

TROY McMILLAN
ROBIN ABERNATHY



Cert Guide

Learn, prepare, and practice for exam success



CompTIA® Advanced
Security Practitioner

CASP

CAS-002

Save 10%
on Exam
Voucher

See Inside

PEARSON IT
CERTIFICATION

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

CompTIA[®] Advanced Security Practitioner (CASP) CAS-002 Cert Guide

Robin Abernathy
Troy McMillan

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA® Advanced Security Practitioner (CASP) CAS-002 Cert Guide

Copyright © 2015 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5401-1

ISBN-10: 0-7897-5401-0

Library of Congress Control Number: 2015930524

Printed in the United States of America

Second Printing: July 2015

Trademarks

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

Windows is a registered trademark of Microsoft Corporation.

Warning and Disclaimer

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

Special Sales

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

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

For questions about sales outside the U.S., please contact international@pearsoned.com.

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Allison Beaumont
Johnson

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Tim Wright

Proofreader
The Wordsmithery LLC

Technical Editors
Chris Crayton
Rob Shimonski

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Lisa Matthews

Designer
Alan Clements

Composition
Tricia Bronkella

Contents at a Glance

Introduction 1

Part I: Enterprise Security

- CHAPTER 1 Cryptographic Concepts and Techniques 31
- CHAPTER 2 Enterprise Storage 77
- CHAPTER 3 Network and Security Components, Concepts, and Architectures 106
- CHAPTER 4 Security Controls for Hosts 189
- CHAPTER 5 Application Vulnerabilities and Security Controls 229

Part II: Risk Management and Incident Response

- CHAPTER 6 Business Influences and Associated Security Risks 267
- CHAPTER 7 Risk Mitigation Planning, Strategies, and Controls 286
- CHAPTER 8 Security, Privacy Policies, and Procedures 331
- CHAPTER 9 Incident Response and Recovery Procedures 365

Part III: Research, Analysis, and Assessment

- CHAPTER 10 Industry Trends 391
- CHAPTER 11 Securing the Enterprise 416
- CHAPTER 12 Assessment Tools and Methods 431

Part IV: Integration of Computing, Communications, and Business Disciplines

- CHAPTER 13 Business Unit Collaboration 461
- CHAPTER 14 Secure Communication and Collaboration 477
- CHAPTER 15 Security Across the Technology Life Cycle 511

Part V: Technical Integration of Enterprise Components

- CHAPTER 16 Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture 533
- CHAPTER 17 Authentication and Authorization Technologies 561

Part VI: Appendixes

APPENDIX A Answers 595

APPENDIX B CASP CAS-002 Exam Updates 615

Glossary 619

Index 662

CD-only Elements:

APPENDIX C Memory Tables

APPENDIX D Memory Tables Answer Key

Table of Contents

Introduction 1

Part I: Enterprise Security

Chapter 1 Cryptographic Concepts and Techniques 31

Cryptographic Techniques	32
Key Stretching	32
Hashing	32
<i>MD2/MD4/MD5/MD6</i>	34
<i>SHA/SHA-2/SHA-3</i>	35
<i>HVAL</i>	36
<i>RIPMD-160</i>	36
Code Signing	36
<i>Message Authentication Code</i>	36
Pseudo-Random Number Generation	37
Perfect Forward Secrecy	37
Transport Encryption	38
<i>SSL/TLS</i>	38
<i>HTTP/HTTPS/SHTTP</i>	39
<i>SET and 3-D Secure</i>	39
<i>IPsec</i>	39
Data at Rest Encryption	40
<i>Symmetric Algorithms</i>	40
<i>Asymmetric Algorithms</i>	44
<i>Hybrid Ciphers</i>	47
Digital Signatures	47
Cryptographic Concepts	48
Entropy	49
Diffusion	49
Confusion	49
Non-repudiation	50
Confidentiality	50
Integrity	50

Chain of Trust/Root of Trust	50
Cryptographic Applications and Proper/Improper Implementations	51
Advanced PKI Concepts	52
<i>Wildcard</i>	52
<i>OCSP Versus CRL</i>	53
<i>Issuance to Entities</i>	53
<i>Users</i>	54
<i>Systems</i>	55
<i>Applications</i>	56
<i>Key Escrow</i>	56
Steganography	56
Implications of Cryptographic Methods and Design	56
<i>Stream Ciphers</i>	56
<i>Block Ciphers</i>	57
<i>Modes</i>	57
<i>Known Flaws/Weaknesses</i>	61
<i>Strength Versus Performance Versus Feasibility to Implement Versus Interoperability</i>	66
Cryptographic Implementations	67
Digital Rights Management (DRM)	67
Watermarking	67
GNU Privacy Guard (GPG)	67
Secure Sockets Layer (SSL)	68
Secure Shell (SSH)	69
Secure Multipurpose Internet Mail Extensions (S/MIME)	69
Review All Key Topics	70
Complete the Tables and Lists from Memory	71
Define Key Terms	71
Chapter 2 Enterprise Storage	77
Storage Types	78
Virtual Storage	78
Cloud Storage	79
Data Warehousing	80
Data Archiving	82

	SANs	83
	NAS	84
	VSANs	86
	Storage Protocols	87
	iSCSI	87
	FCoE	88
	NFS and CIFS	89
	Secure Storage Management	90
	Multipathing	90
	Snapshots	91
	Deduplication	92
	Dynamic Disk Pools	93
	LUN Masking/Mapping	94
	HBA Allocation	95
	Offsite or Multisite Replication	95
	Encryption	96
	<i>Disk-Level Encryption</i>	96
	<i>Block-Level Encryption</i>	96
	<i>File-Level Encryption</i>	97
	<i>Record-Level Encryption</i>	98
	<i>Port-Level Encryption</i>	98
	Review All Key Topics	99
	Define Key Terms	100
Chapter 3	Network and Security Components, Concepts, and Architectures	106
	Advanced Network Design (Wired/Wireless)	107
	Remote Access	107
	<i>VPNs</i>	107
	<i>SSH</i>	108
	<i>RDP</i>	109
	<i>VNC</i>	109
	<i>SSL</i>	110
	IPv6 and Associated Transitional Technologies	111

Transport Encryption	113
<i>FTP, FTPS, and SFTP</i>	113
<i>HTTP, HTTPS, and SHTTP</i>	113
Network Authentication Methods	114
<i>Authentication Factors</i>	116
802.1x	118
Mesh Networks	120
<i>Application of Solutions</i>	121
Security Devices	122
UTM	122
NIPS	123
NIDS	124
INE	126
SIEM	126
HSM	127
Placement of Devices	128
<i>UTM</i>	128
<i>NIDS</i>	129
<i>INE</i>	129
<i>NIPS</i>	130
<i>SIEM</i>	131
<i>HSM</i>	131
Application- and Protocol-Aware Technologies	131
<i>WAF</i>	131
<i>NextGen Firewalls</i>	133
<i>IPS</i>	134
<i>Passive Vulnerability Scanners</i>	134
<i>Active Vulnerability Scanners</i>	134
<i>DAM</i>	135
Networking Devices	136
Switches	137
<i>ARP Poisoning</i>	138
<i>VLANs</i>	139

Firewalls	140
<i>Types</i>	141
<i>Firewall Architecture</i>	143
Wireless Controllers	149
Routers	151
Proxies	152
Ports	152
Virtual Networking and Security Components	153
Virtual Switches	153
Virtual Firewalls	154
Virtual Wireless Controllers	155
Virtual Routers	155
Virtual Proxy Servers	156
Virtual Computing	156
Complex Network Security Solutions for Data Flow	156
SSL Inspection	156
Network Flow Data	157
Secure Configuration and Baselineing of Networking and Security Components	158
ACLs	158
<i>Creating Rule Sets</i>	159
Change Monitoring	159
Configuration Lockdown	160
Availability Controls	160
Software-Defined Networking	166
Cloud-Managed Networks	167
Network Management and Monitoring Tools	169
Advanced Configuration of Routers, Switches, and Other Network Devices	171
Transport Security	171
Trunking Security	172
Route Protection	174

Security Zones	174
Data-Flow Enforcement	175
DMZ	176
Separation of Critical Assets	176
Network Access Control	176
Quarantine/Remediation	177
Operational and Consumer Network-Enabled Devices	178
Building Automation Systems	178
IP Video	179
HVAC Controllers	180
Sensors	180
Physical Access Control Systems	181
A/V Systems	181
Scientific/Industrial Equipment	182
Critical Infrastructure/Supervisory Control and Data Acquisition (SCADA)/ Industrial Control Systems (ICS)	183
Review All Key Topics	184
Define Key Terms	185
Chapter 4 Security Controls for Hosts	189
Trusted OS	190
Endpoint Security Software	191
Antimalware	191
Antivirus	192
Antispyware	192
Spam Filters	192
Patch Management	193
IPS/IDS	193
Data Loss Prevention	194
Host-Based Firewalls	194
Log Monitoring	196
Host Hardening	198
Standard Operating Environment/Configuration Baselineing	199
<i>Application Whitelisting and Blacklisting</i>	199
Security/Group Policy Implementation	200
Command Shell Restrictions	202

Patch Management	203
Configuring Dedicated Interfaces	203
<i>Out-of-Band NICs</i>	203
<i>ACLs</i>	204
<i>Management Interface</i>	205
<i>Data Interface</i>	205
Peripheral Restrictions	206
<i>USB</i>	206
<i>Bluetooth</i>	207
<i>FireWire</i>	207
Full Disk Encryption	208
Security Advantages and Disadvantages of Virtualizing Servers	209
Type I Hypervisor	210
Type II Hypervisor	211
Container-Based Virtualization	211
Cloud-Augmented Security Services	212
Hash Matching	212
<i>Antivirus</i>	213
<i>Antispam</i>	213
<i>Vulnerability Scanning</i>	214
Sandboxing	216
Content Filtering	216
Boot Loader Protections	217
Secure Boot	217
Measured Launch	218
Integrity Measurement Architecture (IMA)	218
BIOS/UEFI	218
Vulnerabilities Associated with Commingling of Hosts with Different Security Requirements	219
VM Escape	219
Privilege Elevation	220
Live VM Migration	220
Data Remnants	221
Virtual Desktop Infrastructure (VDI)	221
Terminal Services/Application Delivery Services	222

Trusted Platform Module (TPM)	223
Virtual TPM (VTPM)	223
Hardware Security Module (HSM)	224
Review All Key Topics	224
Define Key Terms	225
Chapter 5 Application Vulnerabilities and Security Controls	229
Web Application Security Design Considerations	230
Secure by Design, by Default, by Deployment	230
Specific Application Issues	230
Insecure Direct Object References	231
XSS	231
Cross-Site Request Forgery (CSRF)	232
Click-Jacking	232
Session Management	233
Input Validation	235
SQL Injection	235
<i>Identifying a SQL Attack</i>	236
Improper Error and Exception Handling	237
Privilege Escalation	237
Improper Storage of Sensitive Data	237
Fuzzing/Fault Injection	238
Secure Cookie Storage and Transmission	239
Buffer Overflow	239
Memory Leaks	242
Integer Overflows	242
Race Conditions	242
<i>Time of Check/Time of Use</i>	242
Resource Exhaustion	243
Geotagging	243
Data Remnants	244
Application Sandboxing	244
Application Security Frameworks	245
Standard Libraries	245

Industry-Accepted Approaches	245
<i>WASC</i>	245
<i>OWASP</i>	246
<i>BSI</i>	246
<i>ISO/IEC 27000</i>	246
Web Services Security (WS-Security)	246
Secure Coding Standards	247
Software Development Methods	247
Build and Fix	248
Waterfall	248
V-Shaped	249
Prototyping	250
Incremental	250
Spiral	251
Rapid Application Development (RAD)	252
Agile	253
JAD	254
Cleanroom	254
Database Activity Monitoring (DAM)	254
Web Application Firewalls (WAF)	255
Client-Side Processing Versus Server-Side Processing	255
JSON/REST	256
Browser Extensions	256
<i>ActiveX</i>	257
<i>Java Applets</i>	257
<i>Flash</i>	257
HTML5	257
AJAX	258
SOAP	258
State Management	260
JavaScript	260
Review All Key Topics	260
Define Key Terms	261

Part II: Risk Management and Incident Response**Chapter 6 Business Influences and Associated Security Risks 267**

Risk Management of New Products, New Technologies, and User Behaviors	268
New or Changing Business Models/Strategies	268
Partnerships	269
Outsourcing	269
Cloud Computing	270
Merger and Demerger/Divestiture	271
Security Concerns of Integrating Diverse Industries	272
Rules	272
Policies	272
Regulations	272
Geography	273
Ensuring That Third-Party Providers Have Requisite Levels of Information Security	273
Internal and External Influences	275
Competitors	275
Auditors/Audit Findings	275
Regulatory Entities	276
<i>Onsite Assessment</i>	276
<i>Document Exchange/Review</i>	276
<i>Process/Policy Review</i>	276
Internal and External Client Requirements	277
Top-Level Management	277
Impact of De-perimeterization	278
Telecommuting	278
Cloud	278
BYOD (“Bring Your Own Device”)	278
Outsourcing	279
Review All Key Topics	280
Define Key Terms	280

Chapter 7 Risk Mitigation Planning, Strategies, and Controls 286

- Classify Information Types into Levels of CIA Based on Organization/
Industry 287
 - Information Classification and Life Cycle 289
 - Commercial Business Classifications* 289
 - Military and Government Classifications* 290
 - Information Life Cycle* 291
- Incorporate Stakeholder Input into CIA Decisions 291
- Implement Technical Controls Based on CIA Requirements and Policies of
the Organization 291
 - Access Control Categories 292
 - Compensative* 292
 - Corrective* 292
 - Detective* 292
 - Deterrent* 293
 - Directive* 293
 - Preventive* 293
 - Recovery* 293
 - Access Control Types 293
 - Administrative (Management) Controls* 294
 - Logical (Technical) Controls* 295
 - Physical Controls* 296
 - Security Requirements Traceability Matrix (SRTM) 297
- Determine the Aggregate CIA Score 298
- Extreme Scenario/Worst-Case Scenario Planning 299
- Determine Minimum Required Security Controls Based on Aggregate
Score 301
- Conduct System-Specific Risk Analysis 301
- Make Risk Determination 302
 - Qualitative Risk Analysis 302
 - Quantitative Risk Analysis 303
 - Magnitude of Impact 304
 - SLE* 304
 - ALE* 304

Likelihood of Threat	305
<i>Motivation</i>	305
<i>Source</i>	306
<i>ARO</i>	306
<i>Trend Analysis</i>	306
Return on Investment (ROI)	307
<i>Payback</i>	308
<i>Net Present Value (NPV)</i>	308
Total Cost of Ownership	309
Recommend Which Strategy Should be Applied Based on Risk Appetite	310
Avoid	310
Transfer	311
Mitigate	311
Accept	312
Risk Management Processes	312
Information and Asset (Tangible/Intangible) Value and Costs	312
Vulnerabilities and Threats Identification	313
Exemptions	313
Deterrence	314
Inherent	314
Residual	314
Enterprise Security Architecture Frameworks	315
Sherwood Applied Business Security Architecture (SABSA)	315
Control Objectives for Information and Related Technology (CobIT)	316
NIST SP 800-53	317
Continuous Improvement/Monitoring	318
Business Continuity Planning	318
Business Continuity Scope and Plan	318
<i>Personnel Components</i>	319
<i>Project Scope</i>	319
<i>Business Continuity Steps</i>	320
IT Governance	320

	Policies	321
	<i>Organizational Security Policy</i>	322
	<i>System-Specific Security Policy</i>	323
	<i>Issue-Specific Security Policy</i>	323
	<i>Policy Categories</i>	323
	Standards	324
	Baselines	324
	Guidelines	324
	Procedures	324
	Review All Key Topics	324
	Complete the Tables and Lists from Memory	325
	Define Key Terms	326
Chapter 8	Security, Privacy Policies, and Procedures	331
	Policy Development and Updates in Light of New Business, Technology, Risks, and Environment Changes	332
	ISO/IEC 27000 Series	333
	Process/Procedure Development and Updates in Light of Policy, Environment, and Business Changes	336
	Support Legal Compliance and Advocacy by Partnering with HR, Legal, Management, and Other Entities	337
	Sarbanes-Oxley (SOX) Act	337
	Health Insurance Portability and Accountability Act (HIPAA)	338
	Gramm-Leach-Bliley Act (GLBA) of 1999	338
	Computer Fraud and Abuse Act (CFAA)	338
	Federal Privacy Act of 1974	338
	Computer Security Act of 1987	339
	Personal Information Protection and Electronic Documents Act (PIPEDA)	339
	Basel II	339
	Payment Card Industry Data Security Standard (PCI DSS)	339
	Federal Information Security Management Act (FISMA) of 2002	339
	Economic Espionage Act of 1996	339
	USA PATRIOT Act	340
	Health Care and Education Reconciliation Act of 2010	340

Use Common Business Documents to Support Security	340
Risk Assessment (RA)/Statement of Applicability (SOA)	340
Business Impact Analysis (BIA)	341
<i>Business Impact Analysis (BIA) Development</i>	341
Interoperability Agreement (IA)	344
Interconnection Security Agreement (ISA)	345
Memorandum of Understanding (MOU)	345
Service-Level Agreement (SLA)	345
Operating-Level Agreement (OLA)	345
Nondisclosure Agreement (NDA)	346
Business Partnership Agreement (BPA)	346
Use General Privacy Principles for Sensitive Information (PII)	347
Support the Development of Various Policies	348
Separation of Duties	348
Job Rotation	349
Mandatory Vacation	350
Least Privilege	350
Incident Response	351
<i>Event Versus Incident</i>	353
<i>Incident Response Team and Incident Investigations</i>	353
<i>Rules of Engagement, Authorization, and Scope</i>	354
Forensic Tasks	354
Employment and Termination Procedures	356
Continuous Monitoring	356
Training and Awareness for Users	357
Auditing Requirements and Frequency	359
Review All Key Topics	359
Define Key Terms	360
Chapter 9 Incident Response and Recovery Procedures	365
E-Discovery	366
Electronic Inventory and Asset Control	366
Data Retention Policies	367
Data Recovery and Storage	368
<i>Data Backup Types and Schemes</i>	369
<i>Electronic Backup</i>	372

Data Ownership	372
Data Handling	373
Legal Holds	374
Data Breach	374
Detection and Collection	375
<i>Data Analytics</i>	376
Mitigation	376
<i>Minimize</i>	376
<i>Isolate</i>	376
Recovery/Reconstitution	377
Response	377
Disclosure	377
Design Systems to Facilitate Incident Response	378
Internal and External Violations	378
<i>Privacy Policy Violations</i>	379
<i>Criminal Actions</i>	379
<i>Insider Threat</i>	379
<i>Non-Malicious Threats/Misconfigurations</i>	380
Establish and Review System, Audit and Security Logs	380
Incident and Emergency Response	381
Chain of Custody	381
<i>Evidence</i>	381
<i>Surveillance, Search, and Seizure</i>	382
Forensic Analysis of Compromised System	383
<i>Media Analysis</i>	383
<i>Software Analysis</i>	384
<i>Network Analysis</i>	384
<i>Hardware/Embedded Device Analysis</i>	384
Continuity of Operations Plan (COOP)	384
Order of Volatility	385
Review All Key Topics	386
Define Key Terms	387

Part III: Research, Analysis, and Assessment**Chapter 10 Industry Trends 391**

- Perform Ongoing Research 392
 - Best Practices 392
 - New Technologies 393
 - New Security Systems and Services 394
 - Technology Evolution 395
- Situational Awareness 396
 - Latest Client-Side Attacks 396
 - Knowledge of Current Vulnerabilities and Threats 397
- Vulnerability Management Systems 398
- Advanced Persistent Threats 398
- Zero-Day Mitigating Controls and Remediation 398
- Emergent Threats and Issues 399
- Research Security Implications of New Business Tools 400
 - Social Media/Networking 401
 - End-User Cloud Storage 402
 - Integration Within the Business 403
- Global IA Industry/Community 403
 - Computer Emergency Response Team (CERT) 403
 - Conventions/Conferences 404
 - Threat Actors 405
 - Emerging Threat Sources/Threat Intelligence 406
- Research Security Requirements for Contracts 406
 - Request for Proposal (RFP) 407
 - Request for Quote (RFQ) 407
 - Request for Information (RFI) 408
 - Agreements 408
- Review All Key Topics 408
 - Define Key Terms 409

Chapter 11 Securing the Enterprise 416

- Create Benchmarks and Compare to Baselines 417
- Prototype and Test Multiple Solutions 418

Cost/Benefit Analysis	419
ROI	419
TCO	419
Metrics Collection and Analysis	419
Analyze and Interpret Trend Data to Anticipate Cyber Defense Needs	420
Review Effectiveness of Existing Security Controls	421
Reverse Engineer/Deconstruct Existing Solutions	422
Analyze Security Solution Attributes to Ensure They Meet Business Needs	422
Performance	422
Latency	423
Scalability	423
Capability	423
Usability	424
Maintainability	424
Availability	424
Recoverability	424
Conduct a Lessons-Learned/After-Action Report	425
Use Judgment to Solve Difficult Problems That Do Not Have a Best Solution	425
Review All Key Topics	426
Define Key Terms	426
Chapter 12 Assessment Tools and Methods	431
Assessment Tool Types	432
Port Scanners	432
Vulnerability Scanners	434
Protocol Analyzer	434
Network Enumerator	435
Password Cracker	436
Fuzzer	438
HTTP Interceptor	439
Exploitation Tools/Frameworks	439
Passive Reconnaissance and Intelligence-Gathering Tools	440
<i>Social Media</i>	441

<i>Whois</i>	441
<i>Routing Tables</i>	443
Assessment Methods	445
Vulnerability Assessment	445
Malware Sandboxing	446
Memory Dumping, Runtime Debugging	447
Penetration Testing	448
Black Box	451
White Box	451
Gray Box	451
Reconnaissance	452
Fingerprinting	452
Code Review	454
Social Engineering	455
<i>Phishing/Pharming</i>	455
<i>Shoulder Surfing</i>	456
<i>Identity Theft</i>	456
<i>Dumpster Diving</i>	456
Review All Key Topics	456
Define Key Terms	457

Part IV: Integration of Computing, Communications, and Business Disciplines

Chapter 13 Business Unit Collaboration 461

Interpreting Security Requirements and Goals to Communicate with Stakeholders from Other Disciplines	462
Sales Staff	462
Programmer	463
Database Administrator	463
Network Administrator	464
Management/Executive Management	465
Financial	466
Human Resources	467
Emergency Response Team	467
Facilities Manager	468
Physical Security Manager	468

Provide Objective Guidance and Impartial Recommendations to Staff and Senior Management on Security Processes and Controls	469
Establish Effective Collaboration within Teams to Implement Secure Solutions	469
IT Governance	471
Review All Key Topics	471
Define Key Terms	472
Chapter 14 Secure Communication and Collaboration	477
Security of Unified Collaboration Tools	478
Web Conferencing	478
Video Conferencing	479
Instant Messaging	481
Desktop Sharing	481
Remote Assistance	482
Presence	483
Email	484
<i>IMAP</i>	484
<i>POP</i>	484
<i>SMTP</i>	484
<i>Email Spoofing</i>	485
<i>Spear Phishing</i>	485
<i>Whaling</i>	486
<i>Spam</i>	486
<i>Captured Messages</i>	486
<i>Disclosure of Information</i>	487
<i>Malware</i>	487
Telephony	487
<i>VoIP</i>	488
Collaboration Sites	489
<i>Social Media</i>	489
<i>Cloud-Based Collaboration</i>	490
Remote Access	491
Dial-up	491
VPN	492

SSL	495
Remote Administration	495
Mobile Device Management	495
BYOD	495
Over-the-Air Technologies Concerns	497
FHSS, DSSS, OFDM, FDMA, CDMA, OFDMA, and GSM	497
<i>802.11 Techniques</i>	498
<i>Cellular or Mobile Wireless Techniques</i>	498
WLAN Structure	499
<i>Access Point</i>	499
SSID	499
<i>Infrastructure Mode Versus Ad Hoc Mode</i>	499
WLAN Standards	500
<i>802.11a</i>	500
<i>802.11b</i>	500
<i>802.11g</i>	501
<i>802.11n</i>	501
<i>802.11ac</i>	501
<i>Bluetooth</i>	502
<i>Infrared</i>	502
WLAN Security	502
WEP	502
WPA	503
WPA2	503
<i>Personal Versus Enterprise WPA</i>	503
SSID Broadcast	504
MAC Filter	504
Satellites	504
Wireless Attacks	505
<i>Wardriving</i>	505
<i>Warchalking</i>	505
<i>Rogue Access Points</i>	505
Review All Key Topics	506
Define Key Terms	506

Chapter 15 Security Across the Technology Life Cycle 511

- End-to-End Solution Ownership 512
 - Operational Activities 512
 - Maintenance 513
 - Commissioning/Decommissioning 514
 - Asset Disposal 514
 - Asset/Object Reuse 515
 - General Change Management 516
- Systems Development Life Cycle (SDLC) 517
 - Security System Development Life Cycle (SSDLC)/Security Development Life Cycle (SDL) 519
 - Security Requirements Traceability Matrix (SRTM) 522
 - Validation and Acceptance Testing 522
 - Security Implications of Agile, Waterfall, and Spiral Software Development Methodologies 523
 - Agile Software Development* 523
 - The Waterfall Model* 523
 - The Spiral Model* 524
- Adapt Solutions to Address Emerging Threats and Security Trends 525
- Asset Management (Inventory Control) 526
 - Device-Tracking Technologies 526
 - Geolocation/GPS Location* 526
 - Object Tracking and Containment Technologies 526
 - Geotagging/Geofencing* 527
 - RFID* 527
- Review All Key Topics 528
 - Define Key Terms 528

Part V: Technical Integration of Enterprise Components**Chapter 16 Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture 533**

- Secure Data Flows to Meet Changing Business Needs 534
- Standards 535
 - Open Standards 536
 - Adherence to Standards 536
 - Competing Standards 536

Lack of Standards	536
De Facto Standards	536
Interoperability Issues	537
Legacy Systems/Current Systems	537
Application Requirements	538
In-House Developed Versus Commercial Versus Commercial Customized Applications	539
Technical Deployment Models	539
Cloud and Virtualization Considerations and Hosting Options	540
<i>Public Cloud</i>	540
<i>Private Cloud</i>	540
<i>Hybrid Cloud</i>	540
<i>Community Cloud</i>	541
<i>Multi-Tenancy Model</i>	541
<i>Single-Tenancy Model</i>	541
Vulnerabilities Associated with a Single Physical Server Hosting Multiple Companies' Virtual Machines	541
Vulnerabilities Associated with a Single Platform Hosting Multiple Companies' Virtual Machines	542
Secure Use of On-demand/Elastic Cloud Computing	542
Data Remnants	543
Data Aggregation	543
Data Isolation	543
Resource Provisioning and Deprovisioning	543
<i>Users</i>	544
<i>Servers</i>	544
<i>Virtual Devices</i>	544
<i>Applications</i>	545
Securing Virtual Environments, Services, Applications, Appliances, and Equipment	545
Design Considerations During Mergers, Acquisitions, and Demergers/ Divestitures	545
Network Secure Segmentation and Delegation	545
Logical and Physical Deployment Diagrams of Relevant Devices	546

Secure Infrastructure Design	548
DMZs	548
VLANs	549
VPNs	550
Wireless Networks	550
Storage Integration (Security Considerations)	552
Enterprise Application Integration Enablers	552
CRM	552
ERP	553
GRC	553
ESB	553
SOA	553
Directory Services	554
DNS	554
CMDB	555
CMS	555
Review All Key Topics	555
Define Key Terms	556
Chapter 17 Authentication and Authorization Technologies	561
Authentication	562
Identity and Account Management	562
Password Types and Management	563
<i>Characteristic Factors</i>	566
<i>Physiological Characteristics</i>	567
<i>Behavioral Characteristics</i>	568
<i>Biometric Considerations</i>	568
Dual-Factor and Multi-Factor Authentication	570
Certificate-Based Authentication	570
Single Sign-On	571
Authorization	572
Access Control Models	572
<i>Discretionary Access Control</i>	572
<i>Mandatory Access Control</i>	573
<i>Role-Based Access Control</i>	573
<i>Rule-Based Access Control</i>	574

<i>Content-Dependent Versus Context-Dependent Access Control</i>	574
<i>Access Control Matrix</i>	574
<i>ACLs</i>	575
Access Control Policies	575
Default to No Access	575
OAUTH	575
XACML	577
SPML	578
Attestation	579
Identity Propagation	580
Federation	581
SAML	581
OpenID	583
Shibboleth	583
WAYF	584
Advanced Trust Models	585
RADIUS Configurations	585
LDAP	586
Active Directory (AD)	586
Review All Key Topics	588
Define Key Terms	589

Part VI: Appendixes

Appendix A Answers 595

Appendix B CASP CAS-002 Exam Updates 615

Always Get the Latest at the Companion Website 615

Technical Content 616

Glossary 619

Index 662

CD-only Elements:

Appendix C Memory Tables

Appendix D Memory Tables Answer Key

About the Authors

Robin Abernathy, CASP, is a product developer and technical editor for Kaplan IT. 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 includes practice tests and study guides for the Transcender and Self Test Software brands.

Robin most recently co-authored Pearson's *CISSP Cert Guide* with Troy McMillan. 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.

Troy McMillan, CASP, is a product developer and technical editor for Kaplan IT as well as a full-time trainer. He became a professional trainer 13 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)
- 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 and Self-Test brands. Troy lives in Sugarloaf Key, Florida, with his wife, Heike.

Dedication

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

—Robin

I dedicate this book to my father; who passed away this year. I miss you every day.

—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.

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 cert prep, who have helped me to grow over the past 10 years. Thank you, Ann, George, Aima, Bob, Josh, Robin, and Shihara. 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 Reviewers

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

Rob Shimonski (www.shimonski.com) is a best-selling author and editor with over 15 years' experience developing, producing, and distributing print media in the form of books, magazines, and periodicals. To date, Rob has successfully created more than 100 books that are currently in circulation. Rob has worked for countless companies, including CompTIA, Microsoft, Pearson, Elsevier, Wiley, Cisco, the National Security Agency, and Digidesign. Rob has over 20 years' experience working in IT, networking, systems, and security. He is a veteran of the U.S. military and has been entrenched in security topics and assignments throughout his entire professional career.

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

Visit our website and register this book at www.pearsonitcertification.com/title/9780789754011 for convenient access to any updates, downloads, or errata that might be available for this book.

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill.

Certification demonstrates that you have the knowledge and skill to solve technical or business problems in virtually any business environment. CompTIA certifications are highly-valued credentials that qualify you for jobs, increased compensation and promotion.



IT is Everywhere	IT Knowledge and Skills Get Jobs	Job Retention	New Opportunities	High Pay-High Growth Jobs
<p>IT is mission critical to almost all organizations and its importance is increasing.</p> <ul style="list-style-type: none"> 79% of U.S. businesses report IT is either important or very important to the success of their company 	<p>Certifications verify your knowledge and skills that qualifies you for:</p> <ul style="list-style-type: none"> Jobs in the high growth IT career field Increased compensation Challenging assignments and promotions 60% report that being certified is an employer or job requirement 	<p>Competence is noticed and valued in organizations.</p> <ul style="list-style-type: none"> Increased knowledge of new or complex technologies Enhanced productivity More insightful problem solving Better project management and communication skills 47% report being certified helped improve their problem solving skills 	<p>Certifications qualify you for new opportunities in your current job or when you want to change careers.</p> <ul style="list-style-type: none"> 31% report certification improved their career advancement opportunities 	<p>Hiring managers demand the strongest skill set.</p> <ul style="list-style-type: none"> There is a widening IT skills gap with over 300,000 jobs open 88% report being certified enhanced their resume



Certification Helps Your Career

- **The CompTIA Advanced Security Practitioner (CASP)** certification designates IT professionals with advanced-level security skills and knowledge.
- **The CASP** is the first mastery level certification available from CompTIA. It expands on the widely recognized path of CompTIA Security+ with almost 250,000 certified Security+ professionals.
- **Being CASP certified** demonstrates technical competency in enterprise security; risk management; research and analysis; and integration of computing, communications, and business disciplines.
- **Approved by the U.S. Department of Defense (DoD)** for 4 information assurance job roles in the DoD 8570.01-M directive: IA Technical Level III, IA Manager level II, and IA System Architect & Engineer (IASAE) Levels I and II.

Steps to Getting Certified and Staying Certified	
Review Exam Objectives	Review the Certification objectives to make sure you know what is covered in the exam. http://certification.comptia.org/examobjectives.aspx
Practice for the Exam	After you have studied for the certification, review and answer the sample questions to get an idea what type of questions might be on the exam. http://certification.comptia.org/samplequestions.aspx
Purchase an Exam Voucher	Purchase exam vouchers on the CompTIA Marketplace. www.comptiastore.com
Take the Test	Go to the Pearson VUE website and schedule a time to take your exam. http://www.pearsonvue.com/comptia/
Stay Certified! Continuing Education	The CompTIA CASP certification is valid for three years from the date of certification. There are a number of ways the certification can be renewed. For more information go to: http://certification.comptia.org/ce

How to obtain more information

- **Visit CompTIA online:** <http://certification.comptia.org/home.aspx> to learn more about getting CompTIA certified.
- **Contact CompTIA:** call 866-835-8020 and choose Option 2 or email questions@comptia.org.

- **Connect with us :**

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-002 blueprint from CompTIA. This book also helps you demonstrate your knowledge by passing the CAS-002 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 defines the topics that are covered in the chapter.
- **Foundation topics:** At the heart of a chapter, this section explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures that build your knowledge so that you can pass the CAS-002 exam. The chapters are each broken into multiple sections.
- **Key topics:** This indicates 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 DVD, and in Appendix C, "Memory Tables," and Appendix D, "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 [http://certification.comptia.org/getCertified/certifications/comptia-advanced-security-practitioner-\(casp\)](http://certification.comptia.org/getCertified/certifications/comptia-advanced-security-practitioner-(casp)).

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 because of a company policy that mandates 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 CD. 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-002). 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-002 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 1 CompTIA CASP+ Exam Topics

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
1 Cryptographic Concepts and Techniques	1.1 Given a scenario, select appropriate cryptographic concepts and techniques	<ul style="list-style-type: none"> ■ Techniques ■ Concepts ■ Implementations
2 Enterprise Storage	1.2 Explain the security implications associated with enterprise storage	<ul style="list-style-type: none"> ■ Storage types ■ Storage protocols ■ Secure storage management
3 Network and Security Components, Concepts, and Architectures	1.3 Given a scenario, analyze network and security components, concepts and architectures	<ul style="list-style-type: none"> ■ Advanced network design (wired/wireless) ■ Security devices ■ Virtual networking and security components ■ Complex network security solutions for data flow ■ Secure configuration and baselining of networking and security components ■ Software defined networking ■ Cloud managed networks ■ Network management and monitoring tools ■ Advanced configuration of routers, switches and other network devices ■ Security zones ■ Network access control ■ Operational and consumer network enabled devices ■ Critical infrastructure/Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS)

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
4 Security Controls for Hosts	1.4 Given a scenario, select and troubleshoot security controls for hosts	<ul style="list-style-type: none"> ■ Trusted OS (e.g., how and when to use it) ■ Endpoint security software ■ Host hardening ■ Security advantages and disadvantages of virtualizing servers ■ Cloud augmented security services ■ Boot loader protections ■ Vulnerabilities associated with co-mingling of hosts with different security requirements ■ Virtual desktop infrastructure (VDI) ■ Terminal services/application delivery services ■ TPM ■ VTPM ■ HSM
5 Application Vulnerabilities and Security Controls	1.5 Differentiate application vulnerabilities and select appropriate security controls	<ul style="list-style-type: none"> ■ Web application security design considerations ■ Specific application issues ■ Application sandboxing ■ Application security frameworks ■ Secure coding standards ■ Database activity monitor (DAM) ■ Web application firewalls (WAFs) ■ Client-side processing vs. server-side processing
6 Business Influences and Associated Security Risks	2.1 Interpret business and industry influences and explain associated security risks	<ul style="list-style-type: none"> ■ Risk management of new products, new technologies and user behaviors ■ New or changing business models/strategies ■ Security concerns of integrating diverse industries ■ Ensuring that third party providers have requisite levels of information security ■ Internal and external influences ■ Impact of de-perimeterization (e.g., constantly changing network boundary)

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
7 Risk Mitigation Planning, Strategies, and Controls	2.2 Given a scenario, execute risk mitigation planning, strategies, and controls	<ul style="list-style-type: none"> ■ Classify information types into levels of CIA based on organization/industry ■ Incorporate stakeholder input into CIA decisions ■ Implement technical controls based on CIA requirements and policies of the organization ■ Determine aggregate CIA scores ■ Extreme scenario planning/worst case scenario ■ Determine minimum required security controls based on the aggregate score ■ Conduct system specific risk analysis ■ Make risk determination ■ Recommend which strategy should be applied based on risk appetite ■ Risk management processes ■ Enterprise security architecture frameworks ■ Continuous improvement/monitoring ■ Business continuity planning ■ IT governance
8 Security, Privacy Policies, and Procedures	2.3 Compare and contrast security, privacy policies and procedures based on organizational requirements	<ul style="list-style-type: none"> ■ Policy development and updates in light of new business, technology, risks and environment changes ■ Process/procedure development and updates in light of policy, environment and business changes ■ Support legal compliance and advocacy by partnering with HR, legal, management and other entities ■ Use common business documents to support security ■ Use general privacy principles for sensitive information (PII) ■ Support the development of policies

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
9 Incident Response and Recovery Procedures	2.4 Given a scenario, conduct incident response and recovery procedures	<ul style="list-style-type: none"> ■ E-discovery ■ Data breach ■ Design systems to facilitate incident response ■ Incident and emergency response
10 Industry Trends	3.1 Apply research methods to determine industry trends and impact to the enterprise	<ul style="list-style-type: none"> ■ Perform ongoing research ■ Situational awareness ■ Research security implications of new business tools ■ Global IA industry/community ■ Research security requirements for contracts
11 Securing the Enterprise	3.2 Analyze scenarios to secure the enterprise	<ul style="list-style-type: none"> ■ Create benchmarks and compare to baselines ■ Prototype and test multiple solutions ■ Cost benefit analysis ■ Metrics collection and analysis ■ Analyze and interpret trend data to anticipate cyber defense needs ■ Review effectiveness of existing security controls ■ Reverse engineer/deconstruct existing solutions ■ Analyze security solution attributes to ensure they meet business needs ■ Conduct a lessons-learned/after-action report ■ Use judgment to solve difficult problems that do not have a best solution
12 Assessment Tools and Methods	3.3 Given a scenario, select methods or tools appropriate to conduct an assessment and analyze results	<ul style="list-style-type: none"> ■ Tool type ■ Methods

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
13 Business Unit Collaboration	4.1 Given a scenario, facilitate collaboration across diverse business units to achieve security goals	<ul style="list-style-type: none"> ■ Interpreting security requirements and goals to communicate with stakeholders from other disciplines ■ 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 ■ IT governance
14 Secure Communication and Collaboration	4.2 Given a scenario, select the appropriate control to secure communications and collaboration solutions	<ul style="list-style-type: none"> ■ Security of unified collaboration tools ■ Remote access ■ Mobile device management ■ Over-the-air technologies concerns
15 Security Across the Technology Life Cycle	4.3 Implement security activities across the technology life cycle	<ul style="list-style-type: none"> ■ End-to-end solution ownership ■ Systems development life cycle ■ Adapt solutions to address emerging threats and security trends ■ Asset management (inventory control)
16 Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture	5.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture	<ul style="list-style-type: none"> ■ Secure data flows to meet changing business needs ■ Standards ■ Interoperability issues ■ Technical deployment models (Outsourcing/insourcing/managed services/partnership) ■ Logical deployment diagram and corresponding physical deployment diagram of all relevant devices ■ Secure infrastructure design (e.g. decide where to place certain devices/applications) ■ Storage integration (security considerations) ■ Enterprise application integration enablers

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
17 Authentication and Authorization Technologies	5.2 Given a scenario, integrate advanced authentication and authorization technologies to support enterprise objectives	<ul style="list-style-type: none"> ■ Authentication ■ Authorization ■ Attestation ■ Identity propagation ■ Federation ■ Advanced trust models

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:

- Chapter 1, “Cryptographic Concepts and Techniques,” introduces cryptographic techniques and concepts. It presents the uses of these techniques and describes various implementations that currently exist, such as DRM, watermarking, GPG, SSL, SSH, and S/MIME.
- Chapter 2, “Enterprise Storage,” describes various types of storage mechanisms and their distinguishing characteristics. It describes the major protocols used in a storage solution and storage security and performance techniques such as multipath, snapshots, and deduplication.
- Chapter 3, “Network and Security Components, Concepts, and Architectures,” covers issues driving network design, including virtual networking and security. It introduces various security devices, such as UTM, NIDS, INE, and HSM. It also includes a survey of access control issues, including network access control, and finishes with a discussion of the future of network-enabled devices, including building automation.
- Chapter 4, “Security Controls for Hosts,” focuses on protecting the host in the network. Security software such as antivirus is discussed, along with the concepts and steps taken to harden systems. Security issues in a cloud environment are also covered, along with a discussion of virtual desktop security. Finally, full disk encryption is discussed.
- Chapter 5, “Application Vulnerabilities and Security Controls,” discusses the fact that while securing the network is important, security issues can also exist

from the applications created by an organization. This chapter details the various problems that can be present in application code and the attacks that these problems can lead to. It also describes mitigation techniques for securing applications.

- Chapter 6, “Business Influences and Associated Security Risks,” discusses the security risks involved when companies are acquired and networks are combined. This chapter introduces concepts such as security concerns when companies are merging, the risks introduced by the deperimeterization of today’s networks, and the impact of outsourcing.
- As discussed in Chapter 7, “Risk Mitigation Planning, Strategies, and Controls,” businesses face many types of risk in day-to-day operations. Managing risk and mitigating the damage caused by various events is the topic of this chapter. It discusses methods to use to define and quantify risk and covers methods used to select the proper strategy for handling the risks.
- As discussed in Chapter 8, “Security, Privacy Policies, and Procedures,” all organizations should have security policies and procedures in place that address all conceivable events. This chapter discusses how to create a security policy and list some of the sections that should always be included.
- No security policy can protect an organization from all risks. In case a security breach occurs, there should be formal reaction system in place to address the incident. Chapter 9, “Incident Response and Recovery Procedures,” describes an incident response method which ensures that evidence is protected and the proper information is gathered.
- In no industry do changes occur faster than in IT. Security professionals have to keep up with the latest practices and concept. Chapter 10, “Industry Trends,” looks at some of the coming trends and methods to keep abreast of the latest and greatest security innovations and attacks.
- Chapter 11, “Securing the Enterprise,” takes a more holistic security view of the enterprise and discusses how to anticipate the effects of certain security measures and how to mitigate some of these effects.
- To secure a network, you must be able to monitor the network for evidence of mischief. Chapter 12, “Assessment Tools and Methods,” looks at tools used to assess the vulnerability of a network.
- Security in the network can be enhanced by all parts of the organization working together. Chapter 13, “Business Unit Collaboration,” looks at the benefits of including all organizational stakeholders in the development of security policies.

- While data should be protected where it resides in storage on a network, communications crossing the network must also be secured. Chapter 14, “Secure Communication and Collaboration,” looks at securing connections, both remote and local to the enterprise. It also discusses security issues surrounding collaboration tools that are now widely used.
- Security is a never-ending process that requires constant examination and adjustment. Chapter 15, “Security Across the Technology Life Cycle,” covers this life cycle and also discusses change management and the benefits that can be derived from a formal change management process.
- Virtualization and cloud computing are all the rage these days. Chapter 16, “Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture,” discusses the security issues involved with integrating a virtual and physical infrastructure. It covers cloud computing models and best practices for securing a virtual environment.
- Controlling access to resources and the network in general is probably the obvious security function performed by security professionals. Chapter 17, “Authentication and Authorization Technologies,” covers methods of authentication and authorization.

In addition to the 17 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The CD includes practice questions that are an important part of your preparation for certification. The CD also includes a practice test and memory tables that you can work through to verify your knowledge of the subject matter.

Pearson IT Certification Practice Test Engine and Questions on the Disc

The disc in the back of the book includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions.

The installation process requires two major steps: installing the software and then activating the exam. The disc in the back of this book has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on the disc.

NOTE The cardboard disc case in the back of this book includes the disc and a piece of paper. The paper lists the activation code for the practice exam 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.

Install the Software from the Disc

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows Virtual Machine, but it was built specifically for the PC platform.

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

The following steps outline the installation process:

1. Insert the disc into your PC.
2. The software that automatically runs is the Pearson software to access and use all disc-based features, including the exam engine and the disc-only appendixes. From the main menu, click the option to Install the Exam Engine.
3. Respond to Windows prompts as with any typical software installation process.

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

Activate and Download the Practice Exam

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

1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.

2. To activate and download the exam associated with this book, from the My Products or Tools tab, select the Activate button.
3. At the next screen, enter the Activation Key from the paper inside the cardboard disc holder in the back of the book. When it's entered, click the Activate button.
4. The activation process downloads the practice exam. Click Next and then click Finish.

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

To update a particular exam you have already activated and downloaded, simply select the Tools tab, and select the Update Products button. Updating your exams will ensure you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the Tools tab, and select the Update Application button. This will ensure you are running the latest version of the software engine.

Activating Other Exams

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

Premium Edition

In addition to the two free practice exams provided on the disc, you can purchase one additional exam with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains one additional full practice exam as well as an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

If you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the disc sleeve that contains a one-time use code as well as instructions for where you can purchase the Premium Edition.

This page intentionally left blank



This chapter covers the following topics:

- **The Goal 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 that comprise the value of the 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 security skills and knowledge.

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 requires trained professionals that are versed not only in security theory but who can also 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 November 30, 2014. The new exam, CAS-002, replaces CAS-001, which will retire in May 2015. This book is designed to prepare you for the new exam, CAS-002, but can also be used to prepare for the CAS-001.

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 the ability to design, implement, and maintain the correct security posture for an organization, based on the complex environments in which today's organizations exist.

Sponsoring Bodies

CompTIA is an 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, as well as 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 an unethical hacker.

Stated Goals

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

The CASP exam covers the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. It involves applying critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers, while managing risk.

The Value of the CASP Certification

The CASP certification holds value for both the exam candidate and the enterprise. While it is a relatively new exam, already it has been approved by U.S. Department of Defense to meet 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 one's salary

Department of Defense Directive 8570 (DoDD 8570)

DoDD 8570 prescribes 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.

IAT Level I	IAT Level II	IAT Level III
CompTIA A+	GSEC	CASP
CompTIA Network+	CompTIA Security+	CISA
SSCP	SSCP	CISSP (or Associate)
		GCIH
IAM Level I	IAM Level II	IAM Level III
CAP	CASP	GSLC
GSLC	CAP	CISM
CompTIA Security+	GSLC	CISSP (or Associate)
	CISM	
	CISSP (or Associate)	
IASAE I	IASAE II	IASAE III
CASP	CASP	CISSP - ISSEP
CISSP (or Associate)	CISSP (or Associate)	CISSP - ISSAP

Figure I-1 DOD 8570

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-002 exam.

1.0 Enterprise Security

1.1 Given a scenario, select appropriate cryptographic concepts and techniques

- Techniques
 - Key stretching
 - Hashing
 - Code signing
 - Pseudo random number generation
 - Perfect forward secrecy
 - Transport encryption
 - Data at rest encryption
 - Digital signature
- Concepts
 - Entropy
 - Diffusion
 - Confusion
 - Non-repudiation
 - Confidentiality
 - Integrity
 - Chain of trust, Root of trust

- Cryptographic applications and proper/improper implementations
- Advanced PKI concepts
 - Wild card
 - OCSP vs. CRL
 - Issuance to entities
 - Users
 - Systems
 - Applications
 - Key escrow
- Steganography
- Implications of cryptographic methods and design
 - Stream
 - Block
 - Modes
 - ECB
 - CBC
 - CFB
 - OFB
 - Known flaws/weaknesses
 - Strength vs. performance vs. feasibility to implement vs. interoperability
- Implementations
 - DRM
 - Watermarking
 - GPG
 - SSL
 - SSH
 - S/MIME

1.2 Explain the security implications associated with enterprise storage

- Storage types
 - Virtual storage
 - Cloud storage
 - Data warehousing
 - Data archiving
 - NAS
 - SAN
 - vSAN
- Storage protocols
 - iSCSI
 - FCoE
 - NFS, CIFS
- Secure storage management
 - Multipath
 - Snapshots
 - Deduplication
 - Dynamic disk pools
 - LUN masking/mapping
 - HBA allocation
 - Offsite or multisite replication
 - Encryption
 - Disk
 - Block
 - File
 - Record
 - Port

1.3 Given a scenario, analyze network and security components, concepts and architectures

- Advanced network design (wired/wireless)
 - Remote access
 - VPN
 - SSH
 - RDP
 - VNC
 - SSL
 - IPv6 and associated transitional technologies
 - Transport encryption
 - Network authentication methods
 - 802.1x
 - Mesh networks
- Security devices
 - UTM
 - NIPS
 - NIDS
 - INE
 - SIEM
 - HSM
 - Placement of devices
 - Application and protocol aware technologies
 - WAF
 - NextGen firewalls
 - IPS
 - Passive vulnerability scanners
 - DAM

- Virtual networking and security components
 - Switches
 - Firewalls
 - Wireless controllers
 - Routers
 - Proxies
- Complex network security solutions for data flow
 - SSL inspection
 - Network flow data
- Secure configuration and baselining of networking and security components
 - ACLs
 - Change monitoring
 - Configuration lockdown
 - Availability controls
- Software defined networking
- Cloud managed networks
- Network management and monitoring tools
- Advanced configuration of routers, switches and other network devices
 - Transport security
 - Trunking security
 - Route protection
- Security zones
 - Data flow enforcement
 - DMZ
 - Separation of critical assets
- Network access control
 - Quarantine/remediation

- Operational and consumer network enabled devices
 - Building 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)

1.4 Given a scenario, select and troubleshoot security controls for hosts

- Trusted OS (e.g. how and when to use it)
- End point security software
 - Anti-malware
 - Anti-virus
 - Anti-spyware
 - Spam filters
 - Patch management
 - HIPS/HIDS
 - Data loss prevention
 - Host-based firewalls
 - Log monitoring
- Host hardening
 - Standard operating environment/configuration baselining
 - Application whitelisting and blacklisting
 - Security/group policy implementation
 - Command shell restrictions
 - Patch management

- Configuring dedicated interfaces
 - Out-of-band NICs
 - ACLs
 - Management interface
 - Data interface
- Peripheral restrictions
 - USB
 - Bluetooth
 - Firewire
- Full disk encryption
- Security advantages and disadvantages of virtualizing servers
 - Type I
 - Type II
 - Container-based
- Cloud augmented security services
 - Hash matching
 - Anti-virus
 - Anti-spam
 - Vulnerability scanning
 - Sandboxing
 - Content filtering
- Boot loader protections
 - Secure boot
 - Measured launch
 - IMA—Integrity Measurement Architecture
 - BIOS/UEFI

- Vulnerabilities associated with co-mingling of hosts with different security requirements
 - VM Escape
 - Privilege elevation
 - Live VM migration
 - Data remnants
- Virtual Desktop Infrastructure (VDI)
- Terminal services/application delivery services
- TPM
- VTPM
- HSM

1.5 Differentiate application vulnerabilities and select appropriate security controls

- Web application security design considerations
 - Secure: by design, by default, by deployment
- Specific application issues
 - Insecure 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
- Geo-tagging
- Data remnants
- Application sandboxing
- Application security frameworks
 - Standard libraries
 - Industry accepted approaches
 - Web services security (WS-security)
- Secure coding standards
- Database Activity Monitor (DAM)
- Web Application Firewalls (WAF)
- Client-side processing vs. server-side processing
 - JSON/REST
 - Browser extensions
 - ActiveX
 - Java applets
 - Flash
 - HTML5
 - AJAX
 - SOAP
 - State management
 - Javascript

2.0 Risk Management and Incident Response

2.1 Interpret business and industry influences and explain associated security risks

- Risk management of new products, new technologies and user behaviors
- New or changing business models/strategies
 - Partnerships
 - Outsourcing
 - Cloud
 - Merger and demerger/divestiture
- Security concerns of integrating diverse industries
 - Rules
 - Policies
 - Regulations
 - Geography
- Ensuring third party providers have requisite levels of information security
- 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
 - BYOD
 - Outsourcing

2.2 Given a scenario, execute risk mitigation planning, strategies and controls

- Classify information types into levels of CIA based on organization/industry
- Incorporate stakeholder input into CIA decisions

- Implement technical controls based on CIA requirements and policies of the organization
- Determine aggregate score of CIA
- Extreme scenario planning/worst case scenario
- Determine minimum required security controls based on aggregate score
- Conduct system specific risk analysis
- Make risk determination
 - Magnitude of impact
 - ALE
 - SLE
 - Likelihood of threat
 - Motivation
 - Source
 - ARO
 - Trend analysis
 - Return on investment (ROI)
 - Total cost of ownership
- Recommend which strategy should be applied based on risk appetite
 - Avoid
 - Transfer
 - Mitigate
 - Accept
- Risk management processes
 - Exemption
 - Deterrence
 - Inherent
 - Residual
- Enterprise Security Architecture frameworks
- Continuous improvement/monitoring
- Business Continuity Planning
- IT Governance

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

- Policy development and updates in light of new business, technology, risks and environment changes
- Process/procedure development and updates in light of policy, environment and business changes
- Support legal compliance and advocacy by partnering with HR, legal, management and other entities
- Use common business documents to support security
 - Risk assessment (RA)/Statement of Applicability (SOA)
 - 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)
- Use general privacy principles for sensitive information (PII)
- Support the development of policies that contain:
 - 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

2.4 Given a scenario, conduct 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
- Design systems to facilitate incident response
 - Internal and external violations
 - Privacy policy violations
 - Criminal actions
 - Insider threat
 - Non-malicious threats/misconfigurations
 - Establish and review system, audit and security logs
- Incident and emergency response
 - Chain of custody
 - Forensic analysis of compromised system
 - Continuity of Operation Plan (COOP)
 - Order of volatility

3.0 Research, Analysis and Assessment

3.1 Apply research methods to determine industry trends and impact to the enterprise

- Perform ongoing research
 - Best practices
 - New technologies
 - New security systems and services
 - Technology evolution (e.g. RFCs, ISO)
- Situational awareness
 - Latest client-side attacks
 - Knowledge of current vulnerabilities and threats
 - Zero day mitigating controls and remediation
 - Emergent threats and issues
- Research security implications of new business tools
 - Social media/networking
 - End user cloud storage
 - Integration within the business
- Global IA industry/community
 - Computer Emergency Response Team (CERT)
 - Conventions/conferences
 - Threat actors
 - Emerging threat sources/threat intelligence
- Research security requirements for contracts
 - Request for Proposal (RFP)
 - Request for Quote (RFQ)
 - Request for Information (RFI)
 - Agreements

3.2 Analyze scenarios to secure the enterprise

- Create benchmarks and compare to baselines
- Prototype and test multiple solutions
- Cost benefit analysis
 - ROI
 - TCO
- Metrics collection and analysis
- Analyze and interpret trend data to anticipate cyber defense needs
- Review effectiveness of existing security controls
- Reverse engineer/deconstruct existing solutions
- Analyze security solution attributes to ensure they meet business needs:
 - Performance
 - Latency
 - Scalability
 - Capability
 - Usability
 - Maintainability
 - Availability
 - Recoverability
- Conduct a lessons-learned/after-action report
- Use judgment to solve difficult problems that do not have a best solution

3.3 Given a scenario, select methods or tools appropriate to conduct an assessment and analyze results

- Tool type
 - Port scanners
 - Vulnerability scanners
 - Protocol analyzer
 - Network enumerator

- Password cracker
- Fuzzer
- HTTP interceptor
- Exploitation tools/frameworks
- Passive reconnaissance and intelligence gathering tools
 - Social media
 - Whois
 - Routing tables
- Methods
 - Vulnerability assessment
 - Malware sandboxing
 - Memory dumping, runtime debugging
 - Penetration testing
 - Black box
 - White box
 - Grey box
 - Reconnaissance
 - Fingerprinting
 - Code review
 - Social engineering

4.0 Integration of Computing, Communications and Business Disciplines

4.1 Given a scenario, facilitate collaboration 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
- 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
- IT governance

4.2 Given a scenario, select the appropriate control to secure communications and collaboration solutions

- Security of unified collaboration tools
 - Web conferencing
 - Video conferencing
 - Instant messaging
 - Desktop sharing
 - Remote assistance
 - Presence
 - Email
 - Telephony
 - VoIP
 - Collaboration sites
 - Social media
 - Cloud-based
- Remote access
- Mobile device management
 - BYOD
- Over-the-air technologies concerns

4.3 Implement security activities across the technology life cycle

- End-to-end solution ownership
 - Operational activities
 - Maintenance
 - Commissioning/decommissioning
 - Asset disposal
 - Asset/object reuse
 - General change management
- Systems Development Life Cycle
 - Security System Development Life Cycle (SSDLIC)/Security Development Lifecycle (SDL)
 - Security Requirements Traceability Matrix (SRTM)
 - Validation and acceptance testing
 - Security implications of agile, waterfall and spiral software development methodologies
- Adapt solutions to address emerging threats and security trends
- Asset management (inventory control)
 - Device tracking technologies
 - Geo-location/GPS location
 - Object tracking and containment technologies
 - Geo-tagging/geo-fencing
 - RFID

5.0 Technical Integration of Enterprise Components

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

- Secure data flows to meet changing business needs
- Standards
 - Open standards

- Adherence to standards
- Competing standards
- Lack of standards
- Defacto standards
- Interoperability issues
 - Legacy systems/current systems
 - Application requirements
 - In-house developed vs. commercial vs. commercial customized
- Technical deployment models (Outsourcing/insourcing/managed services/partnership)
 - Cloud and virtualization considerations and hosting options
 - Public
 - Private
 - Hybrid
 - Community
 - Multi-tenancy
 - Single tenancy
 - Vulnerabilities associated with a single physical server hosting multiple companies' virtual machines
 - Vulnerabilities associated with a single platform hosting multiple companies' virtual machines
 - Secure use of on-demand/elastic cloud computing
 - Data remnants
 - Data aggregation
 - Data isolation
 - Resources provisioning and de-provisioning
 - Users
 - Servers
 - Virtual devices
 - Applications

- Securing virtual environments, services, applications, appliances and equipment
- 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
- Secure infrastructure design (e.g. decide where to place certain devices/applications)
- Storage integration (security considerations)
- Enterprise application integration enablers
 - CRM
 - ERP
 - GRC
 - ESB
 - SOA
 - Directory Services
 - DNS
 - CMDB
 - CMS

5.2 Given a scenario, integrate advanced authentication and authorization technologies to support enterprise objectives

- Authentication
 - Certificate-based authentication
 - Single sign-on
- Authorization
 - OAUTH
 - XACML
 - SPML

- Attestation
- Identity propagation
- Federation
 - SAML
 - OpenID
 - Shibboleth
 - WAYF
- Advanced trust models
 - RADIUS configurations
 - LDAP
 - AD

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. You can register for the exam at www.pearsonvue.com/comptia/.

About the Exam

The following are the characteristics of the exam:

- **Launches:** January 20, 2015
- **Number of questions:** 80 (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 braindumps 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-002 Blueprint, CompTIA includes a section titled “CompTIA Authorized Materials Use Policy” that details how to determine whether the materials you are using are from a legitimate company or a braindump company. This section includes a link for more information and a link to a site that will tell you if a particular provider is legitimate or a braindump, based on analysis of the content. Remember: Just because you purchase a product does not mean that the product is legitimate. Some of the best braindump companies out there charge for their products. Also, keep in mind that using materials from a braindump can result in certification revocation. Please make sure that all products you use are from a legitimate provider rather than a braindump company. Using a braindump is cheating and directly violates the nondisclosure agreement (NDA) you sign at exam time.

NOTE The following CompTIA Authorized Materials Use Policy is copied directly from the CompTIA exam blueprint. If you have any questions regarding the study materials you are considering using for this or any other CompTIA exam, please visit www.certguard.com. When you reach that site, shown in Figure I-2, simply enter the URL of the site from which materials come, and the site will tell you if the materials are authorized.

CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.



Figure I-2 CompTIA Authorized Materials Use Policy

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 webpage:

<http://certification.comptia.org/Training/testingcenters/policies.aspx>

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 (<http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx>) at the time of exam delivery.

If a candidate has a question as to whether study materials are considered unauthorized (aka brain dumps), he/she should perform a search using CertGuard's engine, found here:

<http://www.certguard.com/search.asp>

Or verify against this list:

<http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx>

NOTE *The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document.*

This page intentionally left blank



This chapter covers the following topics:

- **Secure Data Flows to Meet Changing Business Needs:** This section discusses security controls that can be deployed when business needs change.
- **Standards:** This section describes open standards, adherence to standards, competing standards, lack of standards, and de facto standards.
- **Interoperability Issues:** Topics covered include legacy systems/current systems, application requirements, and in-house developed versus commercial versus commercial customized applications.
- **Technical Deployment Models:** This section explains outsourcing/insourcing/managed services/partnerships, including cloud and virtualization, resource provisioning/deprovisioning, and securing and designing solutions.
- **Logical Deployment Diagram and Corresponding Physical Deployment Diagram of All Relevant Devices:** This section explains the differences between logical and physical deployment diagrams.
- **Secure Infrastructure Design:** This section gives examples of different network design models based on the network types included.
- **Storage Integration (Security Considerations):** This section lists security guidelines for integrating storage solutions.
- **Enterprise Application Integration Enablers:** This section discusses the different options available to the enterprise and when they should be deployed.

This chapter covers CASP objective 5.1.

Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture

Organizations must securely integrate hosts, storage, networks, and applications. It is a security practitioner's responsibility to ensure that the appropriate security controls are implemented and tested. But this isn't the only step a security practitioner must take. Security practitioners must also:

- Secure data flows to meet changing business needs.
- Understand standards.
- Understand interoperability issues.
- Understand technical deployment models, including outsourcing, insourcing, managed services, and partnerships.
- Know how to segment and delegate a secure network.
- Analyze logical and physical deployment diagrams of all relevant devices.
- Design a secure infrastructure.
- Integrate secure storage solutions within the enterprise.
- Deploy enterprise application integration enablers.

All these points are discussed in detail in this chapter.

Foundation Topics

Secure Data Flows to Meet Changing Business Needs

Business needs of an organization may change and require that security devices or controls be deployed in a different manner to protect data flow. As a security practitioner, you should be able to analyze business changes, how they affect security, and then deploy the appropriate controls.

Key Topic

To protect data during transmission, security practitioners should identify confidential and private information. Once this data has been properly identified, the following analysis steps should occur:

1. Determine which applications and services access the information.
2. Document where the information is stored.
3. Document which security controls protect the stored information.
4. Determine how the information is transmitted.
5. Analyze whether authentication is used when accessing the information.
 - If it is, determine whether the authentication information is securely transmitted.
 - If it is not, determine whether authentication can be used.
6. Analyze enterprise password policies, including password length, password complexity, and password expiration.
7. Determine whether encryption is used to transmit data.
 - If it is, ensure that the level of encryption is appropriate and that the encryption algorithm is adequate.
 - If it is not, determine whether encryption can be used.
8. Ensure that the encryption keys are protected.

Security practitioners should adhere to the defense-in-depth principle to ensure that the CIA of data is ensured across its entire life cycle. Applications and services should be analyzed to determine whether more secure alternatives can be used or whether inadequate security controls are deployed. Data at rest may require encryption to provide full protection and appropriate access control lists (ACLs) to ensure that only authorized users have access. For data transmission, secure protocols and

encryption should be employed to prevent unauthorized users from being able to intercept and read data. The most secure level of authentication possible should be used in the enterprise. Appropriate password and account policies can protect against possible password attacks.

NOTE The defense-in-depth principle is further described in the introduction of this book.

Finally, security practitioners should ensure that confidential and private information is isolated from other information, including locating the information on separate physical servers and isolating data using virtual LANs (VLANs). Disable all unnecessary services, protocols, and accounts on all devices. Make sure that all firmware, operating systems, and applications are kept up-to-date, based on the vendor recommendations and releases.

When new technologies are deployed based on the changing business needs of the organization, security practitioners should be diligent to ensure that they understand all the security implications and issues with the new technology. Deploying a new technology before proper security analysis has occurred can result in security breaches that affect more than just the newly deployed technology. Remember that changes are inevitable! How you analyze and plan for these changes is what will set you apart from other security professionals.

Standards

Standards describe how policies will be implemented within an organization. They are actions or rules that are tactical in nature, meaning they provide the steps necessary to achieve security. Just like policies, standards should be regularly reviewed and revised. Standards are usually established by a governing organization, such as the National Institute of Standards and Technology (NIST).

The following sections briefly discuss open standards, adherence to standards, competing standards, lack of standards, and de facto standards.

NOTE Standards are discussed in greater detail in Chapter 5, “Application Vulnerabilities and Security Controls;” Chapter 7, “Risk Mitigation Planning, Strategies, and Controls;” Chapter 8, “Security, Privacy Policies, and Procedures;” Chapter 10, “Industry Trends;” and Chapter 15, “Security Across the Technology Life Cycle.”

Open Standards

Open standards are standards that are open to the general public. The general public can provide feedback on the standards and may use the standards without purchasing any rights to the standards or organizational membership. It is important that subject matter and industry experts help guide the development and maintenance of these standards.

Adherence to Standards

Organizations may opt to adhere entirely to both open standards and those managed by a standards organization. Some organizations may even choose to adopt selected parts of standards, depending on the industry. Remember that an organization should fully review any standard and analyze how its adoption will affect the organization.

Legal implications can arise if an organization ignores well-known standards. Neglecting to use standards to guide your organization's security strategy, especially if others in your industry do, can significantly impact your organization's reputation and standing.

Competing Standards

Competing standards most often come into effect between competing vendors. For example, Microsoft often establishes its own standards for authentication. Many times, its standards are based on an industry standard with slight modifications to suit Microsoft's needs. In contrast, Linux may implement standards, but because it is an open source operating system, changes may have been made along the way that may not fully align with the standards your organization needs to follow. Always compare competing standards to determine which standard best suits your organization's needs.

Lack of Standards

In some new technology areas, standards are not formulated yet. Do not let a lack of formal standards prevent you from providing the best security controls for your organization. If you can find similar technology that has formal adopted standards, test the viability of those standards for your solution. In addition, you may want to solicit input from subject matter experts (SMEs). A lack of standards does not excuse your organization from taking every precaution necessary to protect confidential and private data.

De Facto Standards

De facto standards are standards that are widely accepted but not formally adopted. De jure standards are standards that are based on laws or regulations and are adopted by international standards organizations. De jure standards should take precedence over de facto standards. If possible, your organization should adopt security policies that implement both de facto and de jure standards.

Let's look at an example. Suppose that a chief information officer's (CIO's) main objective is to deploy a system that supports the 802.11r standard, which will help wireless VoIP devices in moving vehicles. However, the 802.11r standard has not been formally ratified. The wireless vendor's products do support 802.11r as it is currently defined. The administrators have tested the product and do not see any security or compatibility issues; however, they are concerned that the standard is not yet final. The best way to proceed would be to purchase the equipment now, as long as its firmware will be upgradable to the final 802.11r standard.

Interoperability Issues

When integrating solutions into a secure enterprise architecture, security practitioners must ensure that they understand all the interoperability issues that can occur with legacy systems/current systems, applications, and in-house versus commercial versus commercial customized applications.

Legacy Systems/Current Systems

Legacy systems are old technologies, computers, or applications that are considered outdated but provide a critical function in the enterprise. Often the vendor no longer supports the legacy systems, meaning that no future updates to the technology, computer, or application will be provided. It is always best to replace these systems as soon as possible because of the security issues they introduce. However, sometimes these systems must be retained because of the critical function they provide.

Key Topic

Some guidelines when retaining legacy systems include:

- If possible, implement the legacy system in a protected network or demilitarized zone (DMZ).
- Limit physical access to the legacy system to administrators.
- If possible, deploy the legacy application on a virtual computer.
- Employ access control lists (ACLs) to protect the data on the system.
- Deploy the highest-level authentication and encryption mechanisms possible.

Let's look at an example. Suppose an organization has a legacy customer relationship application that it needs to retain. The application requires the Windows 2000 operating system (OS), and the vendor no longer supports the application. The organization could deploy a Windows 2000 virtual machine (VM) and move the application to that VM. Users needing access to the application could use Remote Desktop to access the VM and the application.

Let's look at a more complex example. Say that an administrator replaces servers whenever budget money becomes available. Over the past several years, the

company uses 20 servers and 50 desktops from five different vendors. The management challenges and risks associated with this style of technology life cycle management include increased mean time to failure rate of legacy servers, OS variances, patch availability, and the ability to restore dissimilar hardware.

Application Requirements

Any application installed may require certain hardware, software, or other criteria that the organization does not use. However, with recent advances in virtual technology, the organization can implement a virtual machine that fulfills the criteria for the application through virtualization. For example, an application may require a certain screen resolution or graphics driver that is not available on any physical computers in the enterprise. In this case, the organization could deploy a virtual machine that includes the appropriate screen resolution or driver so that the application can be successfully deployed.

Keep in mind that some applications may require older versions of operating systems that are not available. In recent versions of Windows, you can choose to deploy an application in compatibility mode by using the Compatibility tab of the application's executable file, as shown in Figure 16-1.

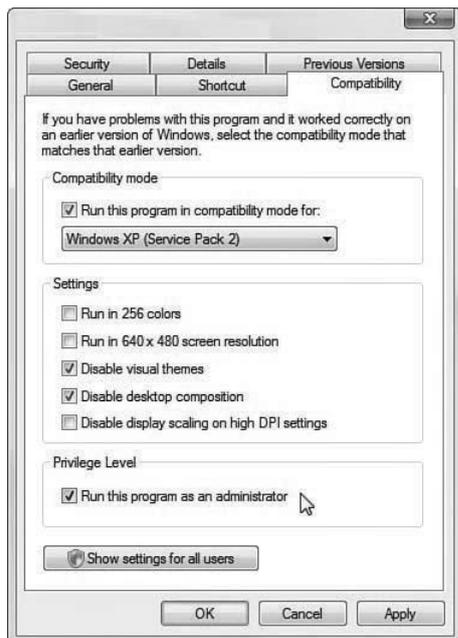


Figure 16-1 Compatibility Tab

In-House Developed Versus Commercial Versus Commercial Customized Applications

Applications can be developed in-house or purchased commercially. Applications that are developed in-house can be completely customized to the organization, provided that developers have the necessary skills, budget, and time. Commercial applications may provide customization options to the organization. However, usually the customization is limited.

Organizations should fully research their options when a new application is needed. Once an organization has documented its needs, it can compare them to all the commercially available applications to see if any of them will work. It is usually more economical to purchase a commercial solution than to develop an in-house solution. However, each organization needs to fully assess the commercial application costs versus in-house development costs.

Commercial software is well known and widely available and is commonly referred to as commercial off-the-shelf (COTS) software. Information concerning vulnerabilities and viable attack patterns is typically shared within the IT community. This means that using commercial software can introduce new security risks in the enterprise. Also, it is difficult to verify the security of commercial software code because the source is not available to customers in most cases.

NOTE For more information regarding application issues and controls, refer to Chapter 5. For more information on the systems development life cycle, refer to Chapter 15.

Technical Deployment Models

To integrate hosts, storage solutions, networks, and applications into a secure enterprise, an organization may use various technical deployment models, including outsourcing, insourcing, managed services, and partnerships. The following sections discuss cloud and virtualization considerations and hosting options, virtual machine vulnerabilities, secure use of on-demand/elastic cloud computing, data remnants, data aggregation, and data isolation.

NOTE For more information on the risks of the different business models, refer to Chapter 6, “Business Influences and Associated Security Risks.”

Cloud and Virtualization Considerations and Hosting Options

Cloud computing allows enterprise assets to be deployed without the end user knowing where the physical assets are located or how they are configured.

Virtualization involves creating a virtual device on a physical resource; physical resources can hold more than one virtual device. For example, you can deploy multiple virtual computers on a Windows computer. But keep in mind that each virtual machine will consume some of the resources of the host machine, and the configuration of the virtual machine cannot exceed the resources of the host machine.

For the CASP exam, you must understand public, private, hybrid, community, multi-tenancy, and single-tenancy cloud options.

NOTE For more information regarding virtualization issues, refer to Chapter 4, “Security Controls for Hosts.” For more information regarding cloud issues, refer to Chapter 6.

Public Cloud

A public cloud is the standard cloud computing model, where a service provider makes resources available to the public over the Internet. Public cloud services may be free or may be offered on a pay-per-use model. An organization needs to have a business or technical liaison responsible for managing the vendor relationship but does not necessarily need a specialist in cloud deployment. Vendors of public cloud solutions include Amazon, IBM, Google, and Microsoft. In a public cloud model, subscribers can add and remove resources as needed, based on their subscription.

Private Cloud

A private cloud is a cloud computing model where a private organization implements a cloud in its internal enterprise, and that cloud is used by the organization’s employees and partners. Private cloud services require an organization to employ a specialist in cloud deployment to manage the private cloud.

Hybrid Cloud

A hybrid cloud is a cloud computing model where an organization provides and manages some resources in-house and has others provided externally via a public cloud. This model requires a relationship with the service provider as well as an in-house cloud deployment specialist. Rules need to be defined to ensure that a hybrid

cloud is deployed properly. Confidential and private information should be limited to the private cloud.

Community Cloud

A community cloud is a cloud computing model where the cloud infrastructure is shared among several organizations from a specific group with common computing needs. In this model, agreements should explicitly define the security controls that will be in place to protect the data of each organization involved in the community cloud and how the cloud will be administered and managed.

Multi-Tenancy Model

A multi-tenancy model is a cloud computing model where multiple organizations share the resources. This model allows the service providers to manage the resource utilization more efficiently. In this model, organizations should ensure that their data is protected from access by other organizations or unauthorized users. In addition, organizations should ensure that the service provider will have enough resources for the future needs of the organization. If multi-tenancy models are not properly managed, one organization can consume more than its share of resources, to the detriment of the other organizations involved in the tenancy.

Single-Tenancy Model

A single-tenancy model is a cloud computing model where a single tenant uses a resource. This model ensures that the tenant organization's data is protected from other organizations. However, this model is more expensive than the multi-tenancy model.

Vulnerabilities Associated with a Single Physical Server Hosting Multiple Companies' Virtual Machines

In some virtualization deployments, a single physical server hosts multiple organizations' VMs. All of the VMs hosted on a single physical computer must share the resources of that physical server. If the physical server crashes or is compromised, all of the organizations that have VMs on that physical server are affected. User access to the VMs should be properly configured, managed, and audited. Appropriate security controls, including antivirus, antimalware, access control lists (ACLs), and auditing, must be implemented on each of the VMs to ensure that each one is properly protected. Other risks to consider include physical server resource depletion, network resource performance, and traffic filtering between virtual machines.

Driven mainly by cost, many companies outsource to cloud providers computing jobs that require a large amount of processor cycles for a short duration. This situation allows a company to avoid a large investment in computing resources that will be used for only a short time. Assuming that the provisioned resources are dedicated to a single company, the main vulnerability associated with on-demand provisioning is traces of proprietary data that can remain on the virtual machine and may be exploited.

Let's look at an example. Say that a security architect is seeking to outsource company server resources to a commercial cloud service provider. The provider under consideration has a reputation for poorly controlling physical access to data centers and has been the victim of social engineering attacks. The service provider regularly assigns VMs from multiple clients to the same physical resource. When conducting the final risk assessment, the security architect should take into consideration the likelihood that a malicious user will obtain proprietary information by gaining local access to the hypervisor platform.

Vulnerabilities Associated with a Single Platform Hosting Multiple Companies' Virtual Machines

In some virtualization deployments, a single platform hosts multiple organizations' VMs. If all of the servers that host VMs use the same platform, attackers will find it much easier to attack the other host servers once the platform is discovered. For example, if all physical servers use VMware to host VMs, any identified vulnerabilities for that platform could be used on all host computers. Other risks to consider include misconfigured platforms, separation of duties, and application of security policy to network interfaces.

If an administrator wants to virtualize the company's web servers, application servers, and database servers, the following should be done to secure the virtual host machines: only access hosts through a secure management interface and restrict physical and network access to the host console.

Secure Use of On-demand/Elastic Cloud Computing

On-demand, or elastic, cloud computing allows administrators to increase or decrease the resources utilized based on organizational needs. As demands increase, the costs increase. Therefore, it is important that resource allocation be closely monitored and managed to ensure that the organization is not paying for more resources than needed. Administrators should always use secure tools (such as Secure Shell) and encryption to connect to the host when allocating or deallocating resources.

Data Remnants

Data remnants are data that is left behind on a computer or another resource when that resource is no longer used. The best way to protect this data is to employ some sort of data encryption. If data is encrypted, it cannot be recovered without the original encryption key. If resources, especially hard drives, are reused frequently, an unauthorized user can access data remnants.

Administrators must understand the kind of data that is stored on physical drives. This helps them determine whether data remnants should be a concern. If the data stored on a drive is not private or confidential, the organization may not be concerned about data remnants. However, if the data stored on the drive is private or confidential, the organization may want to implement asset reuse and disposal policies.

NOTE For more information on asset reuse and disposal, refer to Chapter 15.

Data Aggregation

Data aggregation allows data from multiple resources to be queried and compiled together into a summary report. The account used to access the data needs to have appropriate permissions on all of the domains and servers involved. In most cases, these types of deployments will incorporate a centralized data warehousing and mining solution on a dedicated server.

Data Isolation

Data isolation in databases prevents data from being corrupted by two concurrent operations. Data isolation is used in cloud computing to ensure that tenant data in a multi-tenant solution is isolated from other tenants' data, using a tenant ID in the data labels. Trusted login services are usually used as well. In both of these deployments, data isolation should be monitored to ensure that data is not corrupted. In most cases, some sort of transaction rollback should be employed to ensure that proper recovery can be made.

Resource Provisioning and Deprovisioning

One of the benefits of many cloud deployments is the ability to provision and deprovision resources as needed. This includes provisioning and deprovisioning users, servers, virtual devices, and applications. Depending on the deployment model used, your organization may have an internal administrator that handles these tasks, the

cloud provider may handle these tasks, or you may have some hybrid solution where these tasks are split between the internal administrator and cloud provider personnel. Remember that any solution where cloud provider personnel must provide provisioning and deprovisioning may not be ideal because cloud provider personnel may not be immediately available to perform any tasks that you need.

Users

When provisioning (or creating) user accounts, it is always best to use an account template. This ensures that all of the appropriate password policies, user permissions, and other account settings are applied to the newly created account.

When deprovisioning a user account, you should consider first disabling the account. Once an account is deleted, it may be impossible to access files, folders, and other resources that are owned by that user account. If the account is disabled instead of deleted, the administrator can reenable the account temporarily to access the resources owned by that account.

An organization should adopt a formal procedure for requesting the creation, disablement, or deletion of user accounts. In addition, administrators should monitor account usage to ensure that accounts are active.

Servers

Provisioning and deprovisioning servers should be based on organizational need and performance statistics. To determine when a new server should be provisioned, administrators must monitor the current usage of the server resources. Once a predefined threshold has been reached, procedures should be put in place to ensure that new server resources are provisioned. When those resources are no longer needed, procedures should also be in place to deprovision the servers. Once again, monitoring is key.

Virtual Devices

Virtual devices consume resources of the host machine. For example, the memory on a physical machine is shared among all the virtual devices that are deployed on that physical machine. Administrators should provision new virtual devices when organizational need demands. However, it is just as important that virtual devices be deprovisioned when they are no longer needed to free up the resources for other virtual devices.

Applications

Organizations often need a variety of applications. It is important to maintain the licenses for any commercial applications that are used. When an organization no longer needs applications, administrators must be notified to ensure that licenses are not renewed or that they are renewed at a lower level if usage has simply decreased.

Securing Virtual Environments, Services, Applications, Appliances, and Equipment

When an organization deploys virtual environments, administrators and security practitioners must ensure that the virtual environments are secured in the same manner as any physical deployments of that type. For example, a virtual Windows machine needs to have the same security controls as the host server, including anti-virus/antimalware software, ACLs, operating system updates, and so on. This also applies to services, applications, appliances, and equipment. You should ensure that all of the security controls are deployed as spelled out in the organization's security policies.

Design Considerations During Mergers, Acquisitions, and Demergers/Divestitures

When organizations merge, are acquired, or split, the enterprise design must be considered. In the case of mergers or acquisitions, each separate organization has its own resources, infrastructure, and model. As a security practitioner, it is important that you ensure that two organizations' structures are analyzed thoroughly before deciding how to merge them. For demergers, you probably have to help determine how to best divide the resources. The security of data should always be a top concern.

NOTE For more on the risks of these deployments, refer to Chapter 6.

Network Secure Segmentation and Delegation

An organization may need to segment its network to improve network performance, to protect certain traffic, or for a number of other reasons. Segmenting the enterprise network is usually achieved through the use of routers, switches, and firewalls. A network administrator may decide to implement VLANs using switches or deploy a demilitarized zone (DMZ) using firewalls. No matter how you choose to segment the network, you should ensure that the interfaces that connect the segments are as secure as possible. This may mean closing ports, implementing MAC filtering, and

using other security controls. In a virtualized environment, you can implement separate physical trust zones. When the segments or zones are created, you can delegate separate administrators who are responsible for managing the different segments or zones.

Logical and Physical Deployment Diagrams of Relevant Devices

Key Topic

For the CASP exam, security practitioners must understand two main types of enterprise deployment diagrams: logical deployment diagrams and physical deployment diagrams. A logical deployment diagram shows the architecture, including the domain architecture, with the existing domain hierarchy, names, and addressing scheme; server roles; and trust relationships. A physical deployment diagram shows the details of physical communication links, such as cable length, grade, and wiring paths; servers, with computer name, IP address (if static), server role, and domain membership; device location, such as printer, hub, switch, modem, router, or bridge, as well as proxy location; communication links and the available bandwidth between sites; and the number of users, including mobile users, at each site. A logical diagram usually contains less information than a physical diagram. While you can often create a logical diagram from a physical diagram, it is nearly impossible to create a physical diagram from a logical one.

An example of a logical network diagram is shown in Figure 16-2.

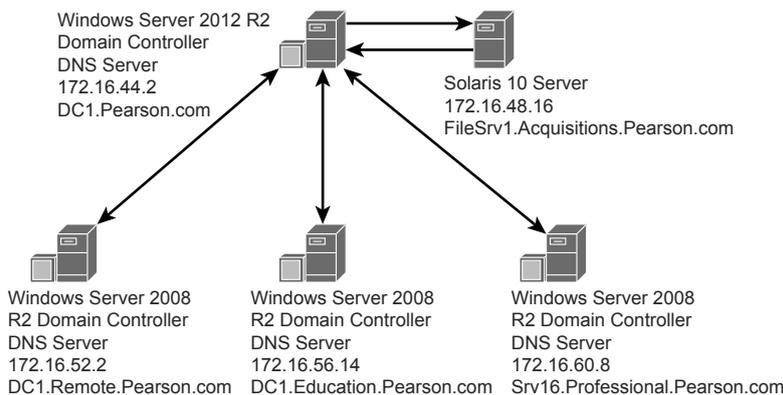


Figure 16-2 Logical Network Diagram

As you can see, the logical diagram shows only a few of the servers in the network, the services they provide, their IP addresses, and their DNS names. The relationships between the different servers are shown by the arrows between them.

Secure Infrastructure Design

As part of the CASP exam, security practitioners must be able to analyze a scenario and decide on the best placement for devices, servers, and applications. To better understand this, it is necessary to understand the different network designs that can be used. Network designs may include demilitarized zones (DMZs), VLANs, virtual private networks (VPNs), and wireless networks. This section shows examples of how these areas look. It also discusses situations in which you may need to decide where to deploy certain devices.

DMZs

A DMZ contains servers that must be accessed by the general public or partners over an Internet connection. DMZs can also be referred to as screened subnets. Placing servers on a DMZ protects the internal network from the traffic that the servers on the DMZ generate. Several examples of networks with DMZs are shown in Figure 16-4.

Key Topic

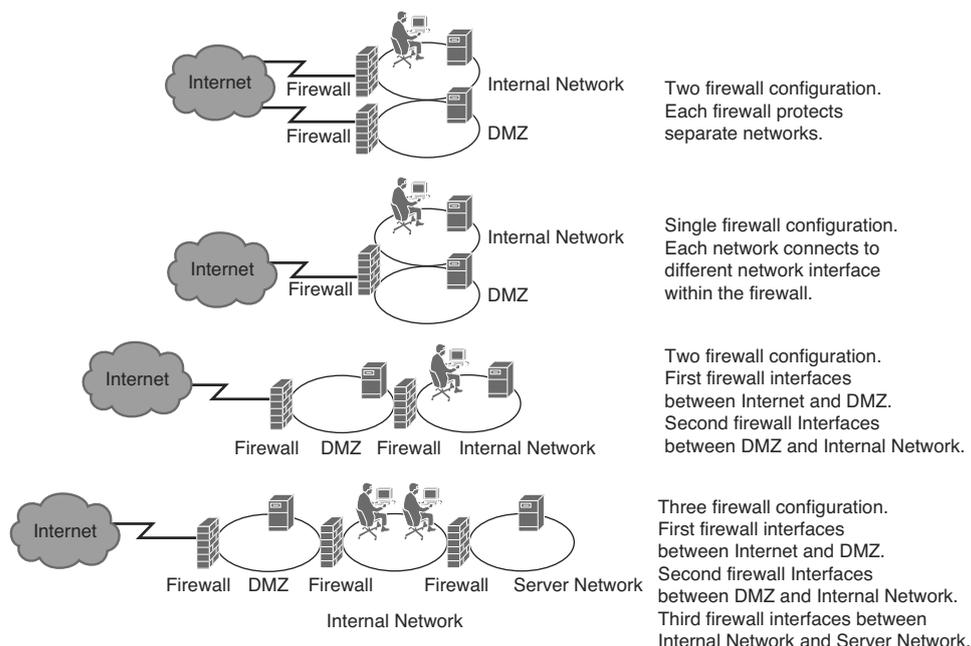


Figure 16-4 DMZ Examples

In DMZ deployments, you can configure the firewalls to allow or deny certain traffic based on a variety of settings, including IP address, MAC address, port number, or protocol. Often web servers and external-facing DNS servers are deployed on a

DMZ, with database servers and internal DNS servers being deployed on the internal network. If this is the case, then it may be necessary to configure the appropriate rules on the firewall to allow the web server to communicate with the database server and allow the external-facing DNS server to communicate with the internal DNS servers. Remember that you can also configure access rules on routers. It is important that you deploy access rules on the appropriate devices. For example, if you deny certain types of traffic on the Internet-facing router, all of that type of traffic will be unable to leave or enter the DMZ or internal network. Always analyze where the rules should be applied before creating them.

VLANs

A VLAN is a virtual network that is created using a switch. All computers and devices that are connected to a switch can be divided into separate VLANs, based on organizational needs. An example of a network with VLANs is shown in Figure 16-5.

**Key
Topic**

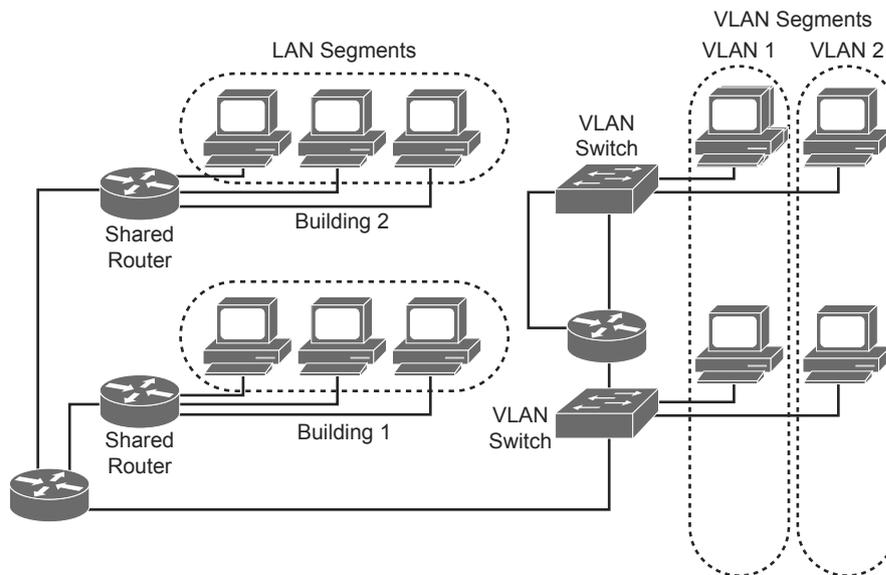


Figure 16-5 VLAN Example

In this type of deployment, each switch can have several VLANs. A single VLAN can exist on a single switch or can span multiple switches. Configuring VLANs helps manage the traffic on the switch. If you have a legacy system that is not scheduled to be decommissioned for two years and requires the use of the standard Telnet protocol, moving the system to a secure VLAN would provide the security needed until the system can be decommissioned.

VPNs

A VPN allows external devices to access an internal network by creating a tunnel over the Internet. Traffic that passes through the VPN tunnel is encrypted and protected. An example of a network with a VPN is shown in Figure 16-6.

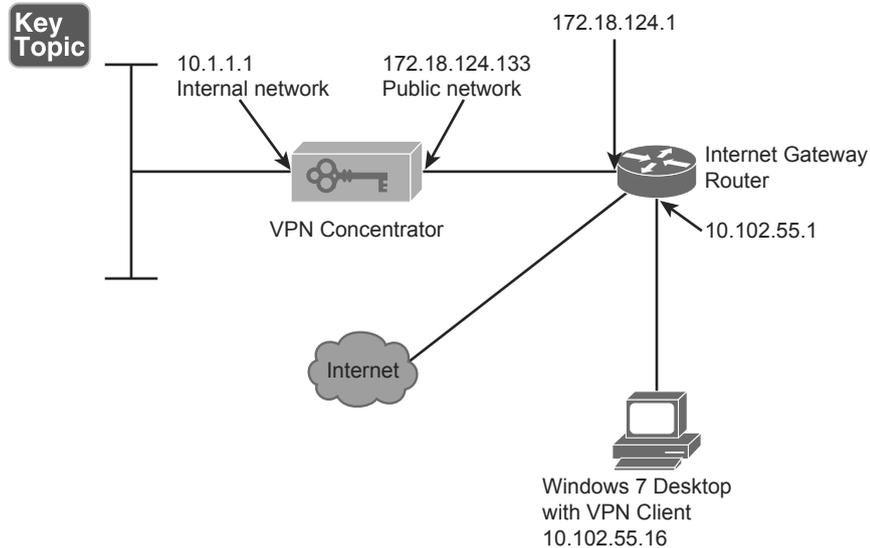


Figure 16-6 VPN Example

In a VPN deployment, only computers that have the VPN client and are able to authenticate will be able to connect to the internal resources through the VPN concentrator.

Wireless Networks

A wireless network allows devices to connect to the internal network through a wireless access point. An example of a network that includes a wireless access point is shown in Figure 16-7.

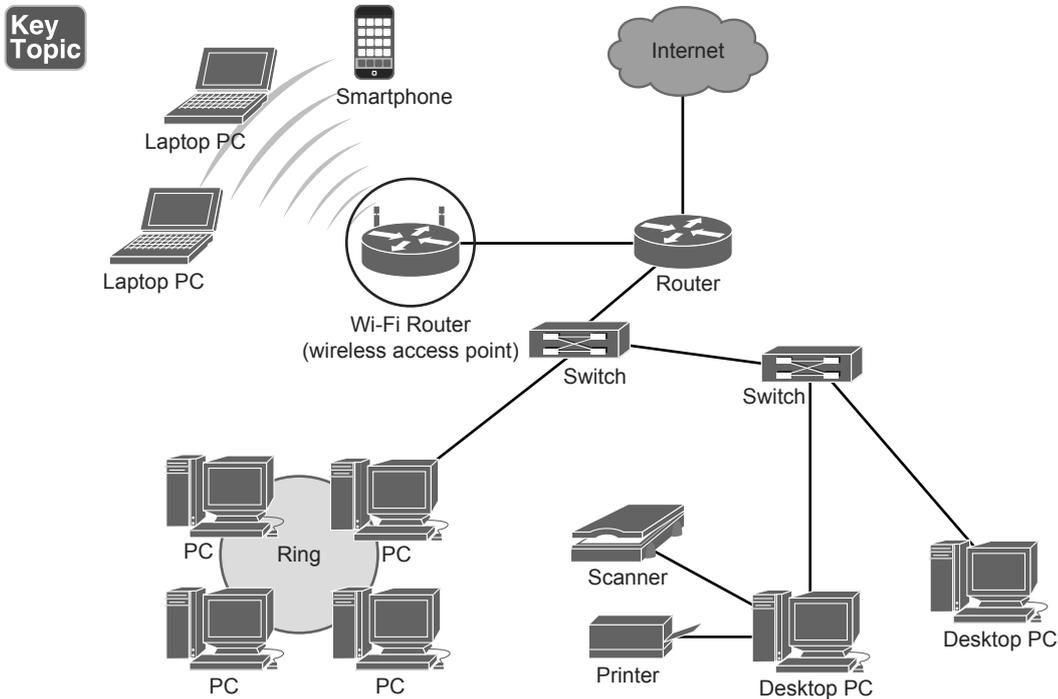


Figure 16-7 Wireless Network Example

In the deployment shown in Figure 16-7, some devices connect to the wired network, while others connect to the wireless network. The wireless network can be protected using a variety of mechanisms, including disabling the service set identifier (SSID), enabling WPA2, and implementing MAC filtering. For some organizations, it may be necessary to implement more than one wireless access point. If this occurs and all the access points use the same 802.11 implementation, then the access points will need to be configured to use different channels within that implementation. In addition, it may be necessary to adjust the signal strength of the access points to limit the coverage area.

Finally, when deciding where to place certain devices, you need to consider whether a device needs to be stored in a secured location. For example, routers, firewalls, switches, server racks, and servers are usually stored in rooms or data centers that have extra physical security controls in addition to the regular physical building security. Always consider the physical security needs when deploying any new devices.

Storage Integration (Security Considerations)

When integrating storage solutions into an enterprise, security practitioners should be involved in the design and deployment to ensure that security considerations are considered.

Key Topic

The following are some of the security considerations for storage integration that you should consider:

- Limit physical access to the storage solution.
- Create a private network to manage the storage solution.
- Implement ACLs for all data, paths, subnets, and networks.
- Implement ACLs at the port level, if possible.
- Implement multi-factor authentication.

Security practitioners should ensure that an organization adopts appropriate security policies for storage solutions to ensure that storage administrators prioritize the security of the storage solutions.

Enterprise Application Integration Enablers

Enterprise application integration enablers ensure that applications and services in an enterprise are able to communicate as needed. For the CASP exam, the primary concerns are understanding which enabler is needed in a particular situation or scenario and ensuring that the solution is deployed in the most secure manner possible. The solutions that you must understand include customer relationship management (CRM); enterprise resource planning (ERP); governance, risk, and compliance (GRC); enterprise service bus (ESB); service-oriented architecture (SOA); Directory Services; Domain Name System (DNS); configuration management database (CMDB); and content management systems (CMSs).

CRM

Customer relationship management (CRM) identifies customers and stores all customer-related data, particularly contact information and data on any direct contacts with customers. The security of CRM is vital to an organization. In most cases, access to the CRM is limited to sales and marketing personnel and management. If remote access to CRM is required, you should deploy a VPN or similar solution to ensure that the CRM data is protected.

ERP

Enterprise resource planning (ERP) collects, stores, manages, and interprets data from product planning, product cost, manufacturing or service delivery, marketing/sales, inventory management, shipping, payment, and any other business processes. ERP is accessed by personnel for reporting purposes. ERP should be deployed on a secured internal network or DMZ. When deploying ERP, you might face objections because some departments may not want to share their process information with other departments.

GRC

Governance, risk, and compliance (GRC) coordinates information and activity across these three areas to be more efficient, to enable information sharing and reporting, and to avoid waste. This integration improves the overall security posture of any organization. However, the information stored in GRC is tied closely to the organization's security. Access to this system should be tightly controlled.

ESB

Enterprise service bus (ESB) designs and implements communication between mutually interacting software applications in a service-oriented architecture (SOA). It allows SOAP, Java, .NET, and other applications to communicate. An ESB solution is usually deployed on a DMZ to allow communication with business partners.

ESB is the most suitable solution for providing event-driven and standards-based secure software architecture.

SOA

Service-oriented architecture (SOA) uses software pieces to provide application functionality as services to other applications. A service is a single unit of functionality. Services are combined to provide the entire functionality needed. This architecture often intersects with web services.

Let's look at an SOA scenario. Suppose a database team suggests deploying an SOA-based system across the enterprise. The chief information officer (CIO) decides to consult the security manager about the risk implications for adopting this architecture. The security manager should present to the CIO two concerns for the SOA system: Users and services are distributed, often over the Internet, and SOA abstracts legacy systems such as web services, which are often exposed to outside threats.

Directory Services

Directory Services stores, organizes, and provides access to information in a computer operating system's directory. With Directory Services, users can access a resource by using the resource's name instead of its IP or MAC address. Most enterprises implement an internal Directory Services server that handles any internal requests. This internal server communicates with a root server on a public network or with an externally facing server that is protected by a firewall or other security device to obtain information on any resources that are not on the local enterprise network. Active Directory, DNS, and LDAP are examples of directory services.

DNS

Domain Name System (DNS) provides a hierarchical naming system for computers, services, and any resources connected to the Internet or a private network. You should enable Domain Name System Security Extensions (DNSSEC) to ensure that a DNS server is authenticated before the transfer of DNS information begins between the DNS server and client. Transaction Signature (TSIG) is a cryptographic mechanism used with DNSSEC that allows a DNS server to automatically update client resource records if their IP addresses or hostnames change. The TSIG record is used to validate a DNS client.

As a security measure, you can configure internal DNS servers to communicate only with root servers. When you configure internal DNS servers to communicate only with root servers, the internal DNS servers are prevented from communicating with any other external DNS servers.

The Start of Authority (SOA) contains the information regarding a DNS zone's authoritative server. A DNS record's Time to Live (TTL) determines how long a DNS record will live before it needs to be refreshed. When a record's TTL expires, the record is removed from the DNS cache. Poisoning the DNS cache involves adding false records to the DNS zone. If you use a longer TTL, the resource record is read less frequently and therefore is less likely to be poisoned.

Let's look at a security issue that involves DNS. An IT administrator installs new DNS name servers that host the company mail exchanger (MX) records and resolve the web server's public address. To secure the zone transfer between the DNS servers, the administrator uses only server ACLs. However, any secondary DNS servers would still be susceptible to IP spoofing attacks.

Another scenario could occur when a security team determines that someone from outside the organization has obtained sensitive information about the internal organization by querying the company's external DNS server. The security manager should address the problem by implementing a split DNS server, allowing the external DNS server to contain only information about domains that the outside world

should be aware of the internal DNS server to maintain authoritative records for internal systems.

CMDB

A configuration management database (CMDB) keeps track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships between such assets. The IT department typically uses CMDBs as data warehouses.

CMS

A content management system (CMS) publishes, edits, modifies, organizes, deletes, and maintains content from a central interface. This central interface allows users to quickly locate content. Because edits occur from this central location, it is easy for users to view the latest version of the content. Microsoft SharePoint is an example of a CMS.

Exam Preparation Tasks

You have a couple of choices for exam preparation: the exercises here and the exam simulation questions on the CD-ROM.

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 16-1 lists these key topics and the page number on which each is found.



Table 16-1 Key Topics for Chapter 16

Key Topic Element	Description	Page Number
Paragraph/numbered list	Secure data flow steps	534
Bulleted list	Legacy system guidelines	537
Paragraph	Logical versus physical deployment models	546
Figure 16-4	DMZ example	548
Figure 16-5	VLAN example	549
Figure 16-6	VPN example	550
Figure 16-7	Wireless example	551
Bulleted list	Storage integration security considerations	552

Define Key Terms

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

open standards; de facto standards; de jure standards; legacy system; public cloud; private cloud; hybrid cloud; community cloud; multi-tenancy cloud model; single-tenancy cloud model; data remnants; data aggregation; data isolation; logical deployment diagram; physical deployment diagram; customer relationship management (CRM); enterprise resource planning (ERP); governance, risk, and compliance (GRC), enterprise service bus (ESB); service-oriented architecture (SOA); directory services; Domain Name System (DNS); configuration management database (CMDB); content management system (CMS)

Review Questions

- Several business changes have occurred in your company over the past six months. You must analyze your enterprise's data to ensure that data flows are protected. Which of the following guidelines should you follow? (Choose all that apply.)
 - Determine which applications and services access the data.
 - Determine where the data is stored.
 - Share encryption keys with all users.
 - Determine how the data is transmitted.
- During a recent security analysis, you determine that users do not use authentication when accessing some private data. What should you do first?
 - Encrypt the data.
 - Configure the appropriate ACL for the data.
 - Determine whether authentication can be used.
 - Implement complex user passwords.
- Your organization must comply with several industry and governmental standards to protect private and confidential information. You must analyze which standards to implement. Which standards should you consider?
 - open standards, de facto standards, and de jure standards
 - open standards only
 - de facto standards only
 - de jure standards only

4. Your organization has recently experienced issues with data storage. The servers you currently use do not provide adequate storage. After researching the issues and the options available, you decide that data storage needs for your organization will grow exponentially over the next couple years. However, within three years, data storage needs will return to the current demand. Management wants to implement a solution that will provide for the current and future needs without investing in hardware that will no longer be needed in the future. Which recommendation should you make?
 - a. Deploy virtual servers on the existing machines.
 - b. Contract with a public cloud service provider.
 - c. Deploy a private cloud service.
 - d. Deploy a community cloud service.

5. Management expresses concerns about using multi-tenant public cloud solutions to store organizational data. You explain that tenant data in a multi-tenant solution is quarantined from other tenants' data using a tenant ID in the data labels. What is this condition referred to?
 - a. data remnants
 - b. data aggregation
 - c. data purging
 - d. data isolation

6. You have been hired as a security practitioner for an organization. You ask the network administrator for any network diagrams that are available. Which network diagram would give you the most information?
 - a. logical network diagram
 - b. wireless network diagram
 - c. physical network diagram
 - d. DMZ diagram

7. Your organization has recently partnered with another organization. The partner organization needs access to certain resources. Management wants you to create a perimeter network that contains only the resources that the partner organization needs to access. What should you do?
 - a. Deploy a DMZ.
 - b. Deploy a VLAN.
 - c. Deploy a wireless network.
 - d. Deploy a VPN.

- 8.** Your organization has recently started allowing sales people to access internal resources remotely. Management wants you to configure the appropriate controls to provide maximum security for these connections. What should you do?

 - a.** Deploy a DMZ.
 - b.** Deploy a VLAN.
 - c.** Deploy a wireless network.
 - d.** Deploy a VPN.

- 9.** Recently, sales people within your organization are having trouble managing customer-related data. Management is concerned that sales figures are being negatively affected as a result of this mismanagement. You have been asked to provide a suggestion to fix this problem. What should you recommend?

 - a.** Deploy an ERP solution.
 - b.** Deploy a CRM solution.
 - c.** Deploy a GRC solution.
 - d.** Deploy a CMS solution.

- 10.** As your enterprise has grown, it has become increasingly hard to access and manage resources. Users often have trouble locating printers, servers, and other resources. You have been asked to deploy a solution that will allow easy access to internal resources. Which solution should you deploy?

 - a.** Directory Services
 - b.** CMDB
 - c.** ESB
 - d.** SOA

This page intentionally left blank



Index

Numerics

3-D Secure, 39

3DES (Triple DES), 41

modes, 61

6 to 4, 112

802.1x, 118

A

accept strategy for risk analysis, 312

acceptance testing, 522

access control models, 572-575

access control matrix, 574

ACLs, 575

administrative controls, 294

compensative controls, 292

content-dependent access control,
574

context-dependent access control, 574

corrective controls, 292

DAC, 572-573

defaulting to no access, 575

detective controls, 292

deterrent controls, 293

directive controls, 293

logical controls, 295

MAC, 573

physical controls, 296

policies, 575

preventive controls, 293

RBAC, 573-574

recovery controls, 293

rule-based access control, 574

access points, 499

account lockout, 565-566

account management, 562-563

ACLs (access control lists), 204, 575

configuring, 158-159

acquisition phase (SDLC), 518

acquisitions

design considerations during, 545

security issues, 271

active fingerprinting, 452-453

**active vulnerability scanners,
134-135**

ActiveX, 257

AD (Active Directory), 586-587

identity propagation, 580

ad hoc mode (WLANs), 499

Adams, Carlisle, 43

adherence to standards, 536

Adleman, Leonard, 45-46

administrative controls, 294

Adobe Flash, 257

advanced trust systems, 585-587

AD, 586-587

LDAP, 586

RADIUS, 585-586

**advancements in technology,
communicating, 395-396****advising staff and senior management,
469****AES (Advanced Encryption Standard),
42****aggregate CIA score, determining,
298-299****Agile development, 253, 523****agreements, 408**

BPA, 346-347

NDA, 346

OLA, 345

SLA, 345

AH (Authentication Header), 40**AIK (attestation identity key), 208****AJAX (Asynchronous JavaScript and
XML), 258****ALE (annualized loss expectancy),
calculating, 304-305****algebraic attacks, 64****algorithms**

asymmetric algorithms

*Diffie-Hellman, 45**ECC, 46**El Gamal, 46**Knapsack, 46**private keys, 44**public keys, 44**RSA, 45-46**weaknesses of, 61**Zero Knowledge Proof, 47*

implementing, 66

Rijndael algorithm, 42

symmetric algorithms, 40-43

*3DES, 41**AES, 42**Blowfish, 42**CAST, 43**DES, 41**IDEA, 42**RC algorithms, 43**session keys, 41**Skipjack, 42**Twofish, 43**weaknesses of, 61***analyzing**

data flows, 534-535

metrics, 419-420

security solutions

*availability, 424**capability, 423**latency, 423**maintainability, 424**performance, 422**recoverability, 424-425**scalability, 423*

trend data, 420-421

anomaly-based IDS, 124-125**anticipating**

cyber defense needs, 420-421

risk changes, 332

antimalware, 191-192**antispam services for the cloud, 213****antispware, 192**

- antivirus software, 192**
 - cloud antivirus, 213
- applications. *See also* software**
 - client-based application virtualization, 222
 - frameworks, 245-247
 - standard libraries, 245*
 - industry-accepted development practices, 245-247
 - BSI initiative, 246*
 - ISO/IEC 27000, 246*
 - OWASP, 246*
 - WASC, 245-246*
 - WS-Security, 246-247*
 - interoperability requirements, 538-539
 - sandboxing, 244-245
 - security issues
 - buffer overflow attacks, 239-241*
 - click-jacking, 232-233*
 - CSRF, 232*
 - fuzzing, 238-239*
 - geotagging, 243*
 - improper error and exception handling, 237*
 - improper storage of sensitive data, 237-238*
 - input validation, 235*
 - insecure direct object references, 231*
 - integer overflows, 242*
 - memory leaks, 242*
 - privilege escalation, 237*
 - race conditions, 242*
 - session hijacking attacks, 233-235*
 - SQL injection, 235-236*
 - time of check/time of use attacks, 242-243*
 - XSS, 231-232*
 - server-based application virtualization, 222
 - session management, 233-235
 - software development methods
 - Agile model, 253*
 - build and fix, 248*
 - Cleanroom model, 254*
 - incremental model, 250*
 - JAD, 254*
 - prototyping, 250*
 - RAD model, 252*
 - spiral model, 251*
 - V-shaped model, 249*
 - Waterfall method, 248-249*
 - web applications
 - browser extensions, 256-259*
 - client-side processing, 255-260*
 - cookies, storing, 239*
 - JavaScript, 260*
 - JSON, 256*
 - REST, 256*
 - security issues, 230*
 - server-side processing, 255-260*
 - state management, 260*
 - whitelisting, 199
- APTs (advanced persistent threats), 398-406**
 - CERT, 403-404
 - emergent threats, 399-400
 - intelligence, 406
 - sources of, 406
 - threat actors, 405-406
 - zero-day attacks, mitigating, 398-399
- ARAT (active reader/active tag), 527**
- archive bits, 369**

ARO (annualized rate of occurrence), 306

ARP poisoning, 138-139

ARPT (active reader/passive tag), 527

assessment methods. See also code review, 454-455

fingerprinting, 452-454

active fingerprinting, 452-453

passive fingerprinting, 453-454

malware sandboxing, 446-447

memory dumping, 447-448

penetration testing, 448-450

black box testing, 451

gray box testing, 451

selecting method, 452

strategies, 450

white box testing, 451

reconnaissance, 452

Retina, 449

runtime debugging, 447-448

social engineering attacks, 455-456

vulnerability assessment, 445-446

assessment tools

exploit kits, 439-440

fuzzers, 438

HTTP interceptors, 439

network enumerators, 435-436

passive reconnaissance tools, 440-444

routing tables, 443-444

social media, 441

Whois, 441-442

password crackers, 436-438

port scanners, 432-433

protocol analyzers, 434-435

vulnerability scanners, 434

asset disposal, 514-515

asset management

device-tracking technologies, 526

geolocation, 526

geotagging, 527

object tracking, 526-527

RFID, 527-528

asymmetric algorithms, 44-47

Diffie-Hellman, 45

ECC, 46

El Gamal, 46

Knapsack, 46

private keys, 44

public keys, 44

RSA, 45-46

weaknesses of, 61

Zero Knowledge Proof, 47

attacks

algebraic attacks, 64

analytic attacks, 65

birthday attacks, 64

brute-force attacks, 63

buffer overflow attacks, 239-241

chosen ciphertext attacks, 62

chosen plaintext attacks, 62

cipher-only attacks, 62

click-jacking, 232-233

client-side attacks, 396-397

CSRF, 232

dictionary attacks, 65

factoring attacks, 65

fault injection attacks, 238-239

frequency analysis, 64

known plaintext attacks, 62

man-in-the-middle attacks, 66

- meet-in-the-middle attacks, 66
 - plaintext attacks, 63-64
 - race conditions, 242
 - time of check/time of use attacks, 242-243*
 - rainbow table attacks, 33
 - replay attacks, 65
 - reverse engineering attacks, 65
 - session hijacking attacks, 233-235
 - side-channel attacks, 63
 - social engineering attacks, 63, 455-456
 - SQL injection, 235-236
 - statistical attacks, 65
 - VLAN hopping attacks, 140
 - VM escape attacks, 219
 - wireless attacks, 505
 - XSS attacks, 231-232
 - zero-day attacks, mitigating, 398-399
- attestation, 579-580**
- ID-FF, 582
 - SAML, 581-582
- audit trails, monitoring, 196-198**
- authentication, 562-572**
- 802.1x, 118
 - access control models, defaulting to no access, 575
 - certificate-based authentication, 570-571
 - characteristic factor authentication, 117, 566-570
 - behavioral characteristics, 568*
 - physiological characteristics, 567-568*
 - dual-factor authentication, 570
 - EAP, 114-115
 - identity and account management, 562-563
 - knowledge factor authentication, 116
 - MAC, 33
 - multi-factor authentication, 570
 - ownership factor authentication, 117
 - RADIUS, 118-120, 585-586
 - SSO, 571-572
 - TACACS+118-120
- authorization, 572-578**
- access control models, 572
 - access control policies, 575*
 - ACLs, 575*
 - content-dependent access control, 574*
 - context-dependent access control, 574*
 - DAC, 572-573*
 - MAC, 573*
 - RBAC, 573-574*
 - rule-based access control, 574*
 - OAUTH, 575-576
 - SPML, 578
 - XACML, 577-578
- automation systems, building, 178**
- A/V (audio/visual) systems, 181-182**
- availability, 160-166, 424**
- avoid strategy for risk analysis, 310-311**

B

backups, 369-372

- archive bits, 369
- daily backups, 370
- differential backups, 369
- electronic backups, 372
- full backups, 369

- incremental backups, 370
- rotation schemes, 370-371
- transaction log backups, 370
- Base II, 339**
- baselining, 199, 417-418**
- bastion hosts, 144**
- bcrypt, key stretching, 32**
- behavioral authentication systems, 568**
- benchmarks, creating, 417-418**
- best practices**
 - industry-accepted development practices, 245-247
 - BSI initiative, 246*
 - ISO/IEC 27000, 246*
 - OWASP, 246*
 - WASC, 245-246*
 - WS-Security, 246-247*
 - researching, 392-393
 - for SANs, 84
- BIA (business impact analysis), 341-344**
- biometric scanning devices, 567-570**
- birthday attacks, 64**
- black box testing, 451**
- Black Hat convention, 405**
- black hats, 406**
- blacklisting**
 - applications, 199
 - character blacklisting, 235
- blind tests, 450**
- block ciphers, 57**
 - Blowfish, 42
 - IDEA, 42
 - Skipjack, 42
- block-level encryption, 96-97**
- Blowfish, 42**
- Bluesnarfing, 207**
- Bluetooth, 502**
 - restricting, 207
- boot loader protections**
 - IMA, 218
 - measured launch, 218
 - Secure Boot, 217-218
 - UEFI, 218-219
- bottom-up policy development, 332**
- boundary errors, 241**
- BPA (business partnership agreement), 346-347**
- bridge model, 581**
- browser extensions, 256-259**
 - ActiveX, 257
 - AJAX, 258
 - Flash, 257
 - HTML5, 257
 - Java applets, 257
- brute-force attacks, 63**
- BSI (Build Security In) initiative, 246**
- buffer overflows, 239-241**
- build and fix software development approach, 248**
- building automation systems, 178**
- business continuity planning, 318-320**
- business tools, security implications of, 400-403**
 - end-user cloud storage, 402-403
 - social media/networking, 401
- BYOD ("bring your own device"), 278-279, 495-497**

C

Cain and Abel, 437

calculating

- ALE, 304-305
- NPV, 308-309
- payback, 308
- ROI, 307-309
- SLE, 304
- TCO, 309-310

CANVAS, 440

capability, analyzing, 423

captured email messages, 486

CAs (certificate authorities), 51

- root CAs, 51

CAST, 43

CBC (cipher block chaining) mode, 58-59

CBC-MAC (cipher block chaining MAC), 37

CC (Common Criteria), 190

CDMA (Code Division Multiple Access), 498

CDP (Cisco Discovery Protocol), 443

centralized VDI model, 221

CER (crossover error rate), 569

CERT (Computer Emergency Response Team) secure coding standards, 247

certificate-based authentication, 570-571

certificates

- classes of, 55
- CRL, 53
- issuance to entities, 53-54

OCSP, 53

wildcard certificates, 52-53

X.509, 54-55

certification, advantages of, 625-626

CFAA (Computer Fraud and Abuse Act), 338

CFB (cipher feedback) mode, 59

chain of trust, 50-51

change control policies, 159-160

change management, 516-517

CHAP (Challenge-Handshake Authentication Protocol), 444

characteristic factor authentication, 117, 566-570

- behavioral characteristics, 568
- physiological characteristics, 567-568

characters, blacklisting/whitelisting, 235

chosen ciphertext attacks, 62

chosen plaintext attacks, 62

chroot, 210

CIA (confidentiality, integrity, and authentication), 30, 287-289

- aggregate score, determining, 298-299
- confidentiality, 30, 50
- incorporating stakeholder input, 291
- integrity, 50
- chain of trust, 50-51*

CIFS (Common Internet File System), 90

cipher-only attacks, 62

ciphers

- block ciphers, 57
- Blowfish, 42*
- IDEA, 42*
- Skipjack, 42*

- concealment ciphers, 56
- stream ciphers, 56-57
- classes of digital certificates, 55**
- Cleanroom development model, 254**
- click-jacking, 232-233**
- client-based application virtualization, 222**
- client-side attacks, identifying, 396-397**
- client-side processing, 255-260**
- clipping level, 566**
- cloud computing, 167-168**
 - collaboration, 490-491
 - communities, 80
 - elastic cloud computing, 542
 - hybrid cloud model, 79, 540
 - multi-tenancy model, 541
 - private cloud model, 79, 540
 - public cloud model, 79, 540
 - resource provisioning, 543-544
 - security issues, 270
 - antispam services, 213*
 - antivirus products, 213*
 - content filtering, 216*
 - hash matching, 212-213*
 - sandboxing, 216*
 - vulnerability scanning, 214-215*
 - services, 80
 - storage, 79-80
- clustering, 165**
- CMAC (cipher-based MAC), 37**
- CMDB (configuration management database), 555**
- CMS (content management system), 555**
- CobiT (Control Objectives for Information and Related Technology), 316**
- code review, 454-455**
- code signing, 36**
- cognitive passwords, 564**
- collaborating with teams, 469-470**
- collecting metrics, 419-420**
- collisions, 33**
- combination passwords, 563**
- command shell, restricting, 202-203**
- commercial business data classifications, 289-290**
- commercial software, interoperability with in-house developed software, 539**
- commissioning an asset, 514**
- communities, 80**
- compensative controls, 292**
- competing standards, 536**
- complex passwords, 564**
- CompTIA career pathway, 625-626**
- Computer Security Act of 1987, 339**
- concealment ciphers, 56**
- conducting**
 - lessons-learned/after action review, 425
 - risk analysis, 301-310
 - accept strategy, 312*
 - ALE, calculating, 304-305*
 - ARO, 306*
 - avoid strategy, 310-311*
 - magnitude of impact, 304*
 - mitigate strategy, 311*
 - NPV, 308-309*

- qualitative risk analysis, 302-303*
- quantitative risk analysis, 303*
- SLE, calculating, 304*
- TCO, calculating, 309-310*
- transfer strategy, 311*
- trend analysis, 306*
- confidentiality, 30, 50**
- configuration lockdown, 160**
- configuring**
 - ACLs, 158-159
 - dedicated interfaces, 203
- confusion, 49**
- container-based virtualization, 211**
- containment technologies, 526-527**
- content filtering, 216**
- content-dependent access control, 574**
- context-dependent access control, 574**
- continuity planning, 318-320**
- contracts, researching security requirements, 406-408**
 - agreements, 408
 - RFIs, 408
 - RFPs, 407
 - RFQs, 407
- control plane, 166**
- controls, advising staff and senior management, 469**
- cookies, storing, 239**
- COOP (continuity of operations plan), 384-385**
- core dumps, 448**
- corrective controls, 292**
- cost/benefit analysis, performing, 419**
- crackers, 406**
- credit card transactions, securing, 39**
 - PCI DSS, 339
- criminal actions, responding to, 379**
- CRL (certificate revocation list), 53**
- CRM (customer relationship management), 552**
- cross-certification model, 581**
- cryptanalysis**
 - differential cryptanalysis, 63
 - linear cryptanalysis, 63-64
- CryptoAPI, 49**
- cryptography, 30, 40-47. *See also* encryption**
 - algorithms, implementing, 66
 - applications
 - S/MIME, 69*
 - SSH, 69*
 - asymmetric algorithms, 44
 - Diffie-Hellman, 45*
 - ECC, 46*
 - El Gamal, 46*
 - Knapsack, 46*
 - RSA, 45-46*
 - Zero Knowledge Proof, 47*
 - chain of trust, 50-51
 - CIA
 - confidentiality, 30*
 - code signing, 36
 - confidentiality, 50
 - confusion, 49
 - diffusion, 49
 - digital signatures, 47-48
 - DRM, 67
 - encryption, 30

- entropy, 49
- GPG, 67-68
- hashing, 32-36
 - hash value, identifying*, 34
 - HAVAL*, 36
 - limitations of*, 33
 - MAC*, 33
 - MD2 algorithm*, 34-35
 - MD4 algorithm*, 34-35
 - MD5 algorithm*, 34-35
 - MD6 algorithm*, 34-35
 - message digests*, 34
 - one-way hash function*, 33
 - RIPMD-160*, 36
 - SHA*, 35-36
 - vulnerabilities*, 33
- hybrid ciphers, 47
- integrity, 50
- key stretching, 32
- MAC, 36
 - CBC-MAC*, 37
 - CMAC*, 37
 - HMAC*, 37
- non-repudiation, 50
- PFS, 37-38
- PKCS, 69
- PKI, 50-51
 - CAs*, 51
 - CRL*, 53
 - issuance of certificates to entities*, 53-54
 - OCSP*, 53
 - systems*, 55
 - users*, 54-55
 - wildcard certificates*, 52-53
 - X.509 standard*, 50, 54-55

- PNRG, 37
- symmetric algorithms, 40
 - 3DES*, 41
 - AES*, 42
 - Blowfish*, 42
 - CAST*, 43
 - DES*, 41
 - IDEA*, 42
 - RC algorithms*, 43
 - session keys*, 41
 - Skipjack*, 42
 - Twofish*, 43
 - weaknesses of*, 61
- technique, selecting, 32
- transport encryption, 38
- watermarking, 67

CSRF (cross-site request forgery), 232

CTR (counter) mode, 60

cyber defense needs, anticipating, 420-421

D

DAC (discretionary access control), 572-573

DAI (dynamic ARP inspection), 138

daily backups, 370

DAM (database activity monitoring), 135-136, 254

data aggregation, 543

data archiving, 82-83

data at rest encryption, 40-47

- asymmetric algorithms, 44

- Diffie-Hellman*, 45

- ECC*, 46

- El Gamal*, 46
- Knapsack*, 46
- RSA*, 45-46
- weaknesses of*, 61
- Zero Knowledge Proof*, 47
- symmetric algorithms, 40
 - 3DES*, 41
 - AES*, 42
 - CAST*, 43
 - DES*, 41
 - IDEA*, 42
 - RC algorithms*, 43
 - session keys*, 41
 - Skipjack*, 42
 - Twofish*, 43
 - weaknesses of*, 61
- data backups. See backups**
- data breaches, incident response, 374-378**
 - facilitating, 378-381
- data clearing, 244**
- data encryption. See encryption**
- data flows**
 - analyzing, 534-535
 - enforcing, 175
 - SSL inspection, 156
- data handling, 373-374**
- data interfaces, 205-206**
- data isolation, 543**
- data ownership, 372-373**
- data plane, 166**
- data purging, 244, 515**
- data remnants, 221, 244, 543**
 - remanence, 515
- data warehousing, 80-82**
- database administrators, security requirements, 463-464**
- DDPs (dynamic disk pools), 93-94**
- de facto standards, 536-537**
- de jure standards, 536**
- decommissioning an asset, 514**
- decryption, key escrow, 56**
- deduplication, 92**
- defaulting to no access, 575**
- DEFCON conferences, 405**
- defense-in-depth principle, 535**
- degaussing, 244**
- de-perimeterization, impact of**
 - BYOD, 278-279
 - cloud computing, 278
 - outsourcing, 279
 - telecommuting, 278
- deprovisioning resources, 543-544**
- DES (Digital Encryption Standard), 41**
 - modes, 58-60
- desktop sharing, securing, 481-482**
- detective controls, 292**
- deterrence, 314**
- deterrent controls, 293**
- developing applications**
 - CERT secure coding standards, 247
 - frameworks, 245-247
 - industry-accepted development practices, 247
 - BSI initiative*, 246
 - ISO/IEC 27000*, 246
 - OWASP*, 246
 - WASC*, 245-246

- software development methods, 247-254
 - Agile model*, 253, 523
 - build and fix*, 248
 - Cleanroom model*, 254
 - incremental model*, 250
 - JAD*, 254
 - prototyping*, 250
 - RAD model*, 252
 - spiral model*, 251, 524
 - V-shaped model*, 249
 - Waterfall method*, 248-249, 523-524
- standard libraries, 245
- WS-Security, 246-247
- device-tracking technologies**, 526
- DHCP snooping**, 139
- diagrams**
 - logical deployment diagrams, 546
 - physical network diagrams, 547
- dial-up access**, 491-492
- dictionary attacks**, 65
- differential backups**, 369
- differential cryptanalysis**, 63
- Diffie-Hellman**, 45
- diffusion**, 49
- digital certificates**, classes of, 55
- digital signatures**, 47-48
- directive controls**, 293
- directory services**, 554
- disk-level encryption**, 96
- disposal phase (SDLC)**, 519
- diverse industry integration**, security concerns
 - geography, 273
 - policies, 272
 - regulations, 272-273
 - rules, 272
- divestitures**, design considerations during, 545
- DLP (data loss prevention) software**, 194
- DMCA (U.S. Digital Millennium Copyright Act of 1998)**, 67
- DMZs (demilitarized zones)**, 176, 548-549
- DNS (Domain Name System)**, 554-555
- document exchange/reviews**, 276
- documentation**
 - BIA, 341-344
 - BPA, 346-347
 - IA, 344
 - ISA, 345
 - MOU, 345
 - NDA, 346
 - NIST SP 800-30, risk management processes, 312-314
 - OLA, 345
 - RAs, 340-341
 - SLA, 345
 - SOA, 340-341
- double tagging**, 140
- double-blind tests**, 450
- downstream liability**, 273
- DRM (digital rights management)**, 67
- Dropbox**, 212-213
- DSA (Digital Security Algorithm)**, 48
- DSS (Digital Signature Standard)**, 48
- DSSS (Direct Sequence Spread Spectrum)**, 498

DSV (dynamic signature verification), 568
 DTP (Dynamic Trunking Protocol), 172
 Dual Stack, 112
 dual-factor authentication, 570
 dual-homed firewalls, 145
 dual-key cryptography. *See* asymmetric algorithms
 due care, 274
 due diligence, 274
 dumpster diving, 456
 dynamic packet-filtering firewalls, 142
 dynamic routing protocols, 174, 443

E

e-discovery, 366-374

backups, 369-372
 daily backups, 370
 differential backups, 369
 electronic backups, 372
 full backups, 369
 incremental backups, 370
 rotation schemes, 370-371
 data ownership, 372-373
 data recovery and storage, 368
 electronic inventory and asset control, 366-367
 legal holds, 374
 transaction log backups, 370

EALs (Evaluation Assurance Levels), 190

EAP (Extensible Authentication Protocol), 114-115

EC-Council (International Council of Electronic Commerce Consultants), 403

ECB (electronic code book) mode, 58

ECC (Elliptic Curve Cryptosystem), 46

ECDSA (Elliptical Curve DSA), 48

Economic Espionage Act of 1996, 339

effectiveness of existing security controls, reviewing, 421

EK (endorsement key), 208

El Gamal, 46

elastic cloud computing, 542

Elastic Sandbox, 446-447

electronic backups, 372

electronic inventory and asset control, 366-367

electronic vaulting, 372

email

antispam services for the cloud, 213
 captured messages, 486
 disclosure of information, 487
 IMAP, 484
 securing, 484-487
 spam filters, 192-193
 spear phishing, 485
 whaling, 486

emergency response

chain of custody, 381
 evidence, 381-382
 search and seizure, 382-383

emergent threats, 399-400, 525-526

employment policies, 356

encryption, 30

block-level encryption, 96-97

ciphers

block ciphers, 57

stream ciphers, 56-57

confusion, 49

data at rest encryption, 40-47

asymmetric algorithms, 44-47

symmetric algorithms, 40-43

disk-level encryption, 96

full disk encryption, 208-209

hybrid ciphers, 47

key escrow, 56

port-level encryption, 98

record-level encryption, 98

steganography, 56

transport encryption

3-D Secure, 39

HTTP, 39

HTTPS, 39

IPsec, 39-40

SET, 39

SHTTP, 39

SSL, 38, 68-69

TLS, 38, 68-69

end-to-end solution ownership

asset disposal, 514-515

change management, 516-517

commissioning an asset, 514

maintenance, 513

object reuse, 515

operational activities, 512-513

end-user cloud storage

integrating into your business, 403

security implications of, 402-403

endpoint security software, 191-198

antimalware, 191-192

antispymware, 192

antivirus software, 192

DLP software, 194

host-based firewalls, 194-196

IDS, 193

log monitoring, 196-198

patch management, 193

spam filters, 192-193

enforcing data flows, 175

enrollment time, 568

enterprise application integration

enablers, 552-555

CMDB, 555

CMS, 555

CRM, 552

directory services, 554

DNS, 554-555

ERP, 553

ESB, 553

GRC, 553

SOA, 553

enterprise security

baselining, 417-418

benchmarks, creating, 417-418

CASP exam objectives, 6-13

cost/benefit analysis, performing, 419

cyber defense needs, anticipating,
420-421

effectiveness of existing security
controls, reviewing, 421

lessons-learned/after action review, 425

metric collection and analysis, 419-420

multiple solutions, testing, 418-419

- prototyping, 418-419
 - reverse engineering existing solutions, 422
 - security solutions, analyzing
 - availability*, 424
 - capability*, 423
 - latency*, 423
 - maintainability*, 424
 - performance*, 422
 - recoverability*, 424-425
 - scalability*, 423
 - enterprise security architecture frameworks, 315-318**
 - CobiT, 316
 - NIST SP 800-53, control families, 317
 - SABSA, 315
 - enterprise storage**
 - cloud storage, 79-80
 - data archiving, 82-83
 - data warehousing, 80-82
 - DDPs, 93-94
 - deduplication, 92
 - encryption
 - block-level encryption*, 96-97
 - disk-level encryption*, 96
 - port-level encryption*, 98
 - record-level encryption*, 98
 - HBA allocation, 95
 - LUN masking, 94
 - multipathing, 90-91
 - multisite replication, 95-96
 - NAS, 84-86
 - offsite replication, 95-96
 - SANs, 83-84
 - snapshots, 91-92
 - virtual storage, 78-79
 - VSANs, 86
 - entropy, 49**
 - ERP (enterprise resource planning), 553**
 - ESB (enterprise service bus), 553**
 - ESP (Encapsulating Security Payload), 40**
 - establishing partnerships, security issues, 269**
 - events versus incidents, 353-354**
 - evidence, 381-382**
 - forensic analysis, 383-384
 - order of volatility, 385-386
 - exam**
 - preparing for, 628
 - topics, 628-638
 - examples of TOS, 191**
 - executive management, security requirements, 465-466**
 - exemptions, 313**
 - exploitation tools, 439-440**
 - external violations, 378-379**
 - extreme scenario planning, 299-301**
-
- F**
- facilitating incident response, 378-381**
 - facilities manager, security requirements, 468**
 - factoring attacks, 65**
 - failover, 165**
 - failsoft, 165**
 - FAR (false acceptance rate), 569**
 - FATKit, 448**

- fault injection, 238-239**
 - FCoE (Fiber Channel over Ethernet), 88-89**
 - FDMA (Frequency Division Multiple Access), 498**
 - feasibility of cryptographic algorithms, 66**
 - feature extraction, 568**
 - Federal Privacy Act of 1974, 338**
 - federated identity management, 581**
 - OpenID, 583
 - Shibboleth, 583-584
 - FHSS (Frequency Hopping Spread Spectrum), 498**
 - FIFO (first in, first out) rotation scheme, 370-371**
 - financial staff, security requirements, 466-467**
 - fingerprinting, 452-454**
 - active fingerprinting, 452-453
 - passive fingerprinting, 453-454
 - FIPS (Federal Information Processing Standard Publication 199), 288**
 - firewalls, 140-143**
 - architecture, 143-144
 - bastion hosts, 144
 - dual-homed firewalls, 145
 - host-based firewalls, 194-196
 - kernel proxy firewalls, 142
 - multihomed firewalls, 146
 - NGFWs, 133-134
 - packet-filtering firewalls, 141
 - placement of, 143
 - proxy firewalls, 141-142
 - screened host firewalls, 147-148
 - screened subnets, 148-149
 - stateful firewalls, 141
 - virtual firewalls, 154-155
 - WAFs, 131-132, 255
 - FireWire, restricting, 207-208**
 - FISMA (Federal Information Security Management Act), 339**
 - forensic analysis, 383-384**
 - hardware/embedded device analysis, 384
 - media analysis, 383
 - network analysis, 384
 - software analysis, 384
 - forensic tasks for incident response team, 354-356**
 - formal code review, 454**
 - frameworks, 245-247**
 - standard libraries, 245
 - frequency analysis, 64**
 - FRR (false rejection rate), 569**
 - FTP (File Transfer Protocol), 113**
 - full backups, 369**
 - full disk encryption, 208-209**
 - full-knowledge tests, 450**
 - fuzzing, 238-239, 438**
-
- G**
-
- generation-based fuzzing, 238**
 - geofencing, 527**
 - geolocation, 526**
 - geotagging, 243, 527**
 - GFS (grandfather/father/son) rotation scheme, 370-371**

global IA industry, 403-405
 CERT, 403-404
 conventions, 404-405

government data classifications, 290

GPG (GNU Privacy Guard), 67-68

GPMC (Group Policy Management Console), 201

GPOs (Group Policy Objects), 200

GPRS (General Packet Radio Service), 499

GPS (Global Positioning System)
 location, 526

Gramm-Leach-Bliley Act of 1999, 338

graphical passwords, 564

gray box testing, 451

gray hats, 406

GRC (governance, risk, and compliance), 553

GRE (Generic Routing Encapsulation) tunnels, 112

Group Policy, 199
 GPMC, 201
 GPOs, 200
 implementing, 200-202

GSM (Global System Mobile Communication), 499

guidelines, 324

H

hackers, 406

hacktivists, 406

hardening, host hardening, 198-209
 ACLs, 204
 applications, blacklisting/whitelisting, 199

baselining, 199

command shell restrictions, 202-203

data interfaces, 205-206

dedicated interfaces, configuring, 203

full disk encryption, 208-209

Group Policy, implementing, 200-202

management interfaces, 205

OOB NICs, 203-204

peripheral restrictions, 206-208

hardware/embedded device analysis, 384

hash matching, 212-213

hashing, 32-36
 hash value, identifying, 34
 HAVAL, 36
 limitations of, 33
 MAC, 33
 MD2 algorithm, 34-35
 message digests, 34-35
 one-way hash function, 33
 RIPEMD-160, 36
 SHA, 35-36
 vulnerabilities, 33

HAVAL, 36

HBA (host bus adapter) allocation, 95

Health Care and Education Reconciliation Act of 2010, 340

high availability, 162-166

HIPAA (Health Insurance Portability and Accountability Act), 338

hiring policies, 356

HMAC (hash MAC), 37

horizontal privilege escalation, 237

host security

- boot loader protections, 217-219
 - IMA*, 218
 - measured launch*, 218
 - Secure Boot*, 217-218
 - UEFI*, 218-219
- endpoint security software, 191-198
 - antimalware*, 191-192
 - antispyware*, 192
 - antivirus software*, 192
 - DLP software*, 194
 - host-based firewalls*, 194-196
 - IDS*, 193
 - log monitoring*, 196-198
 - patch management*, 193
 - spam filters*, 192-193
- hardening, 198-209
 - ACLs*, 204
 - applications, blacklisting/whitelisting*, 199
 - baselining*, 199
 - command shell restrictions*, 202-203
 - data interfaces*, 205-206
 - dedicated interfaces, configuring*, 203
 - full disk encryption*, 208-209
 - Group Policy, implementing*, 200-202
 - management interfaces*, 205
 - OOB NICs*, 203-204
 - peripheral restrictions*, 206-208
- TOS, 190-191
 - CC*, 190
 - examples*, 191
 - TCSEC*, 190
- VDI, 221

virtualization

- client-based application virtualization*, 222
- container-based virtualization*, 211
- server virtualization*, 209-211
- server-based application virtualization*, 222
- VTPM*, 223-224
- vulnerabilities of hosts with differing security requirements, 219-221
 - data remnants*, 221
 - live VM migration*, 220
 - privilege elevation*, 220
 - VM escape attacks*, 219
- host-based firewalls, 194-196**
- hosted VDI model, 221**
- hot fixes, 193**
- HSM (hardware security module), 127-128**
- HSM (hierarchical storage management), 372**
- HTML5, 257**
- HTTP (Hypertext Transfer Protocol), 39**
- HTTP interceptors, 439**
- HTTPS (HTTP Secure), 39**
- human resources, security requirements, 466-467**
- HVAC controllers, 180**
- hybrid ciphers, 47**
- hybrid cloud model, 79, 540**
- hypervisor**
 - Type I hypervisor, 210
 - Type II hypervisor, 211

- I**
-
- IA (interoperability agreement), 344**
- IaaS (Infrastructure as a Service), 80**
- ICANN (Internet Corporation for Assigned Names and Numbers), 442**
- ICS (industrial control systems), 183**
- IDEA (International Data Encryption Algorithm), 42**
- identifying**
- client-side attacks, 396-397
 - hash values, 34
 - SQL attacks, 236-237
 - vulnerabilities, 397-398
- identity management, 562-563**
- identity propagation, 580-581**
- identity theft, 456**
- ID-FF (Liberty Identity Federation Framework), 582**
- IDS (intrusion detection system), 193**
- anomaly-based, 124-125
- IETF (Internet Engineering Task Force), RFCs, 395-396**
- IMA (Integrity Measurement Architecture), 218**
- IMAP (Internet Message Access Protocol), 484**
- IMPACT, 440**
- implementation phase (SDLC), 518**
- implementing**
- cryptographic algorithms, 66
 - Group Policy, 200-202
- in-house developed software, interoperability with commercial software, 539**
- in-line deduplication, 92**
- incident response, 351-356, 364, 374-378. See also e-discovery**
- auditing, 380-381
 - CASP exam objectives, 15-18
 - chain of custody, 381
 - COOP, 384-385
 - criminal actions, 379
 - evidence, 381-382
 - facilitating, 378-381
 - forensic analysis, 383-384
 - hardware/embedded device analysis, 384*
 - media analysis, 383*
 - network analysis, 384*
 - software analysis, 384*
 - forensic tasks, 354-356
 - insider threats, 379-380
 - investigations, 353-354
 - non-malicious threats, responding to, 380
 - order of volatility, 385-386
 - rules of engagement, 354
 - search and seizure, 382-383
- incremental backups, 370**
- incremental software development model, 250**
- industry-accepted development practices**
- BSI initiative, 246
 - ISO/IEC 27000, 246
 - OWASP, 246
 - WASC, 245-246
 - WS-Security, 246-247
- INE (in-line network encryptor), 126**

influences on security policies

- audits, 275
- client requirements, 277
- competitors, 275
- document exchange/review, 276
- onsite assessments, 276
- process/policy reviews, 276
- regulatory entities, 276
- top-level management, 277

information classification, 289-290

- commercial business classifications, 289-290
- military and government classifications, 290

infrared wireless, 502

infrastructure mode (WLANs), 499

inherent risk, 314

initiation phase (SDLC), 517-518

input validation, 235

insecure direct object references, 231

insider threats, 379-380

instant messaging, securing, 481

integer overflows, 242

integrating

- diverse industries, security concerns
 - geography, 273*
 - policies, 272*
 - regulations, 272-273*
 - rules, 272*
- end-user cloud storage into your business, 403
- storage into an enterprise, 552

integrity, 50

- chain of trust, 50-51

intended audience for this book, 628

interfaces

- data interfaces, 205-206
- dedicated interfaces, configuring, 203
- loopback interfaces, 205
- management interfaces, 205
- OOB, 203-204

internal violations, 378-379

interoperability

- application requirements, 538-539
- of cryptographic algorithms, 66
- of legacy and current systems, 537-538

inventory control

- device-tracking technologies, 526
- electronic inventory and asset control, 366-367
- geolocation, 526
- geotagging, 527
- object tracking, 526-527
- RFID, 527-528

IP video systems, 179-180

IPS (intrusion protection system), 193

IPsec (Internet Protocol Security), 39-40, 493-494

iptables, 195

IPv6, 111-113

IrTran-P protocol, 502

ISA (interconnection security agreement), 271, 345

ISAKMP (Internet Security Association and Key Management Protocol), 40

ISC2 (International Information Systems Security Certification Consortium), 403

iSCSI (Internet Small Computer System Interface), 87-88
 ISO/IEC 27000 series standards, 246, 333-336
 issuance of certificates to entities, 53-54
 issue-specific security policies, 323
 IT governance, 320-324, 471
 baselines, 324
 guidelines, 324
 issue-specific security policies, 323
 organizational security policy, 322-323
 policies, 321-322
 procedures, 324
 standards, 324
 system-specific security policies, 323

J

JAD (Joint Analysis Development), 254
 Java applets, 257
 JavaScript, 260
 job rotation, 349
 John the Ripper, 438
 JSON (JavaScript Object Notation), 256
 JVM (Java Virtual Machine), 257

K

kernel proxy firewalls, 142
 key escrow, 56
 key recovery, 56

key stretching, 32
 keystroke dynamics, 568
 Knapsack, 46
 knowledge factor authentication, 116
 known plaintext attacks, 62
 KnTTools, 448

L

L2TP (Layer 2 Tunneling Protocol), 492-493
 latency, 423
 LDAP (Lightweight Directory Access Protocol), 586
 least privilege, 350-351
 legacy systems, interoperability with current systems, 537-538
 legal holds, 374
 legislation
 CFAA, 338
 Computer Security Act of 1987, 339
 DMCA, 67
 Economic Espionage Act of 1996, 339
 Federal Privacy Act of 1974, 338
 FISMA, 339
 Gramm-Leach-Bliley Act of 1999, 338
 Health Care and Education Reconciliation Act of 2010, 340
 HIPAA, 338
 PIPEDA, 339
 SOX, 337
 USA PATRIOT Act, 340
 lessons-learned/after action review, 425

liability

- downstream liability, 273
- due diligence, 274

lightweight code review, 454-455**limitations of hashing, 33****linear cryptanalysis, 63-64****Linux**

- command shell restrictions, 202-203
- iptables, 195
- password storage, 566

load balancing, 165**logical controls, 295****logical deployment diagrams, 546****logs, monitoring, 196-198****loopback interfaces, 205****LUN (logical unit number) masking, 94****M****MAC (mandatory access control), 573****MAC (message authentication code), 33, 36-37**

- CBC-MAC, 37

- CMAC, 37

- HMAC, 37

maintainability, analyzing, 424**maintenance, 513****malware sandboxing, 446-447****MAM (mobile application management), 400****management controls, 294****management interfaces, 205****management plane, 166****managing**

- passwords, 563-566

- reset policies, 565-566*

- software patches, 193

- storage

- DDPs, 93-94*

- deduplication, 92*

- HBA allocation, 95*

- LUN masking, 94*

- multisite replication, 95-96*

- offsite replication, 95-96*

- storage solutions, 90-98

- snapshots, 91-92*

- user accounts, 562-563

mandatory vacation policies, 350**MD2 (message digest 2) algorithm, 34-35****MD2 algorithm, 34-35****MD4 algorithm, 34-35****MD5 algorithm, 34-35****MD6 algorithm, 34-35****MDM (mobile device management), 400, 495-497****measured launch, 218****media analysis, 383****meet-in-the-middle attacks, 66****Memdump, 448****memory**

- buffer overflows, 239-241

- leaks, 242

- on TPM chips, 208-209

memory dumping, 447-448**mergers**

- design considerations during, 545

- security issues, 271

mesh networks, 120
message digests, 34-35
messaging framework (SOAP), 259
Metasploit, 440
metrics
 analyzing, 419-420
 collecting, 419-420
military data classifications, 290
MIME (Multipurpose Internet Mail Extensions), 69
mitigate strategy for risk analysis, 311
mitigating zero-day attacks, 398-399
MITM (man-in-the-middle) attacks, 66
modes
 3DES, 61
 DES, 58-60
monitoring
 DAM, 254
 log files, 196-198
 networks, 169-171
MOU (memorandum of understanding), 345
MPLS (Multiprotocol Label Switching), 108
MTBF (mean time between failures), 162
MTTR (mean time to repair), 162
multi-factor authentication, 570
multihomed firewalls, 146
multipathing, 90-91
multiple solutions, testing, 418-419
multisite replication, 95-96
multi-tenancy model, 541
mutation fuzzing, 238

N

NAC (network access control), 176-178
NAS (network-attached storage), 84-86
NDA (nondisclosure agreement), 346
Nessus, 434
network administrators, security requirements, 464-465
network enumerators, 435-436
network flows, 157-158
network infrastructure design, 548-551
 DMZs, 548-549
 VLANs, 549
 VPNs, 550
 wireless networks, 550-551
new technologies
 business tools, security implications of, 400-403
 end-user cloud storage, 402-403
 social media/networking, 401
 communicating, 395-396
 researching, 393-395
 risk management, 268
NFS (Network File System), 89
NFS (Number Field Sieve), 46
NGFWs (next-generation firewalls), 133-134
NICs (network interface cards), OOB, 203-204
NIDS (network intrusion detection system), 124-125

NIPS (network intrusion prevention system), 123
NIST (National Institute of Standards and Technology), 35
NIST SP 800-30, risk management processes, 312-314
NIST SP 800-53, control families, 317
non-malicious threats, 380
non-repudiation, 50
NPV (net present value), calculating, 308-309
numeric passwords, 564

O

OAKLEY, 40
OAUTH (Open Authorization), 575-576
object reuse, 515
object tracking, 526-527
objectives
 chapter coverage, 628-638
 enterprise security, 6-13
 incident response, 15-18
 integration of computing, communications, and business disciplines, 21-23
 research, analysis, and assessment, 19-21
 risk management, 15-18
 technical integration of enterprise components, 23-26
OCSP (Online Certificate Status Protocol), 53
OFB (output feedback) mode, 60

OFDM (Orthogonal Frequency Division Multiplexing), 498
OFDMA (Orthogonal Frequency Division Multiple Access), 498
OLA (operating-level agreement), 345
on-demand cloud computing, 542
one-way hash function, 33
onsite assessments, 276
OOB (out-of-band) NICs, 203-204
open standards, 536
OpenID, 583
operate/maintain phase (SDLC), 518-519
operational activities, 512-513
optical jukebox, 372
Orange Book, 190
order of volatility, 385-386
organizational security policy, 322-323
OTPs (one-time passwords), 564
outsourcing
 downstream liability, 273
 due diligence, 274
 security issues, 269-270
OWASP (Open Web Application Security Project), 438
ownership factor authentication, 117

P

PaaS (Platform as a Service), 80
packet-filtering firewalls, 141
PAP (Password Authentication Protocol), 444
partial-knowledge tests, 450

- partnerships, establishing**
 - BPAs, 346-347
 - security issues, 269
- passive fingerprinting, 453-454**
- passive reconnaissance tools, 440-444**
 - routing tables, 443-444
 - social media, 441
 - Whois, 441-442
- passive vulnerability scanners, 134**
- passphrase passwords, 564**
- password crackers, 436-438**
- passwords. *See also* authentication; authorization**
 - key stretching, 32
 - managing, 563-566
 - reset policies, 565-566*
- patch management, 193**
- payback, calculating, 308**
- PBKDF2 (Password-Based Key Derivation Function 2), key stretching, 32**
- PCI DSS (Payment Card Industry Data Security Standard), 339**
- PCR (platform configuration register) hash, 209**
- PDP (policy decision point), 577**
- Peach, 438**
- penetration testing, 448-450**
 - black box testing, 451
 - gray box testing, 451
 - Retina, 449
 - selecting method, 452
 - strategies, 450
 - white box testing, 451
- PEP (policy enforcement point), 577**
- performance**
 - analyzing, 422
 - of cryptographic algorithms, 66
- performing ongoing research**
 - best practices, 392-393
 - new technologies, 393-394
 - evolution of technology, 395-396*
 - security systems and services, 394-395*
- peripherals, restricting, 206-208**
- permutation, 49**
- PFS (perfect forward secrecy), 37-38**
- pharming, 455-456**
- phishing, 455-456**
- physical access control systems, 181**
- physical controls, 296**
- physical network diagrams, 547**
- physical security manager, security requirements, 468**
- physiological authentication systems, 567-568**
- PII (personally identifiable information), 347**
- PIPEDA (Personal Information Protection and Electronic Documents Act), 339**
- PKCS (Public Key Cryptography Standards), 69**
- PKI (public key infrastructure)**
 - CAs, 51
 - root CAs, 51*
 - certificates
 - classes of, 55*
 - issuance to entities, 53-54*
 - CRL, 53

- OCSP, 53
- systems, 55
- users, 54-55
- wildcard certificates, 52-53
- X.509 standard, 50, 54-55
- placement of security devices, 128-131**
- plaintext attacks**
 - chosen plaintext attacks, 62
 - known plaintext attacks, 62
- PLCs (programmable logic controllers), 183**
- PNRG (pseudo-random number generator), 37**
- policies**
 - access control policies, 575
 - audit policies, 198, 359
 - change control policies, 159-160
 - continuous monitoring, 356-357
 - developing, 332
 - ISO/IEC 27000 series standards, 333-336*
 - legal compliance, 337-340*
 - hiring policies, 356
 - incident response, 351-356
 - forensic tasks, 354-356*
 - investigations, 353-354*
 - rules of engagement, 354*
 - issue-specific security policies, 323
 - IT governance, 321-322
 - job rotation, 349
 - mandatory vacation policies, 350
 - organizational security policies, 322-323
 - principle of least privilege, 350-351
 - separation of duties, 348-349
 - system-specific security policies, 323
 - termination procedures, 356
 - training policies, 357-359
- POP (Post Office Protocol), 484**
- port scanners, 432-433**
- port-level encryption, 98**
- ports, 152**
- post-process deduplication, 92**
- PPP (Point-to-Point Protocol), 444**
- PPTP (Point-to-Point Tunneling Protocol), 492-493**
- preparing for exam, 628**
- presence, securing, 483-484**
- preventing**
 - fault injection attacks, 239
 - privilege escalation, 237
- preventive controls, 293**
- principle of least privilege, 350-351**
- privacy, 347**
 - PIAs, 379
- private cloud model, 79, 540**
- private keys, 44**
- privilege elevation, 220**
- privilege escalation, 237**
- procedure development, 336**
- process/policy reviews, 276**
- programmers, security requirements, 463**
- protocol analyzers, 434-435**
- prototyping, 250, 418-419**
- provisioning**
 - servers, 544
 - user accounts, 544
 - virtual devices, 544

proxies, 152
 proxy firewalls, 141-142
 PSTN (public switched telephone network), 491
 public cloud model, 79, 540
 public keys, 44
 public-key cryptography. *See* asymmetric algorithms

Q

QoS (quality of service), 158
 qualitative risk analysis, 302-303
 quantitative risk analysis, 303

R

race conditions, time of check/time of use attacks, 242-243
 RAD (Rapid Application Development), 252
 RADIUS (Remote Access Dial-In User Service), 118-120, 585-586
 RAID (redundant array of inexpensive disks), 162-164
 rainbow table attacks, 33
 RAs (registration authorities), 51
 RAs (risk assessments), 340-341
 RBAC (role-based access control), 573-574
 RC algorithms, 43
 RDP (Remote Desktop Protocol), 109
 read-only snapshots, 92

reconnaissance, 452
 passive reconnaissance tools, 440-444
 routing tables, 443-444
 social media, 441
 Whois, 441-442
 record-level encryption, 98
 recoverability, analyzing, 424-425
 recovering data, 368
 daily backups, 370
 differential backups, 369
 full backups, 369
 incremental backups, 370
 transaction log backups, 370
 recovery controls, 293
 regulations, 272-273
 influence on security policies, 276
 remanence, 515
 remote access
 authentication methods, 114-120
 characteristic factor authentication, 117
 EAP, 114-115
 knowledge factor authentication, 116
 ownership factor authentication, 117
 dial-up, 491-492
 RDP, 109
 SSH, 108
 SSL, 110-111
 VNC, 109-110
 VPNs, 107-108, 492-494
 site-to-site VPNs, 494
 SSL, 495
 remote administration, 495
 remote assistance, securing, 482-483

- remote journaling, 372
- remote virtual desktops model (VDI), 221
- removing data from magnetic storage media, 244
- replay attacks, 65
- replication, 372
- researching
 - best practices, 392-393
 - new technologies, 393-394
 - advancements in technology, communicating, 395-396*
 - end-user cloud storage, 402-403*
 - security systems and services, 394-395*
 - social media/networking, security implications of, 401*
 - security requirements for contracts, 406-408
 - agreements, 408*
 - RFIs, 408*
 - RFPs, 407*
 - RFQs, 407*
- residual risk, 314
- resource provisioning, 543-544
- REST (Representational State Transfer), 256
- restricting
 - command shell, 202-203
 - peripherals, 206-208
- Retina, 449
- reverse engineering attacks, 65
- reverse engineering existing solutions, 422
- reviewing effectiveness of existing security controls, 421
- RFCS (requests for comments), 395-396
- RFI (request for information), 408
- RFID, 527-528
- RFP (request for proposal), 407
- RFQ (request for quote), 407
- Rijndael algorithm, 42
- RIPMD-160, 36
- risk analysis, performing, 301-310
 - accept strategy, 312
 - ALE, calculating, 304-305
 - ARO, 306
 - avoid strategy, 310-311
 - magnitude of impact, 304
 - mitigate strategy, 311
 - motivation of risk, 305
 - NPV, calculating, 308-309
 - qualitative risk analysis, 302-303
 - quantitative risk analysis, 303
 - ROI, 307-309
 - SLE, calculating, 304
 - TCO, calculating, 309-310
 - transfer strategy, 311
 - trend analysis, 306
- risk management, 268
 - anticipating changes, 332
 - CASP exam objectives, 15-18
 - continuous improvement, 318
 - due care, 274
- Rivest, Ron, 43-46
- rogue access points, 505
- ROI (return on investment), 419
 - calculating, 307-309
- root CAs, 51

rotation schemes, 370-371
 routers, 151-152
 routing protocols, 174
 routing tables, 443-444
 RSA (Rivest, Shamir, and Adleman), 45-46
 RSA conference, 404
 RTUs (remote terminal units), 183
 rule sets, 159, 195
 rule-based access control, 574
 rules, 272
 runtime debugging, 447-448

S

SaaS (Software as a Service), 80
 vulnerability scanning, 214-215
 SABSA (Sherwood Applied Business Security Architecture), 315
 sales staff, security requirements, 462
 SAML (Security Assertion Markup Language), 581-582
 sandboxing, 216, 244-245
 SANs (storage area networks), 83-84
 SANS (SysAdmin, Audit, Networking, and Security) Institute, 403
 satellite Internet connections, 504
 SCADA (Supervisory Control and Data Acquisition), 183
 scalability, analyzing, 423
 screened host firewalls, 147-148
 screened subnets, 148-149
 scrubbing, 197
 script, key stretching, 32

SDL (Security Development Life Cycle), 519-521
 SDLC (system development life cycle), 517-519
 acquisition phase, 518
 disposal phase, 519
 implementation phase, 518
 initiation phase, 517-518
 operate/maintain phase, 518-519
 sealing, 208
 search and seizure, 382-383
 Secure Boot, 217-218
 SecureCode, 39
 SecureSessionModule, 235
 security policies, 272
 Group Policy
 GPMC, 201
 GPOs, 200
 implementing, 200-202
 influences on
 audits, 275
 client requirements, 277
 competitors, 275
 document exchange/review, 276
 onsite assessments, 276
 process/policy reviews, 276
 regulations, 276
 top-level management, 277
 security zones
 DMZs, 176
 separation of critical assets, 176
 segmentation, 545-546
 selecting
 cryptographic technique, 32
 penetration testing method, 452

- sensitive data, storing, 237-238
- sensors, 180
- separation of critical assets, 176
- separation of duties, 348-349
- server-based application virtualization, 222
- server-side processing, 255-260
- servers
 - provisioning, 544
 - virtualization, 209
 - Type I hypervisor*, 210
 - Type II hypervisor*, 211
- service packs, 193
- services (cloud), 80
- session keys, 41
- session management, 233-235
- SET (Secure Electronic Transaction), 39
- SFTP (SSH File Transfer Protocol), 113
- SHA (Secure Hash Algorithm), 35-36
- SHA-2, 35
- SHA-3, 35
- Shamir, Adi, 45-46
- Shibboleth, 583-584
- shoulder surfing, 456
- SHTTP (Secure HTTP), 39
- side-channel attacks, 63
- SIEM (security information and event management), 126-127
- site-to-site VPNs, 494
- situational awareness, 396-398
 - of client-side attacks, 396-397
 - of vulnerabilities, 397-398
- Skipjack, 42
- SLA (service-level agreement), 162-164, 345
- SLE (single loss expectancy), calculating, 304
- S/MIME (Secure Multipurpose Internet Mail Extensions), 69
- SMTP (Simple Mail Transfer Protocol), 484
- snapshots, 91-92
- sniffing, 434-435
- SNMP (Simple Network Management Protocol), 205
- SOA (service-oriented architecture), 553
- SOA (statement of applicability), 340-341
- SOAP (Simple Object Access Protocol), 246-247, 259
- social engineering attacks, 63, 455-456
- social media/networking, security implications of, 401
- SOEs (standard operating environments), 279
- software
 - antivirus software, cloud antivirus, 213
 - development methods, 247-254
 - Agile model*, 253, 523
 - build and fix*, 248
 - Cleanroom model*, 254
 - incremental model*, 250
 - JAD*, 254
 - prototyping*, 250
 - RAD model*, 252
 - spiral model*, 251, 524

- V-shaped model*, 249
- Waterfall method*, 248-249, 523-524
- endpoint security software, 191-198
 - antimalware*, 191-192
 - antispymware*, 192
 - antivirus software*, 192
 - DLP software*, 194
 - host-based firewalls*, 194-196
 - IDS*, 193
 - log monitoring*, 196-198
 - patch management*, 193
 - spam filters*, 192-193
- in-house developed software, interoperability with commercial software, 539
- secure coding standards, 247
- solving difficult problems**, 425
- sources of emerging threats**, 406
- SOX (Sarbanes-Oxley) Act**, 337
- spam filters**, 192-193
 - antispam services for the cloud, 213
- spear phishing**, 485
- SPI (Security Parameter Index)**, 40
- spin-offs, security issues**, 271
- spiral software development model**, 251, 524
- SPML (Service Provisioning Markup Language)**, 578
- SPOF (single point of failure)**, 166
- SQL injection**, 235-236
- SRK (storage root key)**, 208
- SRTM (Security Requirements Traceability Matrix)**, 297, 522
- SSDLC (Security System Development Life Cycle)**, 519-521
- SSH (Secure Shell)**, 69, 108
- SSID (service set identifier)**, 499
- SSL (Secure Sockets Layer)**, 38, 68-69, 110-111
- SSL inspection**, 156
- SSO (single sign-on)**, 571-572
 - AD, 586-587
 - advanced trust systems, 585-587
 - LDAP*, 586
 - RADIUS*, 585-586
 - Shibboleth, 583-584
 - WAYF, 584-585
- stakeholders**
 - incorporating input into CIA decisions, 291
 - security requirements, 290
 - database administrators*, 463-464
 - facilities manager*, 468
 - financial staff*, 466-467
 - human resources*, 466-467
 - management/executive management*, 465-466
 - network administrators*, 464-465
 - physical security manager*, 468
 - programmers*, 463
 - sales staff*, 462
- standard libraries**, 245
- standard word passwords**, 563
- standards**
 - adherence to, 536
 - competing standards, 536
 - de facto standards, 536-537
 - ISO/IEC 27000 series standards, 333-336
 - lack of, 536

- open standards, 536
- PCI DSS, 339
- PKCS, 69
- WLAN standards, 500-501
- state management, 260**
- stateful firewalls, 141**
- static passwords, 564**
- statistical attacks, 65**
- steganography, 56**
 - watermarking, 67
- storage. *See also* storage keys; storage protocols**
 - cloud storage, 79-80
 - antivirus products, 213*
 - content filtering, 216*
 - hash matching, 212-213*
 - sandboxing, 216*
 - vulnerability scanning, 214-215*
 - cookies, storing, 239
 - data archiving, 82-83
 - data warehousing, 80-82
 - DDPs, 93-94
 - deduplication, 92
 - encryption
 - block-level encryption, 96-97*
 - disk-level encryption, 96*
 - port-level encryption, 98*
 - record-level encryption, 98*
 - HBA allocation, 95
 - HSM, 372
 - integrating into an enterprise, 552
 - LUN masking, 94
 - magnetic storage media, removing data from, 244
 - multipathing, 90-91
 - multisite replication, 95-96
 - NAS, 84-86
 - offsite replication, 95-96
 - password storage, 566
 - SANs, 83-84
 - sensitive data, storing, 237-238
 - snapshots, 91-92
 - virtual storage, 78-79
 - VSANs, 86
- storage keys, 209**
- storage protocols, 87-90**
 - CIFS, 90
 - FCoE, 88-89
 - iSCSI, 87-88
 - NFS, 89
- strategies for penetration testing, 450**
- stream ciphers, 56-57**
- strength of cryptographic algorithms, 66**
- subobjectives**
 - of enterprise security objective, 6-13
 - of integration of computing, communications, and business disciplines objective, 21-23
 - of research, analysis, and assessment objective, 19-21
 - of risk management objectives, 15-18
 - of technical integration of enterprise components objective, 23-26
- switch spoofing, 140**
- switches, 137-138**
 - trunking security, 172-173

symmetric algorithms, 40-43

- 3DES, 41
 - modes, 61*
- AES, 42
- Blowfish, 42
- CAST, 43
- DES, 41
 - modes, 58-60*
- RC algorithms, 43
- session keys, 41
- Skipjack, 42
- Twofish, 43
- weaknesses of, 61

systems (PKI), 55

system-specific security policies, 323

T

TACACS+ (Terminal Access Controller Access Control System +), 118-120

tampering, 367

tape vaulting, 372

target tests, 450

Tavares, Stafford, 43

TCA (third-party connection agreement), 269

TCO (total cost of ownership), 419
 calculating, 309-310

TCSEC (Trusted Computer System Evaluation Criteria), 190

TDMA (Time Division Multiple Access), 498

technical deployment models, 539-546

Teredo, 112

testing

- multiple solutions, 418-419
- validation testing, 522

third-party outsourcing

- security issues, 269-270
 - downstream liability, 273*
 - due care, 274*
 - due diligence, 274*

threat actors, 405-406

threats

- APTs
 - CERT, 403-404*
 - emergent threats, 399-400*
 - intelligence, 406*
 - sources of, 406*
 - threat actors, 405-406*
 - zero-day attacks, mitigating, 398-399*
- insider threats, 379-380
- non-malicious threats, 380
- situational awareness, 397-398
- UTM, 122-123

throughput rate, 568

time of check/time of use attacks, 242-243

TLS (Transport Layer Security), 38, 68-69

top-down policy development, 332

top-level management, influence on security policies, 277

topics covered on exam, 628-638

TOS (trusted operating system), 190-191
CC, 190
examples, 191
TCSEC, 190

TPM (Trusted Platform Module) chips, 208-209
attestation, 579-580
IMA, 218
VTPM, 223-224

training policies, 357-359

transaction log backups, 370

transfer strategy for risk analysis, 311

transport encryption
3-D Secure, 39
FTP, 113
HTTP, 39
HTTPS, 39
IPsec, 39-40
SET, 39
SHTTP, 39
SSL, 38, 68-69
TLS, 38, 68-69

transposition, 49

trends
analyzing, 420-421
vulnerability cycle, 525-526

trunking security, 172-173

trusted third-party model, 581

TSIG (Transaction Signature), 554

Twofish, 43

Type I errors, 569

Type I hypervisor, 210

Type II errors, 569

U

UEFI (Unified Extensible Firmware Interface), 218-219

UMTS (Universal Mobile Telecommunications System), 499

unified collaboration tools, securing
desktop sharing, 481-482
email, 484-487
instant messaging, 481
presence, 483-484
remote assistance, 482-483
social media, 489
telephony, 487-489
video conferences, 479-480
web conferences, 478-479

Unix
chroot, 210
command shell restrictions, 202-203
password storage, 566

updates, 193

US-CERT (U.S. Computer Emergency Readiness Team), 404

USA PATRIOT Act, 340

USB devices, restricting, 206

user accounts
lockout policies, 565-566
managing, 562-563
provisioning, 544

user behaviors, risk management, 268

UTM (unified threat management), 122-123

V

- V-shaped software development model, 249
- validation testing, 522
- VDI (virtual desktop infrastructures), 221
- vertical privilege escalation, 237
- video conferences, securing, 479-480
- virtual devices, provisioning, 544
- virtual storage, 78-79
- virtualization
 - client-based application virtualization, 222
 - container-based virtualization, 211
 - server virtualization, 209-211
 - Type I hypervisor, 210*
 - Type II hypervisor, 211*
 - server-based application virtualization, 222
- VDI, 221
- virtual computing, 156
- virtual environments, securing, 545
- virtual firewalls, 154-155
- virtual proxy servers, 156
- virtual routers, 154-155
- virtual switches, 153-154
- virtual wireless controllers, 155
- VMs, 209
 - live migration, 220*
- VTPM, 223-224
- vulnerabilities
 - single physical server hosting multiple companies' VMs, 541-542*
 - single platform hosting multiple companies' VMs, 542*
- VLANs, 139-140, 549
- VM escape attacks, 219
- VMs (virtual machines), 209
 - live migration, 220
- VNC (Virtual Network Computing), 109-110
- VoIP, securing, 488-489
- VPNs, 107-108, 492-494, 550
 - MPLS, 108
 - site-to-site VPNs, 494
 - SSL, 495
- VSANs (virtual storage area networks), 86
- VTPM (virtual TPM), 223-224
- VTY ports, 205
- vulnerabilities
 - of hashing, 33
 - of hosts with differing security requirements, 219-221
 - data remnants, 221*
 - live VM migration, 220*
 - privilege elevation, 220*
 - VM escape attacks, 219*
 - of virtualization
 - single physical server hosting multiple companies' VMs, 541-542*
 - single platform hosting multiple companies' VMs, 542*
 - situational awareness, 397-398
- vulnerability assessment, 445-446
- vulnerability cycle, 525-526
- vulnerability management systems, 398
- vulnerability scanning, 434
 - for the cloud, 214-215

W

WAFs (web application firewalls),
131-132, 255

Walt Disney Magic Band, 527

warchalking, 505

wardriving, 505

warehousing, 80-82

WASC (Web Application Security Consortium), 245-246

Waterfall software development method, 248-249, 523-524

watermarking, 67

WAYF (Where Are You From?), 584-585

weaknesses

of asymmetric algorithms, 61

of symmetric algorithms, 61

weaknesses of industry-accepted development practices, OWASP, 246

web applications

browser extensions, 256-259

ActiveX, 257

AJAX, 258

Flash, 257

HTML5, 257

Java applets, 257

client-side processing, 255-260

industry-accepted development practices

WASC, 245-246

WS-Security, 246-247

JavaScript, 260

JSON, 256

REST, 256

security issues, 230

cookies, storing, 239

server-side processing, 255-260

SOAP, 259

state management, 260

WAFs, 255

web conferences, securing, 478-479

WEP (Wired Equivalent Privacy), 502-503

whaling, 486

WhatsUp Gold, 436

white box testing, 451

white hats, 406

whitelisting

application whitelisting, 199

character whitelisting, 235

Whois, 441-442

wildcard certificates, 52-53

Windows

Group Policy, 199-202

password storage, 566

WIPS (wireless intrusion prevention systems), 505

wireless controllers, 149-150

wireless networks, 550-551

WLANs (wireless LANs), 497-505

802.11 standard, 498

access points, 499

ad hoc mode, 499

Bluetooth, 502

CDMA, 498

FDMA, 498

GPRS, 499

GSM, 499

infrared, 502

- infrastructure mode, 499
- MAC filters, 504
- OFDMA, 498
- rogue access points, 505
- satellite connections, 504
- SSID, 499
- standards, 500-501
- TDMA, 498
- UMTS, 499
- warchalking, 505
- wardriving, 505
- WEP, 502-503
- wireless attacks, 505
- WPA, 503
- WPA2, 503
- worst-case scenario planning, 299-301**
- WPA (Wi-Fi Protected Access), 503**
- WPA2, 503**
- WS-Security, 246-247**
- WSUS (Windows Server Update Service), 203**

X

- X.500 standard, 586**
- X.509 standard, 50, 54-55**
- XACML (Extensible Access Control Markup Language), 577-578**
- XML, AJAX, 258**
- XOR operation, 56**
- XSS (cross-site scripting), 231-232**

Y-Z

- Zenmap, 432**
- Zero Knowledge Proof, 47**
- zero-day attacks, mitigating, 398-399**
- zero-knowledge tests, 450**