

Microsoft[®]

CISSP

Rapid 
Review

Darril Gibson

Rapid Review

Assess your readiness for the Certified Information Systems Security Professional (CISSP) exam—and quickly identify where you need to focus and practice. This practical, streamlined guide walks you through each exam objective, providing “need to know” checklists, review questions, tips, and links to further study—all designed to help bolster your preparation.

Reinforce your exam prep with a *Rapid Review* of these objectives:

- Access Control
- Telecommunications and Network Security
- Information Security Governance & Risk Management
- Software Development Security
- Cryptography
- Security Architecture & Design
- Operations Security
- Business Continuity & Disaster Recovery Planning
- Legal, Regulations, Investigations, and Compliance
- Physical (Environmental) Security



This book is an ideal complement to the in-depth training of the Microsoft Press® *Training Kit* for the CISSP Exam and other exam-prep resources.

ISBN: 978-0-7356-6678-8



9 0000



U.S.A. \$29.99

Canada \$31.99

[Recommended]

Certification/CISSP

CISSP Exam

ABOUT THE AUTHOR

Darril Gibson regularly teaches, writes, and consults on a wide range of security and technical topics. He holds several certifications including MCT, MCSA, MCSE, A+, Network+, Security+, and CISSP. Darril has written more than 20 books, including several popular certification titles.

SERIES EDITOR

Orin Thomas, MCITP, MCTS, MCSE, Microsoft MVP

microsoft.com/mspress

Microsoft®

Microsoft®

CISSP Rapid Review

Darril Gibson

Copyright © 2012 by Darril Gibson

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

ISBN: 978-0-7356-6678-8

1 2 3 4 5 6 7 8 9 LSI 7 6 5 4 3 2

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspin-put@microsoft.com. Please tell us what you think of this book at <http://www.microsoft.com/learning/booksurvey>.

Microsoft and the trademarks listed at <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions and Development Editor: Kenyon Brown

Production Editor: Rachel Steely

Editorial Production: nSight, Inc.

Technical Reviewer: Andrew Brice

Copyeditor: Richard Carey

Indexer: Nancy Guenther

Cover Design: Best & Company Design

Cover Composition: Zyg Group, LLC

Illustrator: Rebecca Demarest

Contents at a Glance

	<i>Introduction</i>	<i>xxiii</i>
Chapter 1	ACCESS CONTROL	1
Chapter 2	TELECOMMUNICATIONS AND NETWORK SECURITY	25
Chapter 3	INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT	47
Chapter 4	SOFTWARE DEVELOPMENT SECURITY	89
Chapter 5	CRYPTOGRAPHY	105
Chapter 6	SECURITY ARCHITECTURE & DESIGN	145
Chapter 7	OPERATIONS SECURITY	167
Chapter 8	BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING	195
Chapter 9	LEGAL, REGULATIONS, INVESTIGATIONS, AND COMPLIANCE	217
Chapter 10	PHYSICAL (ENVIRONMENTAL) SECURITY	247
	<i>Index</i>	<i>267</i>

Contents

Introduction

xxiii

Chapter 1	Access control	1
	Objective 1.1: Control access by applying the following concepts/methodologies/techniques	1
	Exam need to know...	2
	Policies	2
	Types of controls (preventive, detective, corrective, and so on)	3
	Techniques (non-discretionary, discretionary, and mandatory)	5
	Identification and authentication	6
	Decentralized/distributed access control techniques	8
	Authorization mechanisms	9
	Logging and monitoring	11
	Can you answer these questions?	12
	Objective 1.2: Understand access control attacks	12
	Exam need to know...	12
	Threat modeling	13
	Asset valuation	14
	Vulnerability analysis	15
	Access aggregation	15
	Can you answer these questions?	16
	Objective 1.3: Assess effectiveness of access controls.	17
	Exam need to know...	17
	User entitlement	17
	Access review and audit	18
	Can you answer these questions?	19

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Objective 1.4: Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)	19
Exam need to know...	19
Provisioning	20
Review	21
Revocation	22
Can you answer these questions?	23
Answers	23
Objective 1.1: Control access by applying the following concepts/methodologies/techniques	23
Objective 1.2: Understand access control attacks	23
Objective 1.3: Assess effectiveness of access controls	24
Objective 1.4: Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)	24
Chapter 2 Telecommunications and network security	25
Objective 2.1: Understand secure network architecture and design (e.g., IP & non-IP protocols, segmentation)	25
Exam need to know...	26
OSI and TCP/IP models	26
IP networking	29
Implications of multilayer protocols	30
Can you answer these questions?	31
Objective 2.2: Securing network components	31
Exam need to know...	31
Hardware (modems, switches, routers, wireless access points)	31
Transmission media (wired, wireless, fiber)	32
Network access control devices (firewalls, proxies)	33
End-point security	35
Can you answer these questions?	36

Objective 2.3: Establish secure communication channels (e.g., VPN, TLS/SSL, VLAN)	36
Exam need to know...	36
Voice (for example, POTS, PBX, VoIP)	36
Multimedia collaboration (remote meeting technology, instant messaging)	37
Remote access (screen scraper, virtual application/desktop, telecommuting)	38
Data communications	39
Can you answer these questions?	40
Objective 2.4: Understand network attacks (e.g., DDoS, spoofing)	41
Exam need to know...	41
DoS and DDoS	41
Spoofing	43
Can you answer these questions?	44
Answers	44
Objective 2.1: Understand secure network architecture and design (e.g., IP & non-IP protocols, segmentation)	44
Objective 2.2: Securing network components	44
Objective 2.3: Establish secure communication channels (e.g., VPN, TLS/SSL, VLAN)	45
Objective 2.4: Understand network attacks (e.g., DDoS, spoofing)	45

Chapter 3 Information security governance & risk management 47

Objective 3.1: Understand and align security function to goals, mission, and objectives of the organization	48
Exam need to know...	48
Align security function	48
Can you answer these questions?	49

Objective 3.2: Understand and apply security governance	49
Exam need to know...	49
Organizational processes (e.g., acquisitions, divestitures, governance committees)	50
Security roles and responsibilities	51
Legislative and regulatory compliance	52
Privacy requirements compliance	52
Control frameworks	53
Due care	55
Due diligence	55
Can you answer these questions?	56
Objective 3.3: Understand and apply concepts of confidentiality, integrity, and availability.....	56
Exam need to know...	56
Confidentiality	56
Integrity	57
Availability	58
Can you answer these questions?	58
Objective 3.4: Develop and implement security policy	59
Exam need to know...	59
Security policies	59
Standards/Baselines	60
Procedures	61
Guidelines	62
Documentation	62
Can you answer these questions?	63
Objective 3.5: Manage the information lifecycle (e.g., classification, categorization, and ownership).....	63
Exam need to know...	63
Manage the information lifecycle	64
Can you answer these questions?	65
Objective 3.6: Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)	65
Exam need to know...	65

Third-party governance	65
Can you answer these questions?	67
Objective 3.7: Understand and apply risk management concepts	67
Exam need to know...	67
Identify threats and vulnerabilities	68
Risk assessment/analysis (qualitative, quantitative, hybrid)	69
Risk assignment/acceptance	71
Countermeasure selection	72
Tangible and intangible asset valuation	73
Can you answer these questions?	73
Objective 3.8: Manage personnel security	74
Exam need to know...	74
Employment candidate screening (e.g., reference checks, education verification)	74
Employment agreements and policies	75
Employee termination processes	76
Vendor, consultant, and contractor controls	77
Can you answer these questions?	78
Objective 3.9: Develop and manage security education, training, and awareness	78
Exam need to know...	78
Security education, training, and awareness	78
Can you answer these questions?	79
Objective 3.10: Manage the security function	79
Exam need to know...	80
Budget	80
Metrics	81
Resources	82
Develop and implement information security strategies	83
Assess the completeness and effectiveness of the security program	83
Can you answer these questions?	84

Answers	84
Objective 3.1: Understand and align security function to goals, mission, and objectives of the organization	85
Objective 3.2: Understand and apply security governance	85
Objective 3.3: Understand and apply concepts of confidentiality, integrity, and availability	85
Objective 3.4: Develop and implement security policy	86
Objective 3.5: Manage the information lifecycle (e.g., classification, categorization, and ownership)	86
Objective 3.6: Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)	86
Objective 3.7: Understand and apply risk management concepts	87
Objective 3.8: Manage personnel security	87
Objective 3.9: Develop and manage security education, training, and awareness	88
Objective 3.10: Manage the Security Function	88
Chapter 4 Software development security	89
Objective 4.1: Understand and apply security in the software development lifecycle.....	89
Exam need to know...	90
Development lifecycle	90
Maturity models	92
Operation and maintenance	93
Change management	93
Can you answer these questions?	94
Objective 4.2: Understand the environment and security controls	94
Exam need to know...	94
Security of the software environment	95
Security issues of programming languages	98
Security issues in source code (e.g., buffer overflow, escalation of privilege, backdoor)	99
Configuration management	100
Can you answer these questions?	100

Objective 4.3: Assess the effectiveness of software security ..	100
Exam need to know...	100
Assessment methods	100
Can you answer these questions?	102
Answers	102
Objective 4.1: Understand and apply security in the software development lifecycle	102
Objective 4.2: Understand the environment and security controls	103
Objective 4.3: Assess the effectiveness of software security	103
Chapter 5 Cryptography	105
Objective 5.1: Understand the application and use of cryptography	105
Exam need to know...	106
Data at rest (e.g., hard drive)	106
Data in transit (e.g., on the wire)	106
Can you answer these questions?	107
Objective 5.2: Understand the cryptographic lifecycle (e.g., cryptographic limitations, algorithm/protocol governance)	107
Exam need to know...	108
Cryptographic lifecycle	108
Algorithm/protocol governance	108
Can you answer these questions?	109
Objective 5.3: Understand encryption concepts	109
Exam need to know...	109
Foundational concepts	110
Symmetric cryptography	111
Asymmetric cryptography	113
Hybrid cryptography	115
Message digests	115
Hashing	116
Can you answer these questions?	118

Objective 5.4: Understand key management processes	118
Exam need to know...	118
Creation/distribution	119
Storage/destruction	120
Recovery	120
Key escrow	120
Can you answer these questions?	121
Objective 5.5: Understand digital signatures	121
Exam need to know...	121
Purpose and process of digital signatures	121
Can you answer these questions?	123
Objective 5.6: Understand non-repudiation	123
Exam need to know...	124
Non-repudiation	124
Can you answer these questions?	124
Objective 5.7: Understand methods of cryptanalytic attacks . .	124
Exam need to know...	125
Chosen plaintext	125
Social engineering for key discovery	126
Brute force (e.g., rainbow tables, specialized/ scalable architecture)	126
Ciphertext only	127
Known plaintext	127
Frequency analysis	128
Chosen ciphertext	128
Implementation attacks	128
Can you answer these questions?	129
Objective 5.8: Use cryptography to maintain network security	129
Exam need to know...	129
Link vs. end-to-end encryption	129
SSL and TLS	130
IPsec	132
Can you answer these questions?	132
Objective 5.9: Use cryptography to maintain ap- plication security	132
Exam need to know...	133

Application security	133
Can you answer these questions?	134
Objective 5.10: Understand Public Key Infrastructure (PKI)	135
Exam need to know...	135
PKI	135
Can you answer these questions?	137
Objective 5.11: Understand certificate related issues	137
Exam need to know...	137
Certificates	137
Validating certificates	138
Can you answer these questions?	139
Objective 5.12: Understand information hiding alternatives (e.g., steganography, watermarking)	139
Exam need to know...	139
Information hiding alternatives	139
Can you answer these questions?	140
Answers	140
Objective 5.1: Understand the application and use of cryptography.	140
Objective 5.2: Understand the cryptographic lifecycle (e.g., cryptographic limitations, algorithm/protocol governance)	141
Objective 5.3: Understand encryption concepts	141
Objective 5.4: Understand key management processes	141
Objective 5.5: Understand digital signatures	142
Objective 5.6: Understand non-repudiation	142
Objective 5.7: Understand methods of cryptanalytic attacks	142
Objective 5.8: Use cryptography to maintain network security	143
Objective 5.9: Use cryptography to maintain application security	143
Objective 5.10: Understand Public Key Infrastructure (PKI)	143
Objective 5.11: Understand certificate related issues	144
Objective 5.12: Understand information hiding alternatives (e.g., steganography, watermarking)	144

Chapter 6 Security architecture & design 145

- Objective 6.1: Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-level Models) **145**
 - Exam need to know. **146**
 - Security models **146**
 - Can you answer these questions? **149**

- Objective 6.2: Understand the components of information systems security evaluation models **149**
 - Exam need to know. **149**
 - Product evaluation models (e.g., Common Criteria) **149**
 - Industry and international security implementation guidelines (e.g., PCI DSS, ISO) **151**
 - Can you answer these questions? **153**

- Objective 6.3: Understand security capabilities of information systems (e.g., memory protection, virtualization, Trusted Platform Module) **153**
 - Exam need to know. **153**
 - Security capabilities of information systems **153**
 - Can you answer these questions? **155**

- Objective 6.4: Understand the vulnerabilities of security architectures **155**
 - Exam need to know. **155**
 - System (e.g., covert channels, state attacks, emanations) **155**
 - Technology and process integration (e.g., single point of failure, service-oriented architecture) **157**
 - Can you answer these questions? **158**

- Objective 6.5: Understand software and system vulnerabilities and threats **158**
 - Exam need to know. **158**
 - Web-based (e.g., XML, SAML, OWASP) **158**
 - Client-based (e.g., applets) **159**
 - Server-based (e.g., data flow control) **160**
 - Database security (e.g., inference, aggregation, data mining, warehousing) **160**
 - Distributed systems (e.g., cloud computing, grid computing, peer to peer) **162**
 - Can you answer these questions? **162**

Objective 6.6: Understand countermeasure principles (e.g., defense in depth)	163
Exam need to know...	163
Defense in depth	163
Can you answer these questions?	163
Answers	164
Objective 6.1: Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-level Models)	164
Objective 6.2: Understand the components of information systems security evaluation models	164
Objective 6.3: Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module)	164
Objective 6.4: Understand the vulnerabilities of security architectures	165
Objective 6.5: Understand software and system vulnerabilities and threats	165
Objective 6.6: Understand countermeasure principles (e.g., defense in depth)	165
 Chapter 7 Operations security	 167
Objective 7.1: Understand security operations concepts	167
Exam need to know...	168
Need-to-know/least privilege	168
Separation of duties and responsibilities	169
Monitor special privileges (e.g., operators, administrators)	169
Job rotation	170
Marking, handling, storing, and destroying of sensitive information	170
Record retention	172
Can you answer these questions?	172
Objective 7.2: Employ resource protection	173
Exam need to know...	173
Media management	173
Asset management (e.g., equipment lifecycle, software licensing)	174
Can you answer these questions?	174

Objective 7.3: Manage incident response	174
Exam need to know...	174
Detection	175
Response	175
Reporting	176
Recovery	177
Remediation and review (e.g., root cause analysis)	177
Can you answer these questions?	178
Objective 7.4: Implement preventative measures against attacks (e.g., malicious code, zero-day exploit, denial of service)	178
Exam need to know...	178
Attacks	178
Preventative measures	180
Can you answer these questions?	182
Objective 7.5: Implement and support patch and vulnerability management	182
Exam need to know...	182
Patch management	182
Vulnerability management	183
Can you answer these questions?	184
Objective 7.6: Understand change and configuration management (e.g., versioning, base lining).	185
Exam need to know...	185
Change management	185
Configuration management	186
Can you answer these questions?	187
Objective 7.7: Understand system resilience and fault tolerance requirements	187
Exam need to know...	188
Fault tolerance for disks	188
Fault tolerance for servers	190
Can you answer these questions?	191
Answers	192
Objective 7.1: Understand security operations concepts	192
Objective 7.2: Employ resource protection	192
Objective 7.3: Manage incident response	192

Objective 7.4: Implement preventative measures against attacks (e.g., malicious code, zero-day exploit, denial of service)	193
Objective 7.5: Implement and support patch and vulnerability management	193
Objective 7.6: Understand change and configuration management (e.g., versioning, base lining)	194
Objective 7.7: Understand system resilience and fault tolerance requirements	194
Chapter 8 Business continuity & disaster recovery planning	195
Objective 8.1: Understand business continuity requirements	195
Exam need to know...	196
Develop and document project scope and plan	196
Can you answer these questions?	198
Objective 8.2: Conduct business impact analysis	198
Exam need to know...	198
Identify and prioritize critical business functions	198
Determine maximum tolerable downtime and other criteria	200
Assess exposure to outages (e.g., local, regional, global)	201
Define recovery objectives	201
Can you answer these questions?	202
Objective 8.3: Develop a recovery strategy	202
Exam need to know...	202
Implement a backup storage strategy (e.g., offsite storage, electronic vaulting, tape rotation)	202
Recovery site strategies	204
Can you answer these questions?	206
Objective 8.4: Understand disaster recovery process	206
Exam need to know...	206
Response	207
Personnel	208
Communications	208
Assessment	209
Restoration	209
Provide training	211
Can you answer these questions?	211

Objective 8.5: Exercise, assess, and maintain the plan (e.g., version control, distribution)	211
Exam need to know...	211
Exercises	212
Maintain the plan	213
Can you answer these questions?	214
Answers	214
Objective 8.1: Understand business continuity requirements	214
Objective 8.2: Conduct business impact analysis	214
Objective 8.3: Develop a recovery strategy	214
Objective 8.4: Understand disaster recovery process	215
Objective 8.5: Exercise, assess and maintain the plan (e.g., version control, distribution)	215

Chapter 9 Legal, regulations, investigations, and compliance **217**

Objective 9.1: Understand legal issues that pertain to information security internationally	217
Exam need to know...	218
Computer crime	218
Licensing and intellectual property (e.g., copyright, trademark)	219
Import/Export	222
Trans-border data flow	223
Privacy	224
Can you answer these questions?	225
Objective 9.2: Understand professional ethics	225
Exam need to know...	225
(ISC) ² Code of Professional Ethics	226
Support organization's code of ethics	227
Can you answer these questions?	227
Objective 9.3: Understand and support investigations.	228
Exam need to know...	228
Policy, roles, and responsibilities (e.g., rules of engagement, authorization, scope)	228

Incident handling and response	230
Evidence collection and handling (e.g., chain of custody, interviewing)	230
Reporting and documenting	231
Can you answer these questions?	232
Objective 9.4: Understand forensic procedures	233
Exam need to know...	233
Media analysis	233
Network analysis	235
Software analysis	236
Hardware/embedded device analysis	237
Can you answer these questions?	238
Objective 9.5: Understand compliance requirements and procedures	239
Exam need to know...	239
Regulatory environment	239
Audits	240
Reporting	241
Can you answer these questions?	241
Objective 9.6: Ensure security in contractual agreements and procurement processes (e.g., cloud computing, outsourcing, vendor governance)	242
Exam need to know...	242
Contractual agreements and procurement processes	242
Can you answer these questions?	244
Answers	244
Objective 9.1: Understand legal issues that pertain to information security internationally	244
Objective 9.2: Understand professional ethics	245
Objective 9.3: Understand and support investigations	245
Objective 9.4: Understand forensic procedures	245
Objective 9.5: Understand compliance requirements and procedures	246
Objective 9.6: Ensure security in contractual agreements and procurement processes (e.g., cloud computing, outsourcing, vendor governance)	246

Chapter 10 Physical (environmental) security	247
Objective 10.1: Understand site and facility design considerations	247
Exam need to know...	248
Site and facility design considerations	248
Can you answer these questions?	249
Objective 10.2: Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)	250
Exam need to know...	250
Physical access control and monitoring	250
Audit trails/access logs	252
Can you answer these questions?	252
Objective 10.3: Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)	253
Exam need to know...	253
Escort requirements/visitor control	253
Keys and locks	254
Can you answer these questions?	255
Objective 10.4: Support the implementation and operation of facilities security (e.g., technology convergence)	255
Exam need to know...	255
Communications and server rooms	255
Restricted and work area security	256
Data center security	257
Utilities and heating, ventilation, and air conditioning (HVAC) considerations	257
Water issues (e.g., leakage, flooding)	258
Fire prevention, detection, and suppression	258
Can you answer these questions?	260
Objective 10.5: Support the protection and securing of equipment	260
Exam need to know...	260
Can you answer these questions?	261

Objective 10.6: Understand personnel privacy and safety (e.g., duress, travel, monitoring)	261
Exam need to know...	261
Personnel privacy and safety	262
Can you answer these questions?	263
Answers	263
Objective 10.1: Understand site and facility design considerations	263
Objective 10.2: Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)	263
Objective 10.3: Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)	264
Objective 10.4: Support the implementation and operation of facilities security (e.g., technology convergence)	264
Objective 10.5: Support the protection and securing of equipment	264
Objective 10.6: Understand personnel privacy and safety (e.g., duress, travel, monitoring)	265
 <i>Index</i>	 267

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Introduction

This Rapid Review is designed to assist you with studying for the (ISC)² CISSP exam. The Rapid Review series is designed for exam candidates who already have a good grasp of the exam objectives through a combination of experience, skills, and study and could use a concise review guide to help them assess their readiness for the exam.

The CISSP exam is aimed at an IT security professional who has a minimum of five years of direct full-time security work experience in two or more of the 10 domains of the (ISC)² CISSP Common Body of Knowledge (CBK). One year can be waived for certain college degrees and technical certifications.

Candidates who take this exam should have the knowledge and skills required to do the following:

- Identify risk and participate in risk mitigation activities
- Provide infrastructure, application, operational, and information security
- Apply security controls to maintain confidentiality, integrity, and availability
- Identify appropriate technologies and products
- Operate with an awareness of applicable policies, laws, and regulations

It is important to note that real-world experience with security is required prior to earning the CISSP certification and that having practical knowledge is a key component to achieving a passing score.

This book reviews every concept described in the following exam objective domains:

- 1.0 Access Control
- 2.0 Telecommunications and Network Security
- 3.0 Information Security Governance & Risk Management
- 4.0 Software Development Security
- 5.0 Cryptography
- 6.0 Security Architecture & Design
- 7.0 Operations Security
- 8.0 Business Continuity & Disaster Recovery Planning
- 9.0 Legal, Regulations, Investigations and Compliance
- 10.0 Physical (Environmental) Security

This is a Rapid Review and not a comprehensive guide such as the forthcoming *CISSP Training Kit* (Microsoft Press, 2013). The book covers every exam objective on the CISSP exam but will not necessarily cover every exam question. (ISC)² regularly adds new questions to the exam, making it impossible for this (or any) book to

provide every answer. Instead, this book is designed to supplement your existing independent study and real-world experience.

If you encounter a topic in this book with which you do not feel completely comfortable, you can visit the links described in the text in addition to researching the topic further by using other websites, as well as consulting support forums.

NOTE The Rapid Review is designed to assess your readiness for the CISSP exam. It is not designed as a comprehensive exam preparation guide. If you need that level of training for any or all of the exam objectives covered in this book, we suggest the forthcoming *CISSP Training Kit* (ISBN: 9780735657823). The Training Kit will provide comprehensive coverage of each CISSP exam objective, along with exercises, review questions, and practice tests. The Training Kit will also include a discount voucher for the exam.

(ISC)² professional certification program

(ISC)² professional certifications cover the technical skills and knowledge needed to succeed in different IT careers. The CISSP certification is a vendor-neutral credential. An exam is an internationally recognized validation of skills and knowledge and is used by organizations and professionals around the globe. (ISC)² CISSP certification is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. (ISC)² exam objectives reflect the subject areas in an edition of an exam and result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of a professional with a number of years of experience.

MORE INFO For a full list of (ISC)² certifications, go to <https://www.isc2.org/credentials/>.

Acknowledgments

Books like this are never by just one or two people but instead are created with the combined efforts of a large group of people. I'm grateful for the help and support I received from multiple individuals at O'Reilly and Microsoft Press. I'm especially grateful for the outstanding technical input provided by Andrew Brice, the technical editor.

Support & feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site: <http://www.microsoftpressstore.com/title/9780735666788>

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority and your feedback our most valuable asset. Please tell us what you think of this book at <http://www.microsoft.com/learning/booksurvey>.

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: <http://twitter.com/MicrosoftPress>.

Preparing for the Exam

Certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Rapid Review and another training kit for your “at home” preparation and take an (ISC)² CISSP professional certification course for the classroom experience. Choose the combination that you think works best for you.

Access control

The Access Control domain covers a variety of different controls used to identify subjects, authenticate them, and control the access they are granted to different objects by controlling rights and permissions. Audit trails are an important element of accounting and logging and, combined with effective authentication, provide individual accountability. Access control attacks are common, and it's important for security professionals to have a basic understanding of evaluating threats and analyzing vulnerabilities to determine overall risk. Ideally, access controls are implemented to fully support an organization's security policy, and a way to verify this is through access reviews and audits. These reviews and audits can also detect problems in the identity and access provisioning life cycle, such as inactive accounts that have not been disabled.

This chapter covers the following objectives:

- Objective 1.1: Control access by applying the following concepts/methodologies/techniques
- Objective 1.2: Understand access control attacks
- Objective 1.3: Assess effectiveness of access controls
- Objective 1.4: Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)

Objective 1.1: Control access by applying the following concepts/methodologies/techniques

For this exam objective, you must understand many of the basics related to IT risk management. Security policies provide overall direction for an organization. Personnel within the organization then implement different types of controls to support the policy. At the core of access control is effective authentication, and it's important to understand the authentication factors. Without effective authentication, it isn't possible to enforce authorization and data within audit trails is not useful. Single sign-on (SSO) authentication methods have been widely available within a single organization's environment, but newer methods support SSO in federations. You should have an understanding of federated identity management systems and some of the XML-based protocols that they use to share authentication information.

Exam need to know...

- Policies
For example: Do you know and understand the common elements of a security policy, such as the principle of least privilege and separation of duties? What is an acceptable use policy?
- Types of controls (preventive, detective, corrective, and so on)
For example: What type of control is an audit trail? What type of control is a security guard?
- Techniques (for example, non-discretionary, discretionary, and mandatory)
For example: What is a commonly used non-discretionary model that organizes users into groups?
- Identification and authentication
For example: One authentication method requires users to enter a password and a PIN. Another model requires users to use a smart card and a PIN. Which is stronger?
- Decentralized/distributed access control techniques
For example: What XML-based standards are used to provide SSO capabilities in a federated identity management system?
- Authorization mechanisms
For example: How does a constrained user interface control access? What are the differences among an access control list, a capability table, and an access control matrix?
- Logging and monitoring
For example: What is provided by an audit trail? What is included in log management?

Policies

At the heart of any access control strategy is one or more security policies that identify the overall security goals of an organization. The security policy provides a high-level overview of generalized goals, and it is used to create more specific guidelines, standards, and procedures. Security policies commonly include one or more of the following elements:

- An acceptable use policy (AUP) informs users of their responsibilities when using IT systems and identifies unacceptable behaviors. Users should reread and acknowledge the AUP periodically, such as once a year.
- Least privilege refers to the practice of granting subjects access only to what they need to perform their jobs and no more.
- A separation of duties policy ensures that no single entity can control an entire process. It helps prevent fraud by requiring two or more people to conspire together.
- Job rotation policies help prevent fraud by ensuring that a person does not remain in the same position for an extended period and gain excessive control over any area of the business.

Access Control policies commonly refer to subjects and objects. A subject (such as a user) can access an object (such as a file or other resource). Subjects are often grouped together by using roles or groups to simplify administration. Similarly, objects are also grouped together, such as grouping files within folders or shares to simplify administration. As a best practice, permissions for an object are rarely granted to a single subject.

True or false? The primary goal of security policies is to protect confidentiality, integrity, and availability of an organization's assets.

Answer: *True*. Security policies and procedures are in place to support the core security goals of preventing the loss of confidentiality, integrity, or availability of assets.

EXAM TIP Often a question can sound overly complex when it is referring to *subjects* and *objects*, but you can usually simplify it by substituting the word *users* for *subjects* and the word *files* for *objects*. For example, instead of "Access Control administration is simplified by grouping subjects and objects," you can think of this as "Access Control administration is simplified by grouping users and files." Subjects can be more than just users, and objects can be more than just files, but substituting subjects with users and objects with files works in many instances without changing the meaning.

MORE INFO The Operations Security domain (covered in Chapter 7, "Operations security") specifically mentions some security operations concepts, such as need-to-know, least privilege, separation of duties, and job rotation. Overall, you'll find that many of the Access Control topics have some similarities to the Operations Security topics.

Types of controls (preventive, detective, corrective, and so on)

Security controls are safeguards or countermeasures put into place to reduce overall risk. One way they are classified is based on how they are implemented:

- **Technical or logical** controls are implemented with technology such as protecting objects with permissions or requiring users to change their passwords with a technical password policy.
- **Physical** controls include elements that you can physically touch, such as a door lock or a closed circuit television (CCTV).
- **Administrative or management** controls are written security policies or methods used to check the effectiveness of security, such as assessment or audit.

True or false? Pre-employment background investigations are a type of administrative control.

Answer: *True*. This is a procedure and would be done based on a policy.

Another way controls are classified is based on what they do, and they are often grouped together with the implementation method. Control classifications include the following:

- **Preventive** controls attempt to prevent incidents before they occur. A firewall is a technical preventive control because it can prevent malicious traffic from entering a network. A guard is a physical preventive control. Administrative preventive controls include access reviews and audits.
- **Detective** controls identify security violations after they have occurred, or they provide information about the violation as part of an investigation. An intrusion detection system is a technical detective control, and a motion detector is a physical detective control. Note that both an intrusion detection system and a motion detector include the word “detect,” which is a good clue. Reviewing logs or an audit trail after an incident is an administrative detective control.
- **Corrective** controls attempt to modify the environment after an incident to return it to normal. Antivirus software that quarantines a virus is an example of a technical corrective control. A fire extinguisher is an example of a physical corrective control.
- **Deterrent** controls attempt to discourage someone from taking a specific action. A high fence with lights at night is a physical deterrent control. A strict security policy stating severe consequences for employees if it is violated is an example of an administrative deterrent control. A proxy server that redirects a user to a warning page when a user attempts to access a restricted site is an example of a technical deterrent control.
- **Directive** controls are administrative controls that provide direction or guidance.
- **Compensating** controls are controls used as alternatives to the recommended controls. NIST SP800-53 mentions a compensating control used for an industrial control system (ICS). A change management policy might dictate the testing of all updates on live systems prior to deployment, but this might not be feasible for an ICS. A compensating control is an offline replicated system used for testing.
- **Recovery** controls provide methods to recover from an incident.

True or false? A user entitlement access review and audit is a detective control.

Answer: *False*. It is a preventive control. It is designed to identify whether users have more privileges than necessary prior to an incident. Discrepancies in assigned privileges can be corrected to prevent an incident. If an incident had already occurred, reviewing an audit trail would be a detective control.

EXAM TIP Given a security control, you should be able to identify it as preventive, detective, corrective, deterrent, recovery, or directive in nature. For example, visible security controls are deterrent in nature because they deter attackers. You should also be able to identify it as technical, physical, or administrative. For example, motion-activated lights are a physical preventive control.

MORE INFO National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Information Security," provides in-depth coverage of security controls. You can download it from this page: <http://csrc.nist.gov/publications/PubsSPs.html>. NIST SP 800-53 organizes the controls in families and classes that don't directly relate to the CISSP types of preventive, detective, and corrective, but the document does provide excellent descriptions and information about usage of IT security controls.

Techniques (non-discretionary, discretionary, and mandatory)

Non-discretionary access controls are centrally managed, and discretionary access controls (DAC) are managed by data owners. Mandatory access controls (MACs) are predefined by a higher authority, such as a policy that defines access labels.

In a DAC model, every object is owned by a subject and the owner has full control over the object. For example, when a user creates a file, the user owns the file and can modify the permissions. Common operating systems such as Windows and Linux use the DAC model.

In non-DAC models, subject and object access is controlled centrally, such as by an administrator. Role-Based Access Control (RBAC) is a common example in which subjects are placed into roles or groups by administrators. Access to objects is granted to the roles rather than to individuals.

True or false? Access control administration is simplified by grouping subjects and grouping objects.

Answer: *True*. Users and other subjects are often grouped together by using an RBAC model. Similarly, objects such as files are often grouped together in folders and shares.

EXAM TIP Know the primary differences between the models. DAC grants full control to end users. MAC uses predefined rules and labels to grant access. RBAC is a non-discretionary model that is controlled by administrators.

MAC uses labels assigned to subjects and objects, and when the labels match, subjects are granted access. Labels can be assigned in a hierarchical environment such as Unclassified, Secret, and Top Secret, with higher-level authorization also providing access to lower-level classifications. For example, someone granted Top Secret access also has Secret access. Labels can be assigned in a compartmentalized environment where access to one compartment does not provide access to any other data. A hybrid model uses compartments within classification levels and is easier to manage.

True or false? The Bell-LaPadula model is an example of a MAC model.

Answer: *True*. It uses a basic rule of no read up, no write down. The Simple Security Rule states that a subject cannot read up, and the *-property (star property) rule states that a subject cannot write down. In contrast, the Biba model (which is also a MAC model) uses a Simple Integrity Axiom of no read down and a * (star) Integrity Axiom of no write up.

EXAM TIP Different access control models have different primary goals. For example, the Bell-LaPadula model has a primary focus of ensuring confidentiality (ensuring that unauthorized users cannot access data). The Biba model has a primary focus on integrity (ensuring that unauthorized modification of data does not occur). The Clark-Wilson model and the Chinese Wall (also called Brewer-Nash) model use strict separation of duties rules to enforce integrity.

Identification and authentication

Identification occurs when a user claims an identity, such as with a user name. Authentication occurs when the user proves the claimed identity by using one or more factors of authentication. The three primary factors of authentication are as follows:

- Something you know (such as a password or PIN)
- Something you have (such as a smart card or RSA token)
- Something you are (proven with biometrics)

You can combine two or more factors to provide stronger authentication.

Two-factor authentication uses a method in two of the categories and is stronger than using a single factor. Multifactor authentication uses methods in two or more categories.

Even though passwords are usually stored as a hash, they can be cracked by using common comparative analysis tools. If attackers can access a password database, they can perform an offline analysis and quickly crack the passwords. Rainbow tables are commonly used in these attacks. Salting the hash with random bits protects against many offline password attacks, including the use of rainbow tables.

MORE INFO A hashing algorithm provides one-way encryption of data, creating a unique fixed-size string. Strong hashing algorithms such as SHA-256 are resistant to collisions, meaning that it is not feasible to identify another input to create the same hash. In this case, it would be difficult to identify another password that creates the same hash so that a successful comparative analysis discovers the original password. Salts thwart rainbow table attacks, but other attacks, such as dictionary attacks or brute-force attacks, can still be successful against an offline database of passwords.

True or false? Using a PIN and a password is an example of multifactor authentication.

Answer: *False*. A personal identification number (PIN) and a password are both in the same authentication factor (something you know). This is one-factor authentication, not multifactor authentication.

EXAM TIP Know the differences between the authentication factors. Passwords are the weakest form of authentication, but combining passwords with a method in a different factor, such as a smart card or using biometrics, provides multifactor authentication and increases the strength. Some specific access methods require stronger authentication. For example, remote access connections are vulnerable to attack, and multifactor authentication makes it more difficult for an attacker to impersonate a user.

Biometrics provide strong authentication, but they are susceptible to both false positives and false negatives. A false positive presents the highest risk. This occurs when an unauthorized individual is incorrectly identified as being authorized. The accuracy of a biometric system is identified by the crossover error rate (CER), which is calculated from Type 1 errors (false rejections) and Type 2 errors (false positives). A lower CER indicates a more accurate biometric system.

A simple way to reduce the risk of Type 1 and Type 2 errors is to use two-factor authentication. For example, in addition to the biometric method, the user can also be required to use a password.

A similar concept is used with credit cards and online purchases. Instead of just requiring the user to provide the credit card number and expiration date, users are often required to provide the credit card verification code. This is a 3-digit or 4-digit number on the front or back of the card.

True or false? Between iris scanners and retinal scanners, iris scanners are the most accurate form of biometric authentication.

Answer: *False*. Retinal scans are the most accurate form of biometric authentication. Even identical twins will have identifiable differences.

EXAM TIP Biometric authentication is the strongest form of authentication. Retinal scans measure the blood vessels in the back of the eye and are the most accurate method. Fingerprints are the most common method of biometrics in use.

Single sign-on (SSO) techniques are used in several different access control and identity management systems. These allow a user to log on once and access multiple resources without logging on again.

Internal networks can use a database such as Microsoft's Active Directory to manage user identities and provide SSO. Regular users have a single account and can access any resources in the network as long as they have permissions.

Kerberos is commonly used as an authentication protocol in a centralized model. It requires a central database of accounts and synchronized time (ideally synchronized with an external time source). Kerberos uses time-stamped tickets to authenticate accounts when they try to access a resource. These tickets are encrypted with symmetric encryption. Early versions of Kerberos used Data Encryption Standard (DES), which is now considered cracked, and current versions use Advanced Encryption Standard (AES).

EXAM TIP Know that SSO is part of an identity management system and can be used in a centralized environment such as a Microsoft domain using Kerberos. SSO methods are also implemented in federated identity management systems that include different operating systems.

Remote access protocols provide authentication, authorization, and accounting (AAA) services. Some common AAA protocols include the following:

- **Terminal Access Controller Access-Control System (TACACS)** One of the first AAA protocols used with remote access systems, TACACS has been replaced by RADIUS, TACACS+, or Diameter in most situations. TACACS uses UDP port 49 by default.
- **Remote Authentication Dial-in User Service (RADIUS)** This is a widely used AAA protocol in remote access systems and by Internet service providers (ISPs). It is used with both dial-in and virtual private network (VPN) access. It uses UDP and encrypts the password but not the entire authentication session.
- **TACACS Plus (TACACS+)** Cisco created this as a proprietary upgrade to TACACS. It separates each element of AAA in three processes. In comparison, RADIUS combines authentication and authorization. TACACS+ uses TCP port 49 instead of UDP, and it encrypts the entire authentication session instead of just the password.
- **Diameter** This is an alternative or upgrade to RADIUS, and it has much more flexibility. It can be used with wireless devices, Voice over IP (VoIP), Mobile IP, and smartphones, but it is not backward-compatible with RADIUS. The name implies it is twice as good as RADIUS because the diameter of a circle is twice the length of the radius.

EXAM TIP Common remote access protocols are RADIUS, TACACS+, and Diameter. TACACS+ is proprietary to Cisco and includes several benefits over RADIUS. Diameter has the most flexibility.

MORE INFO RADIUS is defined in RFC 2865 and has been updated by 2868, 3575, and 5080. Diameter is defined in RFC 3588. By replacing *xxxx* with the RFC number, you can view any RFC with the following URL: <http://tools.ietf.org/html/rfcxxxx>. TACACS+ is not defined in a formal RFC, but it is documented in a draft document available here: <http://tools.ietf.org/html/draft-grant-tacacs-02>.

Decentralized/distributed access control techniques

Distributed computing environments (DCEs) use distributed SSO mechanisms to control access. Federated identity management systems are used to provide SSO to Internet users from different entities. In this context, a federation is a group of companies that decide they want to collaborate to share resources.

For example, imagine that employees in Company A are granted access to resources in Company B and Company C. Instead of requiring these users to have three separate passwords, they can log on once within Company A and then access resources in Company B and Company C without logging on again.

MORE INFO The MSDN article “Federated Identity: Scenarios, Architecture, and Implementation” includes excellent examples of when a federated identity management system is needed and of some of the challenges. You can access it here: <http://msdn.microsoft.com/library/aa479079.aspx>.

A significant challenge is sharing the authentication and authorization information between the companies. If everyone used the same technologies, it would be easier to share the data, but more often, the federation has a heterogeneous identity environment. Different companies use different identity management methods.

Standards based on Extensible Markup Language (XML) are often used to share federated identity information over the Internet. Some of the commonly used standards include the following:

- Security Assertion Markup Language (SAML), which includes both authentication and authorization information
- Service Provisioning Markup Language (SPML), which is used to share provisioning information between organizations in the federation
- Extensible Access Control Markup Language (XACML), which provides a standard for evaluating authorization requests

True or false? SAML is used to provide SSO access when users are accessing sites with web browsers.

Answer: *True*. SAML is one of the schemas used with federated access, and it is often used to provide access via web browsers.

EXAM TIP A federated identity is an SSO-based identity that is portable between different organizations within a federation. Federated identity management systems use HTML-based and XML-based languages to share authentication and authorization information with each other. Many e-commerce solutions have implemented federated identity management systems to streamline the customer experience when making purchases from partner companies in a federation.

MORE INFO There are several resources on SAML, SPML, and XACML that you might find valuable. "Demystifying SAML" is available here: <http://www.oracle.com/technetwork/articles/entarch/saml-084342.html>. "XACML Overview" is available here: <http://xml.coverpages.org/xacml.html>. The full SPML v2.0 specification can be downloaded here: <http://www.oasis-open.org/committees/download.php/17708/pstc-spml-2.0-os.zip>.

Authorization mechanisms

After subjects prove their identity, or authenticate, they are granted access to objects based on their proven identity. Most authorization systems start with an implicit deny philosophy. For example, a user is denied access to files and folders unless the user is specifically given permissions to access them.

A common type of access model is RBAC, in which users are placed into roles or groups and privileges are granted to the group. However, there are other authorization mechanisms that can be used either separately or in combination with an RBAC model.

A constrained user interface limits what the user can see or do based on the user's privileges. For example, imagine an application that can be used by both administrators and regular users. When administrators use it, all the menu items

are visible and the application has full functionality. When a regular user starts the application, the menu items are either hidden or dimmed so that they can't be selected. When menu items are hidden, the users are unaware of the advanced capabilities.

Databases commonly use views as a constrained user interface to limit the available data. For example, an employee table might include names, addresses, phone numbers, and salary data. One view might include only names and phone numbers, and another view might include names and salary data. Users are granted access to the view that shows data that they're authorized to view, but they are not granted access to the other view or the underlying table.

Temporal-based authorization controls limit access based on time. For example, a virtual private network (VPN) user might be authorized to connect any weekday between 7:00 A.M. and 7:00 P.M. If the user attempts to connect on a weekend, the connection is blocked.

Location-based authorization controls limit access to specific locations. For example, an employee might be authorized to work from home by using a dial-in connection. Caller ID or callback technologies can be used to ensure that the user is calling from home and that another user is not impersonating the user from another location.

An extension of this is location-based authorization controls using domains. For example, the United States government purchased antivirus (AV) software for all government employees that they can download for free. The AV vendors restrict access to the download websites to allow only traffic coming from .mil domain locations.

Access control lists (ACLs), capability tables, and access control matrices (ACM) are related. An ACL is directly associated with an object, a capability table is directly associated with a subject, and an ACM combines them both. For example, a folder named data (an object) includes an ACL that lists all users granted access to the folder and their specific levels of access, such as read or write. A capability table might be created for a user named Darril (the subject) and include a list of all folders that he can access. The ACM includes all objects and all subjects and can be quite large.

NOTE ACLs are commonly associated with routers as a list of IP addresses, ports, and protocol IDs that are allowed in or out of a network. In this context, the router is the object and the IP address, port, or protocol ID is the subject. An ACL is created for each router, defining the access for different subjects (IP addresses, ports, or protocol IDs). A capability model might be created for different protocols, such as File Transfer Protocol (FTP), and list all routers that allow FTP traffic. An ACM would include all routers and all protocols.

True or false? The security kernel of an operating system controls access between subjects and objects.

Answer: *True*. A security kernel controls access. For example, the Windows kernel-mode security reference monitor in current Windows-based systems uses discretionary ACLs (DACs) to determine access with the DAC model.

EXAM TIP Know the differences among an ACL, a capability table, and an ACM. The ACL is focused on an object and lists subjects that can access it. The capability table is focused on a subject and lists objects the subject can access. The ACM combines them both.

Logging and monitoring

Logs record activity as it occurs and record details such as who did it (which account), what happened, when it happened, and where it happened. You can use one or more audit logs to create an audit trail. An audit trail is a detective control and provides enough information so that you can identify the relevant events leading up to and during an incident.

Audit trails are required to ensure accountability and depend on effective identification and authorization techniques. If users can easily use another account, the audit trail cannot effectively identify who took an action.

Log management methods ensure that logs are maintained to provide a full audit trail, that the logs are protected from modification, and that they are regularly reviewed. Protecting logs from modification is especially important if they will be used as evidence in court. Access to the logs should be restricted to administrators and security personnel only.

Administrators also use logs to manage and maintain systems. They provide key information used during troubleshooting and recovery of systems after a failure. These logs are used to help prevent or minimize loss of availability.

True or false? Audit trails are a type of preventive control that record who took an action, what action the user took, and when the user took it.

Answer: *False*. Audit trails are a type of detective control. An audit trail logs events as they occur, including details on who, what, when, and where. After an incident has occurred, these logs can be examined to re-create the events.

EXAM TIP Log management includes the practice of reviewing the logs (either manually or with an automated system) and protecting the logs from modification after they've been created. Logs should be synchronized with an external time source so that all logs record the same time. They should be stored in a central location that has restricted access. Attackers will often try to erase their recorded activity, but this is more difficult if the log is stored in another location.

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are also used for logging and monitoring. An IDS is a detective control that can detect attacks, and an IPS is a preventive control that can prevent attacks by detecting and

blocking them before they reach an internal network. Both controls send alerts or some type of notification when they detect a potential attack.

However, each alert isn't necessarily an attack. IDSs have adjustable thresholds, and an alert is created only when activity exceeds the threshold. If the threshold is too high, actual attacks can get through undetected. If the threshold is too low, the system generates too many false positives.

True or false? An IPS is placed in line with traffic.

Answer: *True*. All traffic goes through an IPS. The IPS detects and blocks malicious traffic but allows safe traffic through to the network.

MORE INFO IDSs and IPSs are mentioned in the Operations Security domain in Chapter 7, including methods of detection and response.

Can you answer these questions?

You can find the answers to these questions at the end of the chapter.

1. An organization has created a high-level document designed to provide direction to employees about security within the organization. What is this?
2. An audit trail is being used to identify events leading up to a security incident. What type of control is an audit trail in this situation?
3. What is the difference between an ACL and an ACM?
4. What is a measure of a secure biometric authentication system?
5. What is the purpose of SAML?
6. What type of authorization mechanism is a database view?
7. An audit trail is used after an incident. What is required for this audit trail to support individual accountability?

Objective 1.2: Understand access control attacks

Risk is identified by calculating the probability that a threat will exploit a vulnerability. Often, the threats come in the form of attackers attempting to exploit vulnerabilities in an organization's people, processes, or technology. Risk management includes identifying threats by using threat modeling, identifying valuable assets to protect, and analyzing vulnerabilities. Risks can then be mitigated with controls that reduce the impact of threats or reduce vulnerabilities.

Exam need to know...

- Threat modeling
For example: What are some methods of social engineering? What's the difference between a denial of service (DoS) and a distributed denial of service (DDoS) attack?

- **Asset valuation**
For example: When should the value of assets be identified? What assets should be evaluated within an organization as part of a risk management process?
- **Vulnerability analysis**
For example: How often should vulnerability assessments be done? What can a vulnerability scan detect?
- **Access aggregation**
For example: What types of attacks are launched by Advanced Persistent Threats (APTs)? Who can be a target of an APT?

Threat modeling

Threat modeling is the process of identifying potential and realistic threats to an organization's assets. You should be aware of common methods of access control attacks, including the following:

- **Social engineering** Attackers can often gain access simply by asking. This includes in-person, over the phone, and via email such as with phishing, spear-phishing, and whaling. It can also include tailgating and shoulder surfing.
- **Dumpster diving** If papers are thrown in the trash, they can easily be retrieved to gain information.
- **Malware** Viruses, worms, Trojan horses, and logic bombs are common methods that attackers use to gain control of a system or launch access control attacks.
- **Mobile code** Attackers have hijacked legitimate websites and installed malicious ActiveX and Java scripts. This represents a threat to the organization hosting the website. Additionally, visitors can be attacked by a drive-by download.
- **Denial of Service (DoS)** These come from a single attacker and attempt to disrupt normal operation or service of a system. A classic DoS attack is the SYN flood attack. DoS attacks are commonly launched against Internet-facing servers (any server that can be reached by another public IP address).
- **Distributed DoS (DDoS)** These come from multiple attackers, such as zombies in a botnet.
- **Buffer overflow** When input validation isn't used, unexpected code can cause an unhandled error and allow an attacker to install malicious code on a system.
- **Password crackers** Applications are widely available that can crack a password through comparative analysis. If the attacker can gain access to a database with passwords, the attacker can crack the passwords offline.
- **Spoofing** Attackers attempt to impersonate others in many different ways. They can spoof IP addresses, MAC addresses, and email addresses. Similarly, masquerading is when a social engineer impersonates someone such as a repairman.

- **Sniffers** Protocol analyzers placed on a network can capture traffic for later analysis. If passwords or valuable data are sent unencrypted, they can easily be read. Sniffers are often used in man-in-the-middle and replay attacks.
- **DNS-related attacks** Users can be tricked into providing their credentials on a bogus website after a DNS poisoning attack redirects traffic. DNS poisoning is used in pharming attacks.

True or false? Executives can be targeted through a whaling attack.

Answer: *True*. Whaling is a form of phishing that targets executives such as CEOs, presidents, and vice presidents.

True or false? A SYN flood attack uses spoofed IP addresses and causes a buffer overflow.

Answer: *False*. A SYN flood attack commonly uses spoofed IP addresses, but it doesn't cause a buffer overflow. Instead, it disrupts the three-way TCP handshake process by holding back the third packet.

EXAM TIP Know the common methods of attacks and the methods used to mitigate them. For example, the best prevention against social engineering is education, malware is detected and isolated with up to date antivirus software, and many DoS and DDoS attacks can be detected or prevented with IDSs or IPSs.

MORE INFO Attacks come from multiple sources. In "Rethinking the Cyber Threat - A Framework and Path Forward," Scott Charney of the Microsoft Trustworthy Computing Group outlines four categories: conventional cybercrimes, in which attackers target systems for criminal purposes; military espionage, in which nation states sponsor attacks against military targets to obtain military secrets; economic espionage, in which intellectual property is stolen for economic gain; and cyber warfare, in which attackers attempt to disrupt or disable the IT services of an enemy. You can download the white paper here: <http://www.microsoft.com/download/details.aspx?id=747>.

Asset valuation

One of the first steps in risk management is identifying the value of assets within the organization. This includes hardware assets, software assets, data and information assets, system assets, and personnel assets.

Key steps within the risk management process depend on knowing the value of the assets. For example, a cost-benefit analysis helps determine the return on investment (ROI) of a control. The ROI is high if you purchase an effective control for US\$1,000 to protect a web farm generating 1 million dollars a day. It is ridiculously low if you pay US\$1,000 to protect a US\$15 keyboard. These examples represent two extremes where the answer is obvious, but the answers aren't always so clear, especially if the value of assets is not known.

True or false? Asset valuation is done only on hardware assets.

Answer: *False*. Asset valuation should be done on all assets, including hardware, software, data or information, and personnel. Many systems, such as a web farm,

include hardware, software, and data and represent a combined value much greater than that of their individual components.

EXAM TIP Identifying the value of assets is an important first step in risk management and requires input from management. Technicians managing systems don't necessarily realize how much money a system generates, and without guidance, they might give the same amount of attention to a simple file server as they do to a server generating millions in revenue.

Vulnerability analysis

A vulnerability analysis helps determine how vulnerable a system is to one or more threats. This is often referred to as two separate processes: vulnerability scans and vulnerability assessments.

Vulnerability scans are performed with automated tools such as Nmap to determine what vulnerabilities exist at any given time. Vulnerability scanners can detect a wide assortment of vulnerabilities, including open ports, unpatched or misconfigured systems, and weak passwords.

A vulnerability assessment is an overall examination of the organization beyond just a technical scan. It will often attempt to match threats with vulnerabilities and use available data to determine the likelihood or probability that a threat will attempt to exploit a vulnerability. Data reviewed in an assessment includes security policies, historical data on past incidents, audit trails, and the results of various tests, including vulnerability scans.

Threats and the environment regularly change, so these reviews and scans must be repeated. Based on their security policies and available resources, organizations must decide how often to repeat the vulnerability scans and assessments. For example, a large organization might perform vulnerability scans weekly and vulnerability assessments annually, but a smaller organization might do scans only monthly.

True or false? Risk management is an ongoing process, and a vulnerability analysis is a point-in-time assessment.

Answer: *True*. Risk management is a continuous process that needs regular attention. A vulnerability analysis identifies vulnerabilities at a given time, but changes in threats or the environment negate the findings.

EXAM TIP Controls are put into place to support an organization's security policies. Vulnerability assessments and scans evaluate the effectiveness of these controls.

Access aggregation

Access aggregation refers to the combination of methods used to gain progressively more and more access. As a basic example, malware often attempts to progressively increase its privileges until it has full administrative access. On a larger scale, attackers often use a combination of methods to gain more and more access to an organization.

For example, an attacker might decide to target an organization and start with a dozen or so social engineering phone calls. Each call gets one more piece of information, and eventually the attacker has the names and email addresses of several executives. He might then use whaling to send one or more malware-infected phishing emails to these executives. If one of the executives takes the bait, the malware begins collecting information and sending it to the attacker.

This is challenging enough if you are considering only one attacker. Advanced Persistent Threats (APTs) are composed of full teams of attackers. They often have unlimited funding from a nation-state sponsor, but they could just as easily be funded by any group that has the money and a target.

True or false? An APT is a group of attackers, often sponsored by a government, that attacks only military or government targets.

Answer: *False*. An APT is often sponsored by a government, but it can target any organization. Attacks against organizations such as Google and Lockheed Martin are believed to have come from APTs.

EXAM TIP Attacks previously were primarily opportunistic, where the attackers looked for easy targets. When they failed to breach a target, they moved on to an easier one. In contrast, APTs launch targeted attacks against specific organizations and are not deterred by initial failures. They are often composed of state-sponsored personnel and use a wide variety of attack methods to progressively increase their access.

MORE INFO An article posted in the SANS Institute InfoSec Reading Room, "A Detailed Analysis of an Advanced Persistent Threat Malware" (http://www.sans.org/reading_room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware_33814), provides insight into the multiple techniques used by APTs. Malware delivered in a targeted spear-phishing email to a political figure was undetectable as malicious by 29 out of 44 antivirus engines. When successfully installed, it made significant system modifications, installed three Trojan spies, and began capturing and sending data to a command-and-control server. Of course, this would be only the beginning. Information gathered from the attack would be used to launch additional attacks by the APT.

Can you answer these questions?

You can find the answers to these questions at the end of the chapter.

1. An attacker is able to enter data into a webpage and install malware on the system. What should have been done to prevent this?
2. What assets should be evaluated when identifying asset values?
3. What is the primary purpose of vulnerability scans?
4. Who can be a target of an APT?

Objective 1.3: Assess effectiveness of access controls

Access controls should limit access to resources to only the people who need those resources. Two important elements of assessing the effectiveness of the controls are examining user entitlement and performing periodic access reviews and audits.

Exam need to know...

- User entitlement
For example: Which accounts deserve the most attention when considering user entitlement?
- Access review and audit
For example: How can you verify whether the principle of least privilege is being enforced?

User entitlement

User entitlement refers to the privileges granted to users when their accounts are first created and during the lifetime of the accounts. One of the primary considerations is ensuring that the principle of least privilege is followed. Users should not have access to more privileges than they need to perform their jobs.

Managing changes during the lifetime of the account can be challenging. Often, the process requires users to submit a request that must go through an approval process, and during this time, the user isn't able to complete job requirements. Bypassing the process improves productivity but sacrifices security. In some cases, the request process is so cumbersome that it's rarely followed.

Ideally, all changes are recorded in logs, creating an accurate audit trail. The audit trail can be used during an audit or review to determine whether the approval process is being followed. When someone's account is granted administrative privileges, the audit trail provides information about who requested the change, who approved it, and who implemented it. It can also identify the source of unauthorized changes.

Administrator and other accounts with elevated privileges deserve the most attention when considering user entitlement. This includes controlling the number of users granted privileged access and limiting the number of users who can grant elevated privileges to others.

It's common to require administrators to use two accounts. Administrators log on with a regular account to perform typical day-to-day work; this account has limited privileges. They log on with the administrator account only when they need to perform administrative tasks.

True or false? All accounts deserve the same level of attention when managing user entitlement processes.

Answer: *False.* Administrative and other privileged accounts deserve more attention than regular user accounts. Accounts with privileges can cause the most damage to a company if misused.

EXAM TIP User entitlement involves more than just assigning privileges when an account is created. It also includes all the changes that occur during the lifetime of an account.

Access review and audit

Performing routine access reviews and audits helps an organization know whether security policies related to user accounts are being followed. This includes checks related to entitlement, provisioning, usage, and revocation.

One goal is to determine whether least privilege policies are being followed. A simple method is to periodically check the membership of groups that have a high level of privileges. For example, membership in administrative groups should be limited, and a routine audit will detect whether unauthorized individuals have been added.

Another method is reviewing logs that record user access and user provisioning. An organization will often define procedures for granting additional privileges to any user. A review of the logs used to track this process will determine whether the process is being followed or bypassed.

A security policy will typically specify whether accounts should be disabled or deleted for ex-employees, and a review can determine whether the policy is being followed. Cross-checking active accounts with an employee list can identify potential issues.

These checks can also discover unauthorized accounts. Imagine an administrator who is fired for cause but retains administrative access immediately after the exit interview. It takes less than a minute to create an account and give it full administrative privileges, including the ability to access the network from a remote location. Even if the ex-employee's account is disabled, 15 minutes later the damage is done.

A review can also determine whether administrators are using their accounts as dictated by the security policy. For example, administrators are commonly required to use two accounts—one for regular day-to-day work and the other for administrative purposes. Administrators might be tempted to use the administrative account all the time and never use the regular account. A review of the logs can identify whether administrators are using the regular accounts and how often they're using them.

True or false? When performing an access review, access to all data should be examined.

Answer: *False*. Only access to sensitive data should be examined. A review that examines access to all data will be extremely large and include data available to all users.

EXAM TIP Access reviews and audits should be repeated periodically, such as every six months or annually. Additionally, administrative or IT personnel should not do the review because the review is designed to inspect the processes and procedures of administrative and IT personnel.

MORE INFO Symantec published an interesting white paper, “User and Group Entitlement Reporting,” which you can access here: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_entitlement_reporting_01-2006.en-us.pdf. It provides a good overview of user and group entitlement and includes some insight into what to look for when evaluating entitlement processes.

Can you answer these questions?

You can find the answers to these questions at the end of the chapter.

1. A user requires elevated privileges to perform a task once a week. What is the best way to assign these privileges?
2. What can be reviewed to determine whether an organization is complying with existing access control policies?

Objective 1.4: Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)

The identity and access provisioning life cycle directly addresses the management of accounts from creation to deletion. When an account is first created, it is provisioned with appropriate privileges. During the useful lifetime of an account, these privileges are often modified and the account needs to be periodically reviewed to ensure that it has not been granted excessive privileges. When the account is no longer being used, such as when an employee leaves the company, it should be disabled as soon as possible and deleted when it has been determined that it is not needed.

Exam need to know...

- Understand issues related to provisioning of an account
For example: What is permission creep?
- Understand review
For example: Which accounts are the most important to review during the identity and access provisioning life cycle?
- Understand the importance of revocation
For example: What should be done to a user account when an employee leaves the company?

EXAM TIP If you compare the information in the current Candidate Information Bulletin (CIB) with the previous one, you’ll see that the “and access provisioning life cycle” is a new topic. Some of the concepts are similar, but it’s worthwhile to recognize the importance (ISC)² is implying by adding the objective.

Provisioning

Provisioning refers to creating accounts and granting them access to resources. Role-based access control (or group-based) is often used to simplify management. Accounts are placed into groups that have defined privileges. As a best practice, all privileges are assigned via the role or group, and individual accounts are not granted privileges directly.

Some organizations use software to automate the provisioning process. For example, when an employee is hired, someone from the human resources department might enter the employee's information into an internal website application. This application is tied to a database and can automatically create the account and add it to the appropriate groups based on where the new employee will work.

Provisioning also occurs during the lifetime of an account when additional privileges are needed. For example, a salesperson assigned to the sales department needs privileges assigned to salespeople. If this person transfers to the IT department, the account is modified, adding privileges needed in the IT department.

Permission creep is a common problem that occurs when previously needed privileges are never removed. For example, someone who transferred from the sales department to the IT department no longer needs privileges assigned to salespeople. Without a procedure in place to remove unneeded privileges, many users progressively collect more and more privileges.

The use of roles or groups helps prevent permission creep. Users can be added and removed from the roles based on their current jobs, and they will automatically have the correct privileges.

Password policies and account lockout policies are often considered to be part of provisioning. Passwords are the weakest form of authentication, but strong password policies help ensure that users create strong passwords and regularly change them. They commonly include the following elements:

- **Password length** As tools to crack passwords become better and processor strength increases, the recommended length has also increased. An older recommendation is a password length of eight characters, but many security professionals now suggest a password length of 12 or more characters. Privileged accounts should be 15 or more characters.
- **Complexity** Passwords should have at least three of the four character types (uppercase, lowercase, numbers, and symbols). For the greatest complexity, passwords should include all four character types.
- **History** Users should be prevented from reusing the same password. A password history will often remember the last 12 or 24 passwords used by an account.
- **Maximum age** Users should be required to regularly change their passwords. Privileged accounts might be required to change their passwords every 30 days, and regular users might be required to change their passwords every 45, 60, or 90 days.

- **Minimum age** This setting requires users to wait before they can reset their password again, and it is often set to one day. It prevents users from repeatedly resetting their password to bypass the history requirement and reuse the same password.

Account lockout policies lock out accounts when incorrect passwords are entered too many times. For example, they can be set to lock out an account after the user enters the wrong password five times in a 30-minute period. The account can be set to remain locked until an administrator unlocks it or for a set time such as 15 minutes. Some policies implement a delay after two or more failed login attacks and are very effective at preventing brute force attacks.

Password reset systems reduce costs by allowing users to reset their passwords without administrative intervention. Many require users to answer secret questions during a registration process, and these questions are later used to validate the user's identity before resetting the password. Attackers have used social engineering methods to learn these secrets and impersonate the user during the reset process. Password reset systems that communicate via email are less susceptible to these types of attacks.

True or false? Account de-provisioning is an important process that helps ensure that the principle of least privilege is enforced.

Answer: *True*. Account de-provisioning is the practice of removing privileges that are no longer needed and prevents permission creep.

EXAM TIP Processes should be in place to manage and audit the provisioning of an account throughout its lifetime. Without clear procedures, users often collect additional privileges and end up with more privileges they need. A review or audit can discover the problem.

MORE INFO Microsoft published a collection of technical papers titled *Microsoft Identity and Access Management Series*, which is available as a free download from here: <http://www.microsoft.com/download/details.aspx?id=17974>. This package includes a wealth of information that is valuable in understanding provisioning in centralized access control and federated identity management systems. The "Provisioning and Workflow" paper provides some excellent information on provisioning, the identity information life cycle, and different methods used to manage the identity life cycle.

Review

Accounts should be reviewed periodically to ensure that company policies are being followed. Privileged accounts are the most important to monitor so that misuse is quickly detected. It's often possible to detect suspicious activity by reviewing the logged activity of these accounts.

Groups are commonly used to grant privileges, and monitoring membership in these groups is also effective during a review. As a best practice, privileges should be granted only to a group or role rather than to an individual.

Monitoring group membership isn't the only review, though. The privileges assigned to the groups should also be periodically reviewed. Groups are assigned privileges based on job tasks. As additional job responsibilities are added, additional privileges can be added without removing unneeded privileges. Also, it's easy to focus only on permissions during a review, but the rights assigned to subjects should also be reviewed.

True or false? System logging is an effective measure used to identify misuse of privileged accounts.

Answer: *True*. System logs provide accountability as long as effective identification and authentication methods are used.

EXAM TIP Periodic reviews are an important part of identity and access provisioning. They help identify whether security policies are being followed in the provisioning process and can be part of a formal access review and audit.

Revocation

Revocation of account access is a concept that most people understand, yet it is often not followed in practice. When an employee leaves the company, the account should be disabled as soon as possible. When the account is no longer needed, it should be deleted.

This is especially important for employees who have administrative privileges. There are more than a few stories where administrators were fired but retained access long enough to create unauthorized accounts with full administrative privileges that they later used to launch attacks.

Human resources (HR) departments can be valuable in keeping access control current. They know when employees are changing jobs and permissions should be changed, and they know when employees are being terminated and accounts should be revoked.

True or false? It is not necessary to immediately disable an account when an employee leaves after giving a notice.

Answer: *False*. It is just as important to disable accounts for employees who leave on good terms as it is to disable accounts for employees who have been fired.

EXAM TIP Accounts should be disabled as soon as possible for employees who leave the company. When an employee is terminated for cause, a policy should be in place so that the account is disabled during the exit interview.

Can you answer these questions?

You can find the answers to these questions at the end of the chapter.

1. When is an account provisioned?
2. What can be used to review the provisioning process to determine whether the security policy is being followed?
3. When should an account be disabled?

Answers

This section contains the answers to the “Can you answer these questions?” sections in this chapter.

Objective 1.1: Control access by applying the following concepts/methodologies/techniques

1. A security policy. It has an overall goal of preventing loss of confidentiality, loss of integrity, and loss of availability of assets considered valuable by the organization.
2. A detective control. It is being used after an incident to discover what occurred. Audit logs can also be used for access reviews and audits, but, in that case, the logs are a preventive control.
3. An access control list (ACL) is directly associated with an object, and it lists subjects that can access it. An access control matrix combines a capability table with an ACL and lists all subjects and objects.
4. Biometric systems with a low crossover error rate (CER) are better than systems with a high CER. The CER identifies where Type 1 errors (false reject rates) are equal to Type 2 errors (false accept rates).
5. Service Assertion Markup Language (SAML) is used in federated identity management systems to share user information for single sign-on (SSO) between organizations in a federation.
6. A database view is a constrained user interface.
7. Audit trails require strong identification and authorization systems in place. If users are not uniquely identified or can easily be impersonated due to weak authorization, the data in the audit trails cannot be trusted.

Objective 1.2: Understand access control attacks

1. Input validation. Buffer overflow attacks are possible when users can enter unexpected data into a system and access normally inaccessible memory spaces. Input validation checks the data before it is used and prevents this type of attack.
2. All assets, including hardware, software, data, systems, and people, should be evaluated to determine their value.

3. The primary purpose of vulnerability scans is to evaluate the effectiveness of security controls in enforcing security policies.
4. Any person or organization can be a target of an APT. APTs are commonly thought to attack only military and government targets, but they have also targeted civilian organizations and individuals.

Objective 1.3: Assess effectiveness of access controls

1. Create a second account for the user and give it elevated privileges. Instruct the user to use this account only when it is necessary to complete the tasks requiring the elevated privileges.
2. A primary method of review includes the use of audit logs and audit trails. Another method is to identify who is assigned elevated privileges, such as by viewing membership in administrative groups.

Objective 1.4: Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)

1. Accounts are provisioned when they are first created and throughout their lifetime. Provisioning occurs each time privileges are added, and de-provisioning is the process of removing privileges that are no longer needed.
2. Logs and audit trails are the primary method of reviewing the provisioning process. This requires the creation and proper management of logs and audit trails.
3. Accounts should be disabled as soon as it's known that they are not needed. When employees leave a company for cause, their account should be disabled during an exit interview.

Index

Symbols

- 802.11a wireless protocol, 32
- 802.11b wireless protocol, 32
- 802.11g wireless protocol, 32
- 802.11n wireless protocol, 33
- *-Integrity Axiom (star Integrity Axiom), 146
- *-property (star property) rule, 5, 146

A

- academic software, 221
- acceptable use policy (AUP), 2, 76
- access aggregation, 15–16
- access control
 - assessing effectiveness, 17–19
 - basics, 1–12
 - effective practices and accountability, 231
 - natural, 248
 - non-discretionary or discretionary, 5
- access control attacks, 12–16
- Access Control domain, 1
- access control lists (ACLs), 10, 34
- access control matrixes (ACM), 10
- access control policy, 170
- access control strategy, 2
- access reviews, 18–19
- accountability, effective access control practices and, 231
- account lockout policies, 20, 21
- accounts. *See* user accounts
- ACID model, 97
- ACK packet, 29
- acrylic glass, 249
- Active Directory Certificate Services (Microsoft AD CS), 136
- Active Directory (Microsoft), 7
- active IR sensor, 250
- active response by IDS, 181
- ActiveX controls, 98
- Adaptive Data Storage (ADS), 204
- Address Resolution Protocol (ARP), 26
- administrative accounts, 17, 18
 - revocation of account access, 22
- administrative controls, 3
- administrative-level permissions, 169
- Advanced Encryption Standard (AES), 7, 33, 96, 106, 111, 112
- Advanced Persistent Threats (APTs), 16, 219
- advisory security policies, 60
- aggregation attacks, 161
- AIC triad, 56–58
- airplane mode for mobile device, 35
- alarms, 249
- American Standard Code for Information Interchange (ASCII), 27
- annual loss expectancy (ALE), 72
- annual rate of occurrence (ARO), 72
- anomaly-based detection, 180
- anonymous relays, 180
- antivirus software, 181–182
 - on mobile computers, 262
- Apple devices, location data stored on, 238
- Application layer (OSI), 27
- application level firewalls, 34
- applications
 - cryptography for security, 132–134
 - patch management, 182–183
- arc 4 encryption algorithm, 112
- assessment, in disaster recovery process, 209
- assets
 - inventory systems, 260
 - management, 174
 - valuation, 14–15
 - tangible and intangible, 73
- asymmetric cryptography, 113–115
- Asynchronous Transfer Mode (ATM), 30
- atomicity, in ACID model, 97
- attackers, error message information and, 95
- attacks, 178–180
 - cryptanalytic, 124–129
 - preventive measures for, 180–182
- audio file, hiding data in, 139
- audio over IP networks, 37
- audit committee, 50
- audits, 18, 240–241
- audit trails, 11, 231, 252
 - for user account changes, 17

authentication

- authentication, 6–8
 - and confidentiality, 56
 - digital signatures and, 121
 - FFIEC on, 62
 - SSL and TLS for, 39
- authentication, authorization, and accounting (AAA) services, 8
- Authentication Header (AH), 39, 132
- authorization, 9–24
- automated inventory systems, 174
- automated processes to deploy updates, 183
- availability, 56
 - data in cloud computing, 244
 - fault tolerance and, 191
 - protecting, 48
 - of resources, 58
- awareness of employees on security, 78–79

B

- backdoors, 99, 101
- background check of job candidates, 74–75
- backups
 - metrics on, 81
 - storage strategy, 202–204
 - tapes as security resource, 82
- badges, 253
 - proximity, 252
- barcode database systems, for assets, 260
- baseline, 60–61
 - for computer configuration, 187
- bastion host, 34
- beacons, 159
- Bell-LaPadula model, 5, 6, 146
- Biba model, 5, 6, 146
- biometrics, 6, 7
- birthday attack, 126
- bit-level copies, 237
- bit-level image, 233
- BitLocker Drive Encryption (Microsoft), 106, 155
- bits, 28
- black box test, 184
- block ciphers, 112
- Blowfish, 112
- bluejacking, 40
- Bluetooth, 40
- Bosch, on CCTV cameras, 251
- bot herders, 42, 43, 156, 236
- botnet servers, 236
- bounds and boundary checking, 101

- Brewer-Nash model, 6, 147
- browsewrap contract, 222
- brute force attacks, 126
- budget, for security, 80–88
- buffer overflow, 13, 99
- business continuity, 195
- Business Continuity & Disaster Recovery Planning domain, 197
- Business Continuity Management Institute (BCM Institute), 204
- business continuity plan (BCP)
 - creation of, 196
 - exercises and reviews for testing, 211–214
 - focus of, 196
 - maintaining, 213
 - project scope development and documentation, 196–197
 - requirements, 195–198
- business impact analysis (BIA), 195, 198–202
- bus network topology, 28
- bytes, 139

C

- cable locks, 260
- cameras, 31, 32–33, 157
 - disconnecting from network to protect evidence, 230
 - plenum-safe, 259
- call tree for personnel notification of disaster recovery response, 207
- cameras, CCTV, 251
- capability maturity model (CMM), 89, 92
- capability table, 10
- carbon dioxide (CO₂), 259
- carbon footprint, 154
- Carnegie Mellon
 - CERT note, 42
 - Software Engineering Institute, 92
- carrier, for steganography, 140
- CCTV cameras, 251
- certificate authority (CA), 135–136
 - private, 136
- certificate revocation list (CRL), 138
- certificates, 133, 137–139
 - public keys in, 113
 - validation of, 138–139
- certificate trust chain, 136
- chain of custody log, 230–231
- change advisory board (CAB), 186

- change management, 93–94, 185–186
- Chargen protocol, 42
- checkpoint process, 97
- checksum, 116
- chief financial officer (CFO), 53
- children, parental consent for website information collection, 225
- Children's Online Privacy Protection Act (COPPA), 225
- Chinese Wall model, 6, 147
- chosen ciphertext attack, 128
- chosen plaintext attack, 125
- CIA triad, 56–58
- Cipher Block Chaining (CBC), 113
- ciphertext data, 110, 111
- ciphertext-only attack, 127
- Cisco
 - DocWiki site, 28
 - guide to ATM technology, 30
 - NetFlow, 236
- CISSP certification. *See also* exam need to know
 - code of ethics and, 226
- civil laws, 239
- Clark-Wilson model, 6, 147
- Class 1 certificate, 137
- Class A fire extinguishers, 259
- classification of information, senior management responsibility for, 64
- clean desk policies, 257
- clean power, 261
- click fraud, 219
- clickwrap contract, 222
- client-based software, threat against, 159–160
- client-side scripts, 98
- cloud computing, 162, 242
 - data protection and backup, 242
 - solutions for business continuity, 206
- code. *See* source code
- Code of Ethics, 225–227
- cold sites, 204
- collection of evidence, 230–231
- collisions, 127
- committed transactions, 97
- Committee of Sponsoring Organizations for the Treadway Commission (COSO), 54
- common access cards (CACs), 253
- Common Criteria, 149–153
- communication channels, 36–40
- communications
 - in disaster recovery process, 208–209
 - physical security for
 - equipment, 255–256
- compartmentalized environment, for label assignment, 5
- Compartmented security mode, 148
- compensating controls, 4
- computer crime, 217, 218–219
- concurrency controls, 97
- confidentiality of data, 56–57, 65, 110
 - with cloud computing, 243
 - from email cryptography, 133
 - protecting, 48, 105
- configuration management, 61, 100, 185, 186–187
- consistency, in ACID model, 97
- constrained user interface, 9
- consultants, 77
- containment of security incident, 176, 230
- content-dependent access controls, 161
- context-dependent access controls, 161
- continuity of operations plan (COOP) sites, 204
- contractors, 77
- contracts
 - ensuring security in, 242
 - for software, 222
 - with vendors, 242
- Control Objectives for Information and related Technology (COBIT), 53–54
- copyright, 219, 220
 - for software, 221
 - laws, 162
- corrective controls, 4
- cost
 - of backups, 82
 - of countermeasure, 80
- cost-benefit analysis, 14, 80
- counterattacks, 229
- countermeasures
 - cost of, 80
 - in risk management, 72–73
 - principles, 163
- covert channels, 156
- C programming language, 95
- creative works, copyrights to protect, 220
- credit card companies, PCI DSS standard for, 61, 149, 151, 240
- crime prevention through environmental design (CPTED) strategies, 247
- criminal laws, 239

- critical business functions, identifying and prioritizing, 198–200
- crossover error rate (CER), 7
- cross-site script (XSS), 44, 98
 - preventing attacks, 101
- cryptanalytic attacks, 124–129
- cryptographic keys, 110, 111
 - creation/distribution, 119
 - key escrow, 120
 - storage/destruction, 120
- cryptographic life cycle, 107–109
- cryptography
 - algorithm/protocol
 - governance, 108–109
 - application and use, 105–107
 - asymmetric, 113–115
 - basics, 109–118
 - for application security, 132–134
 - for network security, 129–132
 - key transmission, 112
 - symmetric, 111–113
- Cryptography domain, 105
- CSO Online, 257
- customers, communication about
 - disaster, 209

D

- damage assessment team, 208
- data at rest, encryption, 106
- databases
 - access control for, 147
 - deadlock, 161
 - security, 160–161
 - transaction logs, 97
 - views as constrained user interface, 10
- Data Center Physical Security Checklist, 257
- data center, security, 257
- data communications, 39–40
- data custodians, 51
- data emanation, risk of, 157
- Data Encryption Standard (DES), 7, 112
- data flow, trans-border, 223–224
- datagrams, 28
- data integrity, SSL and TLS for, 39
- data in transit, 106–107
- data in use, 153
- data leakage, 39, 160
- Data Link layer (OSI), 28
- data-loss prevention devices, 160
- data-loss prevention software, 40
- data marts, 97
- data mining, 97
- data owners, 51, 64
- data warehouse, 160
- date stamps, 95–96
- deadlock, 97, 161
- decryption process, 110
- Dedicated security mode, 148
- defense in depth, 163
- defense-in-depth strategy, 35
- degaussing, 171, 172
- deleting file, vs. sanitization, 171
- demilitarized zone (DMZ), 34
- denial of service (DoS) attack, 13, 41, 178
 - application failure from, 96
 - attacker identification, 43
- Department of Defense (DoD) model, 26
- design
 - in development life cycle, 90
 - of sites and facilities, for
 - security, 247–249
- detection systems, 250–252
- detective controls, 4
- deterrent controls, 4
- dial-up connections, 38
- Diameter, 8
- differential backups, 202
- Diffie-Hellman algorithm, 115
- digital signatures, 121–123
 - email validation with, 133
 - videos related to, 123
- digital voice communications, 36
- directive controls, 4
- disabled accounts, 22
- disaster recovery plan, for data center, 257
- disaster recovery strategies, 202–206
 - development and
 - documentation, 196–197
 - recovery process, 206–211
 - assessment, 209
 - communications, 208–209
 - employee training, 211
 - personnel, 208
 - response, 207
 - restoration, 209–210
 - recovery site strategies, 204–206
- disasters, impact of, 197
- discretionary access controls, 5
- Discretionary Security property rule, 146
- Discretix Technologies, Ltd., 129
- disks, fault tolerance for, 188–190

- display screen
 - filters, 256
 - harvesting data from, 39
 - disposition/disposal, in development life cycle, 91
 - disruption in service, 195, 199
 - distributed computing environments (DCEs), 8–9
 - distributed denial of service (DDoS)
 - attack, 13, 41, 42, 178
 - attacker identification, 43
 - distributed systems, 162
 - DNS-related attacks, 14
 - DNS spoofing, 43
 - documentation
 - in change management, 185
 - of exercise testing BCP, 213
 - for identifying vulnerabilities, 68
 - and regulation compliance, 66–67
 - for security incidents, 231–232
 - of security policies, 62–63
 - Domain Name System (DNS), 27
 - domains, 10
 - drive-by downloads, 98
 - drug testing, 75
 - due care, 55
 - due diligence, 55
 - in hiring practices, 75
 - dumpster diving, 13
 - duplexing, RAID-1 with, 188
 - durability, in ACID model, 97
 - Dynamic Host Configuration Protocol (DHCP) logs, 236
 - dynamic ports, 29
- E**
- Easter eggs, 101
 - eavesdropping, video conferencing and, 37
 - education of employees on security, 78–79
 - electrical fires, extinguishers for, 259
 - electromagnetic interference (EMI), 32
 - Electronic Code Book (ECB), 113
 - electronic data, movement across government boundaries, 223–224
 - electronic logs, 252
 - electronic vaulting, 203
 - El Gamal algorithm, 115, 128
 - elliptic curve cryptography (ECC), 115
 - email
 - encrypting and sending, 134
 - privacy limitations, 53
 - secure, 133
 - targeting executives with phishing, 159
 - email servers, 180
 - emergency management team, 208
 - employees. *See* personnel
 - EmployeeScreenIQ, 75
 - employment agreements and policies, 75–76
 - Encapsulating Security Payload (ESP), 39, 132
 - encapsulation, 26
 - EnCase, 237
 - enclosures, shielded, 157
 - encryption, 36, 39, 40, 56, 105
 - algorithm, 111
 - basics, 109–118
 - data at rest, 106
 - with hashing algorithm, 6
 - link vs. end-to-end, 129
 - for VPNs, 38
 - end-point security, 35
 - end-to-end encryption, link encryption vs., 129
 - end user license agreement (EULA), 222
 - environment
 - and security controls, 94–100
 - regulatory, 239–240
 - ephemeral ports, 29
 - E-Privacy Directive, 52, 224
 - equipment protection and securing, 260–261
 - error handling, 101
 - error messages, 95
 - escort requirements for visitors, 253–254
 - escrow of cryptographic keys, 120
 - ethics code, 225–227
 - European Union, 52
 - European Union Directive 2002/58/EC, 224
 - Evaluation Assurance Level (EAL), 150
 - evidence
 - collection, 176
 - collection and handling, 230–231
 - corruption risk from combining data
 - from multiple sources, 234
 - protecting, 230
 - evil twin, 33, 262
 - exam need to know
 - on access control, 2, 17
 - on access control attacks, 12–13
 - on business impact analysis, 198
 - on certificates, 137

- on code of professional ethics, 225
- on communication channels, 36
- on contracts, 242
- on cryptanalytic attacks, 125
- on cryptographic life cycle, 108
- on cryptography basics, 109–110
- on digital signatures, 121
- on disaster recovery process, 206
- on facilities security, 255
- on forensic procedures, 233
- on internal security
 - implementation, 253
- on investigations, 228
- on key management, 118
- on legal issues in international information security, 218
- on network attacks, 41
- on network components, 31
- on non-repudiation, 124
- on perimeter security, 250
- on personnel security, 74
- on provisioning life cycle, 19
- on regulations compliance, 239
- on risk management, 67–68
- on secure network architecture, 26
- on security architecture
 - vulnerabilities, 155
- on security function management, 80
- on security governance, 49
- on security incidents, 174–175
- on security models, 146
- on security operations, 168
- on security policy development and implementation, 59
- on software and system vulnerabilities and threats, 158
- on software development, 90
- on software environment, 94

ex-employees, policy on accounts of, 18

exercises for testing BCP, 211, 212–213

exit interview user accounts disabled during, 76

expiration of contractor accounts, 77

exporting goods and services, 222

exposure factor from risk, 70

Extensible Access Control Markup Language (XACML), 9

Extensible Markup Language (XML), 158

- standards based on, 9

external companies, data protection by, 244

extract, transform, load (ETL)
techniques, 160

F

facilities. *See also* physical security

factors of authentication, 6

failover clusters, 187, 190

- Microsoft server support for, 191

fail-safe door, 254

fail-secure, 254

fail-soft, 254

false positives, from IDSs, 180

Faraday cage, 156

fault tolerance, 187

- and backups, 203
- for disks, 188–190
- for servers, 190–191

Federal Deposit Insurance Corporation (FDIC), 170

Federal Desktop Core Configuration (FDCC), 61

Federal Financial Institutions Examination Council (FFIEC), 62

Federal Information Processing Standard Publication 201 on standards for PIVs, 254

federated identity, 9

- management systems, 8

fence disturbance sensors, 252

fiber optic cable, 32, 157

fiduciary relationship, 55

File Checksum Integrity Verifier (FCIV), 117

File Transfer Protocol (FTP), encrypting traffic, 106

fingerprinting, 7, 102

fire, classifications for, 259

fire prevention, detection, and suppression, 258–260

firewalls, 33–34

- deny-all rule, 148
- filtering traffic at, 43
- on mobile computers, 262

fixed focal length lens on CCTV camera, 251

Flash animations, 98

FM-200, 259

focal length lens on CCTV camera, fixed, 251

foreign key in database table, 97

forensic analysis procedures, 231

forensic collection procedures, 231

- forensic procedures, 233–238
 - hardware/embedded device analysis, 237–238
 - media analysis, 233–235
 - network analysis, 235–236
 - software analysis, 236–237
 - forensic toolkit, 237
 - fraggle attack, 42
 - Frame Relay WANs, 30
 - fraud
 - framework to reduce, 54
 - preventing, 167–173
 - reducing risk with job rotation, 170
 - freeware, 221
 - frequency analysis attack, 128
 - full backup, 202
 - full-scale exercises, 212
 - functional exercises, 212
 - functional security policies, 60
- G**
- garbage collection, 153
 - Generic Security Service Application Programming Interface (GSS-API), 95
 - glass for windows, 248–249
 - global positioning system (GPS), 35, 238
 - goals of organization
 - security function and, 48
 - security policies for, 59
 - goodwill, 73
 - risk of loss, 176
 - governance
 - for security, 49–56
 - third-party, 65–67
 - Gramm-Leach-Bliley Act (GLBA), 244
 - grandfather-father-son backup strategy, 203
 - graphic file, hiding data in, 139
 - graphics processing units (GPUs), 108
 - gray box testing, 184
 - grouping subjects and objects, 5
 - Group Policy (Microsoft), 187
 - groups, monitoring membership, 22
 - guidelines, 62
 - standards vs., 60
- H**
- halon, 259
 - hardware components, 31
 - hardware/embedded device analysis, 237–238
 - hash, 115
 - hashed message authentication code (HMAC), 117, 123
 - hashing, 57, 110, 111, 116–118, 235
 - algorithms for steganography detection, 140
 - definition, 96
 - SHA-1 and SHA-256 for, 40
 - Health Insurance Portability and Accountability Act (HIPAA), 66, 239–240
 - Heare, Sean, 257
 - heat-based detectors, 260
 - heating, ventilation and air conditioning (HVAC), 257
 - hierarchical environment, for label assignment, 5
 - high performance computers (HPCs), U.S. regulation of exports, 223
 - hiring, background check before, 74–75
 - honeypots, 43, 179
 - host-based firewalls, 34
 - hot and cold aisles, 58, 258
 - hot sites, 204, 205
 - human threats, 68
 - humidity, in server room, 258
 - hybrid cryptography, 115
 - hybrid risk assessment, 69
 - hyperlink spoofing attack, 43
 - Hypertext Transfer Protocol (HTTP), 27
 - Hyper-V, 154
- I**
- identification, 6–8
 - identity theft, 224
 - implementation attacks, 128
 - implementation, in development life cycle, 91
 - implicit deny rule, 9, 33
 - import/export, 222
 - incident response teams, 228
 - incremental backups, 202
 - Incremental model, 91
 - inference attack, 161
 - information classifications, senior management responsibility for, 64
 - information hiding, 139–140
 - information life cycle, 63–65
 - information security
 - international legal issues, 217
 - strategies, 83

Information Security Governance & Risk Management domain, 47

information systems

- evaluation models for security, 149–153
- security capabilities of, 153–155

Information Systems Audit and Control Association, 54

Information Technology Infrastructure Library (ITIL), 152, 186

informative security policies, 60

infrared (IR) corrected lenses, 251

infrared (IR) sensors, 250

Infrastructure as a Service (IaaS), 243

initiation, in development life cycle, 90

input validation, 99, 101

instant messaging (IM), 37–38

intangible assets, valuation, 73

integration

- in development life cycle, 90
- testing, 101

integrity of data, 56, 57, 95

- with cloud computing, 243
- digital signatures and, 121
- hashing to verify, 116
- protecting, 48

intellectual property, 217, 219–222

internal security, implementation and operation, 253–255

International Data Encryption Algorithm (IDEA), 112

international legal issues in information security, 217

International Telecommunications Union (ITU), 137

Internet Architecture Board (IAB), RFC 1087, on ethics and Internet, 227

Internet Assigned Numbers Authority (IANA), 29, 34

Internet Control Message Protocol (ICMP), 34

Internet Protocol (IP) networking, 29

Internet Protocol security (IPsec), 38, 39, 107, 132

Internet Relay Chat (IRC), 156

Internet Security Association and Key Management Protocol (ISAKMP), 39

Internetworking Technology Handbook, 28

interrogation, 231

intrusion detection systems (IDSs), 11–12, 43, 181

- report, 81

- intrusion prevention systems (IPSs), 11–12, 43, 180, 181
- inventory systems, automated, 174
- investigations of security incidents, 228–232
 - protecting sensitive information in reports, 232
 - roles and responsibilities, 228–229

Invocation property rule, 146

IP addresses

- identifying attack source, 236
- spoofed, 229

IPv4, 29

IPv6, 29

- vulnerabilities, 156

iris scanners, 7

Ironport Systems, 40

ISACA, 54

(ISC)², 225

- Code of Professional Ethics, 226–246

ISO/IEC 15408, 149

ISO/IEC 27002, 152

isolation

- in ACID model, 97
- of attacked system, 230

IT control framework, 53

IT Governance Institute, 67

J

Java, 95, 98

JavaScript, 98

job candidates, background check of, 74–75

job rotation policies, 2, 170

K

Kerberos, 7, 119

- time stamp use, 96

key derivation function (KDF), 119

Key Distribution Center (KDC), 119

key management, 118–121

- recovery, 120

keys and locks, 254

Knowbe4.com, 83

known plaintext attack, 127

L

labels

- for data, 171
- in mandatory access controls, 5

landscaping, 248

- laptops, training users to prevent theft, 260–261
- Layer 2 Tunneling Protocol over IPsec (L2TP/IPsec), 38
- least privilege principle, 2, 17, 99, 168
 - review of, 18
- Legal, Regulations, Investigations, and Compliance domain, 217
- legislative compliance of organization, 52
- “lessons learned” review, 177, 210
- licensing, 219–222
- likelihood values in risk assessment, 70
- limit checks, 101
- link encryption, end-to-end encryption vs., 129
- Linux, discretionary access controls, 5
- Locard’s exchange principle, 228
- location-based authorization controls, 10
- locks and keys, 254
- logging, 11–12
 - chain of custody, 230–231
 - review of, 18
 - system, 22
- logical controls, 3
- logical link control (LLC) sublayer, 28
- logic bombs, 13, 101, 179
- logo, legal protection for, 220
- logs
 - data capture from, 235
 - Dynamic Host Configuration Protocol (DHCP), 236
 - management, 11
 - physical access control, 252
- loss after countermeasure, 80
- loss before countermeasure, 80

M

- macros, 98
- maintenance
 - in development life cycle, 91
 - of software, 93
- malware, 13, 81, 101, 159, 178
 - developers’ use of bogus information, 237
 - incident involving, 177
 - types, 179
 - USB-based, 35
 - USB drives as risk, 173
- management controls, 3
- mandatory access controls (MACs), 5
- man-in-the-middle attack, 43

- maturity models, 92
- maximum tolerable downtimes (MTDs), 196, 200–201
- maximum tolerable period of disruption (MTPOD), 200
- MBSA tool, 184
- media
 - analysis in forensic procedures, 233–235
 - management, 173
 - protection based on data contents, 171
- media access control (MAC) filtering, 33
- media access control (MAC) sublayer, 28
- medium, for steganography, 140
- memory, application deallocation of, 153
- memory leaks, preventing, 153
- mesh network topology, 28
- Message Analyzer (Microsoft), 236
- message digest, 115–116
- Message Digest 5 (MD-5), 96, 116
- metrics, for security management, 81–82
- MH227, 259
- Microsoft
 - Active Directory, 7, 119
 - Active Directory Certificate Services (AD CS), 136
 - BitLocker Drive Encryption, 106
 - Group Policy, 187
 - Identity and Access Management Series, 21
 - Lync Server, 38
 - Message Analyzer, 236
 - Network Monitor, 236
 - server products, 191
 - TechNet, 34
 - trial versions of software, 221
- microwave transmitters, 252
- mirrored sites, 205
- mirroring, 188
 - remote, 204
- mission of organization
 - security function and, 48
- mobile code, 13, 98
- mobile devices
 - protection, 35
 - use in public place, 262
- mobile sites, 205
- module test, 101
- monitoring, 11–12
- motion or movement detectors, 251
- multifactor authentication, 6
 - for VPNs, 38

Multilevel security mode, 148
multimedia collaboration, 37–38

N

National Institute of Standards and Technology (NIST), 5
cryptographic standards, 108–109
on block ciphers, 113
on risk management, 49
on system development life cycle, 91
SP 800-30, on vulnerabilities, 68
SP 800-34, on contingency planning, 197
SP 800-34, on recovery procedures, 210
SP 800-61, on incident response, 175
SP 800-66, on HIPAA Security Rule, 240
SP 800-88 on sanitization, 172
SP 800-122, on PII, 52, 177, 262
natural access control, 248
natural disasters, 175
risks, 248
natural surveillance, 248
natural territorial reinforcement, 248
natural threats, 68
need-to-know, 168
negligence, 55
Nessus, 102, 184
NetFlow (Cisco), 236
network access control devices, 33
network address translation (NAT), 30
network analysis, 235–236
network attacks, 41–44
network components, 31–36
in server room, 256
network interface cards (NICs), 180
Network layer (OSI), 28
Network Monitor (Microsoft), 236
networks, secure architecture, 25–31
New Technology File System (NTFS), 106
Nmap, 15, 102
non-discretionary access controls, 5
non-repudiation, digital signature and, 121, 123–124
NOOP sled, 99
normalization, 97
Northrup, Tony, 34

O

objectives of organization, security function and, 48

objects
in Access Control policies, 3
grouping, 5
in security model, 146
Office Communications Server, 38
Office of Management and Budget (OMB), 61
one-way encryption, 117
online analysis processing (OLAP)
databases, 160
Online Certificate Status Protocol (OCSP), 138
online transaction database (OLTP), 97
online transaction processing (OLTP)
databases, 160
OpenPGP Alliance, 133
open ports, identifying, 102
Open Shortest Path First (OSPF), 32
open source licenses, 221
Open Systems Interconnection (OSI)
model, 26
Open Web Application Security Project (OWASP), 96, 159
operating system
patch management, 182–183
security kernel in, 11, 156
operation of software, 93
operations, in development life cycle, 91
Operations Security domain, 167
Orange Book standard, 149
Organisation for Economic Co-operation and Development (OECD), 223
organization
code of ethics, 227
legislative and regulatory
compliance, 52
location, and exposure to outages, 201
privacy requirements compliance, 52
processes for security governance, 50
restricted areas protection, 253
outages, metrics on, 81

P

packet analyzer, 235
packets, 28
paging file, 154
pan-tilt-zoom (PTZ) cameras, 251
parallel tests, 212
parental consent for website information
collection, 225

- passive infrared (IR) sensors, 250
- passive response by IDS, 181
- password crackers, 13
- passwords, 6, 96
 - masking, 256
 - policies, 20
 - reset systems for, 21
 - storage, 126
- patch management, 182–183
- patch panel, 31
- patents, 219, 220
 - on software, 222
- payload, for steganography, 140
- Payment Card Industry Data Security Standard (PCI DSS), 61, 149, 151, 240
- peer-to-peer (P2P) computing systems, 162
- penetration tests, 84, 184
- perimeter intrusion detection assessment systems (PIDAS), 252
- perimeter security, 250–252
- Permanent Virtual Circuit (PVC), 30
- permission creep, 20
- permissions, 169
- personal identification number (PIN), 6
- personal identity verification (PIV) cards, 253
- personally identifiable information (PII), 52, 176, 224
- personnel
 - code of ethics and decisions of, 227
 - fake phishing emails as test, 83
 - in disaster recovery process, 208
 - communication, 208–209
 - notification in disaster recovery response, 207
 - privacy and safety, 261
 - termination processes, 76–77
 - training in disaster recovery, 211
- personnel security, 74–78
 - education, training and awareness, 78–79
 - employee termination processes, 76–77
 - employment agreements and policies, 75–76
 - screening of job candidates, 74–75
- phishing emails
 - fake as employee test, 83
 - targeting executives with, 159
- photoelectric fire detectors, 259
- physical access control, logs, 252
- physical addressing, 28
- physical controls, 3
- Physical (Environmental) Security domain, 247
- physical intrusion detection systems, 250
- Physical layer (OSI), 28
- physical security, 31, 248–249
 - controls, 250–252
 - design for, 247–249
 - implementation and operation, 255–260
 - keys and locks, 254
 - layers of, 249
 - restricted and work area security, 256–257
- PIN (personal identification number), 6
- ping, 34
- plain old telephone service (POTS), 36
- plaintext data, 110, 111
- planning, in development life cycle, 90
- Platform as a Service (PaaS), 243
- plenum-safe cable, 259
- plenum space, 32
- Point-to-Point Protocol (PPP), 38
- Point to Point Tunneling Protocol (PPTP), 38
- polyinstantiation, 161
- Portable Network Graphics (png), 27
- port mirroring, 31, 235
- ports, 34
 - closing unneeded, 42
 - for TCP and UDP, 29
- port scanners, 102
- positive security model, 147–148
- power line conditioners, 261
- Presentation layer (OSI), 27
- Pretty Good Privacy (PGP), 133–134
- preventive controls, 4
- preventive measures for attacks, 180–182
- primary key in database, 97
- privacy
 - legal protection of data, 224–225
 - of personnel, 261–263
- Privacy Act of 2005, 52
- privacy requirements compliance, 52
- private branch exchange (PBX), 37
- private key, 113–114
- private ports, 29
- privileged accounts, 21
- privileges, monitoring, 169–170
- probability values in risk assessment, 70
- procurement processes, ensuring security in, 242
- product evaluation models, 149–150

- professional ethics, 225–227
- programming languages, security issues, 98
- projected benefits, 80
- promiscuous mode, NICs in, 180
- proprietary data, 64
- Protection Profile (PP), 150
- protocol analyzers, 14, 36, 180
- protocol data unit (PDU), 27
- protocols, implications of multilayer, 30
- prototype test, 90
- Prototyping model, 91
- provisioning life cycle, 19–23
- proximity badges, 252
- proximity volumetric detectors, 251
- proxy servers, 34
- pseudorandom keys, 119
- public information, use for hiring decisions, 75
- public key, 113–114
 - encrypting symmetric key with, 134
- public key infrastructure (PKI), 40, 133, 135–137
- public switched telephone network (PSTN), 36
- purging media, 171

Q

- qualitative risk assessment, 69, 70
- Quality of Service (QoS) technologies, in ATM, 30
- quantitative risk assessments, 69

R

- radio frequency interference (RFI), 32
- RAID (redundant array of independent disks), 187
- RAID-0, 188
- RAID-1, 188
- RAID-3, 189
- RAID-5, 189
- RAID-10, 189–190, 190
- rainbow tables, 6, 126
- random access memory (RAM), 154
- rapid application development (RAD), 91
- RC4 encryption algorithm, 112
- Real-time Transport Protocol (RTP), 37
- reciprocal agreement between companies, 205
- record retention policies, 172
- recovery agent, 120

- recovery controls, 4
- recovery objectives, 201
- recovery strategies, 196
- redundant systems, 58
- registered ports, 29
- registered trademarks, 220
- registration authority (RA), 135
- regulations
 - compliance requirements and procedures, 239–241
 - audits, 240–241
 - on reporting, 241
- regulatory compliance of organization, 52
- regulatory environment, 239–240
- regulatory security policies, 60
- relevant evidence, 231
- reliable evidence, 231
- remote access, 38–39
- remote access protocols, 8
- Remote Authentication Dial-in User Service (RADIUS), 8
- remote journaling, 204
- remote mirroring, 204
- Remote Procedure Calls (RPCs), 97
- remote wipe, 35
- reports
 - regulations on, 241
 - security incidents, 176–177, 231–232
- requirements analysis, in development life cycle, 90
- reset systems for passwords, 21
- residual risk, 71, 72
- resources, protection, 173–174
- restoration in disaster recovery, 209–210
- restricted area security, 256–257
- retinal scans, 7
- return on investment (ROI) of control, 14
- reverse engineering, 96
- reviews, for testing BCP, 211
- revocation of account access, 22
- RFC (Request for Comments)
 - 1122, on TCP/IP, 26
 - 1123, on TCP/IP, 26
 - 1321, on MD5, 116
 - 1918, on private IP address ranges, 30
 - 2246, on TLS, 130
 - 2560, on OSCP, 138
 - 2743, on GSS-API, 95
 - 2744, on C language interfaces, 95
 - 2865, on RADIUS, 8
 - 2868, on RADIUS, 8

- 3575, on RADIUS, 8
 - 3588, on Diameter, 8
 - 3851, on S/MIME, 133
 - 4301, on IPsec, 39
 - 4880, on OpenPGP Alliance, 133
 - 5080, on RADIUS, 8
 - 5246, on TLS, 130
 - 6101, on SSL, 130
 - 6151, on MD5, 116
 - RFID database systems, for assets, 260
 - Rijndael algorithm, 112
 - ring network topology, 28
 - risk, 12, 48
 - of data emanation, 157
 - of goodwill loss, 176
 - natural disaster, 248
 - organization protection against, 55
 - USB flash drives and, 173
 - risk assessments/analysis, 69–70
 - risk management, 67–74
 - asset valuation, 14–15
 - assignment/acceptance, 71–72
 - countermeasure selection, 72–73
 - threats and vulnerabilities
 - identification, 68–69
 - vulnerability analysis and, 15
 - risk mitigation, 71
 - risk transference, 71
 - rogue access point, 33, 256
 - role-based access control (RBAC), 5, 9, 20
 - root cause analysis, 177–178
 - root certificates, 135
 - routers, 31, 32
 - Routing Information Protocol 2 (RIP2), 32
 - RPO, 201
 - RSA (Rivest, Shamir, and Adleman)
 - algorithm, 114–115
 - RSA Factoring Challenge, 115
 - RSA token, 6
 - RTO, 201
- S**
- Safe Harbor framework, 223
 - safety of personnel, 261–263
 - salami attack, 218
 - salting hash, 6, 126
 - sandboxing, 98
 - sanitization, 171, 172
 - SANS Institute Reading Room, 16, 82
 - computer incident response team
 - overview, 229
 - on electronic data retention policy, 172
 - on physical security in data centers, 257
 - SANS Institute, security policy templates, 60
 - Sarbanes-Oxley Act of 2002 (SOX), 54, 67, 241
 - scope
 - of project, development and documentation, 196–197
 - of security incident, 176
 - screening of job candidates, 74–75
 - screen scraping, 39
 - SearchSecurity, 179
 - secret key cryptography, 113
 - Secure FTP (SFTP), 106
 - Secure Hashing Algorithm (SHA), 40
 - Secure Hashing Algorithm 1 (SHA1), 116
 - Secure Hashing Algorithm 256 (SHA-256), 96
 - Secure Multipurpose Internet Mail Extensions (S/MIME), 133
 - Secure Shell (SSH), 39, 106
 - Secure Sockets Layer (SSL), 38, 39, 107, 130–131, 158
 - Security Architecture & Design domain, 145
 - security architectures, vulnerabilities
 - of, 155–158
 - Security Assertion Markup Language (SAML), 9, 158
 - Security Assurance Requirements, 150
 - security controls, 3–5
 - Security Functional Requirements, 150
 - security function, management of, 79–84
 - security governance, 49–56
 - organizational processes, 50
 - security guards, 250
 - security incidents, 81. *See also* investigations
 - of security incidents
 - detection, 175
 - determine the source of, 232
 - handling and response, 230
 - preventative measures, 178–182
 - recovery, 177
 - remediation and review, 177–178
 - reporting, 176–177
 - reporting and documenting, 231–232
 - response management, 174–178
 - scope of, 176
 - verifying occurrence, 230

- security information and event management (SIEM), 35
- security information management (SIM), 35
- security kernel, 11, 156
- security management
 - budget, 80–81
 - metrics, 81–82
 - resources, 82–83
- security models, 145–149
- security operations, 167–173
 - completeness and effectiveness of, 83–84
 - job rotation policy, 170
 - monitoring privileges, 169–170
 - record retention policies, 172
 - roles and responsibilities, 51
 - separation of duties and responsibilities policy, 169
- security policies, 1–3, 49
 - development and implementation, 59–63
 - documentation, 62–63
- Security Target (ST), 150
- security triad, 56–58
- seed value for stream cipher, 113
- segment, 27
- senior management
 - organization security and, 59
 - responsibility for information classifications, 64
 - role in security, 51
- sensitive information
 - marking, handling, storing and destroying, 170
 - storage of backups, 203
- separation of duties policy, 2, 169
- server-based vulnerabilities, 160
- server rooms, physical security for, 255–256
- servers, fault tolerance for, 190–191
- service-oriented architecture (SOA), 157
- Service Provisioning Markup Language (SPML), 9
- service set identifier (SSID), disabling broadcast, 33
- session key cryptography, 113
- Session layer (OSI), 27
- shareware, 221
- shielded enclosures, 157
- shielded twisted-pair (STP) cable, 32, 157
- shoulder surfing, 126, 256
- shredders, 171
- shrinkwrap contract, 222
- Shuart, Donna M., 43
- side-channel attacks, 128
- signature-based IDS, 180
- signed applets, 159
- Simple Integrity Axiom, 146
- Simple Mail Transfer Protocol (SMTP), 27
- Simple Network Management Protocol (SNMP), 29
- Simple Security Rule, 5, 146
- single loss expectancy (SLE), 72
- single point of failure (SPOF), 195, 199
 - eliminating, 157
- single sign-on (SSO) authentication, 1, 7
- site design, for security, 247–249
- slack space, 233, 234
- smart cards, 6, 253
 - attacks on, 128
- smartphones, retrieving information from, 238
- smoke detectors, 259
- smurf attack, 42
- sniffers, 14, 180, 235
- sniffing attacks, 36
- SOAP, 97
- social engineering, 13, 126, 256
 - phone calls, 16
- social media, search by potential employers, 75
- software
 - assessing security effectiveness, 100–102
 - change management in development, 93–94
 - copyright, 221
 - licensing, 221
 - security of environment, 95–97
 - vulnerabilities and threats, 158–162
- software analysis, 236–237
- Software as a Service (SaaS), 243
- software development life cycle (SDLC), 89–94, 90–91
- Software Engineering Institute (Carnegie Mellon), 92
- software keys, 174
- source code
 - obfuscation, 96
 - review, 101
 - security issues, 99
 - signing, 98
- spam, 160, 180
 - metrics for, 81

- spam over instant messaging (SPIM), 38
- spear phishing, 159
- spiral model, 91
- spoofing, 13, 43–44
- spyware, 179
- Stacheldraht, 42
- stack overflow error, 99
- Standard Desktop Configuration (SDC), 61
- standards, 60–61
- star network topology, 28
- stateful inspection, 34
- steering committee, 50
- steganography, 139–140
- stream ciphers, 113
- stripe of mirrors, 190
- striping, 188, 189
- striping with parity, 189
- subject, of security model, 146
- subjects
 - grouping, 5
 - in access control policies, 3
- surge protectors, 261
- swap file, 154, 237
- Switched Virtual Circuit (SVC), 30
- switches, 31
- Symantec, 19, 133
- symmetric cryptography, 111–113, 114
- symmetric key, encrypting with public key, 134
- synchronization of log times, 11
- Synchronous Digital Hierarchy (SDH) fiber WANs, 30
- Synchronous Optical Networking (SONET), 30
- SYN flood attack, 14, 41
- SYN (synchronize) packet, 29
- Sysinternals, 237
- System Center Configuration Manager (SCCM), 183
- system development life cycle, 89, 90
- system event managers (SEMs), 35
- system high-security mode, 148
- system images, 186
- system logging, 22
- system resilience, 187–191
- system security architecture, 155–157
- system security policies, 60
- system vulnerabilities and threats, 158–162

T

- tablet devices, retrieving information
 - from, 238
- tabletop exercises, 212
- TACACS, 29
- TACACS Plus (TACACS+), 8
- tangible assets
 - valuation, 73
- tapes for backups, 203
 - rotating out of service, 173
- tape vaulting, 203
- target of evaluation (TOE), 150
- technical controls, 3
- technical recovery teams, 208
- technology, and process integration, 157
- Telecommunications and Network Security domain, 25
- teleconferencing, 37
- temporal-based authorization controls, 10
- termination process for employees, 76–77
- territorial reinforcement, natural, 248
- testing
 - backup strategy effectiveness, 203
 - black, white, or gray box, 184
 - changes, 186
 - in development life cycle, 90
- thin clients, remote access use by, 39
- third-party governance, 65–67
- threats
 - identifying, 68–69
 - modeling, 13–14
 - software and system, 158–162
- threat-source, 69
- three-way handshake, 29
- time of check (TOC), 156
- time of use (TOU), 156
- time stamps, 95
 - as evidence, 235
- tort laws, 239
- total risk, 71, 72
- Towers of Hanoi tape rotation scheme, 203
- tracert, 34
- trademarks, 219, 220
- trade secrets, 219, 220, 222
- training
 - in disaster recovery, 211
 - of employees on security, 78–79
 - for incident response team members, 229
 - on laptop theft prevention, 260–261
 - on safety and security issues, 262

- transaction logs for databases, 97
- trans-border data flow, 223–224
- Transmission Control Protocol (TCP), 29
- Transmission Control Protocol/Internet Protocol (TCP/IP) model, 26
- transmission media, 32–33
- Transport layer (OSI), 27
- Transport Layer Security (TLS), 39, 107, 130–131, 158
- transport mode in IPsec, 39
- trial software, 221
- Tribe Flood Network (TFN), 42
- Trinoo, 42
- Triple DES (3DES), 112
- Trivial File Transfer Protocol (TFTP), 29
- Trojan horse, 13, 179
- TrueCrypt, 106
- Trusted Computer System Evaluation Criteria (TCSEC), 149
- Trusted Platform Module (TPM), 106, 155
- tunneling, 156
- tunneling protocols, 38
- tunnel mode in IPsec, 39
- twisted-pair cable, 32
- two-factor authentication, 6, 7
- TwoFish, 112
- Type 1 errors, 7
- Type 2 errors, 7

U

- unauthorized access, protection against, 253
- unauthorized accounts, 18
- unhandled error, 99
- uninterruptible power supply (UPS), 261
- U.S. Air Force, Standard Desktop
 - Configuration (SDC)
 - Standard Desktop Configuration (SDC), 61
- U.S. Department of Defense, document 5200.28, 148
- U.S. Federal Bureau of Investigation (FBI)
 - Intellectual Property Theft website, 221
 - on safety for U.S. students traveling abroad, 262
- U.S. Nuclear Regulatory Commission, on intrusion detection systems, 252
- United States Privacy Act of 2005, 224
- unregistered trademarks, 220
- unshielded twisted-pair (UTP) cable, 32

- updates to operating system and applications, 182
- USB devices
 - controls to restrict use, 35
 - risk from, 173
- user accounts
 - de-provisioning, 21
 - disabling during exit interview, 76
 - managing changes, 17
 - of ex-employees, 18
 - review, 21–22
 - revocation of access, 22
- User Data Protocol (UDP), 27, 29
- user entitlement, 17–18
- user interface, constrained, 9
- utilities, 257

V

- vacation, mandatory policies on, 170
- validation
 - of certificates, 138–139
 - of input, 99, 101
- validity of data, 95–96
- valuation of assets, 14–15
- variables, names in code, 96
- varifocal lenses, 251
- VBScript, 98
- vendors, 77
- VeriSign Trust Network Certification Practice Statement document, 136, 137
- version control for BCP, 213
- video
 - hiding data in, 139
 - on security, 123
- video conferencing, 37
- views for databases, 147
- virtualization, 154
- virtual local area networks (VLANs), 40
- virtual memory, 153
- virtual private network (VPN), 38
- virtual solutions for business continuity, 206
- virtual team response, 228–229
- viruses, 13, 179
- visibility of people, facility design to maximize, 248
- visitors, escort requirements for, 253–254
- VM escape attack, 39, 154
- VMware, 206
- voice communications, 36–37
- Voice over Internet Protocol (VoIP), 37

volatile memory, data stored in, 153
volumetric sensors, 251
vulnerabilities
 attack on unknown, 179
 of data stored in cloud, 162
 identifying, 68–69
 in IPv6, 156
 management, 183–184
 of security architectures, 155–158
 server-based, 160
 software and system, 158–162
vulnerability analysis, 15

W

warm sites, 205
Waterfall model, 91
water leaks or flooding, 258
watermarking, 140
web-based languages, vulnerabilities, 158
websites, vulnerabilities, 98
web spoofing attack, 43
well-known ports, 29
whaling, 14, 159
white box testing, 184
whitelisting, 148
Wi-Fi Protected Access 2 (WPA2), 33
window circuit, 250
Windows
 discretionary access controls, 5
 New Technology File System (NTFS), 106
windows, in building design, 248
Windows Live Messenger, 37
Windows Software Update Services (WSUS), 183
Wired Equivalent Privacy (WEP), 33, 113, 127
wireless access points (WAPs)
 isolation mode, 33
wireless access point (WAP), 31
wireless networks, 32–33
wireless routers, 32
Wireshark, 37, 236
wiring closet, best location for, 256
work area security, 256–257
worms, 13, 176, 179
write blocker, 234

X

X.509 standard, 137
XML exploitation attacks, 158
XML (Extensible Markup Language), 158
 standards based on, 9
XSS (cross-site script), 44, 98
 preventing attacks, 101

Z

zero-day exploit, 179
zero knowledge test, 184
Zimmermann, Phil, 133
zombies, 42, 43, 236

About the Author

DARRIL GIBSON, Security+, A+, Network+, CASP, SSCP, CISSP, MCT, CTT+, MCSE, MCITP, is founder and CEO of Security, Consulting, and Training, LLC. Darril has written or co-written more than 25 books, including several on security and security certifications. He regularly posts articles on <http://blogs.GetCertifiedGetAhead.com> and can be reached at darril@GetCertifiedGetAhead.com.

What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

Microsoft[®]
Press