in enterprise security; risk management; incident response; research and analysis; and integration of computing, communications, and business disciplines.

As the number of security threats to organizations grows and the nature of these threats broadens, companies large and small have realized that security can no longer be an afterthought. It must be built into the DNA of the enterprise to be successful. This means trained professionals must not only be versed in security theory but must also be able to implement measures that provide enterprisewide security. While no prerequisites exist to take the exam, it is often the next step for many security professionals after passing the CompTIA Security+ exam.

The Goals of the CASP Certification

The CASP exam is a vendor-neutral exam created and managed by CompTIA. An update to the CASP certification exam launched April 2, 2018. The new exam, CAS-003, replaces CAS-002, which will retire in October 2018. This book is designed to prepare you for the new exam, CAS-003, but can also be used to prepare for the CAS-002 exam. This certification is considered a mastery- or advanced-level certification.

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

Sponsoring Bodies

CompTIA is an American National Standards Institute (ANSI)-accredited certifier that creates and maintains a wide array of IT certification exams, such as A+, Network+, Server+, and Security+. The credentials obtained by passing these various exams are recognized in the industry as demonstrating the skills tested in these exams.
Other Security Exams

The CASP exam is one of several security-related exams that can validate a candidate’s skills and knowledge. The following are some of the most popular ones, to put the CASP exam in proper perspective:

- **Certified Information Systems Security Professional (CISSP); ISC²**: This is a globally recognized standard of achievement that confirms an individual’s knowledge in the field of information security. CISSPs are information assurance professionals who define the architecture, design, management, and/or controls that assure the security of business environments. It was the first certification in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024.

- **Security+ (CompTIA)**: This exam covers the most important foundational principles for securing a network and managing risk. Access control, identity management, and cryptography are important topics on the exam, along with a selection of appropriate mitigation and deterrent techniques to address network attacks and vulnerabilities.

- **Certified Ethical Hacker (CEH; EC Council)**: This exam validates the skills of an ethical hacker. Such individuals are usually trusted people who are employed by organizations to undertake attempts to penetrate networks and/or computer systems using the same methods and techniques as unethical hackers.

Stated Goals

CompTIA’s stated goal (verbatim from the CompTIA CASP web page) is as follows:

Successful candidates will have the knowledge required to:

- Conceptualize, engineer, integrate and implement secure solutions across complex enterprise environments

- Apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies
Introduction: The CASP Exam

- Translate business needs into security requirements
- Analyze risk impact
- Respond to security incidents

The Value of the CASP Certification

The CASP certification holds value for both the exam candidate and the enterprise. The CASP certification has been approved by the U.S. Department of Defense to meet Information Assurance (IA) technical and management certification requirements and has been chosen by Dell and HP advanced security personnel. Advantages can be gained by both the candidate and the organization employing the candidate.

To the Security Professional

There are numerous reasons a security professional would spend the time and effort required to achieve this credential. Here are some of them:

- To meet the 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

Department of Defense Directive 8140 and 8570 (DoDD 8140 and 8570)

DoDD 8140 and 8750 workforce qualification requirements both prescribe that members of the military who hold certain job roles must hold security certifications. The directive lists the CASP certification at several levels. Figure I-1 shows job roles that require various certifications, including CASP.
In short, the CASP certification demonstrates that the holder has the knowledge and skills tested in the exam and also that the candidate has hands-on experience and can organize and implement a successful security solution.

**To the Enterprise**

For the organization, the CASP certification offers a reliable benchmark to which job candidates can be measured by validating knowledge and experience. Candidates who successfully pass this rigorous exam will stand out from the rest, not only making the hiring process easier but also adding a level of confidence in the final hire.
CASP Exam Objectives

The material contained in the CASP exam objectives is divided into five domains. The following pages outline the objectives tested in each of the domains for the CAS-003 exam.

1.0 Risk Management

1.1 Summarize business and industry influences and associated security risks.

- Risk management of new products, new technologies and user behaviors
- New or changing business models/strategies
  - Partnerships
  - Outsourcing
  - Cloud
  - Acquisition/merger–divestiture/demerger
    - Data ownership
    - Data reclassification
- Security concerns of integrating diverse industries
  - Rules
  - Policies
  - Regulations
    - Export controls
    - Legal requirements
  - Geography
    - Data sovereignty
    - Jurisdictions
- Internal and external influences
  - Competitors
  - Auditors/audit findings
  - Regulatory entities
  - Internal and external client requirements
  - Top-level management
Impact of de-perimeterization (e.g., constantly changing network boundary)

- Telecommuting
- Cloud
- Mobile
- BYOD
- Outsourcing
- Ensuring third-party providers have requisite levels of information security

1.2 Compare and contrast security, privacy policies and procedures based on organizational requirements.

- Policy and process life cycle management
  - New business
  - New technologies
  - Environmental changes
  - Regulatory requirements
  - Emerging risks
- Support legal compliance and advocacy by partnering with human resources, legal, management and other entities
- Understand common business documents to support security
  - Risk assessment (RA)
  - Business impact analysis (BIA)
  - Interoperability agreement (IA)
  - Interconnection security agreement (ISA)
  - Memorandum of understanding (MOU)
  - Service-level agreement (SLA)
  - Operating-level agreement (OLA)
  - Non-disclosure agreement (NDA)
  - Business partnership agreement (BPA)
  - Master service agreement (MSA)
- Research security requirements for contracts
  - Request for proposal (RFP)
  - Request for quote (RFQ)
  - Request for information (RFI)
- Understand general privacy principles for sensitive information
- Support the development of policies containing standard security practices
  - Separation of duties
  - Job rotation
  - Mandatory vacation
  - Least privilege
  - Incident response
  - Forensic tasks
  - Employment and termination procedures
  - Continuous monitoring
  - Training and awareness for users
  - Auditing requirements and frequency
  - Information classification

1.3 Given a scenario, execute risk mitigation strategies and controls.
- Categorize data types by impact levels based on CIA
- Incorporate stakeholder input into CIA impact-level decisions
- Determine minimum-required security controls based on aggregate score
- Select and implement controls based on CIA requirements and organizational policies
- Extreme scenario planning/worst-case scenario
- Conduct system-specific risk analysis
- Make risk determination based upon known metrics
  - Magnitude of impact based on ALE and SLE
  - Likelihood of threat
- Motivation
- Source
- ARO
- Trend analysis
- Return on investment (ROI)
- Total cost of ownership
- Translate technical risks in business terms
- Recommend which strategy should be applied based on risk appetite
  - Avoid
  - Transfer
  - Mitigate
  - Accept
- Risk management processes
  - Exemptions
  - Deterrence
  - Inherent
  - Residual
- Continuous improvement/monitoring
- Business continuity planning
  - RTO
  - RPO
  - MTTR
  - MTBF
- IT governance
  - Adherence to risk management frameworks
- Enterprise resilience
1.4 Analyze risk metric scenarios to secure the enterprise.

- Review effectiveness of existing security controls
  - Gap analysis
  - Lessons learned
  - After-action reports
- Reverse engineer/deconstruct existing solutions
- Creation, collection and analysis of metrics
  - KPIs
  - KRIs
- Prototype and test multiple solutions
- Create benchmarks and compare to baselines
- Analyze and interpret trend data to anticipate cyber defense needs
- Analyze security solution metrics and attributes to ensure they meet business needs
  - Performance
  - Latency
  - Scalability
  - Capability
  - Usability
  - Maintainability
  - Availability
  - Recoverability
  - ROI
  - TCO
- Use judgment to solve problems where the most secure solution is not feasible
2.0 Enterprise Security Architecture

2.1 Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

- Physical and virtual network and security devices
  - UTM
  - IDS/IPS
  - NIDS/NIPS
  - INE
  - NAC
  - SIEM
  - Switch
  - Firewall
  - Wireless controller
  - Router
  - Proxy
  - Load balancer
  - HSM
  - MicroSD HSM
- Application and protocol-aware technologies
  - WAF
  - Firewall
  - Passive vulnerability scanners
  - DAM
- Advanced network design (wired/wireless)
  - Remote access
    - VPN
      - IPSec
      - SSL/TLS
- SSH
- RDP
- VNC
- VDI
- Reverse proxy
- IPv4 and IPv6 transitional technologies
- Network authentication methods
- 802.1x
- Mesh networks
- Placement of fixed/mobile devices
- Placement of hardware and applications
- Complex network security solutions for data flow
  - DLP
  - Deep packet inspection
  - Data flow enforcement
  - Network flow (S/flow)
  - Data flow diagram
- Secure configuration and baselining of networking and security components
- Software-defined networking
- Network management and monitoring tools
  - Alert definitions and rule writing
  - Tuning alert thresholds
  - Alert fatigue
- Advanced configuration of routers, switches and other network devices
  - Transport security
  - Trunking security
  - Port security
  - Route protection
DDoS protection
- Remotely triggered black hole
- Security zones
  - DMZ
  - Separation of critical assets
  - Network segmentation
- Network access control
  - Quarantine/remediation
  - Persistent/volatile or non-persistent agent
  - Agent vs. agentless
- Network-enabled devices
  - System on a chip (SoC)
  - Building/home automation systems
  - IP video
  - HVAC controllers
  - Sensors
  - Physical access control systems
  - A/V systems
  - Scientific/industrial equipment
- Critical infrastructure
  - Supervisory control and data acquisition (SCADA)
  - Industrial control systems (ICS)

2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements.

- Trusted OS (e.g., how and when to use it)
  - SELinux
  - SEAndroid
  - TrustedSolaris
  - Least functionality
- Endpoint security software
  - Anti-malware
  - Antivirus
  - Anti-spyware
  - Spam filters
  - Patch management
  - HIPS/HIDS
  - Data loss prevention
  - Host-based firewalls
  - Log monitoring
  - Endpoint detection response

- Host hardening
  - Standard operating environment/configuration baselining
    - Application whitelisting and blacklisting
  - Security/group policy implementation
  - Command shell restrictions
  - Patch management
    - Manual
    - Automated
      - Scripting and replication
  - Configuring dedicated interfaces
    - Out-of-band management
    - ACLs
    - Management interface
    - Data interface
- External I/O restrictions
  - USB
  - Wireless
    - Bluetooth
    - NFC
    - IrDA
  - RF
    - 802.11
    - RFID
  - Drive mounting
  - Drive mapping
  - Webcam
  - Recording mic
  - Audio output
  - SD port
  - HDMI port
- File and disk encryption
- Firmware updates
- Boot loader protections
  - Secure boot
  - Measured launch
  - Integrity measurement architecture
  - BIOS/UEFI
  - Attestation services
  - TPM
- Vulnerabilities associated with hardware
- Terminal services/application delivery services
2.3 Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.

- Enterprise mobility management
  - Containerization
  - Configuration profiles and payloads
  - Personally owned, corporate-enabled
  - Application wrapping
- Remote assistance access
  - VNC
  - Screen mirroring
- Application, content and data management
- Over-the-air updates (software/firmware)
- Remote wiping
- SCEP
- BYOD
- COPE
- VPN
- Application permissions
- Side loading
- Unsigned apps/system apps
- Context-aware management
  - Geolocation/geofencing
  - User behavior
  - Security restrictions
  - Time-based restrictions
- Security implications/privacy concerns
  - Data storage
    - Non-removable storage
    - Removable storage
- Cloud storage
- Transfer/backup data to uncontrolled storage
- USB OTG
- Device loss/theft
- Hardware anti-tamper
  - eFuse
- TPM
- Rooting/jailbreaking
- Push notification services
- Geotagging
- Encrypted instant messaging apps
- Tokenization
- OEM/carrier Android fragmentation
- Mobile payment
  - NFC-enabled
  - Inductance-enabled
  - Mobile wallet
  - Peripheral-enabled payments (credit card reader)
- Tethering
  - USB
  - Spectrum management
  - Bluetooth 3.0 vs. 4.1
- Authentication
  - Swipe pattern
  - Gesture
  - Pin code
  - Biometric
    - Facial
    - Fingerprint
    - Iris scan
Introduction: The CASP Exam

- Malware
- Unauthorized domain bridging
- Baseband radio/SOC
- Augmented reality
- SMS/MMS/messaging

- Wearable technology
  - Devices
    - Cameras
    - Watches
    - Fitness devices
    - Glasses
    - Medical sensors/devices
    - Headsets

- Security implications
  - Unauthorized remote activation/deactivation of devices or features
  - Encrypted and unencrypted communication concerns
  - Physical reconnaissance
  - Personal data theft
  - Health privacy
  - Digital forensics of collected data

2.4 Given software vulnerability scenarios, select appropriate security controls.

- Application security design considerations
  - Secure: by design, by default, by deployment

- Specific application issues
  - Unsecure direct object references
  - XSS
  - Cross-site request forgery (CSRF)
  - Click-jacking
- Session management
- Input validation
- SQL injection
- Improper error and exception handling
- Privilege escalation
- Improper storage of sensitive data
- Fuzzing/fault injection
- Secure cookie storage and transmission
- Buffer overflow
- Memory leaks
- Integer overflows
- Race conditions
  - Time of check
  - Time of use
- Resource exhaustion
- Geotagging
- Data remnants
- Use of third-party libraries
- Code reuse
- Application sandboxing
- Secure encrypted enclaves
- Database activity monitor
- Web application firewalls
- Client-side processing vs. server-side processing
  - JSON/REST
  - Browser extensions
    - ActiveX
    - Java applets
■ HTML5
■ AJAX
■ SOAP
■ State management
■ JavaScript
■ Operating system vulnerabilities
■ Firmware vulnerabilities

3.0 Enterprise Security Operations

3.1 Given a scenario, conduct a security assessment using the appropriate methods.

■ Methods
■ Malware sandboxing
■ Memory dumping, runtime debugging
■ Reconnaissance
■ Fingerprinting
■ Code review
■ Social engineering
■ Pivoting
■ Open source intelligence
■ Social media
■ Whois
■ Routing tables
■ DNS records
■ Search engines
- Types
  - Penetration testing
    - Black box
    - White box
    - Gray box
  - Vulnerability assessment
  - Self-assessment
    - Tabletop exercises
  - Internal and external audits
  - Color team exercises
    - Red team
    - Blue team
    - White team

3.2 Analyze a scenario or output, and select the appropriate tool for a security assessment.

- Network tool types
  - Port scanners
  - Vulnerability scanners
  - Protocol analyzer
    - Wired
    - Wireless
  - SCAP scanner
  - Network enumerator
  - Fuzzer
  - HTTP interceptor
  - Exploitation tools/frameworks
  - Visualization tools
  - Log reduction and analysis tools
● Host tool types
  ● Password cracker
  ● Vulnerability scanner
  ● Command line tools
  ● Local exploitation tools/frameworks
  ● SCAP tool
  ● File integrity monitoring
  ● Log analysis tools
  ● Antivirus
  ● Reverse engineering tools
● Physical security tools
  ● Lock picks
  ● RFID tools
  ● IR camera

3.3 Given a scenario, implement incident response and recovery procedures.

● E-discovery
  ● Electronic inventory and asset control
  ● Data retention policies
  ● Data recovery and storage
  ● Data ownership
  ● Data handling
  ● Legal holds

● Data breach
  ● Detection and collection
    ● Data analytics
  ● Mitigation
    ● Minimize
    ● Isolate
- Recovery/reconstitution
- Response
- Disclosure

- Facilitate incident detection and response
  - Hunt teaming
  - Heuristics/behavioral analytics
  - Establish and review system, audit and security logs

- Incident and emergency response
  - Chain of custody
  - Forensic analysis of compromised system
  - Continuity of operations
  - Disaster recovery
  - Incident response team
  - Order of volatility

- Incident response support tools
  - dd
  - tcpdump
  - nbtstat
  - netstat
  - nc (Netcat)
  - memcopy
  - tshark
  - foremost

- Severity of incident or breach
  - Scope
  - Impact
  - Cost
  - Downtime
  - Legal ramifications
Post-incident response

Root-cause analysis

Lessons learned

After-action report

4.0 Technical Integration of Enterprise Security

4.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

Adapt data flow security to meet changing business needs

Standards

Open standards

Adherence to standards

Competing standards

Lack of standards

De facto standards

Interoperability issues

Legacy systems and software/current systems

Application requirements

Software types

In-house developed

Commercial

Tailored commercial

Open source

Standard data formats

Protocols and APIs

Resilience issues

Use of heterogeneous components

Course of action automation/orchestration

Distribution of critical assets
 Persistence and non-persistence of data
 Redundancy/high availability
 Assumed likelihood of attack
 Data security considerations
 Data remnants
 Data aggregation
 Data isolation
 Data ownership
 Data sovereignty
 Data volume
 Resources provisioning and deprovisioning
 Users
 Servers
 Virtual devices
 Applications
 Data remnants
 Design considerations during mergers, acquisitions and demergers/divestitures
 Network secure segmentation and delegation
 Logical deployment diagram and corresponding physical deployment diagram of all relevant devices
 Security and privacy considerations of storage integration
 Security implications of integrating enterprise applications
 CRM
 ERP
 CMDB
 CMS
 Integration enablers
 Directory services
 DNS
4.2 Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.

- Technical deployment models (outsourcing/insourcing/managed services/partnership)
- Cloud and virtualization considerations and hosting options
  - Public
  - Private
  - Hybrid
  - Community
  - Multitenancy
  - Single tenancy
- On-premise vs. hosted
- Cloud service models
  - SaaS
  - IaaS
  - PaaS
- Security advantages and disadvantages of virtualization
  - Type 1 vs. Type 2 hypervisors
  - Container-based
  - vTPM
  - Hyperconverged infrastructure
  - Virtual desktop infrastructure
  - Secure enclaves and volumes
- Cloud augmented security services
  - Anti-malware
  - Vulnerability scanning
  - Sandboxing
- Content filtering
- Cloud security broker
- Security as a service
- Managed security service providers
- Vulnerabilities associated with comingling of hosts with different security requirements
  - VMEscape
  - Privilege elevation
  - Live VM migration
  - Data remnants
- Data security considerations
  - Vulnerabilities associated with a single server hosting multiple data types
  - Vulnerabilities associated with a single platform hosting multiple data types/owners on multiple virtual machines
- Resources provisioning and deprovisioning
  - Virtual devices
  - Data remnants

4.3 Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

- Authentication
  - Certificate-based authentication
  - Single sign-on
  - 802.1x
  - Context-aware authentication
  - Push-based authentication

- Authorization
  - OAuth
  - XACML
  - SPML
Introduction: The CASP Exam

- Attestation
- Identity proofing
- Identity propagation
- Federation
  - SAML
  - OpenID
  - Shibboleth
  - WAYF
- Trust models
  - RADIUS configurations
- LDAP
- AD

4.4 Given a scenario, implement cryptographic techniques.

- Techniques
  - Key stretching
  - Hashing
  - Digital signature
  - Message authentication
  - Code signing
  - Pseudo-random number generation
  - Perfect forward secrecy
  - Data-in-transit encryption
  - Data-in-memory/processing
  - Data-at-rest encryption
    - Disk
    - Block
    - File
    - Record
  - Steganography
- Implementations
  - Crypto modules
  - Crypto processors
  - Cryptographic service providers
  - DRM
  - Watermarking
  - GPG
  - SSL/TLS
  - SSH
  - S/MIME
- Cryptographic applications and proper/improper implementations
  - Strength
  - Performance
  - Feasibility to implement
  - Interoperability
- Stream vs. block
- PKI
  - Wild card
  - OCSP vs. CRL
  - Issuance to entities
  - Key escrow
  - Certificate
  - Tokens
  - Stapling
  - Pinning
- Cryptocurrency/blockchain
- Mobile device encryption considerations
- Elliptic curve cryptography
  - P256 vs. P384 vs. P512
4.5 Given a scenario, select the appropriate control to secure communications and collaboration solutions.

- Remote access
  - Resource and services
  - Desktop and application sharing
  - Remote assistance
- Unified collaboration tools
  - Conferencing
    - Web
    - Video
    - Audio
  - Storage and document collaboration tools
  - Unified communication
  - Instant messaging
  - Presence
  - Email
  - Telephony and VoIP integration
- Collaboration sites
  - Social media
  - Cloud-based

5.0 Research, Development and Collaboration

5.1 Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

- Perform ongoing research
- Best practices
- New technologies, security systems and services
- Technology evolution (e.g., RFCs, ISO)
■ Threat intelligence
  ■ Latest attacks
  ■ Knowledge of current vulnerabilities and threats
  ■ Zero-day mitigation controls and remediation
  ■ Threat model
■ Research security implications of emerging business tools
  ■ Evolving social media platforms
  ■ Integration within the business
  ■ Big Data
  ■ AI/machine learning
■ Global IA industry/community
  ■ Computer emergency response team (CERT)
  ■ Conventions/conferences
  ■ Research consultants/vendors
  ■ Threat actor activities
  ■ Emerging threat sources

5.2 Given a scenario, implement security activities across the technology life cycle.

■ Systems development life cycle
  ■ Requirements
  ■ Acquisition
  ■ Test and evaluation
  ■ Commissioning/decommissioning
■ Operational activities
  ■ Monitoring
  ■ Maintenance
  ■ Configuration and change management
■ Asset disposal
■ Asset/object reuse
Software development life cycle
  ■ Application security frameworks
■ Software assurance
  ■ Standard libraries
  ■ Industry-accepted approaches
  ■ Web services security (WS-security)
  ■ Forbidden coding techniques
  ■ NX/XN bit use
  ■ ASLR use
■ Code quality
  ■ Code analyzers
  ■ Fuzzer
  ■ Static
  ■ Dynamic
■ Development approaches
  ■ DevOps
  ■ Security implications of agile, waterfall and spiral software development methodologies
  ■ Continuous integration
  ■ Versioning
■ Secure coding standards
■ Documentation
  ■ Security requirements traceability matrix (SRTM)
  ■ Requirements definition
  ■ System design document
  ■ Testing plans
■ Validation and acceptance testing
  ■ Regression
  ■ User acceptance testing
Unit testing
Integration testing
Peer review

Adapt solutions to address:
Emerging threats
Disruptive technologies
Security trends
Asset management (inventory control)

5.3 Explain the importance of interaction across diverse business units to achieve security goals.

- Interpreting security requirements and goals to communicate with stakeholders from other disciplines
  - Sales staff
  - Programmer
  - Database administrator
  - Network administrator
  - Management/executive management
  - Financial
  - Human resources
  - Emergency response team
  - Facilities manager
  - Physical security manager
  - Legal counsel
- Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls
- Establish effective collaboration within teams to implement secure solutions
- Governance, risk and compliance committee
Steps to Becoming a CASP

To become a CASP, there are certain prerequisite procedures to follow. The following sections cover those topics.

Qualifying for the Exam

While there is no required prerequisite, the CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus at the enterprise level.

Signing Up for the Exam

A CompTIA Advanced Security Practitioner (CASP) voucher costs $390.

About the Exam

The following are the characteristics of the exam:

- **Launches**: April 2, 2018
- **Number of questions**: 90 (maximum)
- **Type of questions**: Multiple choice and performance based
- **Length of test**: 165 minutes
- **Passing score**: Pass/fail only; no scaled score
- **Recommended experience**: 10 years’ experience in IT administration, including at least 5 years of hands-on technical security experience
- **Languages**: English

CompTIA Authorized Materials Use Policy

CompTIA has recently started a more proactive movement toward preventing test candidates from using brain dumps in their pursuit of certifications. CompTIA currently implements the CompTIA Authorized Quality Curriculum (CAQC) program, whereby content providers like Pearson can submit their test preparation materials to an authorized third party for audit. The CAQC checks to ensure that adequate topic coverage is provided by the content. Only authorized partners can submit their material to the third party.
In the current CAS-003 Blueprint, CompTIA includes a section titled “CompTIA Authorized Materials Use Policy” that says:

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

Remember: Just because you purchase a product does not mean that the product is legitimate. Some of the best brain dump companies out there charge for their products. Also, keep in mind that using materials from a brain dump can result in certification revocation. Please make sure that all products you use are from a legitimate provider rather than a brain dump company. Using a brain dump is cheating and directly violates the non-disclosure agreement (NDA) you sign at exam time.
This page intentionally left blank
This chapter covers the following topics:

- **Policy and Process Life Cycle Management**: This section discusses the effects that new business, new technologies, environmental changes, and regulatory requirements have on policy and process life cycle management.

- **Support Legal Compliance and Advocacy**: This section covers partnering with human resources, legal, management, and other entities to support legal compliance.

- **Common Business Documents to Support Security**: The documents discussed in this section include risk assessments/statements of applicability, business impact analyses, interoperability agreements, interconnection security agreements, memorandums of understanding, service-level agreements, operating-level agreements, non-disclosure agreements, business partnership agreements, and master service agreements.

- **Security Requirements for Contracts**: Topics include requests for proposal, requests for quote, requests for information, and agreements.

- **General Privacy Principles for Sensitive Information**: This section explains personally identifiable information and details the privacy principles that are important for protecting PII.

- **Policies Containing Standard Security Practices**: The components discussed include separation of duties, job rotation, mandatory vacation, the principle of least privilege, incident response, forensic tasks, employment and termination procedures, continuous monitoring, training and awareness for users, auditing requirements and frequency, and information classification.

This chapter covers CAS-003 objective 1.2.
CHAPTER 2

Security, Privacy Policies, and Procedures

IT governance documents should be implemented to ensure that organizational assets are protected as well as possible. This chapter explains how the process and policy life cycles are managed and how to support legal compliance. It also discusses business documents and contracts that are commonly used to support security. It covers general privacy principles. Finally, it discusses the development of policies containing standard security practices.

Policy and Process Life Cycle Management

In a top-down approach, management initiates, supports, and directs the security program. In a bottom-up approach, staff members develop a security program prior to receiving direction and support from management. A top-down approach is much more efficient than a bottom-up approach because management’s support is one of the most important components of a security program. Using the top-down approach can help ensure that an organization’s policies align with its strategic goals.

In the context of organizational security, a **policy** is a course or principle of action adopted by an organization, and a **process** is a series of actions taken to achieve a particular end. A **procedure** is a series of actions conducted in a certain order or manner. Policies, procedures, and processes determine all major decisions and actions within an organization, and all organizational tasks operate within the boundaries set by policies, procedures, and processes.

To understand the relationship between the three, policies are written first to guide the creation of procedures and processes. Processes then provide a high-level view of tasks within the processes. Procedures are the detailed steps involved to complete the process.

Let’s look at an example. Say that an organization adopts a particular policy for processing accounts payable. The process designed around this policy details the high-level tasks that must occur, which may include receiving the bill, inputting the bill, authorizing the payment, printing the check, signing the check, and mailing the check. The procedures written would include each separate step involved in each task in the process.
Policies should be written based on the following life cycle:

**Step 1.** Develop the policy.

**Step 2.** Perform quality control.

**Step 3.** Obtain approval of the policy.

**Step 4.** Publish the policy.

**Step 5.** Periodically review the policy.

**Step 6.** Archive the policy when no longer needed or applicable.

During this life cycle, the quality control should be performed prior to obtaining approval to ensure that the policy complies with laws, regulations, and standards. When the policy is published, the organization must ensure that the affected personnel are properly educated on the new policy. The new policy should be incorporated into any training received by these personnel. Each policy should at minimum be reviewed annually. If policies must be changed, version control should be implemented to ensure that the most current version of a policy is being used across the enterprise. When a policy is outdated, it should be archived.

Policies should be reviewed often and on a regular schedule. Certain business, technology, risk, and environment changes should always trigger a review of policies, including adoption of a new technology, merger with another organization, and identification of a new attack method.

For example, suppose that employees request remote access to corporate email and shared drives. If remote access has never been offered but the need to improve productivity and rapidly respond to customer demands means staff now require remote access, the organization should analyze the need to determine whether it is valid. Then, if the organization decides to allow remote access, the organization’s security professionals should plan and develop security policies based on the assumption that external environments have active hostile threats.

Policies that should be considered include password policies, data classification policies, wireless and VPN policies, remote access policies, and device access policies. Most organizations develop password and data classification policies first.

A process is a collection of related activities that produce a specific service or product (that is, serve a particular goal) for the organization. Change management and risk management are examples of processes.

Once a policy is written, the appropriate processes should be written based on the following life cycle:

**Step 1.** Analyze

**Step 2.** Design
Step 3. Implement
Step 4. Monitor
Step 5. Retire

During this life cycle, step 1 is the time to analyze the policy, and step 2 is the time to design the process based on the policy. When the new process is implemented, all personnel involved in the process should be informed of how the process works. The process should be monitored regularly and may be modified as issues arise or as the base policy has been updated. Keep in mind that processes are created based on the policy. If a new policy is adopted, then a new process is needed. If a policy is edited or archived, then the process for the policy should also be edited or retired.

Once the policy and associated processes are documented, procedures must be written. Procedures embody all the detailed actions that personnel are required to follow and are the closest to the computers and other devices. Procedures often include step-by-step lists on how policies and processes are implemented.

Once an organization has analyzed the business, technology, risk, and environment changes to develop and update policies, the organization must take the next step: Develop and update its processes and procedures in light of the new or updated policies and environment and business changes. Procedures might have to be changed, for example, if the organization upgrades to the latest version of the backup software it uses. Most software upgrades involve analyzing the current procedures and determining how they should be changed. As another example, say that management decides to use more outside contractors to complete work. The organization may need to add a new process within the organization for reviewing the quality of the outside contractor’s work. As a final example, suppose that an organization decides to purchase several Linux servers to replace the current Microsoft file servers. While the high-level policies will remain the same, the procedures for meeting those high-level policies will have to be changed.

If an organization’s marketing department needs to provide more real-time interaction with its partners and consumers and decides to move forward with a presence on multiple social networking sites for sharing information, the organization would need to establish a specific set of trained people who can release information on the organization’s behalf and provide other personnel with procedures and processes for sharing the information.

Some of the processes and procedures that should be considered include the change management process, the configuration management process, network access procedures, wireless access procedures, and database administration procedures. But remember that procedures and processes should be created or changed only after
the appropriate policies are adopted. The policies will guide the development of the processes and procedures.

Internal organizational drivers are the basis on which policies and processes are developed. Organizations should ensure that policies and processes are designed or reviewed when new business or business changes occur, new technologies are launched, environmental changes occur, or regulatory requirements change.

**New Business**

New business occurs when an organization launches or purchases a new area of business. Business changes are changes dictated by the nature of an organization’s business and are often driven by consumer demands. As a change occurs, an organization must ensure that it understands the change and its implication for the security posture of the organization. Organizations should take a proactive stance when it comes to these changes. Don’t wait for problems. Anticipate the changes and deploy mitigation techniques to help prevent them!

Suppose a business decides to launch a new endeavor whereby consumers can now directly purchase the products that were previously only sold to large retail stores. A new business policy will need to be written based on this new model, and a new process will need to be designed to handle the new business.

Security professionals are integral to any projects wherein new business is starting or business changes are occurring because the security professionals ensure that security controls are considered. Security professionals should ensure that all risks associated with the new business or business change are documented, analyzed, and reported to management. They must also document any suggested security controls that will mitigate these risks.

**New Technologies**

Technology changes are driven by new technological developments that force organizations to adopt new technologies. Again, organizations must ensure that they understand the changes and their implications for the security posture of the organization.

Suppose a business decides to allow personnel to implement a bring your own device (BYOD) policy. Security professionals should work to ensure that the policy defines the parameters wherein BYOD will be allowed or denied. In addition, the process would need to be written and would likely include obtaining formal approval of a device, assessing the security posture of the device, and granting the device full or limited access based on the device’s security posture.
Security professionals are integral to the inclusion or usage of any new technologies because they ensure that security controls will be considered. Security professionals should ensure that all risks associated with new technology are documented, analyzed, and reported to management. They must also suggest and document security controls to mitigate these risks.

**Environmental Changes**

Environmental changes are divided into two categories: those motivated by the culture in an organization and those motivated by the environment of the industry. As with new business or technologies, organizations must ensure that they understand the changes and their implications for the security posture of the organization.

Suppose a business decides to implement a new policy that provides a certain amount of “green space” for each of its facilities. Management would need to develop a process whereby these green spaces could be completed and maintained. It would likely include purchasing the land, designing the plan for the land, implementing the new green space, and maintaining the green space.

**Regulatory Requirements**

Regulatory requirements are any requirements that must be documented and followed based on laws and regulations. Standards can also be used as part of the regulatory environment but are not strictly enforced as laws and regulations. As with new business or technologies or environmental changes, organizations must ensure that they understand the regulations and their implications to the security posture of the organization.

The International Organization for Standardization (ISO) has developed a series of standards that are meant to aid organizations in the development of security policies. Other regulatory bodies include local, state, federal, and other government bodies.

Let’s look at an example. Suppose an organization is rewriting its security policies and has halted the rewriting progress because the executives believe that the organization’s major vendors have a good handle on compliance and regulatory standards. The executive-level managers are allowing vendors to play a large role in writing the organization’s policy. However, the IT director decides that while vendor support is important, it is critical that the company write the policy objectively because vendors may not always put the organization’s interests first. The IT director should make the following recommendations to senior staff:

- Consult legal and regulatory requirements.
- Draft a general organizational policy.
- Specify functional implementation policies.
- Establish necessary standards, procedures, baselines, and guidelines.

As you can see from this example, you don’t have to memorize the specific standards. However, you need to understand how organizations apply them, how they are revised, and how they can be customized to fit organizational needs.

**Emerging Risks**

Emerging risks are any risks that have emerged due to the recent security landscape. Often risks are not identified for new technologies, devices, and applications until after one of them has been deployed. Organizations should write policies and procedures to ensure that security professionals are doing the proper research to understand emerging risks. Emerging risks is an area that can be particularly dependent upon patch management. Often vendors will try to quickly release security fixes for any emerging risks.

Suppose an organization decides to deploy a new Internet of Things (IoT) device. Several weeks into the deployment, the vendor announces a security flaw that allows attackers to take over the device functionality. As a result, they release a security patch that addresses this issue. If the appropriate policies are in place, the organization’s security professionals should be monitoring the vendor for announcements regarding patch management and should deploy the patch once it can be properly tested.

**Support Legal Compliance and Advocacy**

An organization should involve its human resources department, legal department or legal counsel, senior management, and other internal and external entities in its legal compliance and advocacy program. Legal compliance ensures that an organization follows relevant laws, regulations, and business rules. Legal advocacy is the process carried out by or for an organization that aims to influence public policy and resource allocation decisions in political, economic, and social systems and institutions.

Human resources involvement ensures that the organization is addressing all employment laws and regulations to protect its employees. Human resources professionals can help guide an organization’s security policies to ensure that individual rights are upheld while at the same time protecting organizational assets and liability. For example, an organization should ensure that a screen is displayed at login that informs users of the employer’s rights to monitor, seize, and search organizational devices to reduce the likelihood of related legal issues. Then, if a technician...
must take an employee’s workstation into custody in response to an investigation, the organization is protected. Both the HR and legal departments should be involved in creating the statement that will be displayed to ensure that it includes all appropriate information.

**NOTE** Applicable laws are covered in Chapter 1, “Business and Industry Influences and Associated Security Risks.” To learn about specific laws that could affect an organization, refer to the section “Legal Requirements.”

### Common Business Documents to Support Security

Security professionals need to use many common business documents to support the implementation and management of organizational security. Understanding these business documents helps ensure that all areas of security risk are addressed and the appropriate policies, procedures, and processes are developed.

### Risk Assessment (RA)

A risk assessment (RA) is a tool used in risk management to identify vulnerabilities and threats, assess the impacts of those vulnerabilities and threats, and determine which controls to implement. Risk assessment or analysis has four main steps:

- **Step 1.** Identify assets and asset value.
- **Step 2.** Identify vulnerabilities and threats.
- **Step 3.** Calculate threat probability and business impact.
- **Step 4.** Balance threat impact with countermeasure cost.

Prior to starting a risk assessment, management and the risk assessment team must determine which assets and threats to consider. This process involves determining the size of the project. The risk assessment team must then provide a report to management on the value of the assets considered. Next, management reviews and finalizes the asset list, adding and removing assets as it sees fit, and then determines the budget for the risk assessment project.

If a risk assessment is not supported and directed by senior management, it will not be successful. Management must define the purpose and scope of a risk assessment and allocate personnel, time, and monetary resources for the project.
NOTE  To learn more about risk assessment, refer to Chapter 3, “Risk Mitigation Strategies and Controls.”

The statement of applicability (SOA) identifies the controls chosen by an organization and explains how and why the controls are appropriate. The SOA is derived from the output of the risk assessment. If ISO 27001 compliance is important for an organization, its SOA must directly relate the selected controls to the original risks they are intended to mitigate.

The SOA should make reference to the policies, procedures, or other documentation or systems through which the selected control will actually manifest. It is also good practice to document why controls not selected were excluded.

**Business Impact Analysis (BIA)**

A business impact analysis (BIA) is a functional analysis that occurs as part of business continuity and disaster recovery. Performing a thorough BIA will help business units understand the impact of a disaster. The resulting document that is produced from a BIA lists the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization.

**Interoperability Agreement (IA)**

An interoperability agreement (IA) is an agreement between two or more organizations to work together to allow information exchange. The most common implementation of these agreements occurs between sister companies that are owned by the same large corporation. While the companies may be structured and managed differently, they may share systems, telecommunications, software, and data to allow consolidation and better utilization of resources. IAs are considered binding agreements.

Do not confuse an interoperability agreement with a reciprocal agreement. Whereas an IA covers normal operations, a reciprocal agreement is an agreement between two organizations that have similar technological needs and infrastructures. In a reciprocal agreement, each organization agrees to act as an alternate location for the other if the primary facilities of either of the organizations are rendered unusable. Unfortunately, in most cases, these agreements cannot be legally enforced.

**Interconnection Security Agreement (ISA)**

An interconnection security agreement (ISA) is an agreement between two organizations that own and operate connected IT systems to document the technical
requirements of the interconnection. In most cases, the security control needs of each organization are spelled out in detail in the agreement to ensure that there is no misunderstanding. The ISA also supports a memorandum of understanding (described next) between the organizations.

For example, if an organization has completed the connection of its network to a national high-speed network, and local businesses in the area are seeking sponsorship with the organization to connect to the high-speed network by directly connecting through the organization’s network, using an ISA would be the best way to document the technical requirements of the connection.

**Memorandum of Understanding (MOU)**

A memorandum of understanding (MOU) is an agreement between two or more organizations that details a common line of action. MOUs are often used in cases where parties either do not have a legal commitment or in situations where the parties cannot create a legally enforceable agreement. In some cases, it is referred to as a letter of intent.

**Service-Level Agreement (SLA)**

A service-level agreement (SLA) is an agreement about the ability of the support system to respond to problems within a certain time frame while providing an agreed level of service. SLAs can be internal between departments or external with a service provider. Agreeing on the quickness with which various problems are addressed introduces some predictability to the response to problems, which ultimately supports the maintenance of access to resources. Most service contracts are accompanied by an SLA, which may include security priorities, responsibilities, guarantees, and warranties.

For example, an SLA is the best choice when a new third-party vendor, such as a cloud computing provider, has been selected to maintain and manage an organization’s systems. An SLA is also a good choice when an organization needs to provide 24-hour support for certain internal services and decides to use a third-party provider for shifts for which the organization does not have internal personnel on duty.

**Operating-Level Agreement (OLA)**

An operating-level agreement (OLA) is an internal organizational document that details the relationships that exist between departments to support business activities. OLAs are often used with SLAs. A good example of an OLA is an agreement between the IT department and the accounting department in which the IT department agrees to be responsible for the backup services of the accounting server, while
the day-to-day operations of the accounting server are maintained by accounting personnel.

**Non-Disclosure Agreement (NDA)**

A non-disclosure agreement (NDA) is an agreement between two parties that defines what information is considered confidential and cannot be shared outside the two parties. An organization may implement NDAs with personnel regarding the intellectual property of the organization. NDAs can also be used when two organizations work together to develop a new product. Because certain information must be shared to make the partnership successful, NDAs are signed to ensure that each partner’s data is protected.

While an NDA cannot ensure that confidential data is not shared, it usually provides details on the repercussions for the offending party, including but not limited to fines, jail time, and forfeiture of rights. For example, an organization should decide to implement an NDA when it wants to legally ensure that no sensitive information is compromised through a project with a third party or in a cloud-computing environment.

An example of an NDA in use is the one you sign when you take the CompTIA Advanced Security Practitioner exam. You must digitally sign an NDA that clearly states that you are not allowed to share any details regarding the contents of the exam except that which is expressly given in the CompTIA blueprint available on its website. Failure to comply with this NDA can result in forfeiture of your CompTIA credential and being banned from taking future CompTIA certification exams.

**Business Partnership Agreement (BPA)**

A business partnership agreement (BPA) is an agreement between two business partners that establishes the conditions of the partner relationship. A BPA usually includes the responsibilities of each partner, profit/loss sharing details, resource sharing details, and data sharing details.

For example, if an organization has entered into a marketing agreement with a marketing firm whereby the organization will share some of its customer information with the marketing firm, the terms should be spelled out in a BPA. The BPA should state any boundaries for the contract, such as allowing the marketing firm to only contact customers of the organization who explicitly agreed to being contacted by third parties.

BPAs should include any organizational policies that might affect the partner and its personnel. If your organization has a security policy regarding USB flash drives, any BPAs with partners that may have personnel working onsite should include the details of the USB flash drive security policy.
Master Service Agreement (MSA)

A master service agreement (MSA) is a contract between two parties in which both parties agree to most of the terms that will govern future transactions or future agreements. This agreement is ideal if an organization will have a long-term relationship with a vendor or provider. An MSA provides risk allocation strategy that outlines the risk and responsibility of contractors and employees included in the agreement for each contract’s duration. It also provides indemnification that allows one party to hold harmless or safeguard another party against existing or future losses. The indemnifying party agrees to pay for damages it has caused or may cause in the future, regardless of which party is at fault; these damages include legal fees and costs associated with litigation.

An MSA usually includes a statement of work (SOW), which outlines the specific work to be executed by the vendor for the client. It includes the work activities, the deliverables, and the timeline for work to be accomplished.

Security Requirements for Contracts

Contracts with third parties are a normal part of business. Because security has become such a concern for most organizations and government entities, contracts now include sections that explicitly detail the security requirements for the vendor. Organizations should consult with legal counsel to ensure that the contracts they execute include the appropriate security requirements to satisfy not only the organizations’ needs but also any government regulations and laws.

An organization may want to consider including provisions such as the following as part of any contracts:

- Required policies, practices, and procedures related to handling organizational data
- Training or certification requirements for any third-party personnel
- Background investigation or security clearance requirements for any third-party personnel
- Required security reviews of third-party devices
- Physical security requirements for any third-party personnel
- Laws and regulations that will affect the contract

Security professionals should research security requirements for contracts, including RFPs, RFQs, RFI, and other agreements.
**Request for Proposal (RFP)**

An RFP is a bidding-process document issued by an organization that gives details of a commodity, a service, or an asset that the organization wants to purchase. Potential suppliers use the RFP as a guideline for submitting a formal proposal.

Suppose that two members of senior management can better understand what each vendor does and what solutions they can provide after three vendors submit their requested documentation. But now the managers want to see the intricacies of how these solutions can adequately match the requirements needed by the firm. The managers should submit an RFP to the three submitting firms to obtain this information.

**Request for Quote (RFQ)**

An RFQ (sometimes called an invitation for bid [IFB]) is a bidding-process document that invites suppliers to bid on specific products or services. RFQs often include item or service specifications. An RFQ is suitable for sourcing products that are standardized or produced in repetitive quantities, such as desktop computers, RAM modules, or other devices.

Suppose that a security administrator of a small private firm is researching and putting together a proposal to purchase an intrusion prevention system (IPS). A specific brand and model has been selected, but the security administrator needs to gather cost information for that product. The security administrator should prepare an RFQ to perform a cost analysis report. The RFQ would include information such as payment terms.

**Request for Information (RFI)**

An RFI is a bidding-process document that collects written information about the capabilities of various suppliers. An RFI may be used prior to an RFP or RFQ, if needed, but can also be used after these if the RFP or RFQ does not obtain enough specification information.

Suppose that a security administrator of a large private firm is researching and putting together a proposal to purchase an IPS. The specific IPS type has not been selected, and the security administrator needs to gather information from several vendors to determine a specific product. An RFI would assist in choosing a specific brand and model.

Now let’s look at an example where the RFI comes after the RFP or RFQ. Say that three members of senior management have been working together to solicit bids for a series of firewall products for a major installation in the firm’s new office. After reviewing RFQs received from three vendors, the three managers have not gained any
real data regarding the specifications about any of the solutions and want that data before the procurement continues. To get back on track in this procurement process, the managers should contact the three submitting vendor firms and have them submit supporting RFIs to provide more detailed information about their product solutions.

**Agreement or Contract**

Organizations use other types of agreements with third parties besides those already discussed. Even though many of these agreements are not as formal as RFPs, RFQs, or RFIs, it is still important for an organization to address any security requirements in an agreement to ensure that the third party is aware of the requirements. This includes any types of contracts an organization uses to perform business, including purchase orders, sales agreements, manufacturing agreements, and so on.

**General Privacy Principles for Sensitive Information**

When considering technology and its use today, privacy is a major concern of users. This privacy concern usually involves three areas: which personal information can be shared with whom, whether messages can be exchanged confidentially, and whether and how a user can send messages anonymously. Privacy is an integral part of an organization’s security measures.

As part of the security measures that organizations must take to protect privacy, personally identifiable information (PII) must be understood, identified, and protected. PII is any piece of data that can be used alone or with other information to identify a single person. Any PII that an organization collects must be protected in the strongest manner possible. PII includes full name, identification numbers (including driver’s license number and Social Security number), date of birth, place of birth, biometric data, financial account numbers (both bank account and credit card numbers), and digital identities (including social media names and tags).

Keep in mind that different countries and levels of government can have different qualifiers for identifying PII. Security professionals must ensure that they understand international, national, state, and local regulations and laws regarding PII. As the theft of this data becomes even more prevalent, you can expect more laws to be enacted that will affect your job.
Figure 2-1 lists examples of PII.

**Key Topic**

**Support the Development of Policies Containing Standard Security Practices**

Organizational policies must be implemented to support all aspects of security. Experienced security professionals should ensure that organizational security policies include separation of duties, job rotation, mandatory vacation, least privilege, incident response, forensic tasks, employment and termination procedures, continuous monitoring, training and awareness for users, and auditing requirements and frequency.

**Separation of Duties**

Separation of duties is a preventive administrative control 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 among users. This helps to deter fraud and collusion because when an organization implements adequate separation of duties, collusion between two or more personnel would be required to carry out fraud against the organization. A good example of
separation duties is authorizing one person to manage backup procedures and another to manage restore 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 functions. For example, a retail establishment might require two managers to open the safe. Split knowledge ensures that no single user has all the information needed to perform a particular task. An example of split knowledge is the military’s requiring two individuals to each enter a unique combination to authorize missile firing.

Separation of duties ensures that one person is not capable of compromising organizational security. Any activities that are identified as high risk should be divided into individual tasks, which can then be allocated to different personnel or departments.

When an organization adopts a policy which specifies that the systems administrator cannot be present during a system audit, separation of duties is the guiding principle.

Let’s look at an example of the violation of separation of duties. Say that an organization’s internal audit department investigates a possible breach of security. One of the auditors interviews three employees:

- A clerk who works in the accounts receivable office and is in charge of entering data into the finance system
- An administrative assistant who works in the accounts payable office and is in charge of approving purchase orders
- The finance department manager, who can perform the functions of both the clerk and the administrative assistant

To avoid future security breaches, the auditor should suggest that the manager should only be able to review the data and approve purchase orders.

Job Rotation

From a security perspective, job rotation refers to the detective administrative control where multiple users are trained to perform the duties of a position to help prevent fraud by any individual employee. The idea is that by making multiple people familiar with the legitimate functions of the position, the likelihood increases that unusual activities by any one person will be noticed. Job rotation is often used in conjunction with mandatory vacations. Beyond the security aspects of job rotation, additional benefits include:

- Trained backup in case of emergencies
- Protection against fraud
- Cross-training of employees
Mandatory Vacation

With mandatory vacations, all personnel are required to take time off, allowing other personnel to fill their positions while gone. This detective administrative control enhances the opportunity to discover unusual activity.

Some of the security benefits of using mandatory vacations include having the replacement employee:

- Run the same applications as the vacationing employee
- Perform tasks in a different order from the vacationing employee
- Perform the job from a different workstation than the vacationing employee

Replacement employees should avoid running scripts that were created by the vacationing employee. A replacement employee should either develop his or her own script or manually complete the tasks in the script.

Least Privilege

The principle of least privilege requires that a user or process be given only the minimum access privilege needed to perform a particular task. The main purpose of this principle is to ensure that users have access to only 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 to only 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 the minimums for each job or business function. Excessive privileges become a problem when a user has more rights, privileges, and permissions than needed to do his job. Excessive privileges are hard to control in large enterprise 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 her normal user account. When the systems administrator needs to perform administrative-level tasks, she should use the administrative-level account. If the administrator uses her administrative-level account while performing routine tasks, she 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 restrictive 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.

The default level of access should be no access. An organization should give users access only to resources required to do their jobs, and that access should require manual implementation after the requirement is verified by a supervisor.

Discretionary access control (DAC) and role-based access control (RBAC) are examples of systems based on a user’s need to know. Ensuring least privilege requires that the user’s job be identified and each user be granted the lowest clearance required for his or her tasks. Another example is the implementation of views in a database. Need-to-know requires that the operator have the minimum knowledge of the system necessary to perform his or her task.

If an administrator reviews a recent security audit and determines that two users in finance also have access to the human resource data, this could be an example of a violation of the principle of least privilege if either of the identified users works only in the finance department. Users should only be granted access to data necessary to complete their duties. While some users may require access to data outside their department, this is not the norm and should always be fully investigated.

**Incident Response**

Security events are inevitable. The response to an event has a great impact on how damaging the event will be to the organization. Incident response policies should be formally designed, well communicated, and followed. They should specifically address cyber attacks against an organization’s IT systems.

Steps in the incident response system can include the following (see Figure 2-2):

**Step 1.** **Detect:** The first step is to detect the incident. All detective controls, such as auditing, discussed in Chapter 3, are designed to provide this capability. The worst sort of incident is one that goes unnoticed.
Step 2. **Respond:** The response to the incident should be appropriate for the type of incident. Denial-of-service (DoS) attacks against a web server would require a quicker and different response than a missing mouse in the server room. An organization should establish standard responses and response times ahead of time.

Step 3. **Report:** All incidents should be reported within a time frame that reflects the seriousness of the incident. In many cases, establishing a list of incident types and the person to contact when each type of incident occurs is helpful. Attention to detail at this early stage, while time-sensitive information is still available, is critical.

Step 4. **Recover:** Recovery involves a reaction designed to make the network or system affected functional again. Exactly what that means depends on the circumstances and the recovery measures that are available. For example, if fault-tolerance measures are in place, the recovery might consist of simply allowing one server in a cluster to fail over to another. In other cases, it could mean restoring the server from a recent backup. The main goal of this step is to make all resources available again.

Step 5. **Remediate:** This step involves eliminating any residual danger or damage to the network that still might exist. For example, in the case of a virus outbreak, it could mean scanning all systems to root out any additional affected machines. These measures are designed to make a more detailed mitigation when time allows.

Step 6. **Review:** The final step is to review each incident to discover what can be learned from it. Changes to procedures might be called for. It is important to share lessons learned with all personnel who might encounter the same type of incident again. Complete documentation and analysis are the goals of this step.

The actual investigation of an incident occurs during the respond, report, and recover steps. Following appropriate forensic and digital investigation processes during an investigation can help ensure that evidence is preserved.

**Figure 2-2 Incident Response Process**

Incident response is vital to every organization to ensure that any security incidents are detected, contained, and investigated. Incident response is the beginning of any investigation. After an incident has been discovered, incident response personnel
perform specific tasks. During the entire incident response, the incident response team must ensure that it follows proper procedures to ensure that evidence is preserved.

As part of incident response, security professionals must understand the difference between events and incidents. The incident response team must have the appropriate incident response procedures in place to ensure that an incident is handled, but the procedures must not hinder any forensic investigations that might be needed to ensure that parties are held responsible for any illegal actions. Security professionals must understand the rules of engagement and the authorization and scope of any incident investigation.

**Events Versus Incidents**

In regard to incident response, a basic difference exists between events and incidents. An event is a change of state. Whereas events include both negative and positive events, incident response focuses more on negative events—events that have been deemed to negatively impact the organization. An incident is a series of events that negatively impact an organization’s operations and security. For example, an attempt to log on to the server is an event. If a system is breached because of a series of attempts to log on to the server, then an incident has occurred.

Events can be detected only if an organization has established the proper auditing and security mechanisms to monitor activity. A single negative event might occur. For example, the auditing log might show that an invalid login attempt occurred. By itself, this login attempt is not a security concern. However, if many invalid login attempts occur over a period of a few hours, the organization might be undergoing an attack. The initial invalid login is considered an event, but the series of invalid login attempts over a few hours would be an incident, especially if it is discovered that the invalid login attempts all originated from the same IP address.

**Rules of Engagement, Authorization, and Scope**

An organization ought to document the rules of engagement, authorization, and scope for the incident response team. The rules of engagement define which actions are acceptable and unacceptable if an incident has occurred. The authorization and scope provide the incident response team with the authority to perform an investigation and with the allowable scope of any investigation the team must undertake.

The rules of engagement act as a guideline for the incident response team to ensure that it does not cross the line from enticement into entrapment. Enticement occurs when the opportunity for illegal actions is provided (luring), but the attacker makes his own decision to perform the action. Entrapment involves encouraging someone to commit a crime that the individual might have had no intention of committing.
Enticement is legal but does raise ethical arguments and might not be admissible in court. Entrapment is illegal.

**Forensic Tasks**

Computer investigations require different procedures than regular investigations because the time frame for the investigator is compressed, and an expert might be required to assist in the investigation. Also, computer information is intangible and often requires extra care to ensure that the data is retained in its original format. Finally, the evidence in a computer crime can be very difficult to gather.

After a decision has been made to investigate a computer crime, you should follow standardized procedures, including the following:

- Identify what type of system is to be seized.
- Identify the search and seizure team members.
- Determine the risk of the suspect destroying evidence.

After law enforcement has been informed of a computer crime, the organization’s investigator’s constraints are increased. Turning over the investigation to law enforcement to ensure that evidence is preserved properly might be necessary.

When investigating a computer crime, evidentiary rules must be addressed. Computer evidence should prove a fact that is material to the case and must be reliable. The chain of custody must be maintained. Computer evidence is less likely to be admitted in court as evidence if the process for producing it has not been documented.

A forensic investigation involves the following steps:

**Step 1.** Identification

**Step 2.** Preservation

**Step 3.** Collection

**Step 4.** Examination

**Step 5.** Analysis

**Step 6.** Presentation

**Step 7.** Decision

Figure 2-3 illustrates the forensic investigation process.
Forensic investigations are discussed in more detail in Chapter 11, “Incident Response and Recovery.”

Employment and Termination Procedures

Personnel are responsible for the vast majority of security issues within an organization. For this reason, it is vital that an organization implement the appropriate personnel security policies. Organizational personnel security policies should include screening, hiring, and termination policies.

Personnel screening should occur prior to the offer of employment and might include a criminal background check, work history, background investigations, credit history, driving records, substance-abuse testing, and education and licensing verification. Screening needs should be determined based on the organization’s needs and the prospective hire’s employment level.

Personnel hiring procedures should include signing all the appropriate documents, including government-required documentation, no expectation of privacy statements, and NDAs. An organization usually has a personnel handbook and other hiring information that must be communicated to a new employee. The hiring process
should include a formal verification that the employee has completed all the training. Employee IDs and passwords are then issued.

Personnel termination must be handled differently based on whether the termination is friendly or unfriendly. Procedures defined by the human resources department can ensure that organizational property is returned, user access is removed at the appropriate time, and exit interviews are completed. With unfriendly terminations, organizational procedures must be proactive to prevent damage to organizational assets. Therefore, unfriendly termination procedures should include system and facility access termination prior to employee termination notification as well as security escort from the premises.

Management must also ensure that appropriate security policies are in place during employment. Separation of duties, mandatory vacations, and job rotation are covered earlier in this chapter. Some positions might require employment agreements to protect the organization and its assets even after the employee is no longer with the organization. These agreements can include NDAs, non-compete clauses, and code of conduct and ethics agreements.

**Continuous Monitoring**

Before continuous monitoring can be successful, an organization must ensure that the operational baselines are captured. After all, an organization cannot recognize abnormal patterns of behavior if it does not know what “normal” is. Periodically these baselines should also be revisited to ensure that they have not changed. For example, if a single web server is upgraded to a web server farm, a new performance baseline should be captured.

Security professionals must ensure that the organization’s security posture is maintained at all times. This requires continuous monitoring. Auditing and security logs should be reviewed on a regular schedule. Performance metrics should be compared to baselines. Even simple acts such as normal user login/logout times should be monitored. If a user suddenly starts logging in and out at irregular times, the user’s supervisor should be alerted to ensure that the user is authorized. Organizations must always be diligent in monitoring the security of their enterprise.

**Training and Awareness for Users**

*Security awareness training, security training, and security education* are three terms that are often used interchangeably, but these are actually three different things. Awareness training reinforces the fact that valuable resources must be protected by implementing security measures. Security training involves teaching personnel the skills they need to perform their jobs in a secure manner. Awareness training and security training are usually combined as security awareness training, which improves
user awareness of security and ensures that users can be held accountable for their actions. Security education is more independent and is targeted at security professionals who require security expertise to act as in-house experts for managing security programs. So, awareness training addresses the what, security training addresses the how, and security education addresses the why.

Security awareness training should be developed based on the audience. In addition, trainers must understand the corporate culture and how it affects security. For example, in a small customer-focused bank, bank employees may be encouraged to develop friendships with bank clientele. In this case, security awareness training must consider the risks that come with close relationships with clients.

The audiences you need to consider when designing training include high-level management, middle management, technical personnel, and other staff. For high-level management, security awareness training must provide a clear understanding of potential risks and threats, effects of security issues on organizational reputation and financial standing, and any applicable laws and regulations that pertain to the organization’s security program. Middle management training should discuss policies, standards, baselines, guidelines, and procedures, particularly how these components map to the individual departments. Also, middle management must understand their responsibilities regarding security. Technical staff should receive technical training on configuring and maintaining security controls, including how to recognize an attack when it occurs. In addition, technical staff should be encouraged to pursue industry certifications and higher education degrees. Other staff need to understand their responsibilities regarding security so that they perform their day-to-day tasks in a secure manner. With these staff, providing real-world examples to emphasize proper security procedures is effective.

Targeted security training is important to ensure that users at all levels understand their security duties within the organization. Let’s look at an example. Say that a manager is attending an all-day training session. He is overdue on entering bonus and payroll information for subordinates and feels that the best way to get the changes entered is to log into the payroll system and activate desktop sharing with a trusted subordinate. The manager grants the subordinate control of the desktop, thereby giving the subordinate full access to the payroll system. The subordinate does not have authorization to be in the payroll system. Another employee reports the incident to the security team. The most appropriate method for dealing with this issue going forward is to provide targeted security awareness training and impose termination for repeat violators.

Personnel should sign a document indicating that they have completed the training and understand all the topics. Although the initial training should occur when someone is hired, security awareness training should be considered a continuous process, with future training sessions occurring annually at a minimum.
It is important for organizations to constantly ensure that procedures are properly followed. If an organization discovers that personnel are not following proper procedures of any kind, the organization should review the procedures to ensure that they are correct. Then the personnel should be given the appropriate training so that the proper procedures are followed.

For example, if there has been a recent security breach leading to the release of sensitive customer information, the organization must ensure that staff are trained appropriately to improve security and reduce the risk of disclosing customer data. In this case, the primary focus of the privacy compliance training program should be to explain to personnel how customer data is gathered, used, disclosed, and managed.

It is also important that security audits be performed periodically. For example, say that an organization’s security audit has uncovered a lack of security controls with respect to employees’ account management. Specifically, the audit reveals that accounts are not disabled in a timely manner after an employee departs the organization. The company policy states that an employee’s account should be disabled within eight hours of termination. However, the audit shows that 10% of the accounts were not disabled until seven days after a dismissed employee departed. Furthermore, 5% of the accounts are still active. Security professionals should review the termination policy with the organization’s managers to ensure prompt reporting of employee terminations. It may be necessary to establish a formal procedure for reporting terminations to ensure that accounts are disabled when appropriate.

**Auditing Requirements and Frequency**

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. 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.

Audit trails detect computer penetrations and reveal actions that identify misuse. As a security professional, you should use 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. 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 was reached.
Information Classification and Life Cycle

Data should be classified based on its value to the organization and its sensitivity to disclosure. As mentioned earlier in this chapter, assigning a value to data allows an organization to determine the resources that should be used to protect the data. Resources that are used to protect data include personnel resources, monetary resources, and access control resources. Classifying data as it relates to confidentiality, integrity, and availability (CIA) allows you to apply different protective measures.

After data is classified, the data can be segmented based on the level of protection it needs. The classification levels ensure that data is handled and protected in the most cost-effective manner possible. An organization should determine the classification levels it uses based on the needs of the organization. A number of commercial business and military and government information classifications are commonly used.

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

Commercial Business Classifications

Commercial businesses usually classify data using four main classification levels, listed here from the highest sensitivity level to the lowest:

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

Data that is confidential includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred. Data at this level would be available only to personnel in the organization whose work relates to the data’s subject. Access to confidential data usually requires authorization for each access. Confidential data is exempt from disclosure under the Freedom of Information Act. In most cases, the only way for external entities to have authorized access to confidential data is as follows:

- After signing a confidentiality agreement
- When complying with a court order
- As part of a government project or contract procurement agreement
Data that is private includes any information related to personnel—including human resources records, medical records, and salary information—that is used only within the organization. Data that is sensitive includes organizational financial information and requires extra measures to ensure its CIA and accuracy. Public data is data that would not cause a negative impact on the organization.

**Military and Government Classifications**

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

1. Top secret
2. Secret
3. Confidential
4. Sensitive but unclassified
5. Unclassified

Data that is top secret includes weapons blueprints, technology specifications, spy satellite information, and other military information that could gravely damage national security if disclosed. Data that is secret includes deployment plans, missile placement, and other information that could seriously damage national security if disclosed. Data that is confidential includes patents, trade secrets, and other information that could seriously affect the government if unauthorized disclosure occurred. Data that is sensitive but unclassified includes medical or other personal data that might not cause serious damage to national security but could cause citizens to question the reputation of the government. Military and government information that does not fall into any of the other four categories is considered unclassified and usually has to be granted to the public based on the Freedom of Information Act.

**Information Life Cycle**

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

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

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 2-1 lists these key topics and the page number on which each is found.

Table 2-1  Key Topics for Chapter 2

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>List</td>
<td>Policy life cycle</td>
<td>66</td>
</tr>
<tr>
<td>List</td>
<td>Process life cycle</td>
<td>66</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Risk assessment description and steps</td>
<td>71</td>
</tr>
<tr>
<td>List</td>
<td>Contract security provisions</td>
<td>75</td>
</tr>
<tr>
<td>Paragraph</td>
<td>RFP</td>
<td>76</td>
</tr>
<tr>
<td>Paragraph</td>
<td>RFQ</td>
<td>76</td>
</tr>
<tr>
<td>Paragraph</td>
<td>RFI</td>
<td>76</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Agreements</td>
<td>77</td>
</tr>
<tr>
<td>Figure 2-1</td>
<td>Different types of PII</td>
<td>78</td>
</tr>
<tr>
<td>List</td>
<td>Least privilege rules</td>
<td>81</td>
</tr>
<tr>
<td>List</td>
<td>Incident response steps</td>
<td>81</td>
</tr>
<tr>
<td>List</td>
<td>Forensic investigation steps</td>
<td>84</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Security awareness training audiences</td>
<td>87</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Auditing guidelines</td>
<td>88</td>
</tr>
<tr>
<td>List</td>
<td>Commercial business classifications</td>
<td>89</td>
</tr>
<tr>
<td>List</td>
<td>Military and government classifications</td>
<td>90</td>
</tr>
</tbody>
</table>
Define Key Terms

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

- business impact analysis (BIA)
- business partnership agreement (BPA)
- interconnection security agreement (ISA)
- interoperability agreement (IA)
- job rotation
- least privilege
- mandatory vacation
- master service agreement (MSA)
- memorandum of understanding (MOU)
- need to know
- non-disclosure agreement (NDA)
- operating-level agreement (OLA)
- personally identifiable information (PII)
- request for information (RFI)
- request for proposal (RFP)
- request for quote (RFQ)
- risk assessment
- separation of duties
- service-level agreement (SLA)
- statement of applicability (SOA)

Review Questions

1. Your organization has recently been the victim of fraud perpetrated by a single employee. After a thorough analysis has been completed of the event, security experts recommend that security controls be established to require multiple employees to complete a task. Which control should you implement, based on the expert recommendations?
   a. mandatory vacation
   b. separation of duties
   c. least privilege
   d. continuous monitoring

2. Your company has recently decided to switch Internet service providers. The new provider has provided a document that lists all the guaranteed performance levels of the new connection. Which document contains this information?
   a. SLA
   b. ISA
   c. MOU
   d. IA
3. Your organization has signed a new contract to provide database services to another company. The partner company has requested that the appropriate privacy protections be in place within your organization. Which document should be used to ensure data privacy?
   a. ISA
   b. IA
   c. NDA
   d. PII

4. Your organization has recently undergone major restructuring. During this time, a new chief security officer (CSO) was hired. He has asked you to make recommendations for the implementation of organizational security policies. Which of the following should you not recommend?
   a. All personnel are required to use their vacation time.
   b. All personnel should be cross-trained and should rotate to multiple positions throughout the year.
   c. All high-level transactions should require a minimum of two personnel to complete.
   d. The principle of least privilege should be implemented only for all high-level positions.

5. What is the primary concern of PII?
   a. availability
   b. confidentiality
   c. integrity
   d. authentication

6. Which of the following is an example of an incident?
   a. an invalid user account’s login attempt
   b. account lockout for a single user account
   c. several invalid password attempts for multiple users
   d. a user attempting to access a folder to which he does not have access
7. What is the first step of a risk assessment?
   a. Balance threat impact with countermeasure cost.
   b. Calculate threat probability and business impact.
   c. Identify vulnerabilities and threats.
   d. Identify assets and asset value.

8. During a recent security audit, your organization provided the auditor with an SOA. What was the purpose of this document?
   a. to identify the controls chosen by an organization and explain how and why the controls are appropriate
   b. to document the performance levels that are guaranteed
   c. to document risks
   d. to prevent the disclosure of confidential information

9. Which document requires that a vendor reply with a formal bid proposal?
   a. RFI
   b. RFP
   c. RFQ
   d. agreement

10. Your company has decided to deploy network access control (NAC) on the enterprise to ensure that all devices comply with corporate security policies. Which of the following should be done first?
    a. Develop the process for NAC.
    b. Develop the procedures for NAC.
    c. Develop the policy for NAC.
    d. Implement NAC.
This page intentionally left blank
## Symbols

3-D Secure, 580
3DES (Triple Digital Encryption Standard), 583-585, 602
6to4, 223
802.1x, 226, 235, 549
802.11 (WLAN), 308-313

## A

A (Availability) metric, CVSS, 417
A records (DNS), 395
A/V systems, 278-279
AAAA records (DNS), 395
AC (Access Complexity) metric, CVSS, 417
accept risk reduction strategy, 137
acceptability (biometrics), 546
acceptance testing, 678, 704
accepting/monitoring phase (software acquisitions), 679
access
DAP, 564
EAC, 442
LDAP, 564-565
NAC, 199, 232, 269-271, 644
physical access control systems, 277
SCAP scanners, 418

## access control
access control matrices, 552
access control models, 550-553
access control policies, 553
ACL, 54, 210, 246-247, 304-305, 488, 553, 658
administrative (management) controls, 104-105
compensative controls, 103
content-dependent access control, 498
corrective controls, 103
dac, 81
data flow enforcement, 243
detective controls, 103
deterrent controls, 103
directive controls, 103
IP-based access control, 277
logical (technical) controls, 106-107
physical controls, 107-108
preventive controls, 104
RBAC, 81
recovery controls, 104
selecting/implementing based on CIA requirements, 102

## accountability and audits, 52

## accounts
lockout policies, passwords, 543
managing, 540-541
policies (Group Policy), 300
accreditation, 666, 676
accuracy (biometrics), 546
ACL (Access Control Lists), 54, 210, 246-247, 304-305, 488, 553, 658
acquisition/development stage (SDLC), 666-668
acquisitions
integrated solutions, 501
mergers and, 42-44
software, 679
action factor authentication, 538
activation/deactivation (unauthorized), wearable technology security/privacy, 349
Active Directory, IPsec policies (Group Policy), 301
active fingerprinting tools, 386
ActiveX, 373
AD (Active Directory), 565-566
Ad Hoc mode (WLAN), 309
Adams and CAST, Carlisle, 585
adapt solutions, 706-709
ADC (Application Delivery Controllers), 211
add-ons (browser extensions), 373-374
AddressSanitizer, runtime debugging, 385
Adleman and RSA, Leonard, 586-587
administration
database administration, 719-720
executive administration, 104-105, 720-726
management controls, 104-105, 720-726
network administration, 720
remote administration, 618
security, 105, 724
AES (Advanced Encryption Standard), 583-585, 620
after-action reports (incident response/recovery), 177, 481
agent-based log collection (SIEM), 425
agentless log collection (SIEM), 425
agentless NAC (Network Access Control), 271
aggregate CIA scoring, 101-102
aggregating data, data security in integrated solutions, 498
Agile model, software development, 694-697
agreements, 75-77, 249
AH (Authentication Headers), 216, 580
AI (Artificial Intelligence)
identity management, 708
security trends/threats, researching, 653
AIK (Attestation Identity Keys), TPM chips, 320, 558
air gaps, 269
AJAX (Asynchronous JavaScript and XML), 374
ALE (Annualized Loss Expectancy), magnitude of risk (risk impact), 128
alerts, 259-260
analyzing
behavioral analytics, 460, 708
code, 683-688
communications analysis, 464
content analysis, 464
cost/benefits, 186
data analysis, 455, 460
data flow security for changing business needs, 487-488
forensic analysis (incident response/recovery), 464
log reduction/analysis tools, 425-426, 438-439, 464
media, 464
Microsoft Baseline Security Analyzer, 428
network analysis, 464
protocol analyzers, 257-258
risk analysis, 126-127, 678
root-cause analysis (incident response/recovery), 480
security solutions, 183-186
slack space analysis, 464
software, 464
steganography analysis, 464
test coverage analysis, 687
trend analysis, 130, 182, 424

Android
APK format, 334
fragmentation, mobile device security/privacy, 340
Lost Android app, 332
remote wiping, 332
SEAndroid, trusted OS, 289
anomaly-based IDS/IPS, 196
anti-tamper technology, 338
antimalware, 291, 522
antispam services, clouds, 523
antisyware, 291
antivirus software, 291, 439
AP (Access Points), 208-209, 239, 308
API (Application Programming Interfaces), 337, 494, 581
APK (Android Package) format, 334
Apktool, 441
Apple, Xcode 7, 334
applications
API, interoperability issues with integrated solutions, 494
blacklists, 299, 360-362
client-based application virtualization (application streaming), 322-323
client-side processing versus server-side processing, 371-376
Compatibility tab, 492
DAM, 371
deploying, secure design, 356
digital certificates, 606
geofencing, 335
in-house developed applications/software, 493
integration solutions, 487-507
managing, 56, 331
mobile applications, social media attacks, 390
OWASP, 355, 362
permissions, mobile devices, 333
proxies, 203-204, 233, 236
requirements, interoperability issues with integrated solutions, 492
resource provisioning/deprovisioning, 501
sandboxing, 370
secure design, 355
secure enclaves, 371
security frameworks, SDLC, 677
server-based application virtualization (terminal services), 322-323
sharing, 619-620
side loading, 334
standard libraries, 679
streaming, 322-323
system applications, 334
unsigned applications, 334
updates, 670
vulnerabilities, 356-370
WAF, 371
whitelists, 299, 360-362
wrapping, 330
AR (Augmented Reality), mobile device security/privacy, 345
ARAT (Active Reader/Active Tag) RFID systems, 710
ARC4. See RC4
architectures
architecture design (SDD), 701
SOA, integration solutions, 506
archiving data, 453-454
ARO (Annualized Rate of Occurrence), 128, 130
ARPT (Active Reader/Passive Tag) RFID systems, 710
ASLR (Address Space Layout Randomization), 682
assertion tickets, 560
assessments
onsite assessments, 53
risk assessments, 125-126, 137-140
security assessments, 383-405, 411-444
self-assessments (security-based), 402
tools, 411, 414-444
vulnerability assessments, 401-402, 647, 667, 670, 675
assets
commissioning/decommissioning, 668-669
critical asset distribution, 495
disposal of, 672-673
inventory control, 450-451
managing (inventory control), 709
reusing, 673
tangible/intangible value/costs (risk assessments), 138-139
assigning system ports, 264
assurance (software)
acquiring software, 679
auditing, 677
development best practices, 680-688
logging, 677
risk analysis/mitigation, 678
standard libraries, 679
asymmetric cryptography, 585-591, 602-603, 610
attacks
assumed likelihood of attacks, 496
attack surfaces, 206, 675
authentication attacks, 258
Bluejacking, 307
Bluesnarfing, 307
brute force attacks, 427
buffer overflow attacks, 364-366
click-jacking, 358
client-side attacks, 644
CSRF, application vulnerabilities, 357
DDoS attacks, 266
dictionary attacks, 427
DNS harvesting, 395
DoS attacks, 266, 621, 626, 630-631
drive-by download attacks, 377
dronejacking, 647
dumpster diving, 389
eavesdropping, 414. See also packets, sniffing
fault injection attacks, 363-364, 684
firewall attacks, 258
honenets, 647
honeypots, 647
hopping attacks, 261-262
identity theft, 389
integer overflow attacks, 367
IPS/IDS, 258
latest attacks, researching, 644-645
live migration, 529
LPE attacks, 377
malware, 291, 630
man-in-the-middle attacks, 218
NOP slides, 365-366
pharming, 389
phishing, 388, 659
poisoning DNS caches, 506
privilege elevation, 528
race conditions, 367-368
reconnaissance (information-gathering), 385
resource exhaustion, 368
session hijacking, 359
shoulder surfing, 389
snooping, VoIP, 631
social engineering attacks, 388-389, 626, 659
spam, 292, 628-629
spoofing attacks, 261, 628
spyware, 291
SQL injection attacks, 360-362
switch spoofing, 261
time of check/time of use attacks, 367-368
viruses, 291
VLAN hopping, 261-262
VMEscape, 527
whaling, 629
XSS, application vulnerabilities, 356
zero-day attacks, 647

**auditing, 719**
audit logs, 255
audit trails, 88, 296
auditing/monitoring services, data flow enforcement, 243
auditors, risk management, 52
code audits, 718
effective protection, 295-297
incident response/recovery, 461
time of check/time of use attacks, 367-368
ISO, 52
SAS 70, 403
scrubbing, 296
security audits, 88
SOC reports, 404
software assurance, 677
SSAE 16 audits, 404
Windows audit policies, 297

**authentication**
802.1, 226, 235
802.1x, 549
account management, 540-541
action factor authentication, 538
AD, 565-566
AH, 216
authentication attacks, 258
biometrics, 343-344, 539, 546-547
certificate-based authentication, 548
CHAP, 224-225, 394
dual-factor authentication, 548
effective protection, 295-297
context-aware authentication/management, 334, 550
dual-factor authentication, 548
EAP, 225-226
gestures, 343

**attestation, 557**
boot loaders, 319
SAML, 560-562
TPM chips, 558

**Au (Authentication) metric, CVSS, 417**

**audio**
A/V systems, 278-279
conferencing, 623
output, host security, 314
HOTP algorithm, 540
HSM, 211-212, 233
identification and the authentication process, 537
identity management, 540, 559-563
identity proofing, 558
identity propagation, 558
IKE, 581
Kerberos, 565
knowledge factor authentication, 538
LDAP, 564-565
location factor authentication, 538
MD5 authentication, 266
message authentication, 577-578
mobile devices, 342-344
multi-factor authentication, 548
network authentication, 224-226, 235
OSA, 312
ownership factor authentication, 538-539
PAP, 224-225, 394
passwords, 541-544
PIN, 343
ports, 226, 235
proximity authentication devices, 442
push-based authentication, 550
RADIUS, 226, 563-564
SAML, 560-562
single-factor authentication, 538
SKA, 313
SSL, 579, 595
SSO, 540, 548-549, 558-560, 563-565
swipe patterns, 343
system failures, cloud storage, 337
TACACS+, 226
TLS, 579, 595
TOTP algorithm, 540
Type III authentication. See characteristic factor authentication
user behavior, 335
WPA-PSK, 313
author identification, software analysis, 464
authorization
access control models, 550-553
attestation, 557
OAuth, 553
SPML, 556
XACML, 555-556
automation
BACnet, 276
building automation systems, 274
patch management, 302
resiliency issues with integrated solutions, 495
SCAP, 437
AV (Access Vector) metric, CVSS, 417
availability
availability controls, 248-253
CIA triad, categorizing data, 99
high availability, resiliency issues with integrated solutions, 496
presence, 626-627
security solutions, analyzing, 185
virtualization, 513
avoid risk reduction strategy, 135
AVS (Active Vulnerability Scanners), 214
awareness training, 86-87, 105
B
backups, 338, 453, 465-469, 719
BACnet (Building Automation and Control Network), 276
base metric group (CVSS), 416
baseband radio/SOC, mobile device
security/privacy, 345
Basel II, 48
baselines
  benchmark comparisons, 181-182
capturing, 181-182
clipping levels, 543
defined, 167, 181
host security, 298
Microsoft Baseline Security Analyzer,
428
performance baselines, 669
bastion hosts, 206, 237
BCP (Business Continuity Planning),
141-148
behavioral analytics, 460, 708
behavioral characteristics (authentication),
539, 545-546
benchmarks, capturing, 181-182
benefit/cost analysis, analyzing security
solutions, 186
best practices, researching security
trends/threats, 640-641
BGP (Border Gateway Protocol),
RTBH routing, 267
BIA (Business Impact Analysis), 72, 145
bidding (RFQ), 76
big data, researching security trends/threats,
652-653
biometrics, 343-344, 539, 546-547
BIOS, 316-318
BitLocker, 320
BitLocker Drive Encryption, 719
BitLocker to Go, 320
black box (zero-knowledge) testing,
400-401
black hats, 655-656
blacklists, 299, 360-362
blind penetration testing, 399
block ciphers, 582-585, 597-602
block-level encryption, 589
blockchains, 609, 709
Blowfish, 584-585
blue team exercises, security
assessments, 405
Bluetooth
  Bluejacking, 307
  Bluesnarfing, 307
  host security, 306
tethering, 342
wearable technology security/technology, 349
boot loaders, 316-320, 520
booting (secure) and SoC, 271
boundaries (networks)
  boundary control services, data flow enforcement, 243
de-perimeterization, 54-59
BPA (Business Partnership Agreements), 74
breaches (data)
  central security breach response, SoC, 274
cloud storage, 337
defined, 454
incident response process, 454-457, 461-463, 470-471
internal/external violations, 458-459
severity of, 478-480
bridge (trusted third-party) model
(federated identities), 560
bridges
  transparent bridging, 201
unauthorized domain bridging, 344
browser extensions (add-ons), 373-374
brute force attacks, 427
BSI (Build Security In), software
development best practices, 680
buffer overflow attacks, 364-366
build and fix software development
method, 689
Burp Suite, 422
business models/strategies, 40-44
business units
  collaboration in security solutions,
    725-726
  security controls/processes, 724-725
  security requirements/goals, 717-724
BYOD (Bring Your Own Device)
policies, 56-57, 68, 332

C
C (Confidentiality) metric, CVSS, 417
CA (Certificate Authorities), 548,
  604-607
cable locks, 444
Cain and Abel, 427
cameras
  IR cameras, 444
  wearable cameras, 346
CANVAS, 423
CAPTCHA passwords, 542
capturing
  data, web conferences, 621
  email messages, 629
  packets, 657
CASB (Cloud Security Broker), 526
CAST, 585
categorizing data, 98-102
CBC (Cipher Block Chaining) mode
  (DES), 599
CBC-MAC (Cipher Block Chaining
  MAC), 577
CC (Common Criteria), 287-289. See
  also TCSEC
CCE (Common Configuration Enum-
  eration), SCAP scanners, 416
central security breach response, SoC,
  274
CEO (Chief Executive Officers), 720,
  726
CER (Crossover Error Rates), bio-
  metrics, 546-547
CERT (Computer Emergency
  Readiness Teams), 654, 700
certificates
  accreditation process, 666
  applications, 606
  authentication, 548
  certification/accreditation phase
    (SDLC), 676
  classes, 607
  CRL, 604
  defined, 666
  issuance of, 604
  OCSP, 604, 608
  RA, 605
  SCEP, 332
  tokens, 607
  user credentials, 605
  wildcard certificates, 603-604
  X.509 certificates, 606
CFAA (Computer Fraud and Abuse
  Act), 47
CFB (Cipher Feedback) mode (DES),
  600
CFO (Chief Financial Officers),
  security requirements/goals, 721
chain of custody (incident response/
  recovery), 461-463, 470-471
change control process, 481
change management, 670-672, 677
change monitoring, 247-248
CHAP (Challenge Handshake Authentication Protocol), 224-225, 394
characteristic factor authentication, 538-539, 544-547
CI (Configuration Items), 672
CI (Continuous Integration), software development, 698
CIA (Confidentiality, Integrity, Availability) triad, 98-102, 571
CIO (Chief Information Officers), security requirements/goals, 721
CIP (Critical Infrastructure Protection) plans, 144
cipher locks, 442
circles of trust, SAML, 560
circuit-level proxies, 203-204, 233, 236
CIS (Center for Internet Security), Critical Security Controls, 118-119
classifying information, 89-90
Cleanroom model, software development, 695
clearing data, 369, 454, 497
click-jacking, 358
clients
application virtualization (application streaming), 322-323
client-side attacks, 644
risk management, client requirements, 53
server-side processing versus client-side processing, 371-376
clipping levels, 543
cloud computing
antimalware, 522
antispm services, 523
antivirus software, 439, 522
backups, 469
CASB, 526
collaboration, 633-634
community clouds, 42, 514
content filtering, 525
critical assets, separating, 268
data storage, 337
de-perimeterization, 55
elasticity, 42
end-user cloud storage, 650
hash matching, 522
hosted solution, 515
hybrid clouds, 42, 514
latest attacks, researching, 645
MSSP, 527
multitenancy model, 515-516
on-premise solution, 515
private clouds, 42, 513-514, 651
public clouds, 41, 513-516, 651
resource provisioning/deprovisioning, 531
risk management, 41-42, 55
sandboxing, 525
SecaaS, 527
single-tenancy model, 515
SLA, 531
virtualization, 513, 527-530
vulnerability scanning, 523-524
clustering, 253
CMAC (Cipher MAC), 578
CMDB (Configuration Management Database), 505
CMMI (Capability Maturity Model Integration), 123
CMS (Content Management System), 505
CNAME records (DNS), 395
COBIT (Control Objectives for Information and Related Technology), 114-115
coding
analyzing code, 683-688
audits, 718
dynamic testing, 686
forbidden coding techniques, 681-682
formal code reviews, 686
fuzzing, 683-684
interface testing, 688
lightweight code reviews, 686
misuse case (negative) testing, 687
quality of, 683
reusing code, application vulnerabilities, 370
reviews, 387-388
secure coding standards, 700
signing, 578
software development best practices, 681-688
static testing, 686
test coverage analysis, 687
cognitive passwords, 542
collaboration
audio conferencing, 623
cloud-based collaboration, 633-634
color teams, security assessments, 405
document collaboration tools, 624-625
email, 627-632
IM, 625-626
presence (user availability), 626-627
security risks, 625
security solutions, 725-726
social media, 632
storage collaboration tools, 624-625
telephony systems, 630-632
texting, 625-626
video conferencing, 622-623
web conferencing, 621-622
combination locks, 443
combination passwords, 541
command shell, host security, 301
command-line tools, 429-438
comments, RFC, 643
commercial business classifications
(information classification), 89-90
commercial customized (tailored commercial) software, 493
commissioning/decommissioning assets, 668-669
communications
analysis, 464
crisis communications plans, 144
encrypted/unencrypted communication, 349
remote access, 617-621
wearable technology security/privacy, 349
community clouds, 42, 514
compartmentalization, 81
Compatibility tab (applications), 492
compensative controls, 103
competing standards, integration solutions, 490
competitors, risk management, 52
complex passwords, 542
compliance, 726-727
Computer Security Act, 47
conferencing, 621-623
confidentiality (CIA), categorizing data, 98-100
configuration profiles (MDM), payloads, 329
configuring
configuration lockdown, 248
managing configurations, 671-672, 677
misconfigurations/nonmalicious threats, 459
network components, 246-253
consultants/vendors, 41, 655
containers
containerization, defined, 329
Group Policy (Windows), 300
virtualization, 520
containment technologies, 709-711
content analysis, 464
content-aware authentication/management, 334
content-dependent access control, 498, 552
content filtering, clouds, 525
content management, mobile devices, 331
context analysis, 464
context-aware (context-dependent) authentication, 550
context-dependent access control, 498
contingency planning, 144, 148
continuity planning, 141-148, 465
continuous monitoring, 86, 141
contracting phase (software acquisitions), 679
contracts, 41, 75-77
control plane (networks), 254
conventions/conferences, 654-655
cookies, storing/transmitting, 364
COOP (Continuity of Operations Plan), 144, 465
COPE (Corporate-Owned, Personally Enabled) policies, 332
copy backups, 467
corrective controls, 103
COSO (Committee of Sponsoring Organizations), 119, 163
costs
analysis of (security solutions), 186
asset value/costs (tangible/intangible), risk assessments, 138-139
information value/costs (tangible/intangible), risk assessments, 138-139
repair costs, 131
ROI, 131, 186
severity of data breaches, 479
TCO, 133-134, 186
COTS (Commercial-Off-The-Shelf) software, 493-494
coverage gap detection, wireless controllers, 209
CPE (Common Platform Enumeration), SCAP scanners, 416
CPO (Chief Privacy Officers), security requirements/goals, 721
crackers, 656
CRAMM (CCTA Risk Analysis and Management Method), 123
credential breaches, 624
credit card readers (peripheral-enabled mobile payments), 341
credit card security, 580, 590
CredSSP (Credential Security Support Provider), identity propagation, 559
crisis communications plans, 144
critical assets, 268, 495
Critical Security Controls (CIS), 118-119
critical systems, 479
criticality (system process), severity of data breaches, 479
CRL (Certificate Revocation Lists), 604
CRM (Customer Relationship Management), 504
cross-certification model (federated identities), 559

CRR (Cyber Resilience Review) assessments, 168-169
crypto processing, HSM, 211-212, 233
cryptography
- asymmetric cryptography, 586-591, 610
- block ciphers, 597-598
- blockchain, 609
- CIA triad, 571
- code signing, 578
- cryptocurrencies, 609
- crypto modules, 592
- crypto processors, 593
- CSP, 593
data flow enforcement, 243
data-at-rest encryption, 581-591, 602-603
data-in-memory/processing, 581
data-in-transit encryption, 579-580, 595
digital signatures, 576-577
digital watermarking, 591, 594
DRM, 593-594
encryption, 571, 581-602, 610
GPG, 594
hashing, 572-577
implementing algorithms, 596-597
interoperability of algorithms, 596-597
key stretching, 572
message authentication, 577-578
performance of algorithms, 596-597
PFS, 578
PGP, 594
PKI/digital certificates, 603-608
PRNG, 578
public key cryptography, digital signatures, 577 S/MIME, 596
SSH, 595
steganography, 591
stream ciphers, 597-598
strength of algorithms, 596-597
symmetric cryptography, 588, 602
CSO (Chief Security Officers), security requirements/goals, 721
CSP (Cryptographic Service Providers), 593
CSRF (Cross-Site Request Forgery), application vulnerabilities, 357
CTR (Counter) mode (DES), 601
Cuckoo malware sandboxing tool, 383
custody, chain of (incident response/recovery), 461-463, 471
customer requirements, risk management, 53
CVE (Common Vulnerabilities and Exposures), SCAP scanners, 416
CVSS (Common Vulnerability Scoring System), 416-418
CWE (Common Weakness Enumeration), SCAP scanners, 416
cyber incident response plans, 144

D

DAC (Discretionary Access Control), 81, 551
daily backups, 467
DAM (Database Activity Monitoring), 214, 240, 371, 634
DAP (Directory Access Protocol), 564
data
aggregation, data security in integrated solutions, 498
analytics, 455, 460
archives, 453-454
breaches, 337, 454-463, 470-471, 478-480
capturing, web conferencing, 621
categorizing, 98-102
clearing, 369, 454
compromise, ROI, 131
design (SDD), 701
exfiltration, 242, 293
flow, 241-245, 487-488
forensic data, 350
formats, 493-494
handling policies, 453-454
havens, 50
inference, 498
integrity, 579, 595
interfaces, host security, 305
isolation, data security in integrated solutions, 498
jurisdiction, public clouds, 516
leakage, 293, 621
loss, ROI, 131
management, mobile devices, 331
normalization, 494
ownership of, 43, 452, 499
purging, 369, 453
reclassiﬁcation of, 44
recovery, 451-452
remnants, 369, 497-498, 501, 529-531, 673
retention policies, 451, 500
security, integrated solutions, 497-500
sovereignty of, 50-51, 499
storage, 336-338, 362, 451-452
theft (personal), wearable technology security/privacy, 350
warehouses, 494
data plane (networks), 254

Data Protection Directive (EU), 49
data-at-rest encryption, 581-591, 599-603, 610
data-in-memory/processing, 581
data-in-transit encryption, 579-581, 595
databases
administration, 719
CMDB, 505
DAM, 214, 240, 371, 634
heterogeneous databases, 494
permissions, granting, 719
RDBMS, 558
security requirements/goals, 719
dcfldd command, 471
dd command, 471
DDoS (Distributed Denial-of-Service) attacks, 266
de facto standards, integrated solutions, 490
de-perimeterization, 54-59
deactivation/activation (unauthorized), wearable technology security/privacy, 349
debugging (runtime), 385
deception technology, 708
decommissioning/commissioning assets, 668-669
deconstructing/reverse engineering security solutions, 177
dedicated interfaces, host security, 303-305
deep packet inspection, 242
default to no access (authorization), 553
DEFCON conference, 655
Deleaker, runtime debugging, 385
delegation in networks, integrated solutions, 502
Delphi technique, 126

demergers/divestitures, 42-44, 501
deploying
  applications, secure design, 356
  deployment diagrams, integrated solutions, 502-504
deprovisioning/provisioning resources, integrated solutions, 500-501, 531
DES (Digital Encryption Standard), 582, 585, 599-601
DES-X (Digital Encryption Standard X), 583
design phase (SDLC), 675
designing
  applications, secure design, 355
  integration solutions, 501
desktops
  sharing, 619-620
  VDI, 521
Destination Unreachable code (ping command), 432
destruction/disposal
  data, 453-454, 497
  remanence, 454
  storage media, 453
detective controls, 103
deterrence
  deterrent controls, 103
  risk assessment, 140
develop phase (SDLC), 675
developing software
  acceptance testing, 704
  best practices, 680-688
  CI, 698
  documentation, 700-704
  integration testing, 705
  methods, 688-698
  peer reviews, 706
  regression testing, 706
  secure coding standards, 700
  unit testing, 704
  user acceptance testing, 705
  validation testing, 704
  versioning, 698
development life cycles, 665-677
development/acquisition stage (SDLC), 666-668
device fingerprinting, 420
device tracking, 709-711
DevOps, software development, 695
dex2jar, 441
DFD (Data Flow Diagrams), 245
dial-up connections, 617-618
dictionary attacks, 427
differential backups, 466
Diffie-Hellman, 586
dig command, 435
digital certificates, 603-608
digital forensics, 350
digital keys, HSM, 211-212, 233
digital signatures, 576-577
digital watermarking, 591, 594
direct objects references (unsecure), application vulnerabilities, 356
directive controls, 103
Directory Services, 505, 564-565
disaster recovery, 144, 465-469
disclosure policies, 630
disk encryption, 315, 320, 718
disk imaging, 464
disk-level encryption, 588-591
disk mirroring. See RAID
disk striping. See RAID
disposal stage (SDLC), 667
disposal/destruction
assets, 672-673
data clearing, 454
data purging, 453
remanence, 454
storage media, 453
disruptive technologies, addressing, 707-708
diStorm3, 441
diverse industries, integrating, 44-51
divestitures/demergers, 42-44, 501
DLP (Data Loss Prevention), 241-242, 293
DMADV (Six Sigma), 121
DMAIC (Six Sigma), 121
DMZ (Demilitarized Zones), 207, 268
DNS (Domain Name System), 394-397, 506
DNSSEC (Domain Name System Security Extensions), 506
documentation
after-action reports (incident response/recovery), 481
bidding-process documents, 76-77
collaboration tools, 624-625
exchanges/reviews, 53
lessons learned reports (incident response/recovery), 480
maintenance, 671
outsourcing, 41
PIPEDA, 48
security documents, 71-77
SLA, 249
SOC reports, 404
software development documentation, 700-704
TCA, 40
trend data, 183

DoDAF (Department of Defense Architecture Framework), 113
domain bridging (unauthorized), mobile device security/privacy, 344
door locks, 442
DoS (Denial of Service) attacks, 266, 621, 626, 630-631
double-blind penetration testing, 399
Double-DES (Digital Encryption Standard), 583
double tagging, 261
downloading, drive-by download attacks, 377
downstream liability, 58
downtime, 146, 479
DPAPI (Data-Protection API), 581
drive mapping, host security, 314
drive mounting, host security, 313
drive-by download attacks, 377
DRM (Digital Rights Management), 593-594
dronejacking, 647
Dropbox, hash matching, 522
DRP (Disaster Recovery Plans), 144
DSA (Digital Security Algorithm), 577
DSS (Digital Signature Standard), 577
DTP (Dynamic Trunking Protocol), 261
dual-factor authentication, 548
dual-homed firewalls, 206, 238
dual stack solutions, 223
due care, risk management, 59
due diligence, 43, 59
dumpster diving, 389
duties, separation of (security policies), 78-79
dwell time, keystroke dynamics (authentication), 546
dynamic packet filtering, 203
dynamic passwords, 542
dynamic testing, 686

E
e-discovery, 449-454
EAC (Electronic Access Control), 442
EAL (Evaluation Assurance Levels), CC, 287
EAP (Extensible Authentication Protocol), 225-226
eavesdropping, 414. See also packets, sniffing
ECB (Electronic Code Book) mode (DES), 599
ECC (Elliptic Curve Cryptography), 587, 610
Economic Espionage Act, 48-49
ECPA (Electronic Communications Privacy Act), 49
edb-debugger, 441
EDR (Endpoint Detection Response), endpoint security, 297
EFS (Encrypting File Systems), 719
eFuse, finding lost/stolen devices, 338
egress filters (DLP), 242
EK (Endorsement Keys), TPM chips, 319, 558
Elastic Sandbox, 383
elasticity (clouds), 42
electric locks, 442
electronic backups, 469
Electronic Security Directive (EU), 50
electronic signatures, 50
electronic vaulting, 469
El Gamal, 587
e-mail, 388, 596, 627-630, 658

emergency response teams, security requirements/goals, 723
emerging risks, updating policies/procedures, 70
employment, hiring personnel, 85-86
encapsulation PPP command, 394
enclaves (secure), 371, 521
encryption
3-D Secure, 580
3DES, 583-585
3ES, modes of, 602
AES, 583-585, 620
benefits of, 571
BitLocker Drive Encryption, 719
block ciphers, 597-598
block-level encryption, 589
Blowfish, 584-585
CAST, 585
data-at-rest encryption, 581-591, 602-603
data-in-memory/processing, 581
data-in-transit encryption, 579-580, 595
DES, 582, 585, 599-601
DES-X, 583
Diffie-Hellman, 586
disk encryption, 315, 320, 588-591
document collaboration, 624
Double-DES, 583
DPAPI, 581
DRM, 593-594
ECC, 587, 610
EFS, 719
El Gamal, 587
e-mail, 629
enclaves, 371
file encryption, 315, 589-591
full disk encryption, 718
exploitation frameworks 815

hard drives, 673
HTTP, 579
HTTPS, 580
hybrid ciphers, 588
IDEA, 583-585
IM, 340
INE, 198, 231
IPsec, 580-581
Knapsack, 588
mobile devices, 610
PGP, 594
port-level encryption, 591
RC4, 584-585
RC5, 584-585
RC6, 584-585
record-level encryption, 589-591
RSA, 586-587
S/MIME, 596
SET, 580
SGX, 581
SHTTP, 580
Skipjack, 584-585
SSL, 579, 595
storage collaboration, 624
storage encryption, 589-590
stream ciphers, 597-598
TDE, 719
TLS, 579, 595
TwoFish, 584-585
wearable technology security/privacy, 349
Zero Knowledge Proof, 588
endpoint DLP (Data Loss Prevention), 242
endpoint security, 290-297
engagement, rules of (incident response), 83
enrollment time (biometrics), 546
enterprise resilience, 168-169
enticement, incident response, 83
entrapment, incident response, 83
environmental changes, updating policies/procedures, 69
environmental metric group (CVSS), 416
EPA (U.S. Environmental Protection Agency), exemptions to risk assessment, 139
ERM (Enterprise Risk Management), COSO, 163
ERP (Enterprise Resource Planning), 505
error handling, application vulnerabilities, 362
ESB (Enterprise Service Buses), integration solutions, 507
ESP (Encapsulating Security Payloads), 217, 580
EU (European Union), laws/regulations, 49-50
evaluation/testing phase (SDLC), 668
event handlers, 376
event log policies (Group Policy), 300
events
  incidents versus, 83
  SIEM, 199, 232
evidence (data breaches), 455, 461-463, 470-471
evolving technologies, researching security trends/threats, 642
exception handling, application vulnerabilities, 362
executive management, 720-721, 724-726
exemptions, risk assessment, 139
exploitation frameworks, 422-423, 436
export controls, integrating diverse industries, 45
external I/O, host security, 305-313
external/internal audits, 403-404
extranets, 268
extreme (worst-case) scenario planning, 123-125
eye (iris) scanning (biometrics), 344

facial scanning (biometrics), 344, 545
facilities managers, security requirements/goals, 723
Failover, 253
Failsoft, 253
failures
   MTBF, 146
   SPOF, 253
FAR (False Acceptance Rates), biometrics, 546-547
FATKit, 385
fault injection attacks, 363-364, 684
fault-tolerance, 249, 496
feature extraction (biometrics), 546
Federal Privacy Act, 47
federated identities, 559-563
federation, 560
FERMA (Federation of European Risk Management Associations), 164-166
Fiddler, 422
FIFO (First-In, First-Out) rotation scheme, backups, 467
file encryption, 315, 589-591
File Fuzzer, 685
file integrity monitoring, 437
file system policies (Group Policy), 301
financial staff, security requirements/goals, 722
finding lost/stolen devices, 338
fingerprinting
   authentication, 544
   biometrics, 344
   device fingerprinting, 420
   fingerprinting tools, 385-386
   OS fingerprinting, 657
FIPS 199 (Federal Information Processing Standard), 99-102
firewalls
   ACL reviews, 658
   bastion hosts, 206, 237
dual-homed firewalls, 206, 238
dynamic packet filtering, 203
firewall attacks, 258
host-based firewalls, endpoint security, 294
multihomed firewalls, 207, 239
network segmentation, 269
NGFW, 205, 236
packet-filtering firewalls, 202-204, 236
proxy firewalls, 203-204, 233, 236
remote access networks, 236
screened subnets, 208, 239
screen host firewalls, 207-208, 239
stateful firewalls, 202-203
three-legged firewalls, 207, 239
WAF, 212-213, 234, 371
firing personnel, 86
firmware
   FOTA updates, 331
   threats to, 647
   UEFI, boot loaders, 318
   updates, 316, 377
   vulnerabilities, 377
FISA (Foreign Intelligence Surveillance Act), 49
FISMA (Federal Information Security Management Act), 47-48
fitness trackers, 347, 350
flashing BIOS, 316
flight time, keystroke dynamics (authentication), 546
follow-on phase (software acquisitions), 679
foremost command, 477
forensic analysis (incident response/recovery), 464
forensic data, 350
forensic investigations, 84
forensic recovery, hard drives, 673
formal code reviews, 387, 686
forward proxies, 203
forwarding plane. See data plane (networks)
FOTA (Firmware-Over-The-Air) updates, 331
fragmentation (Android), mobile device security/privacy, 340
frameworks
application security frameworks, SDLC, 677
exploitation frameworks, 422-423, 436
NIST Framework for Improving Critical Infrastructure Cybersecurity, 160
risk management frameworks, 149-158
security control, 110-123, 137, 143, 150-163, 280, 673
frequencies (radio)
restrictions, mobile device security, 336
spectrum management, 342
FRR (False Rejection Rates), biometrics, 546-547
full backups, 466
full disk encryption, mobile devices, 718
full-knowledge testing, 400
fuzzing, 363-364, 421-422, 683-685
G
gap analysis, 176
gather requirements (SDLC), 674
generation-based fuzzing, 363, 684
geofencing, 335, 710
geography, integrating diverse industries, 50-51
geolocation/GPS location devices, 335, 709-711
geotagging, 339, 368-369, 710
gestures, mobile device authentication, 343
GFS (Grandfather/Father/Son) rotation scheme, backups, 468
glasses (wearable technology), 347
GLBA (Gramm-Leach-Bliley Act), 47
global IA industry/community, researching security trends/threats, 653-659
GoAccess, 438
goals/requirements (security), 717-724
Google Glass, 347
governance (IT), 148-166, 726-727
government/military classifications (information classification), 90
GPG (GNU Privacy Guard), 594
GPMC (Group Policy Management Console), 296, 300
GPO (Group Policy Objects), 300
GPS (Global Positioning System) devices, 709-711
graphical passwords, 542
gray box testing, 400-401
gray hats, 656
Graylog, 439
GRE tunnels, 223
Group Policy (Windows), 299-301, 306
guidelines, 167
GUI testing, 688

H
hackers/hacking
  CFAA, 47
  hacktivists, 656
  OSINT, 390-397
Hadoop, 652
hand geometry scans, authentication, 545
hand topography scans, authentication, 545
hand/palm scans, authentication, 545
handling data, 453-454
hard drives, 673
hardware
  anti-tamper technology, 338
  redundant hardware, 248
  threats to, 647
  updates, 670
  vulnerabilities, host security, 322
harvesting email, 658
hash matching (hash spoofing), clouds, 522
hashing, 572-577
HAVAL, 576
HC1 headset computer (Zebra), 348
HDMI ports, host security, 315
headsets (wearable technology), 348
Health Care and Education Reconciliation Act, 49
health privacy, wearable technology
  security/privacy, 350
Herzog and OSSTMM, Pete, 163
heterogeneous components, resiliency
  issues with integrate solutions, 494
heterogeneous computing, 494
heterogeneous databases, 494
heuristic (rule-based) IDS/IPS, 196
heuristics/behavioral analytics, 460
HIDS/HIPS (Host-based IDS/IPS), 197, 230, 293
high availability, 496, 513
hijacked user accounts, 626
HIPAA (Health Insurance Portability and Accountability Act), 46
hiring personnel, 85-86
HITRUST CSF (Common Security Framework), 118
HMAC (Hash MAC), 577
honeynets, 647
honeypots, 647
hopping attacks (VLAN), 261-262
horizontal privilege escalation, 362
hosts
  cloud computing, 515
  firewalls, endpoint security, 294
  integration solutions, 487-504
  security, 287-297, 302-323, 520
  single platform hosts, 530
  single server hosts, 530
  tools, 427-441
  virtualization and data security, 530
  vulnerability scanners, 428
hot fixes, 292
HOTP (HMAC-Based One-Time Password) algorithm, authenti-
cation, 540
hotspots, tethering, 341-342
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR</td>
<td>Human Resources, security requirements/goals, 722</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Modules, 211-212, 233-234</td>
</tr>
<tr>
<td>HSM</td>
<td>Hierarchical Storage Management, 469</td>
</tr>
<tr>
<td>HTML5</td>
<td>Hypertext Markup Language 5, 374</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol, 579</td>
</tr>
<tr>
<td>HTTP interceptors</td>
<td>422</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTP Secure, 580</td>
</tr>
<tr>
<td>human resources, legal advocacy/compliance</td>
<td>70</td>
</tr>
<tr>
<td>hunt teaming</td>
<td>460</td>
</tr>
<tr>
<td>HVAC controllers</td>
<td>276</td>
</tr>
<tr>
<td>hybrid ciphers</td>
<td>588</td>
</tr>
<tr>
<td>hybrid clouds</td>
<td>42, 514</td>
</tr>
<tr>
<td>hyperconverged infrastructures, virtualization</td>
<td>521</td>
</tr>
<tr>
<td>hypervisors</td>
<td>518-519</td>
</tr>
<tr>
<td>I (Integrity) metric</td>
<td>CVSS, 418</td>
</tr>
<tr>
<td>I/O (external)</td>
<td>host security, 305-313</td>
</tr>
<tr>
<td>IA (Interoperability Agreements)</td>
<td>72</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service, public clouds, 516</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems, SCADA, 279-280</td>
</tr>
<tr>
<td>ID-FF</td>
<td>Identity Federation Framework, SAML, 560</td>
</tr>
<tr>
<td>IDEA</td>
<td>International Data Encryption Algorithm, 583-585</td>
</tr>
<tr>
<td>identifying</td>
<td>attack surfaces, 675</td>
</tr>
<tr>
<td>threats, risk assessments</td>
<td>139</td>
</tr>
<tr>
<td>identity/identification</td>
<td>authentication process, 537</td>
</tr>
<tr>
<td>configuration identification</td>
<td>672</td>
</tr>
<tr>
<td>managing</td>
<td>540, 559-563, 708</td>
</tr>
<tr>
<td>proofing</td>
<td>558</td>
</tr>
<tr>
<td>propagation</td>
<td>558</td>
</tr>
<tr>
<td>RFID</td>
<td>710-711</td>
</tr>
<tr>
<td>theft</td>
<td>47, 389, 624</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>Intrusion Detection Systems/Intrusion Prevention Systems</td>
</tr>
<tr>
<td>anomaly-based IDS/IPS</td>
<td>196</td>
</tr>
<tr>
<td>endpoint security</td>
<td>293</td>
</tr>
<tr>
<td>HIDS/HIPS</td>
<td>197, 230, 293</td>
</tr>
<tr>
<td>IPS/IDS attacks</td>
<td>258</td>
</tr>
<tr>
<td>NIDS</td>
<td>198, 230</td>
</tr>
<tr>
<td>NIPS</td>
<td>197, 230</td>
</tr>
<tr>
<td>remote access networks</td>
<td>230</td>
</tr>
<tr>
<td>rule-based (heuristic) IDS/IPS</td>
<td>196</td>
</tr>
<tr>
<td>signature-based IDS/IPS</td>
<td>195</td>
</tr>
<tr>
<td>Snort IDS, writing rules</td>
<td>259</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force, RFC, 643</td>
</tr>
<tr>
<td>IFB</td>
<td>Invitations For Bids. See RFQ</td>
</tr>
<tr>
<td>ifconfig command</td>
<td>435</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange, 217, 581</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging, 340, 345, 349, 625-627</td>
</tr>
<tr>
<td>IMA</td>
<td>Integrity Measurement Architecture, boot loaders, 318</td>
</tr>
<tr>
<td>imaging disks</td>
<td>464</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol and email, 627</td>
</tr>
<tr>
<td>IMPACT</td>
<td>423</td>
</tr>
<tr>
<td>impact, severity of data breaches</td>
<td>478</td>
</tr>
<tr>
<td>implementation stage (SDLC)</td>
<td>666</td>
</tr>
<tr>
<td>in-house developed applications/software</td>
<td>493</td>
</tr>
</tbody>
</table>
incident response/recovery, 449
  audits, 461
  chain of custody, 461-463, 470-471
  continuity planning, 465
  COOP, 465
  cyber incident response plans, 444
  data breaches, 454-463, 470-471, 478-480
  dcfldd command, 471
  dd command, 471
  disaster recovery, 465-469
  e-discovery, 449-454
  enticement, 83
  entrapment, 83
  events, 83
  foremost command, 477
  forensic analysis, 464
  heuristics/behavioral analytics, 460
  hunt teaming, 460
  incident detection/response, 458
  incident response teams, 454-455, 469
  memcpy command, 476
  nbstat command, 473
  nc command, 475
  netstat command, 474
  policies, 81-82
  post-incident response, 480-481
  process of, 81, 454-457, 461-463, 470-471
  review systems, 461
  rules of engagement, 83
  search/seizure, 463
  security logs, 461
  surveillance, 463
  tcpdump command, 472
  tshark command, 476-477
incremental backups, 466
incremental software development method, 691
inductance-enabled mobile payments, 341
industrial/scientific equipment, 279
INE (In-line Network Encryptors), 198, 231
inference, 498
information
  classifying, 89-90
  disclosure policies, 630
  gathering (reconnaissance), 385
  governance, 148-166
  ISCP, 144
  life cycle of, 89-90
  security, 89-90
  SIEM, 199, 232
  tangible/intangible value/costs (risk assessments), 138-139
Infrastructure mode (WLAN), 308
infrastructures, CIP plans, 144
ingress filters (DLP), 242
inherent risk, risk assessment, 140
initiate/plan phase (SDLC), 674
initiation phase (SDLC), 665
input validation, application vulnerabilities, 360-362, 366
insider threats, incident response/recovery, 459
insurance, HIPAA, 46
integer overflow attacks, 367
integration
  acquisitions, 501
  application integration, 504-507, 564-565
  CI, software development, 698
  cloud computing, 527-530
data flow analysis for changing business needs, 487, 488

data security, 497-500
delegating, networks, 502
demergers/divestitures, 501
deployment diagrams, 502-504
design considerations, 501
diverse industries, 44-51
interoperability issues, 491-494
mergers, 501
resiliency issues, 494-496
resource provisioning/deprovisioning, 500-501
segmenting, networks, 502
standards, 489-490
storage integration, 504
testing, 705
virtualization, 527-530

**integrity**

CIA triad, categorizing data, 99-100
data, 579, 595
file integrity monitoring, 437
integrity services, data flow enforcement, 243

**interfaces**

data, host security, 305
dedicated interfaces, host security, 303-305
design (SDD), 701
loopback interfaces, 305
management interfaces, host security, 304
OOB interfaces, 303
testing, 688
weak interfaces, cloud storage, 337

**interference detection/avoidance**, wireless controllers, 209

internal/external audits, 403-404

**interoperability issues with integrated solutions**, 491-494

inventory control, 450-451, 709
investments (ROI/TCO), 131-134
IoT (Internet of Things), deception technology, 708

IP video, 275

IP-based access control, 277

ipconfig command, 434

IPsec (Internet Protocol Security), 216-218, 260, 301, 580-581

IPS (Intrusion Prevention Systems). See IDS/IPS

IPv4 (Internet Protocol version 4), 222-224

IPv6 (Internet Protocol version 6), 222-224

IR (Infrared) cameras, 444

IrDA (Infrared Data Association), host security, 307

iris scanning (biometrics), 344, 545

IriusRisk, threat modeling, 648

ISA (Interconnection Security Agreements), 72

ISAKMP (Internet Security Association and Key Management Protocol), 217, 581

ISCP (Information System Contingency Plans), 144

ISECOM (Institute for Security and Open Methodologies), OSSTMM, 163

ISMS (Information Security Management Systems), 110-112

ISO (International Organization for Standardization), 52, 110-112, 162, 680

isolating data, data security in integrated solutions, 498
issue-specific security policies (FERMA Risk Management Standard), 166
IT governance, 148-166, 726-727
ITIL (Information Technology Infrastructure Library), 120

J

JAD (Joint Analysis Development) model, software development, 694
Jad Debugger, 441
jailbreaking mobile devices, 339
Java applets, 373-374
JavaScript, 374-376
Javasnoopy, 441
job rotation, security policies, 79
John the Ripper, 428
journaling (remote), 469
JSM (Java Security Model), 374
JSON (JavaScript Object Notation), 372-373
judgment in problem-solving, 187
jurisdictions, 51, 516
JVM (Java Virtual Machines), 373

K

Kali Linux, Metasploit, 423
Kennedy-Kassebaum Act. See HIPAA
Kerberos authentication, 565
kernel proxy firewalls, 204, 233, 236
key escrow, 606
key management, ISAKMP, 581
key recovery, 606
key stretching (key strengthening), 572
keystroke dynamics, authentication, 545
Knapsack, 588
knowledge factor authentication, 538
KnTTools, 384
KPI (Key Performance Indicators), 178-180
KRI (Key Risk Indicators), 178-180
L

L2TP (Layer 2 Tunneling Protocol), 216
laptops
cable locks, 444
TPM chips, 339
latency, analyzing security solutions, 184
launches (measured), 317
laws
Basel II, 48
CFAA, 47
Computer Security Act, 47
diverse industries, integrating, 46-50
Economic Espionage Act, 48-49
ECPSA, 49
EU laws, 49-50
Federal Privacy Act, 47
FISA, 49
FISMA, 47-48
GLBA, 47
Health Care and Education Reconciliation Act, 49
HIPAA, 46
Identity Theft Enforcement and Restitution Act, 47
PCI DSS, 48
PIPEDA, 48
Sarbanes-Oxley (SOX) Act, 46
USA PATRIOT Act, 47-49
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP (Lightweight Directory Access Protocol)</td>
<td>564-565</td>
</tr>
<tr>
<td>leaking data, web conferencing</td>
<td>621</td>
</tr>
<tr>
<td>least functionality, principle of</td>
<td>290</td>
</tr>
<tr>
<td>least privilege, principle of</td>
<td>80-81</td>
</tr>
<tr>
<td>legacy systems, interoperability issues</td>
<td>491</td>
</tr>
<tr>
<td>with integrated solutions</td>
<td></td>
</tr>
<tr>
<td>legal advocacy</td>
<td>70</td>
</tr>
<tr>
<td>legal compliance</td>
<td>70</td>
</tr>
<tr>
<td>legal counsel, security requirements/goals</td>
<td>724</td>
</tr>
<tr>
<td>legal holds</td>
<td>454</td>
</tr>
<tr>
<td>legal ramifications of data breaches</td>
<td>480</td>
</tr>
<tr>
<td>legal requirements, integrating diverse industries</td>
<td>46-50</td>
</tr>
<tr>
<td>lessons learned reports (incident response/recovery)</td>
<td>480</td>
</tr>
<tr>
<td>liabilities (downstream)</td>
<td>58</td>
</tr>
<tr>
<td>libraries</td>
<td></td>
</tr>
<tr>
<td>software libraries</td>
<td>672</td>
</tr>
<tr>
<td>standard libraries</td>
<td>679</td>
</tr>
<tr>
<td>third-party libraries</td>
<td>369</td>
</tr>
<tr>
<td>life cycle of information</td>
<td>89-90</td>
</tr>
<tr>
<td>lightweight code reviews</td>
<td>388, 686</td>
</tr>
<tr>
<td>likelihood of threats</td>
<td>128-130</td>
</tr>
<tr>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>command shell, host security</td>
<td>301</td>
</tr>
<tr>
<td>Kali Linux, Metasploit</td>
<td>423</td>
</tr>
<tr>
<td>passwords</td>
<td>544</td>
</tr>
<tr>
<td>Perl, swatch script</td>
<td>425</td>
</tr>
<tr>
<td>SELinux, trusted OS</td>
<td>289</td>
</tr>
<tr>
<td>live migration, cloud computing virtualization vulnerabilities</td>
<td>529</td>
</tr>
<tr>
<td>load balancers</td>
<td>209-211, 233, 253</td>
</tr>
<tr>
<td>local exploitation frameworks</td>
<td>436</td>
</tr>
<tr>
<td>local policies (Group Policy)</td>
<td>300</td>
</tr>
<tr>
<td>location factor authentication</td>
<td>538</td>
</tr>
<tr>
<td>lockout policies, passwords</td>
<td>543</td>
</tr>
<tr>
<td>locks</td>
<td>441-444, 718</td>
</tr>
<tr>
<td>Logentries</td>
<td>438</td>
</tr>
<tr>
<td>Loggly</td>
<td>438</td>
</tr>
<tr>
<td>logical (technical) controls</td>
<td>106-107, 725</td>
</tr>
<tr>
<td>logical deployment diagrams, integrated solutions</td>
<td>502-504</td>
</tr>
<tr>
<td>logins, credential breaches</td>
<td>624</td>
</tr>
<tr>
<td>logs</td>
<td></td>
</tr>
<tr>
<td>analyzing</td>
<td>425-426, 438-439, 464</td>
</tr>
<tr>
<td>audits, incident response/recovery</td>
<td>461</td>
</tr>
<tr>
<td>collecting SIEM</td>
<td>425</td>
</tr>
<tr>
<td>event log policies (Group Policy)</td>
<td>300</td>
</tr>
<tr>
<td>log reduction/analysis tools</td>
<td>425-426, 438-439</td>
</tr>
<tr>
<td>managing</td>
<td>256-257</td>
</tr>
<tr>
<td>monitoring, endpoint security</td>
<td>295-297</td>
</tr>
<tr>
<td>reviewing</td>
<td>461, 658</td>
</tr>
<tr>
<td>security logs, incident response/recovery</td>
<td>461</td>
</tr>
<tr>
<td>SIEM, log collection</td>
<td>425</td>
</tr>
<tr>
<td>software assurance</td>
<td>677</td>
</tr>
<tr>
<td>transaction log backups</td>
<td>467, 719</td>
</tr>
<tr>
<td>loopback interfaces</td>
<td>305</td>
</tr>
<tr>
<td>Lost Android app</td>
<td>332</td>
</tr>
<tr>
<td>lost/stolen devices</td>
<td>388</td>
</tr>
<tr>
<td>LPE (Local Privilege Escalation)</td>
<td></td>
</tr>
<tr>
<td>attacks</td>
<td>377</td>
</tr>
<tr>
<td>Lpogz.io</td>
<td>438</td>
</tr>
</tbody>
</table>

**M**

<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC (Mandatory Access Control)</td>
<td>551</td>
</tr>
<tr>
<td>MAC addresses, port security</td>
<td>263</td>
</tr>
<tr>
<td>MAC filters, host security</td>
<td>312</td>
</tr>
<tr>
<td>Sticky Mac</td>
<td>263</td>
</tr>
</tbody>
</table>
MAC (Message Authentication Code), 577-578
machine learning/AI (Artificial Intelligence), researching security trends, 653
magnitude of impact (risk impact), 128
maintenance
  analyzing security solutions, 185
  BCP, 148
  documenting, 671
  maintenance/operational stage (SDLC), 666
  release/maintenance phase (SDLC), 676
  SDLC, 670
  temporary roll backs, 670
  updates, 670
malware
  antimalware, 291, 522
  document collaboration, 624
  email, 630
  IM, 626
  mobile device security/privacy, 344
  sandboxing, 383
  social media, 391
  storage collaboration, 624
MAM (Mobile Application Management), 56
man-in-the-middle attacks, 218
management interfaces, host security, 304
management plane (networks), 254
management/administration (executive)
  administrative controls, 104-105
  CEO, 720, 726
  CFO, 721
  CIO, 721
  CPO, 721
CSO, 721
  facilities managers, 723
  physical security managers, 723-724
  security controls/processes, 724-725
  security requirements/goals, 720-721
managing
  accounts, 540-541
  applications, 56, 331
  assets (inventory control), 709
  changes, 670-672, 677
  configurations, 671-672, 677
  content, mobile devices, 331
  context-aware authentication/administration, 334
  data, mobile devices, 331
  events, SIEM, 199, 232
  identity, 540, 559-563, 708
  keys, ISAKMP, 581
  logs, 256-257
  mobile devices, 56-57, 331
  network management/monitoring tools, 255-260
  OOB interfaces, 303
  passwords, 543
  patches, 292-293, 302
  risk. See risk management
  spectrum management and tethering, 342
  state, 376
  storage, HSM, 469
  threats, UTM, 194-195, 230
  top-level management, risk, 54
  user behaviors, 39
  vendors, 41
mandatory vacations, security policies, 80
mantraps, 277
mapping/deployment diagrams, integrated solutions, 502-504
master test plans, 702
MD2 (Message Digest 2) algorithm, hashing, 574
MD4 (Message Digest 4) algorithm, 574
MD5 (Message Digest 5) algorithm, 266, 574
MD6 (Message Digest 6) algorithm, 574
MDM (Mobile Device Management), 56-57, 329
Measured Boot, 318
measured launches, 317
media
analyzing, 464
backup media, 467
libraries, archiving data, 453
medical sensors/devices (wearable technology), 348-350
memcpy command, 476
memory
data-in-memory processing, 581
dumping, 384-385
FATKit, 385
KnTTTools, 384
leaks, application vulnerabilities, 367
Memdump memory-reading tool, 384
memory cards, ownership factor authentication, 539
secure memory and SoC, 272
mergers/acquisitions, 42-44, 501
mesh networks, 228
message authentication, 577-578
Metasploit, 423
metrics (security), 177
availability, 185
capability, 185
cost/benefit analysis, 186
KPI, 178-180
KRI, 178-180
latency, 184
maintainability, 185
performance, 183
recoverability, 186
scalability, 184
usability, 185
microSD HSM, 212, 234
Microsoft Baseline Security Analyzer, 428
Microsoft SDL File/Regex Fuzzer, 685
mics (recording), host security, 314
migration (live), cloud computing virtualization vulnerabilities, 529
MIL, CRR assessments, 169
military/government classifications (information classification), 90
MIME (Multipurpose Internet Mail Extensions), 596
mirroring (screen), mobile devices, 330
misconfigurations/nonmalicious threats, incident response/recovery, 459
misuse case (negative) testing, 687
mitigating risk. See risk management
MMS (Multimedia Messaging Service), mobile device security/privacy, 345
mobile applications, social media attacks, 390
mobile devices. See also wearable technology
applications, 331-335
authentication, 335, 342-344
BYOD, 332
configuration profiles (MDM), 329
containerization, 329
content management, 331
COPE, 332
data management, 331
data storage, 336-338
de-perimeterization, 55-56
encryption, 610
full disk encryption, 718
geolocation, 335
latest attacks, researching, 645
lost/stolen devices, 338
managing, 56-57, 334
personally owned, corporate-enabled mobile device policies, 330
remote assistance, 330
remote wiping, 332, 718
risk management, 55-56
SCEP, 332
security/privacy, 336-341, 344-345, 350
TPM chips, 339
tracking, 718
updates, 331
user behavior and authentication, 335
VPN, 333

mobile payments, 340-341
Mobile Wallet, 341
MODAF (British Ministry of Defense Architecture Framework), 113
monitoring
auditing/monitoring services, data flow enforcement, 243
change monitoring, 247-248
continuous monitoring/improvement, 86, 141
DAM, 214, 240, 634
file integrity monitoring, 437
fitness monitors, 347, 350
logs, endpoint security, 295-297
monitoring/accepting phase (software acquisitions), 679
network management/monitoring tools, 256-260
performance, 669-670
RUM, 687
security, 669-670
synthetic transaction monitoring, 686
user behaviors, 40

motivation (likelihood of threat), 129
MOU (Memorandums Of Understanding), 73
MPTD (Maximum Period Time of Disruption), 146
MSA (Master Service Agreements), 75
MS-CHAP v1 (Microsoft Challenge Handshake Authentication Protocol v1), 224-225
MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol v2), 225
MSRD (Microsoft’s Security Risk Detection), 685
MSSP (Managed Security Service Providers), 527
MTBF (Mean Time Between Failures), 146, 249
MTD (Maximum Tolerable Downtime), 146
MTTR (Mean Time To Repair), 146, 249
multi-factor authentication, 548
multihomed firewalls, 207, 239
multitenancy cloud computing model, public clouds, 515-516
mutation fuzzing, 363, 684
MX (Mail Exchange) records, 395, 506
MyAppSecurity, threat modeling, 648
N

NAC (Network Access Control), 55, 199, 232, 269-271, 644
NAP (Network Access Protection), 269
nbstat command, 473
nc (Netcat) command, 475
NDA (Non-Disclosure Agreements), 74
need-to-know principle, 80-81
negative (misuse case) testing, 687
Nessus, 413, 419
NetBIOS, nbstat command, 473
netstat (network status) command, 429-430, 474
NetworkMiner fingerprinting tool, 386
networks
A/V systems, 278-279
administrators, security requirements/goals, 720
analyzing, 464
authentication, 224-226, 235
automation systems, 274
configuring components, 246-253
control plane, 254
data flow enforcement, 244-245
data plane, 254
de-perimeterization of boundaries, 54-59
delegation, integrated solutions, 502
DLP, 242
enumerators, 420
HVAC controllers, 276
integration solutions, 487-504
IP video, 275
management plane, 254
management/monitoring tools, 255-260
mesh networks, 228
NAC, 55, 269-271, 644
physical access control systems, 277
remote access, 216-237, 240
SAN, 253
scientific/industrial equipment, 279
SDN, 254
security assessment tools, 411-426
segmentation, 269, 502
sensors, 277
testing, 646
virtual networks, researching latest attacks, 645
VLAN, 260-262, 488
VPN, 215-219, 235, 333, 618
vulnerability scanners, 413, 419
new technologies/systems/services,
security trends/threats, researching, 641-642
NFC (Near Field Communication), 307, 340-341
NFS (Number Field Sieve), 587
NGFW (Next-Generation Firewalls), 205, 236
NIDS (Network IDS), 198, 230
NIPS (Network IPS), 197, 230
NIST (National Institute of Standards and Technology)
Framework for Improving Critical Infrastructure Cybersecurity, 160
risk management frameworks, 149-158
SP 800 Series, 115-117, 137, 143, 150-158, 280, 673
Nmap (Network Mapper), 411
no access (authorization), default to, 553
non-removable data storage, 337
nonmalicious threats/misconfigurations, incident response/recovery, 459
nonpersistent agents (NAC), 270
nonpersistent/persistent data, resiliency issues with integrated solutions, 495
NOP (No-Operation) slides, 365-366
notifications (push), mobile device security/privacy, 339
NPV (Net Present Value), ROI, 132
NS records (DNS), 395
nslookup command, 396-397, 435
numeric passwords, 542
NX (No Execute) bits (processors), 682

O

OAKLEY, 581
OAuth (Open Authorization), 553
object tracking technologies, 709-711
occupant emergency plans, 144
OCSP (Online Certificate Status Protocol), 604, 608
OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), 120
OEM/carrier Android fragmentation, 340
OFB (Output Feedback) mode (DES), 601
OLA (Operating-Level Agreements), 73
OllyDbg, 441
on-premise cloud computing, 515
onsite assessments, 53
OOB (Out-of-Band) interfaces, host security, 303
OpenID, 561
open message format, asymmetric cryptography, 586
open source software, interoperability issues with integrated solutions, 493
open standards, 489
OpenSSL, 436
operating system (container-based) virtualization, 520
operational activities (SDLC), 669-673
operational/maintenance stage (SDLC), 666
optical jukeboxes, 469
Orange Book (TCSEC), 287
order of volatility (evidence collection), 470-471
organizational security policies (FERMA Risk Management Standard), 165
OS (Operating Systems)
fingerprinting, 657
secure enclaves, 371
trusted OS, 287-290
vulnerabilities, 377
OSA (Open Source Authentication), host security, 312
OSINT (Open Source Intelligence), 390-397
OSSTMM (Open Source Security Testing Methodology Manual), 163
OTP (One-Time Passwords), 542
outages
BCP outage impacts/downtime, 146
revenue loss during outages, ROI, 131
outsourcing, 41, 58-59
over-the-air updates, 331
over the shoulder code reviews, 388
overwriting hard drives, 673
OWASP (Open Web Application Security Project), 355, 362, 648, 680
ownership
data, 43, 452, 499
factor authentication, 538-539
TCO, 133-134, 186
P
PaaS (Platform as a Service), public clouds, 516
packets
  capturing, 657
  deep packet inspection, 242
  filtering, 202-204, 236
  NOP slides, 365
  sniffing, 414-415. See also eavesdropping
pair programming, 388
palm/hand scans, authentication, 545
PAP (Password Authentication Protocol), 224-225, 394
partial-knowledge testing, 400
partnerships
  downstream liability, 58
  risk management, 40, 58
  TCA, 40
passive fingerprinting tools, 386
passwords, 224-225, 394, 427-428, 540-544
patches, 292-293, 302
path tracing, 465
pattern matching, signature-based
  IDS/IPS, 195
payback (ROI), 132
payloads, configuration profiles (MDM), 329
payments (mobile), 340-341
PCI DSS (Payment Card Industry Data Security Standard), 48
PCR (Platform Configuration Register) hashes, TPM chips, 320
PDP (Policy Decision Points), 555
Peach, 421, 684
peer reviews, 706
penetration testing, 384-385, 398-401, 667, 670
PEP (Policy Enforcement Points), 555
performance
  baselines, 669
  monitoring, 669-670
  security solutions, analyzing, 183
peripheral devices
  host security, 305-313
  mobile payments (credit card readers), 341
Perl, swatch script, 425
permissions
  application permissions, 333
  granting, 719
  SCAP scanners, 418
persistent/nonpersistent data,
  resiliency issues with integrated solutions, 495
persistent/volatile agents (NAC), 270
personal data theft, wearable technology security/privacy, 350
personal information, PIPEDA, 48
personally owned, corporate-enabled mobile device policies, 330
personnel
  BCP, 142
  hiring, 85-86
  occupant emergency plans, 144
  screening, 85
  terminating, 86
  testing, 646
PFS (Perfect Forward Secrecy), 578
PGP (Pretty Good Privacy), 594, 629
pharming, 389
phishing, 388, 628, 659
physical access control systems, 277
physical controls, 107-108
physical deployment diagrams, integrated solutions, 502-504
physical reconnaissance, wearable technology security/privacy, 349
physical security controls/processes, 725
physical security managers, 723-724
tools, 441-444
physical testing, 646
physiological characteristics (authentication), 539, 544-545
PII (Personally Identifiable Information), 77
PIN, mobile device authentication, 343
ping command, 431-432
ping scans, 386
pinning (public key), 608
PIPEDA (Personal Information Protection and Electronic Documents Act), 48
pivoting, 389
PKI (Public Key Infrastructure)/digital certificates, 548, 603-608
plan/initiate phase (SDLC), 674
planning BCP, 141-148
CIP plans, 144
continuity planning, 465
COOP, 144, 465
crisis communications plans, 144
cyber incident response plans, 144
DRP, 144
ERP, 505
incident response plans, updating, 481
ISCP, 144
occupant emergency plans, 144
testing plans, 702-704
worst-case (extreme) scenario planning, 123-125
planning phase (software acquisitions), 679
platforms PaaS, public clouds, 516
single platform hosts, virtualization and data security, 530
PLC (Programmable Logic Controllers), SCADA, 279
poisoning DNS caches, 506
policies access control policies, 553
account policies (Group Policy), 300
application wrapping, 330
baselines, 167
BCP policies, developing, 144
BYOD policies, 68
categories of, 167
COPE, 332
data handling policies, 453-454
data retention policies, 451, 500
defined, 65
disclosure policies, 630
diverse industries, integrating, 45
event log policies (Group Policy), 301
FERMA Risk Management Standard, 165-166
file system policies (Group Policy), 301
guidelines, 167
incident response policies, 81-82
IPsec policies on Active Directory (Group Policy), 301
life cycle of, 66
local policies (Group Policy), 300
NAC policies, 644
PDP, 555
PEP, 555
personally-owned, corporate-enabled mobile device policies, 330
principles of privacy (eu), 49
print recognition, authentication, 546
privacy/security
CPO, 721
EU Principles of Privacy, 49
EU Safe Harbor Privacy Principles, 49
Federal Privacy Act, 47
health privacy, wearable technology
security/privacy, 350
impact ratings, 675
incident response/recovery, 458
mobile devices, 336-345, 350
PGP, 594, 629
PII, 77
policies, 458
wearable technology, 349-350
private clouds, 42, 513-514, 651
principles of privacy (eu), 49
print recognition, authentication, 546
privacy/security
CPO, 721
EU Principles of Privacy, 49
EU Safe Harbor Privacy Principles, 49
Federal Privacy Act, 47
health privacy, wearable technology
security/privacy, 350
impact ratings, 675
incident response/recovery, 458
mobile devices, 336-345, 350
PGP, 594, 629
PII, 77
policies, 458
wearable technology, 349-350
private clouds, 42, 513-514, 651
privileges
elevation of, 528
escalation of, 362, 377
least privilege, principle of, 80-81
PRL (Preferred Roaming List)
updates, 331
PRNG (Pseudo-Random Number Generators), 578
problem-solving, judgment in, 187
procedural design (SDD), 701
procedures
defined, 65-67, 167
employment procedures, 85-86
reviewing, 68-70
types of, 67
updating, 68-70
processes
BCP critical processes/resources, 145
defined, 65-66, 167
forensic investigations, 84

POP (Post Office Protocol), 627
portable media devices, inventory/asset control, 450
ports
authentication, 802.1x, 226, 235
encryption, 591
HDMI ports, host security, 315
scanners, 411
SD ports, host security, 315
security, 262-265, 305
system ports, assigning, 264
TCP/UDP port numbers, 265
post-incident response (incident response/recovery), 480-481
PPP (Point-to-Point Protocol), 394, 618
PPTP (Point-to-Point Tunneling Protocol), 216
presence (user availability), 626-627
preventive controls, 104, 147
PRI (Product Release Information)
updates, 331
life cycle of, 66
reviewing, 53, 67
risk assessment, 137
types of, 67
updating, 67
processors, 682
productivity loss, ROI, 131
profiling, social media, 659
programmers, security requirements/goals, 718-719
proposals (bidding), RFP, 76
protection profiles (CC), 288-289
protocols
    analyzers, 257-258, 414-415
    anomaly-based IDS/IPS, 196
    interoperability issues with integrated solutions, 494
prototyping
    security solutions, 181
    software development method, 691
provisional accreditation, 676
provisioning/deprovisioning resources, integrated solutions, 500-501, 531
proxies, remote access networks, 233
proximity authentication devices, 442
proximity readers, 277
proxy firewalls, 203-204, 233, 236
proxy servers, 210
PST (Provisioning Service Targets), SPML, 556
public clouds, 41, 513-516, 651
public key cryptography, digital signatures, 577
public key pinning, 608
public key policies (Group Policy), 301
purging data, 369, 453, 497
push notification services, mobile device security/privacy, 339
push-based authentication, 550
PVS (Passive Vulnerability Scanners), 213
qualitative risk analysis, 126-127
quality of coding, 683
quantitative risk analysis, 127
quarantine/remediation (NAC), 270
quotes (bidding), RFQ, 76
radio frequencies
    restrictions, mobile device security, 336
    spectrum management, 342
RADIUS (Remote Authentication Dial-In User Service), 226, 563-564
RAID (Redundant Array of Inexpensive/Independent Disks), 249-253
Rainbow Series (TCSEC), 287
ransomware, 647
RAT (Remote Access Trojans), 647
RBAC (Role-Based Access Control), 81, 551
RC4, 584-585
RC5, 584-585
RC6, 584-585
RDBMS (Relational Database Management System), identity propagation, 558
RDP (Remote Desktop Protocol), 220
reclassification of data, 44
reconnaissance
  information-gathering, 385
  physical reconnaissance, wearable technology security/privacy, 349
record-level encryption, 589-591
recording mics, host security, 314
recoverability, analyzing security solutions, 186
recovery
  BCP recovery priorities, 147-148
data recovery, 451-452
  MTBF, 146
  MTD, 146
  recovery controls, 104
  RPO, 146
  RTO, 146
  WRT, 146
red team exercises, security assessments, 405
reducing
  attack surfaces, 206
  risk, 135-137
redundancy
  hardware, 248
  resiliency issues with integrated solutions, 496
Regex Fuzzer, 685
registry policies (Group Policy), 300
regression testing, 678, 706
regulations
  diverse industries, integrating, 45-50
  EU regulations, 49-50
  export controls, 45
  policies/procedures, updating, 69
  regulatory entities, 53
release/maintenance phase (SDLC), 676
remanence, 454
remediation/quarantine (NAC), 270
remnants (data), 673
  application vulnerabilities, 369
  cloud computing virtualization vulnerabilities, 529
  data security in integrated solutions, 497-498
  resource provisioning/deprovisioning, 501, 531
remote access
  application sharing, 619-620
desktop sharing, 619-620
dial-up connections, 617-618
  network design, 215-226, 229-237, 240
  RAT, 647
remote administration, 618
remote assistance, 620-621
resources/services, 618
SSL, 618
VPN, 216, 618
remote activation/deactivation (unauthorized), wearable technology security/privacy, 349
remote administration, 618
remote assistance, 330, 620-621
remote journaling, 469
remote locks, mobile devices, 718
remote wiping devices, 332, 450, 718
removable data storage, 337
repairs
  costs, ROI, 131
  MTTR, 146
replication, backups, 469
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>reports</td>
<td>834</td>
</tr>
<tr>
<td>after-action reports, security control</td>
<td>177</td>
</tr>
<tr>
<td>reviews</td>
<td>404</td>
</tr>
<tr>
<td>SOC reports</td>
<td>404</td>
</tr>
<tr>
<td>reputation (ROI), loss of</td>
<td>131</td>
</tr>
<tr>
<td>Request Timed Out code (ping command)</td>
<td>432</td>
</tr>
<tr>
<td>requirements/goals</td>
<td>700</td>
</tr>
<tr>
<td>gather phase (SDLC), 674</td>
<td></td>
</tr>
<tr>
<td>requirements definitions lists, 701</td>
<td></td>
</tr>
<tr>
<td>security, 717-724</td>
<td></td>
</tr>
<tr>
<td>SRTM documents, 700</td>
<td></td>
</tr>
<tr>
<td>researching security trends/threats</td>
<td>640-641</td>
</tr>
<tr>
<td>best practices, 640-641</td>
<td></td>
</tr>
<tr>
<td>emerging business tools, 651-653</td>
<td></td>
</tr>
<tr>
<td>emerging threat sources, 660</td>
<td></td>
</tr>
<tr>
<td>security, 642</td>
<td></td>
</tr>
<tr>
<td>evolving technologies, 642</td>
<td></td>
</tr>
<tr>
<td>global IA industry/community, 653-659</td>
<td></td>
</tr>
<tr>
<td>new technologies/systems/services, 641-642</td>
<td></td>
</tr>
<tr>
<td>RFC, 643</td>
<td></td>
</tr>
<tr>
<td>threat intelligence, 643-649</td>
<td></td>
</tr>
<tr>
<td>resetting passwords, 543</td>
<td></td>
</tr>
<tr>
<td>residual risk, risk assessment, 140</td>
<td></td>
</tr>
<tr>
<td>resiliency issues with integrated solutions, 494-496</td>
<td></td>
</tr>
<tr>
<td>resources</td>
<td>145</td>
</tr>
<tr>
<td>BCP critical processes/resources, 145</td>
<td></td>
</tr>
<tr>
<td>BCP resource requirements, 147</td>
<td></td>
</tr>
<tr>
<td>exhaustion, application vulnerabilities, 368</td>
<td></td>
</tr>
<tr>
<td>provisioning/deprovisioning, 500-501, 531</td>
<td></td>
</tr>
<tr>
<td>REST (Representational State Transfer), 372-373</td>
<td></td>
</tr>
<tr>
<td>restricted group policies (Group Policy), 300</td>
<td></td>
</tr>
<tr>
<td>retaining data, 451, 500</td>
<td></td>
</tr>
<tr>
<td>retina scans, authentication, 545</td>
<td></td>
</tr>
<tr>
<td>reusing</td>
<td>370</td>
</tr>
<tr>
<td>assets, 673</td>
<td></td>
</tr>
<tr>
<td>codes, application vulnerabilities, 370</td>
<td></td>
</tr>
<tr>
<td>revenue loss during outage, ROI, 131</td>
<td></td>
</tr>
<tr>
<td>reverse engineering, 177, 440-441, 464</td>
<td></td>
</tr>
<tr>
<td>reverse proxies, 222, 235</td>
<td></td>
</tr>
<tr>
<td>review systems, incident response/recovery, 461</td>
<td></td>
</tr>
<tr>
<td>reviewing</td>
<td>658</td>
</tr>
<tr>
<td>code, 387-388</td>
<td></td>
</tr>
<tr>
<td>logs, 658</td>
<td></td>
</tr>
<tr>
<td>policies, 66-70</td>
<td></td>
</tr>
<tr>
<td>procedures, 68-70</td>
<td></td>
</tr>
<tr>
<td>processes, 67</td>
<td></td>
</tr>
<tr>
<td>security controls, 175-177</td>
<td></td>
</tr>
<tr>
<td>RF (Radio Frequencies), host security,</td>
<td>308-311</td>
</tr>
<tr>
<td>308-311</td>
<td></td>
</tr>
<tr>
<td>RFC (Requests For Comments), 643</td>
<td></td>
</tr>
<tr>
<td>RFC 2138, RADIUS, 564</td>
<td></td>
</tr>
<tr>
<td>RFI (Requests For Information), 76</td>
<td></td>
</tr>
<tr>
<td>RFID (Radio Frequency Identification), 313, 444, 710-711</td>
<td></td>
</tr>
<tr>
<td>RFP (Requests For Proposal), 76</td>
<td></td>
</tr>
<tr>
<td>RFQ (Requests For Quotes), 76</td>
<td></td>
</tr>
<tr>
<td>Rijndael algorithm, AES, 583</td>
<td></td>
</tr>
<tr>
<td>RIPEMD-160, 576</td>
<td></td>
</tr>
<tr>
<td>risk management/mitigation, 726-727</td>
<td></td>
</tr>
<tr>
<td>access controls, 103-108</td>
<td></td>
</tr>
<tr>
<td>acquisitions/mergers, 42-43</td>
<td></td>
</tr>
<tr>
<td>analysis, 125-127, 678</td>
<td></td>
</tr>
<tr>
<td>appetite, defined, 135</td>
<td></td>
</tr>
<tr>
<td>assessments, 125-126, 137-140</td>
<td></td>
</tr>
<tr>
<td>auditors, 52</td>
<td></td>
</tr>
<tr>
<td>BCP, 141-148</td>
<td></td>
</tr>
<tr>
<td>BYOD, 56, 57</td>
<td></td>
</tr>
</tbody>
</table>
CIA, 98-102
client requirements, 53
clouds, 41-42, 55
competitors, 52
continuous improvement/monitoring, 141
COSO ERM, 163
CRR assessments, 168-169
detection, MSRD, 685
diverse industries, integrating, 44-51
divestitures/demergers, 42-43
downstream liability, 58
due care, 59
due diligence, 59
emerging risks, updating policies/procedures, 70
FERMA Risk Management Standard, 164-166
impact of (magnitude of risk), 128
ISO/IES 27005:2008 risk management process, 162
IT governance, 148-166
likelihood of threats, 128-130
magnitude of impact (risk impact), 128
mobile devices, 55-56
network boundaries, 54-59
NIST Framework for Improving Critical Infrastructure Cybersecurity, 160
OSSTMM, 163
outsourcing, 41, 58-59
partnerships, 40
policies/procedures, 70
profiles, 39
reduction, 135-137
regulatory entities, 53
risk analysis, 125-127
risk assessments, 125-126, 137-140
risk management frameworks, NIST, 149-158
risk profiles, 39
risk reduction, 135-137
ROI, 131-132
security control frameworks, 109-120, 123, 162-163
software assurance, 678
source code escrow, 39
SRTM, 108
TCO, 133-134
technical risk, translating in business terms, 134-135
telecommuting, 55
top-level management, 54
updating policies/procedures, 70
user behaviors, 39
worst-case (extreme) scenario planning, 123-125
Rivest and RSA, Ron, 586-587
robo hunters, 708
ROI (Return on Investment), 131, 186
roll backs (temporary), 670
root-cause analysis (incident response/recovery), 480
rooting mobile devices, 339
rotating jobs, security policies, 79
rotation schemes (backups), 467-468
routers
access lists, 305
ACL, 54, 210, 658
MD5 authentication, 266
network segmentation, 269
remote access networks, 233
route protection, 266
RTBH routing, 267
security, 210
transport security, 260
trunking security, 260-262
routing tables, 392-394
RPO (Recovery Point Objective), 146
RSA, 586-587, 655
RTBH (Remotely Triggered Black Hole) routing, 267
RTO (Recovery Time Objective), 146
RTU (Remote Terminal Units), SCADA, 279
rules
access control, 552
diverse industries, integrating, 44-45
engagement, incident response, 83
export controls, 45
IDS/IPS, 196
Snort IDS rules, writing, 259
RUM (Real User Monitoring), 687
runtime data integrity checks, SoC, 273
runtime debugging, 385

S
S/flow (Sampled Flow), data flow enforcement, 244
S/MIME (Secure MIME), 596
SA (Security Associations), IPsec, 580
SaaS (Software as a Service), public clouds, 516
SABSA (Sherwood Applied Business Security Architecture), 113-114
Safe Harbor Privacy Principles (EU), 49
safe harbors, 50
sales staff, security requirements/goals, 717-718
same-origin policies (AJAX), 374
SAML (Security Assertion Markup Language), 560-562
sandboxing, 370, 383, 525
SAN (Storage Area Networks), 253
Sarbanes-Oxley (SOX) Act, 46
SAS (Statement on Auditing Standards) 70, 403
SC (Security Categories), aggregate CIA scoring, 101-102
SCADA (Supervisory Control and Data Acquisition), 279-280
scalability, analyzing security solutions, 184
scanners
SCAP scanners, 416-419
vulnerability scanners, 213-214, 235
SCAP (Security Content Automation Protocol), 416-419, 437
SCEP (Simple Certificate Enrollment Protocol), mobile devices, 332
scientific/industrial equipment, 279
scope
BCP, 142
severity of data breaches, 478
scoring (aggregate CIA), 101-102
screen mirroring, mobile devices, 330
screened host firewalls, 207-208, 239
screened subnets, 208, 239
screening personnel, 85
scripting (XSS), application vulnerabilities, 356
scrubbing, defined, 296
SD Elements, threat modeling, 649
SD ports, host security, 315
SDD (Software Design Documents), 701
SDL File/Regex Fuzzer, 685
security

SDLC (Systems Development Life Cycle), 665-673
SDN (Software-Defined Networking), 254
sealing TPM chips, 319
SEAndroid (Security-Enhanced Android), 289
search engines, 397
search/seizure (incident response/recovery), 463
search warrants, 463
SecaaS (Security as a Service), 527
secure boot, 317
secure enclaves, 371, 521
secure message format, asymmetric cryptography, 586
secure volumes, 521
securiCAD, threat modeling, 648
security
access controls, 103-108
analyzing solutions, 184-186
assessments, 383-405, 411, 414-444
auditing, 88
awareness training, 86-87
BIA, 72
BPA, 74
categorizing data, 98-102
CIA, 98-102
Computer Security Act, 47
contracts, 75-77
controls/processes, 175-177, 724-725
credit cards, 580, 590
data categorization, 98-102
deconstructing/reverse engineering security solutions, 177
employment procedures, 85-86
EU Electronic Security Directive, 50
events versus incidents, 83
FISMA, 47-48
forensic investigations, 84
IA, 72
incident response, 81-83
information, 89-90
ISA, 72
logs, incident response/recovery, 461
metrics, 177-180, 183-186
mobile devices, 336-345, 350
monitoring, 86, 669-670
MOU, 73
MSA, 75
NDA, 74
OLA, 73
PCI DSS, 48
physical security, 723-725
policies, 78-82
port security, 262-265
prototyping solutions, 181
RA, 71-72
requirements/goals, 717-724
reverse engineering/deconstructing security solutions, 177
routers, 210, 266-267
security control frameworks, 109-123, 162-163
SLA, 73
SRTM, 108
testing solutions, 181
threats, likelihood of, 128-130
training, 86-87
transport security, 260
trends/threats, researching, 640-660, 708-709
trunking security, 260-262
unauthorized remote activation/deactivation, 349
wearable technology, 349-350
worst-case (extreme) scenario planning, 123-125
zones, 268-269
segmenting networks, integrated solution, 502
seizure (search and), incident response/recovery, 463
self-assessments (security-based), 402
SELinux (Security-Enhanced Linux), trusted OS, 289
sensitive data, improper storage of, 362
sensors, 277-279
separation of duties, security policies, 78-79
sequence-based versioning, 698
servers
  application virtualization (terminal services), 322-323
  client-side processing versus, 371-376
  email servers and spam, 629
  proxy servers, 210
RADIUS servers, 564
resource provisioning/deprovisioning, 501
single server hosts, virtualization and data security, 530
service packs, patch management, 293
services
  discovery, 657
  remote access, 618
  security trends/threats, researching, 641-642
session hijacking, 359
SET (Secure Electronic Transactions), 580
SFC (System File Checker), switches, 437-438
SGX (Software Guard Extensions), 581
SHA-0 (Secure Hash Algorithm 0), 575
SHA-1 (Secure Hash Algorithm 1), 575
SHA-2 (Secure Hash Algorithm 2), 575
SHA-3 (Secure Hash Algorithm 3), 575
Shamir and RSA, Adi, 586-587
sharing applications/desktops, 619-620
Shibboleth, 561-562
shoulder surfing, 389
SHTTP (Secure HTTP), 580
side loading applications, 334
SIEM (Security Information and Event Management), 199, 232, 425-426
signatures
  digital, 576-577
  electronic, 50
  IDS/IPS, 195
  signature dynamics, authentication, 545
SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions), 627
single platform hosts, virtualization and data security, 530
single server hosts, virtualization and data security, 530
single-factor authentication, 538
single-tenancy cloud computing model, 515
site-to-site VPN, 216-217
Six Sigma, 121
SKA (Shared Key Authentication), host security, 313
Skipjack, 584-585
slack space analysis, 464
SLA (Service-Level Agreements), 73, 249, 531
SLE (Single Loss Expectancy), magnitude of risk (risk impact), 128
SLIP (Serial Line Internet Protocol), dial-up connections, 618
smart cards, ownership factor authentication, 539
smart watches, 346
SMS (Short Message Service), mobile device security/privacy, 345
SMTP (Simple Mail Transfer Protocol), 628
sniffing (packet), 257-258, 414-415. See also eavesdropping
snooping, VoIP, 631
Snort IDS, writing rules, 259
SOA (Service-Oriented Architectures), integration solutions, 506
SOA (Statements of Applicability), 72
SOA records (DNS), 395
SOAP (Simple Object Access Protocol), 376. See also WSS
SoC (System on a Chip), 271-274, 345
SOC reports, 404
social engineering attacks, 388-389, 626, 659
social media
  collaboration sites, 632
evolving platforms, 650
malware, 391
OSINT, 390-391
policies, 391
profiling, 659
trust an, 390
software
  acceptance testing, 678
acquiring, 679
analyzing, 464
antimalware, 291
antispyware, 291
antivirus software, 291, 439
assurance, 677-688
COTS software, 493
deploying, secure design, 356
development, 673-677, 680-706
development methods, 688
IaaS, public clouds, 516
in-house developed applications/software, 493
libraries, 672
open source software, 493
regression testing, 678
SaaS, public clouds, 516
secure design, 355
standard libraries, 679
tailored commercial (commercial customized) software, 493
updates, 670
vulnerabilities, 356-370
Software Verify tool, runtime debugging, 385
Solaris 10, TrustedSolaris, 290
source (likelihood of threat), 130
source code escrow, 39
sovereignty of data, 50-51, 499
SOW (Statements of Work), 75
SP 800-12 Rev. 1, 115
SP 800-16 Rev. 1, 115
SP 800-18 Rev. 1, 115
SP 800-30 Rev. 1, 115, 137
SP 800-34 Rev. 1, 115, 143
SP 800-35, 115
SP 800-36, 115
SP 800-37 Rev. 1, 115, 156-158
SP 800-39, 116, 158
SP 800-50, 116
SP 800-53 Rev. 4, 116
SP 800-53A Rev. 4, 116, 152-153
SP 800-55 Rev. 1, 116
SP 800-60 Vol. 1 Rev. 1, 116, 150-151
SP 800-61 Rev. 2, 116
SP 800-82 Rev. 2, 116, 280
SP 800-84, 116
SP 800-86, 116
SP 800-88 Rev. 1, 116, 673
SP 800-92, 116
SP 800-101 Rev. 1, 116
SP 800-115, 116
SP 800-122, 116
SP 800-123, 116
SP 800-124 Rev. 1, 116
SP 800-137, 116
SP 800-144, 117
SP 800-145, 117
SP 800-146, 117
SP 800-150, 117
SP 800-153, 117
SP 800-154 (Draft), 117
SP 800-160, 117, 153-156
SP 800-161, 117
SP 800-162, 117
SP 800-163, 117
SP 800-164, 117
SP 800-167, 117
SP 800-175A and B, 117
SP 800-181, 117
SP 800-183, 117
spam, 292, 523, 629
spear phishing, 628
spectrum management and tethering, 342
SPF (Sender Policy Framework), email validating, 628
spiral model, software development, 692, 698
SPML (Service Provisioning Markup Language), 556
SPOF (Single Point of Failure), 253
spoofing attacks, 261, 522, 628
spyware, 291
SQL injection attacks, 360-362
SRK (Storage Root Keys), TPM chips, 319
SRTM (Security Requirements Traceability Matrix), 108, 700
SSAE 16 audits, 404
SSH (Secure Shell), 220, 595
SSID (Service Set Identifiers), 308, 312
SSL (Secure Sockets Layer), 218, 579, 595, 618
SSO (Single Sign-On), 540, 548-549, 558-560, 565
stakeholders, security, 100, 717-726
standard libraries, 679
standard word passwords, 541
standards, 167
adherence to, 489
competing standards, integration solutions, 490
de facto standards, integrate solutions, 490
ISO/IEC 27000 series, software development best practices, 680
lack of standards in integration solutions, 490
open standards, 489
secure coding standards, 700
stapling (OCSP), 608
stateful firewalls, 202-203
stateful matching, signature-based
IDS/IPS, 195
state management, 376
static passwords, 541
static testing, 686
statistical anomaly–based IDS/IPS, 196
steganography, 464, 591
Sticky Mac, 263
stolen/lost devices, 338
storage
\begin{itemize}
  \item cloud storage (end-user), 650
  \item collaboration tools, 624-625
  \item cookies, 364
  \item data storage, 336-338, 362, 451-452
  \item encryption, 589-590
  \item HSM, 469
  \item integration solutions, 487-504
  \item media, disposal of, 453
\end{itemize}
storage keys, TPM chips, 320
stream ciphers, 584-585, 597-598
subnets (screened), 208, 239
surveillance, 275, 463
swatch script (Perl), 425
swipe patterns, mobile device authentication, 343
switches
\begin{itemize}
  \item network segmentation, 269
  \item port security, 262-265, 305
  \item remote access networks, 232
  \item SFC, 437-438
  \item spoofing, 261
  \item transparent bridging, 201
  \item transport security, 260
  \item trunking security, 260-262
\end{itemize}
symmetric algorithms, 582-585, 599-602
symmetric cryptography, 588, 602
synthetic transaction monitoring, 686
Sysinternals, 435-436
systems
\begin{itemize}
  \item applications, 334
  \item failures (authentication), cloud storage, 337
  \item lock down. See configuring, configuration lockdown
  \item ports, assigning, 264
  \item process criticality, severity of data breaches, 479
  \item requirements (SDLC), 667
  \item security policies (FERMA Risk Management Standard), 166
  \item security trends/threats, researching, 641-642
  \item services policies (Group Policy), 300
  \item testing, 646
\end{itemize}
tabletop exercises, security self-assessments, 403
TACACS+ (Terminal Access Controller Access-Control System Plus), 226
tags
\begin{itemize}
  \item ARAT systems (RFID), 710
  \item ARPT systems (RFID), 710
  \item double tagging, 261
  \item RFID tags, 313
  \item trunking security, 261
tailgating, 277
tailored commercial (commercial customized) software, 493
tampering, anti-tamper technology, 338
tape vaulting, 469
target penetration testing, 399
Tastic RFID Thief, 444
Tavares and CAST, Stafford, 585
TCA (Third-Party Connection Agreements), 40
TCO (Total Cost of Ownership), 133-134, 186
TCP/UDP, port numbers, 265
tcpdump command, 472
TCSEC (Trusted Computer System Evaluation Criteria), 287. See also CC
TDE (Transparent Data Encryption), 719
TDF (Trusted Data Format), 494
technical (logical) controls, 106-107, 725
technical risk, translating in business terms, 134-135
technologies, researching security trends/threats, 641-642
telecommuting, 55, 618
telemetry systems, SCADA, 279
telephony systems, 630-632
temporal metric group (CVSS), 416
temporary roll backs, 670
Teredo, 223
terminal services, host security, 322-323
terminating personnel, 86
test data method, 668
test/evaluation phase (SDLC), 668
tests
  acceptance testing, 678, 704
  BCP, 148
  black box (zero-knowledge) testing, 400-401
  blind penetration testing, 399
  document exchanged/reviews, 53
  double-blind penetration testing, 399
dynamic testing, 686
  formal code reviews, 686
  full-knowledge testing, 400
  fuzzing, 363, 683-684
  gray box testing, 400-401
  GUI testing, 688
  integration testing, 705
  interface testing, 688
  level-specific test plans, 702
  lightweight code reviews, 686
  misuse case (negative) testing, 687
  network testing, 646
  onsite assessments, 53
  partial-knowledge testing, 400
  peer reviews, 706
  penetration testing, 398-401, 667, 670
  personnel testing, 646
  physical testing, 646
  policy reviews, 53
  process reviews, 53
  regression testing, 678, 706
  security solutions, 181
  static testing, 686
  systems testing, 646
  target penetration testing, 399
test coverage analysis, 687
test data method, 676
test/validate phase (SDLC), 676
testing plans, 702-704
type-specific test plans, 702
unit testing, 704
user acceptance testing, 705
validation testing, 676, 704
verification testing, 676
white box testing, 400-401
zero-knowledge (black box) testing, 400-401
tethering, 341-342

texting
  collaboration risks, 625, 626
  encrypted IM, mobile device security/privacy, 340
  encrypted/unencrypted communication, wearable technology security/privacy, 349
  MMS, 345
  mobile device security/privacy, 340, 345
thief of personal data and wearable technology security/privacy, 350
third-party libraries, application vulnerabilities, 369
third-party outsourcing, 41, 58-59

threats
  agents, 139
  best practices, 640-641
  current threats, knowledge of, 646-647
  emerging business tools, 650-653
  emerging threats, 660, 706-707
  evolving technologies, 642
  global IA industry/community, 653-659
  identifying, risk assessments, 139
  insider threats, 459
  likelihood of threats, 128-130
  modeling, 648-649
  new technologies/systems/services, 641-642
  nonmalicious threats/misconfigurations, 459
  RFC, 643
  robo hunters, 708
  threat actors, 655-659
  threat intelligence, 643-649, 707
  Threat Modeling Tool, 648
  UTM, 194-195, 230
three-legged firewalls, 207, 239

throughput rate (biometrics), 546
time of check/time of use attacks, 367-368
time-based restrictions, mobile device security, 336
TLS (Transport Layer Security), 218-219, 579, 595
TOGAF (The Open Group Architecture Framework), 113
token devices, ownership factor authentication, 539
tokenization, mobile device security/privacy, 340
tokens, 607
top-level management, risk management, 54
topology discovery, 656
TOTP (Time-Based One-Time Password) algorithm, authentication, 540
TPM (Trusted Platform Module) chips, 315, 319-320, 339, 520, 558
traceroute tool, 395
tracert tool, 395
tracert/traceroute command, 433
tracing paths, 465

tracking
  devices, 450
  fitness trackers, 347, 350
  geolocation/GPS devices, 709-711
  mobile device, 718
  object tracking technologies, 709-711
  unauthorized tracking, 624
traffic anomaly-based IDS/IPS, 196
training, BCP training/exercises, 148
transaction log backups, 467, 719
transactional security, 580
transfer risk reduction strategy, 136
transferring data to uncontrolled storage, 338
transparent bridging, 201
transponders (RFID), 313
transport security, 260
Treadway Commission Framework, COSO, 119
trends/threats of security, researching
- analysis, 130, 182-183, 424
- best practices, 640-641
- emerging business tools, 650-653
- emerging threat sources, 660
- evolving technologies, 642
- global IA industry/community, 653-659
- new technologies/systems/services, 641-642
- RFC, 643
- threat intelligence, 643-649
Trojans, 626, 647
trunking security, 260-262
trust
- circles of (SAML), 560
- social media and, 390
trusted OS (Operating Systems), 287-290
trusted third-part (bridge) model (federated identities), 560
TrustedSolaris, 290
tshark command, 476-477
TSIG (Transaction Signatures), 506
TT&E (Testing, Training and Exercises), BCP, 148
TTL (Time to Live), DNS records, 506
tumbler locks, 442
Twofish, 584, 585
Type 1 hypervisors, 519
Type 2 hypervisors, 519
Type I errors. See FRR
Type II. See FAR
Type III authentication. See characteristic factor authentication

UDP (User Datagram Protocol), port numbers, 265
UEFI (Unified Extensible Firmware Interface), boot loaders, 318
unauthorized domain bridging, mobile device security/privacy, 344
unauthorized remote activation/deactivation, wearable technology security/privacy, 349
uncontrolled storage, transferring/backing up data to, 338
unencrypted/encrypted communication, wearable technology security/privacy, 349
unified collaboration tools, 621-634
uninvited guests, web conferencing, 621
unit testing, 704
UNIX
- command shell, host security, 301
- passwords, 544
- traceroute tool, 395
unsecure direct object references, application vulnerabilities, 356
unsigned applications, 334
updates
- firmware, 316, 377
- FOTA updates, 331
- incident response plans, 481
- mobile devices, 331
- over-the-air updates, 331
- patches, 292-293, 302
policies, 67-70
PRI updates, 331
PRL updates, 331
procedures, 68-70
processes, 67
temporary roll backs, 670
Zeeis updates, 331
URL (Uniform Resource Locators),
document collaboration, 624
usability, analyzing security solutions, 185
USA PATRIOT Act, 47-49
USB (Universal Serial Bus) devices,
306, 338, 342, 607
users
acceptance testing, 705
behaviors, 39-40, 335
der-end user cloud storage, 650
hijacked accounts, 626
managing, 39
monitoring, 40
personnel testing, 646
PKI and digital certificates, 605
presence (availability), 626-627
resource provisioning/deprovisioning, 500
security, 86-87
UTM (Unified Threat Management),
194-195, 230
validating
e-mail, 628
input, application vulnerabilities,
360-362, 366
validation testing, 676, 704
value (assets/information), risk
assessment, 138-139
vascular scans, authentication, 545
vaulting, 469
VDI (Virtual Desktop Infrastructure),
221, 521
vendors/consultants, 41, 655
verification
Software Verify tool, runtime
debugging, 385
verification testing, 676
VeriSign, 605-607
versioning, software development, 698
vertical privilege escalation, 362
video
A/V systems, 278-279
conferencing, 622-623
IP video, 275
physical access control systems, 277
virtualization, 513
client-based application virtualization
(application streaming), 322-323
container-based (operating system) vir-
tualization, 520
data remnants, resource provisioning/
deprovisioning, 531
high availability, 513
hyperconverged infrastructures, 521
hypervisors, 518-519
JVM, 373
secure enclaves, 521
secure volumes, 521
V-shaped software development
method, 690
vacations (mandatory), security
policies, 80
Valgrind, 441
validate/test phase (SDLC), 676
之争

virtualization

server-based application virtualization (terminal services), 322-323
VDI, 521
virtual devices, resource provisioning/deprovisioning, 501, 531
virtual networks, researching latest attacks, 645
VNC, 330
VPN, 618
VTPM, 320, 520
vulnerabilities, 527-530
viruses, antivirus software, 291, 439
visualization tools, 424
VLAN (Virtual LAN), 198, 260-262, 488
VMEscape, 527
VNC (Virtual Network Computing), 221, 235, 330
voice pattern recognition, authentication, 546
VoIP (Voice over IP), 630-632
volatile/persistent agents (NAC), 270
volatility, order of (evidence collection), 470-471
volumes (secure), 521
VPN (Virtual Private Networks), 215-219, 235, 333, 618, 718
VTPM (Virtual TPM), 320, 520
vulnerabilities
applications, 357-370
assessments, 401-402, 647, 667, 670, 675
current vulnerabilities, knowledge of, 646-647
CVE, SCAP scanners, 416
CVSS, 416-418
emerging threats, adapt solutions, 706-707
firmware, 377
management systems, 402
network vulnerability scanners, 413, 419
OS, 377
risk assessment, 139
software, 356-370
vulnerability cycles, 706
vulnerability scanners, 213-214, 235, 428, 523-524
zero-day vulnerabilities, 647, 676

W

WAF (Web Application Firewalls), 212-213, 234, 371
Walt Disney Magic Band and RFID, 710
WAP (Wireless Access Points), 208-209, 239
warded locks, 442
warehouses (data), 494
WASC (Web Application Security Consortium), software development best practices, 680
watches (smart), 346
Waterfall software development method, 689, 694, 697
watermarking (digital), 591, 594
WAYF (Where Are You From), 563
weak interfaces/API (Application Programming Interfaces), cloud storage, 337
wearable technology, 346-350. See also mobile devices
web conferencing, 621-622
webcams, host security, 314
WEP (Wired Equivalent Privacy), host security, 310-311
whaling, 629
white box testing, 400-401
white hats, 656
white team exercises, security assessments, 405
whitelists, 299, 360-362
Whois protocol, OSINT, 391
wildcard certificates, 603-604
Windows Group Policy, 299-301, 306
Windows Security Log, 439
Windows Server 2003, passwords, 544
wiping
  hard drives, 673
  mobile devices, 332, 450, 718
  remote wiping devices, 332, 450
wireless controllers, 208-209, 239
wireless devices, host security, 306-313
wireless networks. See WLAN
wireless security, 311-313
Wireshark, 257-258, 414-415
WLAN (Wireless LAN), 208-209, 232, 308-313
worms, IM, 626
worst-case (extreme) scenario planning, 123-125
WPA (Wi-Fi Protected Access), 311
WPA-PSK, host security, 313
WPA2 (Wi-Fi Protected Access 2), 311
wrapping applications, 330
WRT (Work Recovery Time), 146
WSS (Web Services Security), 681. See also SOAP

X

X.500, DAP, 564
X.509 certificates, 606
XACML (Extensible Access Control Markup Language), 555-556
Xcode 7, 334
XHTML (Extensible Hypertext Markup Language), SAML, 560
XML (Extensible Markup Language), 374, 555-556
XMPP (Extensible Messaging and Presence Protocol), 627
XN (Never Execute) bits (processors), 682
XSS (Cross-Site Scripting), 356

Y-Z

Zachman Framework, 112
Zebra, HC1 headset computer, 348
Zeeis updates, 331
Zenmap, 411
Zephyr charts, 546
zero-day vulnerabilities, 647, 676
Zero Knowledge Proof, 588
zero-knowledge (black box) testing, 400-401
zero-trust models, 708
zone transfers (DNS), 395