EXAM/CRAM



Fourth Edition

PEARSON IT CERTIFICATION

MICHAEL GREGG

FREE SAMPLE CHAPTER

SHARE WITH OTHERS F 💟 8 🛅 🚾

EXAM/CRAM

CISSP[®] Exam Cram

Fourth Edition

Michael Gregg

CISSP[®] Exam Cram, Fourth Edition

Copyright © 2017 by Pearson Education, Inc.

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

ISBN-13: 978-0-7897-5553-7

ISBN-10: 0-7897-5553-X

Library of Congress Control Number: 2016940474

Printed in the United States of America

First Printing: August 2016

Trademarks

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

Warning and Disclaimer

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

Special Sales

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

For government sales inquiries, please contact

governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief Mark Taub

Product Line Manager Brett Bartow

Acquisitions Editor Michelle Newcomb

Development Editor Ellie C. Bru

Managing Editor Sandra Schroeder

Project Editor Mandie Frank

Copy Editor Larry Sulky

Indexer Lisa Stumpf

Proofreader H.S. Rupa

Technical Editors

Chris Crayton Michael Angelo

Publishing Coordinator Vanessa Evans

Page Layout codeMantra

Contents at a Glance

	Introduction	1
CHAPTER 1	The CISSP Certification Exam	17
CHAPTER 2	Logical Asset Security	27
CHAPTER 3	Physical Asset Security	71
CHAPTER 4	Security and Risk Management	115
CHAPTER 5	Security Engineering	175
CHAPTER 6	The Application and Use of Cryptography	233
CHAPTER 7	Communications and Network Security	295
CHAPTER 8	Identity and Access Management	373
CHAPTER 9	Security Assessment and Testing	425
CHAPTER 10	Security Operations	491
CHAPTER 11	Software Development Security	541
CHAPTER 12	Business Continuity Planning	587
	Practice Exam I	631
	Answers to Practice Exam I	645
	Practice Exam II	661
	Answers to Practice Exam II	675
	Glossary	691
	Index	729

Table of Contents

Introduction	. 1
CHAPTER 1: The CISSP Certification Exam	17
Introduction	18
Assessing Exam Readiness	18
Taking the Exam	19
Examples of CISSP Test Questions	21
Answer to Multiple-Choice Question	23
Answer to Drag and Drop Question	23
Answer to Hotspot Question	23
Exam Strategy	24
Question-Handling Strategies	25
Mastering the Inner Game.	26
Need to Know More?	26
CHAPTER 2: Logical Asset Security	27
Introduction	28
Basic Security Principles	28
Data Management: Determine and Maintain Ownership	30
Data Governance Policy	30
Roles and Responsibility	32
Data Ownership	33
Data Custodians	34
Data Documentation and Organization	35
Data Warehousing	35
Data Mining	35
Knowledge Management	36
Data Standards	37
Data Lifecycle Control	37
Data Audit	37
Data Storage and Archiving	38
Data Security, Protection, Sharing, and Dissemination.	41
Privacy Impact Assessment	42
Information Handling Requirements	43

Contents

	44
Data Remanence and Decommissioning	45
Classifying Information and Supporting Assets	46
Data Classification	46
Asset Management and Governance	49
Software Licensing	50
Equipment Lifecycle.	51
Determine Data Security Controls	52
Data at Rest.	52
Data in Transit.	54
Endpoint Security	56
Baselines	57
Laws, Standards, Mandates and Resources	58
United States Resources	60
International Resources.	61
Exam Prep Questions	64
Answers to Exam Prep Questions	67
Need to Know More?	68
CHAPTER 3: Physical Assot Security	71
CHAPTER 3: Physical Asset Security	71
CHAPTER 3: Physical Asset Security	71 72
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks	71 72 72
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters	71 72 72 73
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Man-Made Threats.	71 72 72 73 74
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Man-Made Threats. Technical Problems	71 72 72 73 74 75
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Man-Made Threats. Technical Problems Facility Concerns and Requirements.	71 72 73 74 75 76
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Natural Disasters Man-Made Threats. Technical Problems Facility Concerns and Requirements CPTED CPTED	71 72 73 74 75 76 76
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Natural Disasters Man-Made Threats. Technical Problems Facility Concerns and Requirements CPTED Area Concerns.	71 72 73 74 75 76 76 76
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Man-Made Threats. Technical Problems Facility Concerns and Requirements CPTED Area Concerns Location	71 72 72 73 74 75 76 76 76 77
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Natural Disasters Nan-Made Threats. Technical Problems Facility Concerns and Requirements CPTED Area Concerns Location Construction	71 72 73 74 75 76 76 76 76 77 78 78
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Natural Disasters Nan-Made Threats. Technical Problems Facility Concerns and Requirements CPTED Area Concerns Location Construction Doors, Walls, Windows, and Ceilings	71 72 73 74 75 76 76 76 76 78 78 78 78
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Man-Made Threats. Technical Problems Facility Concerns and Requirements CPTED Area Concerns Location Construction Doors, Walls, Windows, and Ceilings Asset Placement	71 72 73 74 75 76 76 76 76 77 78 78 78 79 82
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Man-Made Threats. Technical Problems Facility Concerns and Requirements CPTED Area Concerns. Location Construction Doors, Walls, Windows, and Ceilings Asset Placement Physical Port Controls	71 72 73 74 75 76 76 76 76 77 78 78 78 82 82
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Natural Disasters Man-Made Threats. Technical Problems Facility Concerns and Requirements CPTED Area Concerns Location Construction Doors, Walls, Windows, and Ceilings Asset Placement Physical Port Controls Perimeter Controls.	71 72 73 74 75 76 76 76 77 78 78 78 78 82 82 82 83
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Man-Made Threats Technical Problems Facility Concerns and Requirements CPTED Area Concerns Location Construction Doors, Walls, Windows, and Ceilings Asset Placement Physical Port Controls Perimeter Controls Fences	71 72 73 74 75 76 76 76 76 78 78 78 82 82 83 83
CHAPTER 3: Physical Asset Security Introduction Physical Security Risks Natural Disasters Man-Made Threats. Technical Problems Facility Concerns and Requirements CPTED Area Concerns. Location Construction Doors, Walls, Windows, and Ceilings Asset Placement. Physical Port Controls Perimeter Controls Fences Gates	71 72 72 73 74 75 76 76 76 76 78 78 79 82 83 83 83 84

CCTV Cameras
Lighting
Guards and Dogs
Locks
Employee Access Control
Badges, Tokens, and Cards
Biometric Access Controls
Environmental Controls
Heating, Ventilating, and Air Conditioning
Electrical Power
Uninterruptible Power Supply 100
Equipment Life Cycle
Fire Prevention, Detection, and Suppression
Fire-Detection Equipment
Fire Suppression 103
Alarm Systems
Intrusion Detection Systems
Monitoring and Detection
Exam Prep Questions
Answers to Exam Prep Questions
Suggested Reading and Resources
CHAPTER 4:
Security and Risk Management 115
Introduction
Security Governance
Third-Party Governance
Organization Processes
Protection of Intellectual Properly 121
Privacy Laws and Protection of Personal Information
Relevant Laws and Regulations
United States Legal System and Laws
International Legal Systems and Laws
Computer Crime and Hackers
Sexual Harassment
Risk Management Concepts
Risk Management Frameworks
Risk Assessment

Countermeasure Selection		 	1	46
Develop and Implement Security Policy		 	1	49
Security Policy		 	1	50
Standards		 	1	52
Baselines		 	1	52
Guidelines		 	1	53
Procedures		 	1	53
Types of Controls		 	1	54
Administrative Controls		 	1	54
Technical Controls		 	1	55
Physical Controls		 	1	55
Access Control Categories		 	1	55
Implement Personnel Security		 	1	56
New-Hire Agreements and Policies		 	1	57
Separation of Duties		 	1	57
Job Rotation		 	1	58
Least Privilege		 	1	58
Mandatory Vacations		 	1	59
Termination		 	1	59
Security Education, Training, and Awareness		 	1	60
Security Awareness		 	1	61
Social Engineering		 	1	62
Professional Ethics Training and Awareness		 	1	63
ISC ² Code of Ethics		 	1	64
Computer Ethics Institute		 	1	65
Internet Architecture Board		 	1	65
NIST SP 800-14		 	1	66
Common Computer Ethics Fallacies		 	1	67
Regulatory Requirements for Ethics Program	S	 	1	67
Exam Prep Questions		 	1	69
Answers to Exam Prep Questions		 	1	72
Need to Know More?		 	1	73
CHAPTER 5:				
Security Engineering		 	1	75
Introduction		 	1	76
Fundamental Concepts of Security Models		 	1	76
Central Processing Unit		 	1	76
Storage Media		 	1	81

I/O Bus Standards
Virtual Memory and Virtual Machines
Computer Configurations
Security Architecture
Protection Rings
Trusted Computer Base
Open and Closed Systems
Security Modes of Operation
Operating States
Recovery Procedures
Process Isolation
Common Formal Security Models
State Machine Model
Information Flow Model
Noninterference Model
Confidentiality
Integrity
Other Models
Product Security Evaluation Models
The Rainbow Series
Information Technology Security Evaluation Criteria
Common Criteria
System Validation
Certification and Accreditation
Security Guidelines and Governance
Enterprise Architecture
Regulatory Compliance and Process Control
Vulnerabilities of Security Architectures
Buffer Overflow
Back Doors
State Attacks
Covert Channels
Incremental Attacks
Emanations
Web-based Vulnerabilities
Mobile System Vulnerabilities
Exam Prep Ouestions

Answers to Exam Prep Questions	30
Need to Know More?	31
CHAPTER 6: The Application and Use of Cryptography 22	23
	24
Compto anombio Decise)+)/
Listory of Energetian)+ ,7
Storepography 2/)/ 12
Steganography Operation	г <i>э</i> 1/1
Digital Watermark	15
	17 17
Cipher Times and Methods	FO 17
Support Types and Methods	F/ 10
Data Energytion Standard	57 57
Trialo DES	, Z
Advanced Energytion Standard (AES)	7
International Data Encryption Algorithm	, / 58
Rivect Cinher Algorithms	,0 58
Asymmetric Energation 2	,0 50
Diffie_Hellman 2/	51
PSA 2/	52
Fl Gamal 24	52
Filiptical Curve Cryptosystem	53
Merkle-Hellman Knapsack	54 54
Review of Symmetric and Asymmetric Cryptographic Systems 20	54
Hybrid Encryption	55
Integrity and Authentication	56
Hashing and Message Digests	57
Digital Signatures	70
Cryptographic System Review	72
Public Key Infrastructure	72
Certificate Authority	72
Registration Authority	73
Certificate Revocation List	73
Digital Certificates	74
The Client's Role in PKI	6

Email Protection Mechanisms
Pretty Good Privacy
Other Email Security Applications
Securing TCP/IP with Cryptographic Solutions
Application/Process Layer Controls
Host to Host Layer Controls
Internet Layer Controls
Network Access Layer Controls
Link and End-to-End Encryption
Cryptographic Attacks
Exam Prep Questions
Answers to Exam Prep Questions
Need to Know More?
CHARTER 7.
Communications and Network Security
Introduction 206
Secure Network Design 206
Network Models and Standards 296
OSI Model 207
Encapsulation/De-encapsulation 303
TCP/IP 304
Network Access Laver 305
Internet Laver 306
Host-to-Host (Transport) Laver 311
Application Layer 314
LANs and Their Components
LAN Communication Protocols
Network Topologies
LAN Cabling
Network Types
Network Storage
Communication Standards
Network Equipment
Repeaters
Hubs
Bridges
Switches
Mirrored Ports and Network Taps

VLANs	1
Routers	2
Gateways	3
Routing	3
WANs and Their Components	6
Packet Switching	6
Circuit Switching	7
Cloud Computing	1
Voice Communications and Wireless Communications	2
Voice over IP	3
Cell Phones	4
802.11 Wireless Networks and Standards	6
Network Access Control Devices	5
Firewalls	5
Demilitarized Zone	7
Firewall Design	9
Remote Access	9
Point-to-Point Protocol	0
Remote Authentication Dial-in User Service	2
Terminal Access Controller Access Control System	2
IPsec	2
Message Privacy and Multimedia Collaboration	4
Exam Prep Questions	6
Answers to Exam Prep Questions	0
Need to Know More?	1
CHAPTER 8:	
Identity and Access Management	3
Introduction	4
Identification, Authentication, and Authorization	_
of People and Devices	5
Authentication Techniques	6
Identity Management Implementation	1
Single Sign-On	2
Kerberos	3
Sesame	6
Authorization and Access Control Techniques	7
Discretionary Access Control	7
Mandatory Access Control	8

Role-Based Access Control	401
Other Types of Access Controls	402
Access Control Models	403
Centralized Access Control	403
Decentralized Access Control	407
Audit and Monitoring	408
Monitoring Access and Usage	408
Intrusion Detection Systems	409
Intrusion Prevention Systems.	414
Network Access Control	414
Keystroke Monitoring	415
Exam Prep Questions	417
Answers to Exam Prep Questions	421
Suggesting Reading and Resources	422
CHAPTER 9: Security Assessment and Testing	425
Introduction	426
Sequrity Assessments and Departmention Test Strategies	+20
Audite	420
Vulnerability Assessments	427
Papatration Testing	427
Test Techniques and Methods	1 20
Security Threats and Vulnerabilities	435
Threat Actors	435
Attack Methodologies	4 37
Network Security Threats and Attack Techniques	430
Session Hijacking	440
Sniffing	440
Wiretanning	441
DoS Attacks	442
Distributed Denial of Service	443
Botnets	443
Other Network Attack Techniques	446
Access Control Threats and Attack Techniques	448
Unauthorized Access	448
Access Aggregation	448
Password Attacks	449
Spoofing	453
I U	

Eavesdropping and Shoulder Surfing	453
Identity Theft	453
Social-based Threats and Attack Techniques.	454
Malicious Software Threats and Attack Techniques	456
Viruses	456
Worms	457
Logic Bombs	457
Backdoors and Trojans	458
Rootkits	461
Crimeware Kits	461
Advanced Persistent Threats	462
Ransomware	462
How Computer Crime Has Changed	464
Well-Known Computer Crimes and Criminals	465
Investigating Computer Crime	466
Computer Crime Jurisdiction.	467
Incident Response	467
Forensics	472
Standardization of Forensic Procedures	473
Computer Forensics	474
Investigations	479
Search, Seizure, and Surveillance	479
Interviews and Interrogations.	480
Honevpots and Honevnets	480
Evidence Types	481
Trial	482
The Evidence Life-Cvcle	483
Exam Prep Ouestions	484
Answers to Exam Prep Questions	487
Need to Know More?	488
CHAPTER 10:	404
Security Operations	491
Introduction	492
Foundational Security Operations Concepts.	492
Managing Users and Accounts	493
Privileged Entities	495
Controlling Access	495
Clipping Levels	496

Resource Protection
Due Care and Due Diligence
Asset Management
System Hardening 497
Change and Configuration Management
Trusted Recovery
Remote Access
Media Management, Retention, and Destruction
Telecommunication Controls
Cloud Computing 503
Email
Whitelisting, Blacklisting, and Graylisting
Fax
PBX
Anti-malware
Honeypots and Honeynets
Patch Management
System Resilience, Fault Tolerance, and Recovery Controls
Backups
Fault Tolerance
RAID
Recovery Controls
Monitoring and Auditing Controls
Auditing User Activity
Monitoring Application Transactions
Security Information and Event Management (SIEM)
Network Access Control
Keystroke Monitoring
Emanation Security
Controlling Physical Access
Intrusion Detection Systems
Network-Based Intrusion Detection Systems
Host-Based Intrusion-Detection Systems
Signature-Based, Anomaly-Based, and Rule-Based
IDS Engines
Intrusion Prevention Systems
Responding to Operational Security Incidents
Incident Response

	The Disaster Recovery Life Cycle
	Teams and Responsibilities
	Exam Prep Questions
	Answers to Exam Prep Questions
	Need to Know More?
СНА	PTER 11:
Softv	vare Development Security
	Introduction
	Software Development
	Avoiding System Failure
	The System Development Lifecycle
	Development Methods
	The Waterfall Model 554
	The Spiral Model
	Joint Application Development
	Rapid Application Development
	Incremental Development
	Prototyping
	Modified Prototype Model (MPM)
	Computer-Aided Software Engineering
	Agile Development Methods
	Capability Maturity Model
	Scheduling
	Change Management
	Programming Languages
	Object-Oriented Programming
	CORBA
	Database Management
	Database Terms
	Integrity
	Transaction Processing
	Artificial Intelligence and Expert Systems
	Security of the Software Environment
	Mobile Code
	Buffer Overflow
	Financial Attacks
	Change Detection

xvi CISSP Exam Cram

Viruses	5
Worms	7
Exam Prep Questions)
Answers to Exam Prep Questions	3
Need to Know More?	5
CHAPTER 12: Business Continuity Planning	7
Introduction	3
Threats to Business Operations	3
Business Continuity Planning (BCP))
Project Management and Initiation	Ĺ
Business Impact Analysis	3
Recovery Strategy)
Plan Design and Development	5
Implementation	3
Testing)
Monitoring and Maintenance	l
Exam Prep Questions	3
Answers to Exam Prep Questions	7
Need to Know More?)
Practice Exam I	ł
Answers to Practice Exam I	5
Practice Exam II	
Answers to Practice Exam II	5
Glossary	l
Index)

About the Author

As the CEO of Superior Solutions, Inc., a Houston-based IT security consulting and auditing firm, **Michael Gregg** has more than 20 years of experience in information security and risk management. He holds two associate's degrees, a bachelor's degree, and a master's degree. Some of the certifications he holds include CISSP, SSCP, MCSE, CTT+, A+, N+, Security+, CASP, CCNA, GSEC, CEH, CHFI, CEI, CISA, CISM, and CGEIT.

In addition to his experience with performing security audits and assessments, Gregg has authored or coauthored more than 20 books, including *Certified Ethical Hacker Exam Prep* (Que), *CISSP Exam Cram 2* (Que), and *Security Administrator Street Smarts* (Sybex). He has testified before U.S. Congress, his articles have been published on IT websites, and he has been sourced as an industry expert for CBS, ABC, CNN, Fox News and the New York Times. He has created more than 15 security-related courses and training classes for various companies and universities. Although audits and assessments are where he spends the bulk of his time, teaching and contributing to the written body of IT security knowledge are how Michael believes he can give something back to the community that has given him so much.

He is a board member for Habitat for Humanity and when not working, Michael enjoys traveling and restoring muscle cars.

About the Technical Reviewers

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

Michael Angelo During his tenure in security he was responsible for the secure development, implementation, and deployment of products. This included driving the creation of security solutions, policies and procedures, threat modeling and product analysis exercises, practical encryption techniques, biometric and token access authentication technology, common criteria certifications, and residual risk management scoring methodologies.

Amongst his accomplishments, Michael has 57 U.S. patents, was recognized by the City of Houston as the "2003 Inventor of the Year," and is a former Sigma-Xi distinguished lecturer. In 2011, he was named ISSA Security Professional of the Year and in 2013 was added to the ISSA Hall of Fame.

Dedication

I dedicate this book to my godson, Alexander Bucio. May his life be filled with success and happiness. Mucho gusto!

Acknowledgments

I would like to thank my wife, Christine, for understanding the long hours such a project entails. Also, thanks to Michelle Newcomb and the entire Pearson crew.

We Want to Hear from You!

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

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

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

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

Email: feedback@pearsonitcertification.com Mail: Pearson IT Certification ATTN: Reader Feedback 800 East 96th Street Indianapolis, IN 46240 USA

Reader Services

Register your copy of *CISSP Exam Cram* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789755537 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

This page intentionally left blank

Introduction

Welcome to *CISSP® Exam Cram!* This book covers the CISSP certification exam. Whether this is your first or your fifteenth *Exam Cram*, you'll find information here and in Chapter 1 that will ensure your success as you pursue knowledge, experience, and certification. This introduction explains the ISC² certification programs in general and talks about how the *Exam Cram* series can help you prepare for the CISSP exam.

This book is one of the *Exam Cram* series of books and will help by getting you on your way to becoming an ISC² Certified Information Systems Security Professional (CISSP).

This introduction discusses the basics of the CISSP exam. Included are sections covering preparation, how to take an exam, a description of this book's contents, how this book is organized, and, finally, author contact information.

Each chapter in this book contains practice questions. There are also two full-length practice exams at the end of the book. Practice exams in this book should provide an accurate assessment of the level of expertise you need to obtain to pass the test. Answers and explanations are included for all test questions. It is best to obtain a level of understanding equivalent to a consistent pass rate of at least 95% on the practice questions and exams in this book before you attempt the real exam.

Let's begin by looking at preparation for the exam.

How to Prepare for the Exam

Preparing for the CISSP exam requires that you obtain and study materials designed to provide comprehensive information about security. The following list of materials will help you study and prepare:

- ▶ The ISC² website at www.isc2.org
- ▶ The exam outline available at the ISC² website

Many people form study groups, attend seminars, and attend training classes to help them study for and master the material needed to pass the CISSP exam.

Practice Tests

You don't need to know much about practice tests, other than that they are a worthwhile expense for three reasons:

- ▶ They help you diagnose areas of weakness.
- ▶ They are useful for getting used to the format of questions.
- ▶ They help you to decide when you are ready to take the exam.

This book contains questions at the end of each chapter and includes two full-length practice tests. However, if you still want more, a related *Exam Cram CISSP Practice Questions* book has more than 500 additional questions. Many other companies provide CISSP certification practice tests, flash cards, and aids as well.

Taking a Certification Exam

When you have prepared for the exam, you must register with ISC^2 to take the exam. The CISSP exam is given at Pearson VUE testing centers. ISC^2 has implemented regional pricing: As an example, as of the publication of this book registration is \$599 in the United States. Check the Pearson VUE website at www.pearsonvue.com to get specific details.

After you register, you will receive a confirmation notice. Some locations may have limited test centers available, which means that you should schedule your exam in advance to make sure you can get the specific date and time you would like.

Arriving at the Exam Location

As with any examination, arrive at the testing center early. Be prepared! You will need to bring the confirmation letter and identification, such as a driver's license, green card, or passport. Any photo ID will suffice. Two forms of ID are usually required. The testing center staff requires proof that you are who you say you are and that someone else is not taking the test for you. Arrive early because if you are late, you will be barred from entry and will not receive a refund for the cost of the exam.

ExamAlert

You'll be spending a lot of time in the exam room. The total test time is six hours, so eat a good breakfast. Policies differ from location to location regarding bathroom breaks—check with the testing center before beginning the exam.

In the Testing Center

You will not be allowed to take study materials or anything else into the examination room with you that could raise suspicion that you're cheating. This includes practice test material, books, exam prep guides, or other test aids.

After the Exam

Examination results are available after the exam. If you pass the exam, you will simply receive a passing grade—your exact score will not be provided. Candidates who do not pass will receive a complete breakdown on their score by domain. This allows those individuals to see what areas they are weak in.

Retaking a Test

If you fail the exam, you must wait at least 30 days to take it again. Each of the ten domains will be shown, with your score in each. As an example, you may have received a 95% score in the Communications and Network Security domain and only 12% in Asset Security. Use this feedback to better understand what areas you were weak in and where to spend your time and effort in your studies. Additionally, invest in some practice tests if you have not already done so. There is much to be said for getting used to a testing format.

Tracking Your CISSP Status

When you pass the exam, you still need to attest to the CISSP code of ethics and have an existing CISSP complete an endorsement form for you.

When you pass the exam, you will next be required to complete an endorsement form. The endorsement form must be completed by someone who can attest to your professional experience and who is an active CISSP in good standing. If you don't know anyone who is CISSP-certified, ISC² allows endorsements from other professionals who are certified, licensed, or

commissioned, and an officer of the corporation where you are employed. You can review complete information on the endorsement form at the ISC^2 website.

About This Book

The ideal reader for an *Exam Cram* book is someone seeking certification. However, it should be noted that an *Exam Cram* book is an easily readable, rapid presentation of facts. Therefore, an *Exam Cram* book is also extremely useful as a quick reference manual.

Most people seeking certification use multiple sources of information. Check out the links at the end of each chapter to get more information about subjects you're weak in. Various security books from retailers also describe the topics in this book in much greater detail. Don't forget that many have described the CISSP exam as being a "mile wide."

This book includes other helpful elements in addition to the actual logical, step-by-step learning progression of the chapters themselves. *Exam Cram* books use elements such as exam alerts, tips, notes, and practice questions to make information easier to read and absorb.

Note

Reading this book from start to finish is not necessary; this book is set up so that you can quickly jump back and forth to find sections you need to study.

Use the *Cram Sheet* to remember last-minute facts immediately before the exam. Use the practice questions to test your knowledge. You can always brush up on specific topics in detail by referring to the table of contents and the index. Even after you achieve certification, you can use this book as a rapid-access reference manual.

The Chapter Elements

Each *Exam Cram* book has chapters that follow a predefined structure. This structure makes *Exam Cram* books easy to read and provides a familiar format for all *Exam Cram* books. The following elements typically are used:

- Opening hotlists
- Chapter topics

- ► Exam Alerts
- Notes
- Tips
- Sidebars
- Cautions
- Exam preparation practice questions and answers
- ▶ A "Need to Know More?" section at the end of each chapter

Note

Bulleted lists, numbered lists, tables, and graphics are also used where appropriate. A picture can paint a thousand words sometimes, and tables can help to associate different elements with each other visually.

Now let's look at each of the elements in detail.

- ▶ **Opening hotlists**—The start of every chapter contains a list of terms you should understand. A second hotlist identifies all the techniques and skills covered in the chapter.
- ▶ Chapter topics—Each chapter contains details of all subject matter listed in the table of contents for that particular chapter. The objective of an *Exam Cram* book is to cover all the important facts without giving too much detail; it is an exam cram. When examples are required, they are included.
- ► Exam Alerts—Exam Alerts address exam-specific, exam-related information. An Exam Alert addresses content that is particularly important, tricky, or likely to appear on the exam. An Exam Alert looks like this:

ExamAlert

Make sure you remember the different ways in which DES can be implemented and that ECB is considered the weakest form of DES.

▶ Notes—Notes typically contain useful information that is not directly related to the current topic under consideration. To avoid breaking up the flow of the text, they are set off from the regular text.

Note

Tip

This is a note. You have already seen several notes.

▶ Tips—Tips often provide shortcuts or better ways to do things.

A clipping level is the point at which you set a control to distinguish between activity that should be investigated and activity that should not be investigated.

► **Sidebars**—Sidebars are longer and run beside the text. They often describe real-world examples or situations.

How Caller ID Can Be Hacked

Sure, we all trust caller ID, but some Voice over IP (VoIP) providers allow users to inject their own call party number (CPN) into the call. Because VoIP is currently outside FCC regulation, these hacks are now possible.

► **Cautions**—Cautions apply directly to the use of the technology being discussed in the Exam Cram. For example, a Caution might point out that the CER is one of the most important items to examine when examining biometric devices.

Caution

The crossover error rate (CER) is the point at which Type 1 errors and Type 2 errors intersect. The lower the CER is, the more accurate the device is.

- Exam preparation practice questions—At the end of every chapter is a list of at least 10 exam practice questions similar to those in the actual exam. Each chapter contains a list of questions relevant to that chapter, including answers and explanations. Test your skills as you read.
- ▶ "Need to Know More?" section—This section at the end of each chapter describes other relevant sources of information. With respect to this chapter, the best place to look for CISSP certification information is at the ISC² website, www.ISC2.org.

Other Book Elements

Most of this *Exam Cram* book on CISSP follows the consistent chapter structure already described. However, there are various, important elements that are not part of the standard chapter format. These elements apply to the entire book as a whole.

- ▶ **Practice exams**—In addition to exam-preparation questions at the end of each chapter, two full practice exams are included at the end of the book.
- ► Answers and explanations for practice exams—These follow each practice exam, providing answers and explanations to the questions in the exams.
- ▶ **Glossary**—The glossary contains a listing of important terms used in this book with explanations.
- ► **Cram Sheet**—The Cram Sheet is a quick-reference, tear-out cardboard sheet of important facts useful for last-minute preparation. Cram Sheets often include a simple summary of facts that are most difficult to remember.
- ► Companion website—The companion website contains the Pearson IT Certification Practice Test engine, which provides multiple test modes that you can use for exam preparation. The practice tests are designed to appropriately balance the questions over each technical area (domain) covered by the exam. All concepts from the actual exam are covered thoroughly to ensure you're prepared for the exam.

Chapter Contents

The following list provides an overview of the chapters.

- Chapter 1, "The CISSP Certification Exam"—This chapter introduces exam strategies and considerations.
- Chapter 2, "Logical Asset Security"—This chapter discusses logical security and the countermeasures available for protecting an organization's resources. Key topics include CIA, data classification, and control of an organization's assets from creation to destruction.
- ► Chapter 3, "Physical Asset Security"—This chapter discusses physical security and the importance of providing physical protection for an organization's resources. Physical security plays a key role in securing an organization's assets. Without effective physical security, there can be no effective security structure at all.

- ► Chapter 4, "Security and Risk Management"—This chapter discusses asset management and the protection of critical resources. Quantitative and qualitative risk assessment are two major topics of this chapter. Readers must understand how these concepts are used to assess and measure risk while reducing threats to the organization. Key concepts include the development of policies, procedures, guidelines, and assorted controls.
- Chapter 5, "Security Engineering"—This chapter discusses key concepts such as computer hardware, operating system design, security models (Biba, Bell-LaPadula, Clark-Wilson, etc.) and documentation used to verify, certify, and accredit systems and networks.
- ► Chapter 6, "The Application and Use of Cryptography"—This chapter discusses the methods and systems used to encrypt and protect data. Symmetric, asymmetric, and hashing algorithms are introduced, along with PKI and cryptographic methods of attack.
- Chapter 7, "Communication and Network Security"—This chapter discusses telecommunication technology. Items such as the OSI model, TCP/IP, network equipment, LAN, MAN, and WAN protocols, and wireless technologies are just a few of the technologies discussed. This is an expansive domain and covers a lot of information for the CISSP candidate to master.
- ► Chapter 8, "Identity and Access Management"—This chapter covers the basics of access control. It addresses the three A's: authentication, authorization, and accountability. Items like identification, single sign-on, centralized authentication, and federation are discussed.
- ► Chapter 9, "Security Assessment and Testing"—This chapter discusses security assessments, ethical hacking, and vulnerability scanning. It also reviews common types of malware and various attack methodologies.
- ► Chapter 10, "Security Operations"—This chapter covers operation controls—that is, the types of controls that the organization can implement. Topics such as background checks, dual controls, mandatory vacations, rotation of duties, and auditing are introduced.
- ► Chapter 11, "Software Development Security"—This chapter discusses databases, the system development life cycle, and the importance of building security into applications and systems as early as possible during the development process. Project management is reviewed, as are malicious code, knowledge-based systems, and application issues.

- ▶ Chapter 12, "Business Continuity Planning"—This chapter covers all the aspects of the BCP process. Although some may discount the importance of this domain, storms, floods, hurricanes, earthquakes, and other natural disasters. should demonstrate the criticality of this domain. This chapter addresses key elements of disaster recovery. One important item is that no demonstrated recovery exists until the business continuity plan has been tested. Exam candidates must understand what is needed to prevent, minimize, and recover from disasters.
- ▶ **Practice Exam I**—This is a full-length practice exam.
- ► Answers to Practice Exam I—This element contains the answers and explanations for the first practice exam.
- **Practice Exam II**—This is a second full-length practice exam.
- ► Answers to Practice Exam II—This element contains the answers and explanations for the second practice exam.

Companion Website

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

To access this companion website, follow the steps below:

- **1.** Go to www.pearsonITcertification.com/register and log in or create a new account.
- 2. Enter the ISBN: 9780789757142.
- 3. Answer the challenge question as proof of purchase.
- **4.** Click on the "Access Bonus Content" link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

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

10 CISSP Exam Cram

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

Pearson IT Certification Practice Test Engine and Questions

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

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

Note

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

Install the Software

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

- ▶ Windows 10, Windows 8.1, or Windows 7
- ▶ Microsoft .NET Framework 4.5 Client
- ▶ Pentium class 1 GHz processor (or equivalent)
- ▶ 512 MB RAM

- ▶ 650 MB disc space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

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

The following steps outline the installation process:

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

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

Activate and Download the Practice Exam

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

- **Step 1:** Start the Pearson IT Certification Practice Test software from the Windows **Start** menu or from your desktop shortcut icon.
- Step 2: To activate and download the exam associated with this book, from the My Products or Tools tab, select the Activate button.
- **Step 3:** At the next screen, enter the activation code from the paper inside the cardboard holder in the back of the book. Once entered, click the **Activate** button.
- **Step 4:** The activation process will download the practice exam. Click **Next**, and then click **Finish**.

12 CISSP Exam Cram

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

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

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

Activating Other Exams

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

Contacting the Author

Hopefully, this book provides you with the tools you need to pass the CISSP exam. Feedback is appreciated. You can contact the author at mikeg@thesolutionfirm.com.

Thank you for selecting my book; I have worked to apply the same concepts in this book that I have used in the hundreds of training classes I have taught. Spend your study time wisely and you, too, can become a CISSP. Good luck on the exam!

Self-Assessment

This self-assessment section enables you to evaluate your readiness to take the CISSP certification exam. It should also help you understand what's required to obtain the CISSP certification. Are you ready?

CISSPs in the Real World

Security continues to be on everyone's mind. The CISSP certification continues to be one of the most sought-after security certifications. Increasing numbers of people are studying for and obtaining their CISSP certifications. Congratulations on making the decision to follow in their footsteps. If you are willing to tackle the process seriously and do what it takes to obtain the necessary experience and knowledge, you can pass the exam on the first try.

Tip

You can also assess your CISSP skill set by using the MeasureUp Certification Mode.

The Ideal CISSP Candidate

The CISSP is designed for individuals who are leading, planning, organizing, or controlling the security initiative of an organization. The ideal CISSP candidate is likely to have a 4-year college education and have at least 5–7 years' experience in one or more of the 8 CISSP domains. The most applicable degree is in computer science or perhaps a related field. A degree is not a prerequisite for taking the test. However, exam candidates must have a minimum of 5 years of direct full-time security work experience in 2 or more of the 8 domains. One year of experience can be substituted for a 4-year college degree or an approved certification such as CompTIA Security+ or CASP. The complete list of approved certifications can be found at www.isc2.org/credential_waiver/default.aspx

Don't be lulled into thinking that this is an easy test. Some words of caution might be in order:

- ▶ The CISSP exam requires the candidate to absorb a substantial amount of material. The test is 6 hours long and consists of 225 graded questions. This is longer than typical exams at Microsoft and most other IT vendors.
- The pass mark is set high, at 700 points. The individual questions are weighted, which means that harder questions are worth more than easier ones.
- ▶ Most of the individuals attempting the exam are familiar with one to three of the domains. This means that studying for the exam can be
overwhelming because there is so much material to cover. This book can help by guiding you to the areas in which you are weak or strong.

► To be eligible for the CISSP exam, students are required to have five years of experience, or four years of experience and a college degree.

Put Yourself to the Test

In this section, you answer some simple questions. The objective is for you to understand exactly how much work and effort you must invest to pass the CISSP certification exam. The simple answer to this question is this: The experience and education you have will dictate how difficult it will be for you to pass. Be honest in your answers or you will end up wasting around \$600 on an exam you were not ready to take. From the beginning, two things should be clear:

- ► Any educational background in computer science will be helpful, as will other IT certifications you have achieved.
- ▶ Hands-on actual experience is not only essential, but also required to obtain this certification.

Your Educational Background

▶ Do you have a computer science degree?

You'll have a good basic knowledge needed for three or more of the eight domains, assuming that you finished your degree and your schooling and have some fairly sophisticated computer skills. Subject areas such as application development, networking, and database design are a great help.

Did you attend some type of technical school or week-long CISSP course?

This question applies to low-level or short-term computer courses. Many of these courses are extremely basic or focused in one particular area. Although the CISSP exam is not platform-specific, training classes that focused on networking, security, hacking, or database design will help you pass the exam.

Have you developed any security policies, performed security audits, performed penetration tests, or developed response plans?

If yes, you will probably be able to handle about half of the CISSP exam domains.

Do you have a photographic memory?

If yes, you might have a slim chance of passing simply by reading this book, taking some practice exams, and using the Internet to brush up on the subjects you are weak in. However, the goal here is to gain a real understanding of the material. As a CISSP, you might be asked to lead, plan, organize, or control your organization's security operations; if that happens, you'll need a real understanding of how the various technologies and techniques work. Don't cheat yourself or gamble with your career.

Again, the education and requirements given here are by no means absolute. Still, an education can give you a very good grounding in any endeavor—the higher the level of education, the better.

Testing Your Exam Readiness

Whether you attend a training class, form a study group, or study on your own, preparing for the CISSP exam is essential. The exam will cost you about \$600, depending on where you are located, so you'll want to do everything you can to make sure you pass on the first try. Reading, studying, and taking practice exams are the best ways to increase your readiness. Practice exams help in two main ways:

- ▶ Practice exams highlight weak spots for further study.
- Practice exams give you a general perspective on the question format. Practicing the questions the way they are asked can help enormously on the actual testing day.

Two full-length practice exams are provided with this book. Que also publishes a second book, CISSP Practice Questions Exam, with more than 500 practice CISSP test questions; it is an excellent supplement to this book.

After the Exam

After you have passed the exam, you will need to gain continuing education credits each year to maintain your certification. Your certification will come up for renewal every 3 years, so you'll need to obtain 120 continuing education credits (CPE) or retake the exam. Retaking the exam is not a popular choice. These are some ways to gain CPEs to keep your certification current:

- ▶ Write a book.
- Read a book. (Only one per year can be used for credit.) This will give you a couple of credits, but not enough to keep your certification current.

- ▶ Do volunteer work that is approved by ISC². When you are certified, you can log on to the ISC² website for more information. A variety of volunteer work is available.
- Attend a training class. Just about any type of technology training class is accepted as long as it is tied to one of the domains.
- ▶ Teach a training class.
- ► Attend a college-level security class.

As you can see, the goal here is to help you stay current. As technology changes, we all must continue to learn to keep up the pace.

Now that we have covered some of the ways in which to assess your exam readiness, let's move on to Chapter 1, "The CISSP Certification Exam," where you will learn more about how the exam is structured and some effective test-taking strategies.

CHAPTER 2 Logical Asset Security

Terms you'll need to understand:

- Confidentiality
- Integrity
- Availability
- SANs
- Information lifecycle management
- Privacy impact assessment
- Data classification
- Data destruction
- Data remanence

Techniques you'll need to master:

- Proper methods for destruction of data
- Development of documents that can aid in compliance of all local, state, and federal laws
- The implementation of encryption and its use for the protection of data
- International concerns of data management

Introduction

Asset security addresses the controls needed to protect data throughout its lifecycle. From the point of creation to the end of its life, data protection controls must be implemented to ensure that information is adequately protected during each life cycle phase. This chapter starts by reviewing the basic security principles of confidentiality, integrity, and availability and moves on to data management and governance.

A CISSP must know the importance of data security and how to protect it while it is in transit, in storage, and at rest. A CISSP must understand that protection of data is much more important today than it was ten to fifteen years ago because data is no longer in just a paper form. Today, data can be found on local systems, RAID arrays, or even in the cloud. Regardless of where the data is stored it must have adequate protection and be properly disposed of at the end of its useful life.

Basic Security Principles

Confidentiality, integrity, and availability (CIA) define the basic building blocks of any good security program when defining the goals for network, asset, information, and/or information system security and are commonly referred to collectively as the CIA triad. Although the abbreviation CIA might not be as intriguing as the United States government's spy organization, it is a concept that security professionals must know and understand.

Confidentiality addresses the secrecy and privacy of information and preventing unauthorized persons from viewing sensitive information. There are a number of controls used in the real world to protect the confidentiality of information, such as locked doors, armed guards, and fences. Administrative controls that can enhance confidentiality include the use of information classification systems, such as requiring sensitive data be encrypted. For example, news reports have detailed several large-scale breaches in confidentiality as a result of corporations misplacing or losing laptops, data, and even backup media containing customer account, name, and credit information. The simple act of encrypting this data could have prevented or mitigated the damage. Sending information in an encrypted format denies attackers the opportunity to intercept and sniff clear text information. *Integrity* is the second leg in the security triad. Integrity provides accuracy of information, and offers users a higher degree of confidence that the information they are viewing has not been tampered with. Integrity must be protected while in storage, at rest, and in transit. Information in storage can be protected by using access controls and audit controls. Cryptography can enhance this protection through the use of hashing algorithms. Real-life examples of this technology can be seen in programs such as Tripwire, and MD5Sum. Likewise, integrity in transit can be ensured primarily by the use of transport protocols, such as PKI, hashing, and digital signatures.

The concept of *availability* requires that information and systems be available when needed. Although many people think of availability only in electronic terms, availability also applies to physical access. If, at 2 a.m., you need access to backup media stored in a facility that allows access only from 8 a.m. to 5 p.m., you definitely have an availability problem. Availability in the world of electronics can manifest itself in many ways. Access to a backup facility 24×7 does little good if there are no updated backups to restore from.

Backups are the simplest way to ensure availability. Backups provide a copy of critical information, should data be destroyed or equipment fail. Failover equipment is another way to ensure availability. Systems such as redundant arrays of independent disks (RAID) and redundant sites (hot, cold, and warm) are two other examples. Disaster recovery is tied closely to availability because it's all about getting critical systems up and running quickly.

Which link in the security triad is considered most important? That depends. In different organizations with different priorities, one link might take the lead over the other two. For example, your local bank might consider integrity the most important; however, an organization responsible for data processing might see availability as the primary concern, whereas an organization such as the NSA might value confidentiality the most. Finally, you should be comfortable seeing the triad in any form. Even though this book refers to it as CIA, others might refer to it as AIC, or as CAIN (where the "N" stands for *nonrepudiation*).

Security management does not stop at CIA. These are but three of the core techniques that apply to asset security. True security requires defense-in-depth. In reality, many techniques are required to protect the assets of an organization; take a moment to look over Figure 2.1.



FIGURE 2.1 Asset protection triad.

Data Management: Determine and Maintain Ownership

Data management is not easy and has only become more complex over the last ten to fifteen years. Years ago, people only had to be concerned with paper documents and control might have only meant locking a file cabinet. Today, electronic data might be found on thumb drives, SAN storage arrays, laptop hard drives, mobile devices, or might even be stored in a public cloud.

Data Governance Policy

Generally you can think of policies as high-level documents developed by management to transmit the guiding strategy and philosophy of management to employees. A data governance policy is a documented set of specifications for the guarantee of approved management and control of an organization's digital assets and information. Data governance programs generally address the following types of data:

- Sets of master data
- ▶ Metadata

- Sensitive data
- Acquired data

Such specifications can involve directives for business process management (BPM) and enterprise risk planning (ERP), as well as security, data quality, and privacy. The goal of data governance is:

- ▶ To establish appropriate responsibility for the management of data
- ▶ To improve ease of access to data
- ► To ensure that once data are located, users have enough information about the data to interpret them correctly and consistently
- ► To improve the security of data, including confidentiality, integrity, and availability

Issues to consider include:

- Cost—This can include the cost of providing access to the data as well as the cost to protect it.
- ▶ Ownership—This includes concerns as to who owns the data or who might be a custodian. As an example, you may be the custodian of fifty copies of Microsoft Windows Server 2012 yet the code is owned by Microsoft. This is why users pay for a software license and not the ownership of the software itself, and typically have only the compiled ".exe" file and not the source code itself.
- ► Liability—This refers to the financial and legal costs an organization would bear should data be lost, stolen, or hacked.
- ► Sensitivity—This includes issues related to the sensitivity of data that should be protected against unwarranted disclosure. As an example, social security numbers, data of birth, medical history, etc.
- ▶ Ensuring Law/Legal Compliance—This includes items related to legal compliance. As examples, you must retain tax records for a minimum number of years, while you may only retain customers' for only the time it takes to process a single transaction.
- ▶ **Process**—This includes methods and tools used to transmit or modify the data.

Roles and Responsibility

Data security requires responsibility. There must be a clear division of roles and responsibility. This will be a tremendous help when dealing with any security issues. Everyone should be subject to the organization's security policy, including employees, management, consultants, and vendors. The following list describes some general areas of responsibility. Specific roles have unique requirements. Some key players and their responsibilities are as follows:

- ▶ Data Owner—Because senior management is ultimately responsible for data and can be held liable if it is compromised, the data owner is usually a member of senior management, or head of that department. The data owner is responsible for setting the data's security classification. The data owner can delegate some day-to-day responsibility.
- ▶ Data Custodian—Usually a member of the IT department. The data custodian does not decide what controls are needed, but does implement controls on behalf of the data owner. Other responsibilities include the day-to-day management of data, controlling access, adding and removing privileges for individual users, and ensuring that the proper controls have been implemented.
- ► IS Security Steering Committee—These are individuals from various levels of management that represent the various departments of the organization. They meet to discuss and make recommendations on security issues.
- ► Senior Management—These individuals are ultimately responsible for the security practices of the organization. Senior management might delegate day-to-day responsibility to another party or someone else, but cannot delegate overall responsibility for the security of the organization's data.
- ► Security Advisory Group—These individuals are responsible for reviewing security issues with the chief security officer and they are also responsible for reviewing security plans and procedures.
- Chief Security Officer—The individual responsible for the day-to-day security of the organization and its critical assets.
- ▶ **Users**—This is a role that most of us are familiar with because this is the end user in an organization. Users do have responsibilities; they must comply with the requirements laid out in policies and procedures.
- ▶ **Developers**—These individuals develop code and applications for the organization. They are responsible for implementing the proper security controls within the programs they develop.

33

► Auditor—This individual is responsible for examining the organization's security procedures and mechanisms. The auditor's job is to provide an independent objective as to the effectiveness of the organization's security controls. How often this process is performed depends on the industry and its related regulations. As an example, the health care industry in the United States is governed by the Health Insurance Portability and Accountability Act (HIPAA) regulations and requires yearly reviews.

ExamAlert

The CISSP candidate might be tested on the concept that data access does not extend indefinitely. It is not uncommon for an employee to gain more and more access over time while moving to different positions within a company. Such poor management can endanger an organization. When employees are terminated, data access should be withdrawn. If unfriendly termination is known in advance, access should be terminated as soon as possible to reduce the threat of potential damage.

Data Ownership

All data objects within an organization must have an owner. Objects without a data owner will be left unprotected. The process of assigning a data owner and set of controls to information is known as information lifecycle management (ILM). ILM is the science of creating and using policies for effective information management. ILM includes every phase of a data object from its creation to its end. This applies to any and all information assets.

ILM is focused on fixed content or static data. While data may not stay in a fixed format throughout its lifecycle there will be times when it is static. As an example consider this book; after it has been published it will stay in a fixed format until the next version is released.

For the purposes of business records, there are five phases identified as being part of the lifecycle process. These include the following:

- Creation and Receipt
- Distribution
- ► Use
- ► Maintenance
- Disposition

Data owners typically have legal rights over the data. The data owner typically is responsible for understanding the intellectual property rights and copyright of their data. Intellectual property is agreed on and enforced worldwide by various organizations, including the United Nations Commission on International Trade Law (UNCITRAL), the European Union (EU), and the World Trade Organization (WTO). International property laws protect trade secrets, trademarks, patents, and copyrights:

- ▶ **Trade secret**—A *trade secret* is a confidential design, practice, or method that must be proprietary or business related. For a trade secret to remain valid, the owner must take precautions to ensure the data remains secure. Examples include encryption, document marking, and physical security.
- ▶ **Trademark**—A *trademark* is a symbol, word, name, sound, or thing that identifies the origin of a product or service in a particular trade. The ISC² logo is an example of a trademarked logo. The term *service mark* is sometimes used to distinguish a trademark that applies to a service rather than to a product.
- ▶ **Patent**—A *patent* documents a process or synthesis and grants the owner a legally enforceable right to exclude others from practicing or using the invention's design for a defined period of time.
- ► **Copyright**—A *copyright* is a legal device that provides the creator of a work of authorship the right to control how the work is used and protects that person's expression on a specific subject. This includes the reproduction rights, distribution rights, music, right to create, and right to public display.

Data Custodians

Data custodians are responsible for the safe custody, transport, and storage of data and the implementation of business rules. This can include the practice of due care and the implementation of good practices to protect intellectual assets such as patents or trade secrets. Some common responsibilities for a data custodian include the following:

- ▶ Data owner identification—A data owner must be identified and known for each data set and be formally appointed. Too many times data owners do not know that they are data owners and do not understand the role and its responsibilities. In many organizations the data custodian or IT department by default assumes the role of data owner.
- ▶ Data controls—Access to data is authorized and managed. Adequate controls must be in place to protect the confidentiality, integrity, and

availability of the data. This includes administrative, technical, and physical controls.

- Change control—A change control process must be implemented so that change and access can be audited.
- End-of-life provisions or disposal—Controls must be in place so that when data is no longer needed or is not accurate it can be destroyed in an approved method.

Data Documentation and Organization

Data that is organized and structured can help ensure that that it is better understood and interpreted by users. Data documentation should detail how data was created, what the context is for the data, the format of the data and its contents, and any changes that have occurred to the data. It's important to document the following:

- Data context
- Methodology of data collection
- Data structure and organization
- ▶ Validity of data and quality assurance controls
- Data manipulations through data analysis from raw data
- ▶ Data confidentiality, access, and integrity controls

Data Warehousing

A *data warehouse* is a database that contains data from many other databases. This allows for trend analysis and marketing decisions through data analytics (discussed below). Data warehousing is used to enable a strategic view. Because of the amount of data stored in one location, data warehouses are tempting targets for attackers who can comb through and discover sensitive information.

Data Mining

Data mining is the process of analyzing data to find and understand patterns and relationships about the data (see Figure 2.2). There are many things that must be in place for data mining to occur. These include multiple data sources, access, and warehousing. Data becomes information, information becomes knowledge, and knowledge becomes intelligence through a process called data analytics, which is simply examination of the data. *Metadata* is best described

36 CHAPTER 2: Logical Asset Security

as being "data about data". As an example, the number 212 has no meaning by itself. But, when qualifications are added, such as to state the field is an area code, it is then understood the information represents an area code on Manhattan Island. Organizations treasure data and the relationships that can be deduced between individual elements. The relationships discovered can help companies understand their competitors and the usage patterns of their customers, and can result in targeted marketing. As an example, it might not be obvious why the diapers are at the back of the store by the beer case until you learn from data mining that after 10 p.m., more men than women buy diapers, and that they tend to buy beer at the same time.



FIGURE 2.2 Data mining.

Knowledge Management

Knowledge management seeks to make intelligent use of all the data in an organization by applying wisdom to it. This is called turning data into intelligence through analytics. This skill attempts to tie together databases, document management, business processes, and information systems. The result is a huge store of data that can be mined to extract knowledge using artificial intelligence techniques. These are the three main approaches to knowledge extraction:

Classification approach—Used to discover patterns; can be used to reduce large databases to only a few individual records or data marts. Think of data marts as small slices of data from the data warehouse.

- Probabilistic approach—Used to permit statistical analysis, often in planning and control systems or in applications that involve uncertainty.
- ► Statistical approach—A number-crunching approach; rules are constructed that identify generalized patterns in the data.

Data Standards

Data standards provide consistent meaning to data shared among different information systems, programs, and departments throughout the product's life cycle. Data standards are part of any good enterprise architecture. The use of data standards makes data much easier to use. As an example, say you get a new 850-lumen flashlight that uses two AA batteries. You don't need to worry about what brand of battery you buy as all AA batteries are manufactured to the same size and voltage.

Tip

If you would like to see an example of a data standard check out Texas Education Agency. It requires all Texas school districts to submit data to the PEIMS data standard. Learn more at: tea.texas.gov/Reports_and_Data/Data_Submission/PEIMS/ PEIMS_Data_Standards/PEIMS_Data_Standards/

Data Lifecycle Control

Data lifecycle control is a policy-based approach to managing the flow of an information system's data throughout its life cycle from the point of creation to the point at which it is out of date and is destroyed or archived.

Data Audit

After all the previous tasks discussed in this chapter have been performed, the organization's security-management practices will need to be evaluated periodically. This is accomplished by means of an *audit process*. The audit process can be used to verify that each individual's responsibility is clearly defined. Employees should know their accountability and their assigned duties. Most audits follow a code or set of documentation. As an example, financial audits can be performed using Committee of Sponsoring Organizations of the Treadway Commission (COSO). IT audits typically follow the Information Systems Audit and Control Association (ISACA) Control Objectives for Information and related Technology (COBIT) framework. COBIT is designed around four domains:

- Plan and organize
- Acquire and implement
- Deliver and support
- Monitor and evaluate

Although the CISSP exam will not expect you to understand the inner workings of COBIT, you should understand that it is a framework to help provide governance and assurance. COBIT was designed for performance management and IT management. It is considered a system of best practices. COBIT was created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992.

Although auditors can use COBIT, it is also useful for IT users and managers designing controls and optimizing processes. It is designed around 34 key controls that address:

- Performance concerns
- ► IT control profiling
- ► Awareness
- Benchmarking

Audits are the only way to verify that the controls put in place are working, that the policies that were written are being followed, and that the training provided to the employees actually works. To learn more about COBIT, check out www.isaca.org/cobit/. Another set of documents that can be used to benchmark the infrastructure is the family of ISO 27000 standards.

Data Storage and Archiving

Organizations have a never-ending need for increased storage. My first 10-megabyte thumb drive is rather puny by today's standards. Data storage can include:

- ► Network attached storage (NAS)
- ► Storage area network (SAN)
- Cloud

Organizations should fully define their security requirements for data storage before a technology is deployed. For example, NAS devices are small, easy to use, and can be implemented quickly, but physical security is a real concern, as is implementing strong controls over the data. A SAN can be implemented with much greater security than a NAS. Cloud-based storage offers yet another option but also presents concerns such as:

- ▶ Is it a private or public cloud?
- Does it use physical or virtual servers?
- ▶ How are the servers provisioned and decommissioned?
- ▶ Is the data encrypted and if so what kind of encryption is used?
- ▶ Where is the data actually stored?
- ▶ How is the data transferred (data flow)?
- ▶ Where are the encryption keys kept?
- ► Are there co-tenants?

Keep in mind that storage integration also includes securing virtual environments, services, applications, appliances, and equipment that provide storage.

SAN

The Storage Network Industry Association (SNIA) defines a SAN as "a data storage system consisting of various storage elements, storage devices, computer systems, and/or appliances, plus all the control software, all communicating in efficient harmony over a network." A SAN appears to the client OS as a local disk or volume that is available to be formatted and used locally as needed.

- ▶ Virtual SAN—A virtual SAN (VSAN) is a SAN that offers isolation among devices that are physically connected to the same SAN fabric. A VSAN is sometimes called fabric virtualization. VSANs were developed to support independent virtual fabrics on a single switch. VSANs improve consolidation and simplify management by allowing for more efficient SAN utilization. A VSAN will allow a resource on any individual VSAN to be shared by other users on a different VSAN without merging the SAN fabrics.
- ► Internet Small Computer System Interface (iSCSI)—iSCSI is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. Many see it as a replacement for

fiber channel, because it does not require any special infrastructure and can run over existing IP LAN, MAN, or WAN networks.

- ▶ Fiber Channel over Ethernet (FCoE)—FCoE is another transport protocol that is similar to iSCSI. FCoE can operate at speeds of 10 GB per second and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is non-routable. iSCSI is, by contrast, routable because it operates higher up the stack, on top of the TCP and UDP protocols.
- ▶ Host Bus Adapter (HBA) Allocation—The host bus adapter is used to connect a host system to an enterprise storage device. HBAs can be allocated by either soft zoning or by persistent binding. Soft zoning is more permissive, whereas persistent binding decreases address space and increases network complexity.
- ▶ LUN Masking—LUN masking is implemented primarily at the HBA level. It is a number system that makes LUN numbers available to some but not to others. LUN masking implemented at this level is vulnerable to any attack that compromises the local adapter.
- ▶ **Redundancy (Location)**—Location redundancy is the idea that content should be accessible from more than one location. An extra measure of redundancy can be provided by means of a replication service so that data is available even if the main storage backup system fails.
- Secure Storage Management and Replication—Secure storage management and replication systems are designed to allow an organization to manage and handle all its data in a secure manner with a focus on the confidentiality, integrity, and availability of the data. The replication service allows the data to be duplicated in real time so that additional fault tolerance is achieved.
- ▶ Multipath Solutions—Enterprise storage multipath solutions reduce the risk of data loss or lack of availability by setting up multiple routes between a server and its drives. The multipath software maintains a listing of all requests, passes them through the best possible path, and reroutes communication if a path fails.
- ► SAN Snapshots—SAN snapshot software is typically sold with SAN solutions and offers a way to bypass typical backup operations. The snapshot software has the ability to temporarily stop writing to physical disk and then make a point-in-time backup copy. Snapshot software is typically fast and makes a copy quickly, regardless of the drive size.

41

Data De-Duplication (DDP)—Data de-duplication is the process of removing redundant data to improve enterprise storage utilization. Redundant data is not copied. It is replaced with a pointer to the one unique copy of the data. Only one instance of redundant data is retained on the enterprise storage media, such as disk or tape.

Data Security, Protection, Sharing, and Dissemination

Data security is the protection of data from unauthorized activity by authorized users and from access by unauthorized users. Although laws differ depending on which country an organization is operating in, organizations must make the protection of personal information in particular a priority. To understand the level of importance, consider that according to the Privacy Rights Clearing-house (www.privacyrights.org), the total number of records containing sensitive personal information accumulated from security breaches in the United States between January 2005 and December 2015 is 895,531,860.

From a global standpoint the international standard ISO/IEC 17799 covers data security. ISO 17799 makes clear the fact that all data should have a data owner and data custodian so that it is clear whose responsibility it is to secure and protect access to that data.

An example of a proprietary international information security standard is the Payment Card Industry Data Security Standard. PCI-DSS sets standards for any entity that handles cardholder information for credit cards, prepaid cards, and POS cards. PCI DSS version is comprised of six control objectives that contain one or more requirements:

1. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2. Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

3. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

4. Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

5. Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

6. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Privacy Impact Assessment

Another approach for organizations seeking to improve their protection of personal information is to develop an organization-wide policy based on a *privacy impact analysis* (PIA). A PIA should determine the risks and effects of collecting, maintaining, and distributing personal information in electronic-based systems. The PIA should be used to evaluate privacy risks and ensure that appropriate privacy controls exist. Existing data controls should be examined to verify that accountability is present and that compliance is built-in every time new projects or processes are planned to come online. The PIA must include a review of the following items as they adversely affect the CIA of privacy records:

- **Technology**—Any time new systems are added or modifications are made, reviews are needed.
- ▶ **Processes**—Business processes change, and even though a company might have a good change policy, the change management system might be overlooking personal information privacy.
- ▶ **People**—Companies change employees and others with whom they do business. Any time business partners, vendors, or service providers change, the impact of the change on privacy needs to be reexamined.

43

Privacy controls tend to be overlooked for the same reason many security controls are. Management might have a preconceived idea that security controls will reduce the efficiency or speed of business processes. To overcome these types of barriers, senior management must make a strong commitment to protection of personal information and demonstrate its support. Risk-assessment activities aid in the process by informing stakeholders of the actual costs for the loss of personal information of clients and customers. These costs can include fines, lawsuits, lost customers, reputation, and the company going out of business.

Information Handling Requirements

Organizations handle large amounts of information and should have policies and procedures in place that detail how information is to be stored. Think of policies as high level documents, whereas procedures offer step-by-step instructions. Many organizations are within industries that fall under regulatory standards that detail how and how long information must be retained.

One key concern with storage is to ensure that media is appropriately labeled. Media should be labeled so that the data librarian or individual in charge of media management can identify the media owner, when the content was created, the classification level, and when the content is to be destroyed. Figure 2.3 shows an example of appropriate media labeling.

> Date: Oct 31, 2016 Author: Christine Gregg Classification: Top Secret Retention Period: 3 Years Title and Description: Project X



FIGURE 2.3 Data labeling.

Data Retention and Destruction

All data has a lifetime. Eventually it should either be purged, released, or unclassified. As an example, consider the JFK Records Act. The JFK Records Act was put in place to eventually declassify all records dealing with the assassination of President John F. Kennedy. The JFK Records Act states that all assassination records must finally be made public by 2017. This is an example of declassification, but sometimes data in an organization will never be released and will need to be destroyed.

If the media is held on hard drives, magnetic media, or thumb drives, it must be sanitized. *Sanitization* is the process of clearing all identified content, such that no data remnants can be recovered. Some of the methods used for sanitization are as follows:

- ▶ **Drive wiping**—This is the act of overwriting all information on the drive. As an example, DoD.5200.28-STD (7) specifies overwriting the drive with a special digital pattern through seven passes. Drive wiping allows the drive to be reused.
- ▶ **Zeroization**—This process is usually associated with cryptographic processes. The term was originally used with mechanical cryptographic devices. These devices would be reset to 0 to prevent anyone from recovering the key. In the electronic realm, *zeroization* involves overwriting the data with zeros. Zeroization is defined as a standard in ANSI X9.17.
- ▶ **Degaussing**—This process is used to permanently destroy the contents of a hard drive or magnetic media. Degaussing works by means of a powerful magnet whose field strength penetrates the media and reverses the polarity of the magnetic particles on the tape or hard disk. After media has been degaussed, it cannot be reused. The only method more secure than degaussing is physical destruction.

Data Disposal is a Big Problem

While hard drive size and performance has continued to grow at a rapid pace most hard drive and thumb drives are still shipped without encryption enabled. What this means is that you can take a hard drive from a computer you bought at an auction that will not boot up, plug the drive into another computer, and possibly have access to the data on the drive. While many of us have used a shredder, few have probably ever sanitized a hard drive. Whether your organization is planning to sell old hard drives, give them to charity, or just throw them away, you need to make sure the data on the drive is impossible to recover.

45

If you are thinking that most organizations already do this, consider the following. Two researchers from MIT bought 158 used hard drives from eBay. Out of the 158 hard drives, 129 had data that the researchers were able to copy. Some of the data on these drives included personal information, company HR records, medical information, a pharmacies database, and another database with 3,700 credit card numbers.

Physical media should be protected with a level of control equal to electronic media. These issues are covered in much greater detail in Chapter 3, "Physical Asset Security."

With the discussion of controls concluded, the next section focuses on auditing and monitoring. It is time to review some of the ways organizations can maintain accountability.

Note

Unless you're a 1960s car enthusiast like I am, it might have been a while since you have seen a working 8-track player. The point is that technology changes and the requirement to be able to read and access old media is something to consider. Be it 8-tracks, laser discs, Zip drives, or floppy disks, stored media must be readable to be useful.

Data Remanence and Decommissioning

Object reuse is important because of the remaining information that may reside on a hard disk or any other type of media. Even when data has been sanitized there may be some remaining information. This is known as data remanence. Data remanence is the residual data that remains after data has been erased. Most objects that may be reused will have some remaining amount of information left on media after it has been erased. If the media is not going to be destroyed outright, best practice is to overwrite it with a minimum of seven passes of random ones and zeros.

When information is deemed too sensitive assets such as hard drive, media, and other storage devices may not be reused and the decision may be made for asset disposal. Asset disposal must be handled in an approved manner and part of the system development life cycle. As an example, media that has been used to store sensitive or secret information should be physically destroyed. Before systems or data are decommissioned or disposed of, you must understand any existing legal requirements pertaining to records retention. When archiving information, you must consider the method for retrieving the information.

Classifying Information and Supporting Assets

Organizational information that is proprietary or confidential in nature must be protected. Data classification is a useful way to rank an organization's informational assets. A well-planned data classification system makes it easy to store and access data. It also makes it easier for users of data to understand its importance. As an example, if an organization has a clean desk policy and mandates that company documents, memos, and electronic media not be left on desks, it can change people's attitudes about the value of that information. However, whatever data classification system is used, it should be simple enough that all employees can understand it and execute it properly. Two common data classification plans are discussed next.

Data Classification

The two most common data-classification schemes are military and public. Organizations store and process so much electronic information about their customers and employees that it's critical for them to take appropriate precautions to protect this information. The responsibility for the classification of data lies with the data owner. Both military and private data classification systems accomplish this task by placing information into categories and applying labels to data and clearances to people that access the data.

The first step of this process is to assess the value of the information. When the value is known, it becomes much easier to decide the amount of resources that should be used to protect the data. It would make no sense to spend more on protecting something with a lesser value. By using this system, not all data is treated equally; data that requires more protection gets it, and funds are not wasted protecting data that does not need it.

Each level of classification established should have specific requirements and procedures. The military and commercial data-classification models have predefined labels and levels. When an organization decides which model to use, it can evaluate data placement by using criteria such as the following:

- Data value
- Data age
- Laws pertaining to data

- ▶ Regulations pertaining to disclosure
- Replacement cost

Regardless of which model is used, the following questions will help determine the proper placement of the information:

- ▶ Who owns the asset or data?
- ▶ Who controls access rights and privileges?
- ▶ Who approves access rights and privileges?
- ▶ What level of access is granted to the asset or data?
- ▶ Who currently has access to the asset or data?

Classification of data requires several steps:

- **1.** Identify the data custodian.
- 2. Determine the criteria used for data classification.
- **3.** Task the owner with classifying and labeling the information.
- 4. Identify any exceptions to the data classification policy.
- **5.** Determine security controls to be applied to protect each category of information.
- **6.** Specify sunset policy or end of life policy and detail in a step-by-step manner how data will be reclassified or declassified. Reviews specifying rentention and end of life should occur at specific periods of time.
- 7. Develop awareness program.

Military Data Classification

The military data-classification system is mandatory within the U.S. Department of Defense. This system has five levels of classification:

- **Top Secret**—Grave damage if exposed.
- ► Secret—Serious damage if exposed.
- ▶ **Confidential**—Disclosure could cause damage.
- Sensitive but Unclassified or Restricted—Disclosure should be avoided.
- ▶ Unclassified or Official—If released, no damage should result.

Each classification represents a level of sensitivity. *Sensitivity* is the desired degree of secrecy that the information should maintain. If you hold a confidential clearance, it means that you could access unclassified, sensitive, or confidential information for which you have a need to know. Your need to know would not extend to the secret or top secret levels. The concept of need-to-know is similar to the principle of least privilege in that employees should have access only to information that they need to know to complete their assigned duties.

Public/Private Data Classification

The public or commercial data classification is also built on a four-level model:

- **Confidential**—This is the highest level of sensitivity and disclosure could cause extreme damage to the organization.
- ▶ **Private**—This information is for organization use only and its disclosure would damage the organization.
- Sensitive—This information requires a greater level of protection to prevent loss of confidentiality.
- ▶ **Public**—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.

Table 2.1 provides details about the military and public/private data-classification models.

Commercial Business Classifications	Military Classifications
Confidential	Top secret
Private	Secret
Sensitive	Confidential
Public	Sensitive (BU)
	Unclassified

TABLE 2.1 Commercial and Military Data Classifications

Caution

Information has a useful life. Data classification systems need to build in mechanisms to monitor whether information has become obsolete. Obsolete information should be declassified or destroyed.

Asset Management and Governance

The job of asset management and governance is to align the goals of IT to the business functions of the organization, to track assets throughout their lifecycle, and to protect the assets of the organization. Asset management can be defined as any system that inventories, monitors, and maintains items of value. Assets can be both tangible and intangible. Assets can include the following:

- ▶ Hardware
- Software
- Employees
- Services
- Reputation
- Documentation

You can think of asset management as a structured approach of deploying, operating, maintaining, upgrading, and disposing of assets cost-effectively. Asset management is required for proper risk assessment. Before you can start to place a value on an asset you must know what it is and what it is worth. Its value can be assessed either quantitatively or qualitative. A quantitative approach requires:

- 1. Estimation of potential losses and determination of single loss expectancy (SLE)
- **2.** Completion of a threat frequency analysis and calculation of the annual rate of occurrence (ARO)
- 3. Determination of the annual loss expectancy (ALE)

A qualitative approach does not place a dollar value on the asset and ranks it as high, medium, or low concern. The downside of performing qualitative evaluations is that you are not working with dollar values, so it is sometimes harder to communicate the results of the assessment to management.

One key asset is software. CISSP candidates should understand common issues related to software licensing. Because software vendors usually license their software rather than sell it, and license it for a number of users on a number of systems, software licenses must be accounted for by the purchasing organization. If users or systems exceed the licensed number, the organization can be held legally liable. As we move into an age where software is being delivered over the Internet and not with media (CD), software asset management is an important concern.

Software Licensing

Intellectual property rights issues have always been hard to enforce. Just consider the uproar that Napster caused years ago as the courts tried to work out issues of intellectual property and the rights of individuals to share music and files. The software industry has long dealt with this same issue. From the early days of computing, some individuals have been swapping, sharing, and illegally copying computer software. The unauthorized copying and sharing of software is considered software piracy, which is illegal. Many don't think that the copy of that computer game you gave a friend is hurting anyone. But software piracy is big business, and accumulated loss to the property's owners is staggering. According to a 2008 report on intellectual property to the United States Congress, in just one raid in June 2007, the FBI recovered more than two billion dollars worth of illegal Microsoft and Symantec software. Internationally, losses from illegal software are estimated to be in excess of \$200 billion.

Microsoft and other companies are actively fighting to protect their property rights. Some organizations have formed the Software Protection Association, which is one of the primary bodies that work to enforce licensing agreements. The Business Software Alliance (BSA) and the Federation Against Software Theft are international groups targeting software piracy. These associations target organizations of all sizes from small, two-person companies to large multinationals.

Software companies are making clear in their licenses what a user can and cannot do with their software. As an example, Microsoft Windows XP allowed multiple transfers of licenses whereas Windows 8 and 10 have different transfer rules. As an example, Windows 8 allows only one transfer. The user license states, "The first user of the software may reassign the license to another device one time." Some vendors even place limits on virtualization. License agreements can actually be distributed in several different ways, including the following:

- ▶ **Click-wrap license agreements**—Found in many software products, these agreements require you to click through and agree to terms to install the software product. These are often called *contracts of adhesion*; they are "take it or leave it" propositions.
- ► Master license agreements—Used by large companies that develop specific software solutions that specify how the customer can use the product.

Shrink-wrap license agreements—Created when software started to be sold commercially and named for the fact that breaking the shrink wrap signifies your acceptance of the license.

Even with licensing and increased policing activities by organizations such as the BSA, improved technologies make it increasingly easy to pirate software, music, books, and other types of intellectual property. These factors and the need to comply with two World Trade Organization (WTO) treaties led to the passage of the 1998 Digital Millennium Copyright Act (DMCA). Here are some salient highlights:

- ► The DMCA makes it a crime to bypass or circumvent antipiracy measures built into commercial software products.
- ► The DMCA outlaws the manufacture, sale, or distribution of any equipment or device that can be used for code-cracking or illegally copying software.
- ▶ The DMCA provides exemptions from anti-circumvention provisions for libraries and educational institutions under certain circumstances; however, for those not covered by such exceptions, the act provides penalties up to \$1,000,000 and 10 years in prison.
- ► The DMCA provides Internet service providers exceptions from copyright infringement liability enabling transmission of information across the Internet.

Equipment Lifecycle

The equipment lifecycle begins at the time equipment is requested to the end of its useful life or when it is discarded. The equipment lifecycle typically consist of four phases:

- Defining requirements
- Acquisition and implementation
- Operation and maintenance
- ▶ Disposal and decommission

While some may think that much of the work is done once equipment has been acquired, that is far from the truth. There will need to be some established support functions. Routine maintenance is one important item. Without routine maintenance equipment will fail, and those costs can be calculated. Items to consider include:

- Lost productivity
- Delayed or canceled orders
- Cost of repair
- Cost of rental equipment
- Cost of emergency services
- Cost to replace equipment or reload data
- Cost to pay personnel to maintain the equipment

Technical support is another consideration. The longer a piece of equipment has been in use the more issues it may have. As an example, if you did a search for exploits for Windows 7 or Windows 10 which do you think would return more results? Most likely Windows 7. This all points to the need for more support the longer the resource has been in use.

Determine Data Security Controls

Any discussion on logical asset security must at some point discuss encryption. While there is certainly more to protecting data than just encrypting it, encryption is one of the primary controls used to protect data. Just consider all the cases of lost hard drives, laptops, and thumb drives that have made the news because they contained data that was not encrypted. In many cases encryption is not just a good idea; it is also mandated by law. CISSP candidates must ensure that corporate policies addressing where and how encryption will be used are well defined and being followed by all employees.

Let's examine the two areas at which encryption can be used to protect data at a high level. These topics will be expanded on in Chapter 6, "The Application and Use of Cryptography."

Data at Rest

Data at rest is information stored on some form of media that is not traversing a network or residing in temporary memory. Failure to properly protect data at rest can lead to attacks such as the following:

 Pod slurping, a technique for illicitly downloading or copying data from a computer. Typically used for data exfiltration.

- Various forms of USB (Universal Serial Bus) malware, including but not limited to USB Switchblade and Hacksaw.
- Other forms of malicious software, including but not limited to viruses, worms, Trojans, and various types of key loggers.

Data at rest can be protected via different technical and physical hardware or software controls that should be defined in your security policy. Some hardware offers the ability to build in encryption. A relatively new hardware security device for computers is called the *trusted platform module* (TPM) chip. The TPM is a "slow" cryptographic hardware processor which can be used to provide a greater level of security than software encryption. A TPM chip installed on the motherboard of a client computer can also be used for system state authentication. The TPM can also be used to store the encryption keys.

The TPM measures the system and stores the measurements as it traverses through the boot sequence. When queried, the TPM will return these values signed by a local private key. These values can be used to discover the status of a platform. The recognition of the state and validation of these values is referred to as *attestation*. Phrased differently, attestation allows one to confirm, authenticate, or prove a system to be in a specific state. Data can also be encrypted using these values. This process is referred to as *sealing a configuration*. In short, the TPM is also a tamper-resistant cryptographic module that can provide a means to report the system configuration to a policy enforcer or "health monitor."

The TPM also provides the ability to encrypt information to a specific platform configuration by calculating hashed values based on items such as the system's firmware, configuration details, and core components of the operating system as it boots. These values, along with a secret key stored in the TPM, can be used to encrypt information and only allow it to become usable in a specific machine configuration. This process is called *sealing*.

The TPM is now addressed by ISO 11889-1:2009. It can also be used with other forms of data and system protection to provide a layered approach, referred to as defense in depth. For example, the TPM can help protect the actual system, while another set of encryption keys can be stored on a user's common access card or smart card to decrypt and access the data set.

Another potential option that builds on this technology is self-encrypting hard drives (SEDs). These pieces of hardware offer many advantages over non-encrypted drives:

► Compliance—SEDs have the ability to offer built-in encryption. This can help with compliance laws that many organizations must adhere to.

- Strong security—SEDs make use of strong encryption. The contents of an SED are always encrypted and the encryption keys are themselves encrypted and protected in hardware.
- ► Ease of use—Users only have to authenticate to the drive when the device boots up or when they change passwords/credentials. The encryption is not visible to the user.
- Performance—As SEDs are not visible to the user and are integrated into hardware, the system operates at full performance with no impact on user productivity.

Software encryption is another protection mechanism for data at rest. There are many options available, such as EFS, BitLocker, and PGP. Software encryption can be used on specific files, databases, or even entire RAID arrays that store sensitive data. What is most important about any potential software option is that not only must the encrypted data remain secure and remain inaccessible when access controls, such as usernames and passwords, are incorrect; the encryption keys themselves must be protected, and should therefore be updated on a regular basis.

Caution

Encryption keys should be stored separately from the data.

Data in Transit

Any time data is being processed or moved from one location to the next, it requires proper controls. The basic problem is that many protocols and applications send information via clear text. Services such as email, web, and FTP were not designed with security in mind and send information with few security controls and no encryption. Examples of insecure protocols include:

- ▶ FTP—Clear-text username and password
- ▶ Telnet—Clear-text username and password
- ► HTTP—Clear text
- SMTP—All data is passed in the clear

For data in transit that is not being protected by some form of encryption, there are many dangers, which include the following:

- Eavesdropping
- Sniffing

- Hijacking
- Data alteration

Today, many people connect to corporate networks from many different locations. Employees may connect via free Wi-Fi from coffee shops, restaurants, airports, or even hotels.

One way to protect this type of data in transit is by means of a Virtual Private Network (VPN). VPNs are used to connect devices through the public Internet. Three protocols are used to provide a tunneling mechanism in support of VPNs: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IP Security (IPSec). When an appropriate protocol is defined, the VPN traffic will be encrypted. Microsoft supplies Microsoft Point-to-Point Encryption (MPPE), with PPTP, native to the Microsoft operating systems. L2TP offers no encryption, and as such is usually used with IPSec in ESP mode to protect data in transit. IPSec can provide both tunneling and encryption.

Two types of tunnels can be implemented:

- ► LAN-to-LAN tunnels—Users can tunnel transparently to each other on separate LANS.
- ▶ Host-to-LAN tunnels—Mobile users can connect to the corporate LAN.

Having an encrypted tunnel is just one part of protecting data in transit. Another important concept is that of authentication. Almost all VPNs use digital certificates as the primary means of authentication. X.509 v3 is the de facto standard. X.509 specifies certificate requirements and their contents. Much like that of a state driver's license office, the Certificate Authority (CA) guarantees the authenticity of the certificate and its contents. These certificates act as an approval mechanism.

Just as with other services, organizations need to develop policies to define who will have access to the VPN and what encryption mechanisms will be used. It's important that VPN policies be designed to map to the organization's security policy. As senior management is ultimately responsible, they must approve and support this policy.

Standard email is also very insecure and can be exposed while in transit. Standard email protocols such as SMTP, POP3, and IMAP all send data via clear text. To protect email in transit you must use encryption. Email protection mechanisms include PGP, Secure Multipurpose Internet Mail Extensions (S/MIME), and Privacy Enhanced Mail (PEM). Regardless of what is being protected periodic auditing of sensitive data should be part of policy and should occur on a regular schedule. Data in transit will also require a discussion of how the encryption will be applied. Encryption can be performed at different locations with different amounts of protection applied.

- ▶ Link encryption—The data is encrypted through the entire communication path. Because all header information is encrypted each node must decrypt and encrypt the routing information. Source and destination address cannot be seen to someone sniffing traffic.
- End to end encryption—Generally performed by the end user and as such can pass through each node without further processing. However, source and destination addresses are passed in clear text, so they can be seen to someone sniffing traffic.

Endpoint Security

No review of logical asset security would be complete without a discussion of endpoint security. Endpoint security consists of the controls placed on client or end user systems, such as control of USB and CD/DVD, antivirus, antimalware, anti-spyware, and so on. The controls placed on a client system are very important.

- Removable media—A common vector for malware propagation is via USB thumb drive. Malware such as Stuxnet, Conficker, and Flame all had the capability to spread by thumb drives. Removable drives should be restricted and turned off when possible.
- Disk encryption—Disk encryption software such as EFS and BitLocker can be used to encrypt the contents of desktop and laptop hard drives. Also, corporate smartphones and tablets should have encryption enabled.
- ► Application whitelisting—This approach only allows known good applications and software to be installed, updated, and used. Whitelisting techniques can include code signing, digital certificates, known good cryptographic hashes, or trusted full paths and names. Blacklisting, alternatively, blocks known bad software from being downloaded and installed.
- Host-based firewalls—Defense in depth dictates that the company should consider not just enterprise firewalls but also host-based firewalls.
- Configuration lockdown—Not just anyone should have the ability to make changes to equipment or hardware. Configurations controls can be used to prevent unauthorized changes.
- ► Antivirus—This is the most commonly deployed endpoint security product. While it is a needed component, antivirus has become much less effective over the last several years.

One basic starting point is to implement the principle of least privilege. This concept can also be applied to each logical asset: each computer, system component or process should have the least authority necessary to perform its duties.

Baselines

A baseline can be described as a standard of security. Baselines are usually mapped to industry standards. As an example, an organization might specify that all computer systems be certified by Common Criteria to an Evaluation Assurance Level (EAL) 3. Another example of baselining can be seen in NIST 800-53. NIST 800-53 describes a tailored baseline as a starting point for determining the needed level of security as seen in Figure 2.4.

- ▶ IT structure analysis (survey)—Includes analysis of technical, operation, and physical aspects of the organization, division, or group.
- Assessment of protection needs—Determination of the needed level of protection. This activity can be quantitative or qualitative.
- Selection of actions—Determination of what specific controls need to be implemented.
- Running comparison of nominal and actual—Periodic review of activities and actions to measure the change between what was previously occurring and what is currently occurring.



Baselines Provided by Special Publication 800-53

FIGURE 2.4 NIST 800-53 Scoping and Baselining Controls.

NIST 800-53 specifies scoping or tailoring activities and categorizes information based on impact.

- ► Low impact
- Moderate impact
- ▶ High impact

Scoping or tailoring is the act of adding or removing controls as needed to get the right level of protection. Obviously, adding controls will increase cost and generally increase system security, whereas removing controls reduces costs but can expose the system to unnecessary threats. Therefore due care must be used to determine the proper level of controls. Scoping and tailoring activities should be well documented with appropriate justification. In some cases, information and information systems must be protected regardless of the cost, because of laws that may govern certain industries.

Laws, Standards, Mandates and Resources

The following laws, standards, and mandates have an impact on information security and can affect the risk profile of an organization. Regardless of the laws and mandates, organizations should be proactive when it comes to corporate governance. Several laws and mandates are described here:

▶ Health Insurance Portability and Accountability Act (HIPAA)—HIPAA was signed into law in 1996. It has two areas. Title I of the HIPAA of 1996 protects health insurance coverage for workers and their families when they change or lose their jobs. Title II requires the U.S. Department of Health and Human Services (DHHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.

Under HIPAA, the U.S. DHHS was required to publish a set of rules regarding privacy. The Privacy Rule dictates controls that organizations must put in place to protect personal information. The privacy rule defines three major purposes:

• "To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information."

- "To improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care."
- "To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals."

Gramm-Leach-Bliley Act (GLBA)—GLBA was signed into law in 1999 and resulted in the most sweeping overhaul of financial services regulation in the United States.

Title V of GLBA addresses financial institution privacy with two subtitles. Subtitle A requires financial institutions to make certain disclosures about their privacy policies and to give individuals an opt-out capability. Subtitle B criminalizes the practice known as pretexting, which can be described as the practice of obtaining personal information under false pretenses.

Under GLBA, financial institutions are required to protect the confidentiality of individual privacy information. As specified in GLBA, financial institutions are required to develop, implement, and maintain a comprehensive information security program with appropriate administrative, technical, and physical safeguards. Administrative controls include items such as background checks and separation of duties. Technical controls can be hardware or software, such as encryption or an IDS. Physical controls include gates, guards, and fences. The controls specified in the information security program must include:

- The assignment of a designated program manager for the organization's information security program
- ▶ A periodic risk and vulnerability assessment and audit
- ▶ A program of regular testing and monitoring
- ► The development of policies and procedures for control of sensitive information and PII

Federal Information Security Management Act (FISMA)—FISMA was signed into law in 2002. One of the big changes that FISMA brought about was a set of clear guidelines for information security designed for the protection of
federal government IT infrastructure and data assets. FISMA requirements specify the following responsibilities:

- Develop and maintain an information assurance (IA) program with an entire IT security architecture and framework.
- Ensure that information security training is conducted to keep IAT and IAM personnel properly trained and certified in accordance with DoD. 8570.
- Implement accountability for personnel with significant responsibilities for information security.

FISMA also requires periodic risk assessments, risk assessment policies and procedures, periodic (at least annual) testing and evaluation, and proper training and awareness to senior management so that proper security awareness programs can be deployed.

Sarbanes-Oxley Act (SOX)—SOX was signed into law in 2002. This act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. Sections 302 and 404 are the two sections that address IT infrastructures and information security. Section 302 requires the CEO and CFO to personally certify that the organization has the proper internal controls. It also mandates that the CEO and CFO report on effectiveness of internal controls around financial reporting.

Section 404 sets requirements on management's structure, control objectives, and control procedures. Staying compliant with Section 404 requires companies to establish an infrastructure that is designed to archive records and data and protect them from destruction, loss, unauthorized alteration, or other misuse. It requires that a set of comprehensive controls be put in place and holds CEOs and CFOs accountable.

United States Resources

NIST started as the National Bureau of Standards and changed its name in 1989 to the National Institute of Standards and Technology. Some of the NIST documents a CISSP should have knowledge of are:

- ▶ NIST 800-37—Guide for applying risk management.
- ► NIST 800-53—Government publication that provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. Many

61

organizations in private industry use NIST SP 800-53 as a guide for their own security management.

▶ NIST 800-60—Guide for Mapping Types of Information and Information.

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.

- ▶ FIPS 199—Establishes security categories of information systems used by the federal government.
- ▶ FIPS 200—Mandatory security standards for government systems.

International Resources

Our first item is the information technology infrastructure library (ITIL). ITIL provides a framework for identifying, planning, delivering, and supporting IT services for business.

The IT Governance Institute has developed a process that begins with setting objectives for the enterprise's IT, providing the initial direction and then evolving into a continuous loop.

ITIL presents a service lifecycle that includes

- Continual service improvement
- Service strategy
- Service design
- Service transition
- Service operation

Next up are some of the standards from the International Organization for Standardization that a CISSP should be familiar with:

- ▶ ISO **27001**—This standard describes requirements on how to establish, implement, operate, monitor, review, and maintain an information security management system (ISMS); it is based on British Standard 7799.
- ► ISO **27002**—This standard is considered a code of practice that describes ways to develop a security program within the organization.

- ▶ ISO **27003**—This standard focuses on implementation.
- ► ISO **27004**—This standard is a standard for information security measurements.
- ▶ ISO **27005**—This standard describes how to implement solutions based on risk management.
- ▶ ISO **27799**—This standard describes how to protect personal health information.

ISO 9001 is a quality management standard that has widespread support and attention. ISO 9001 describes how production processes are to be managed and reviewed. It is not a standard of quality; it is about how well a system or process is documented. Companies that wish to obtain 9001 certification will need to perform a gap analysis to determine areas that need improvement. ISO 9001 is actually six documents that specify:

- Control of Documents
- Control of Records
- ► Control of Non-conforming Product
- Corrective Action
- Preventive Action
- Internal Audits

Tip

Achieving ISO 9001:2000 Certification—ISO 9001 certification requires an organization to perform a gap analysis. This allows the company to identify shortcomings that need to be addressed in order to obtain certification.

Being ISO-certified means that the organization has the capability to provide products that meet specific requirements, and includes a process for continual improvement. It may also have a direct bearing on an audit as it places strong controls on documented procedures. Another ISO standard that the auditor should be aware of is ISO 17799. 17799 provides the best practice guidance on information security management. It is divided into 12 main sections:

- ▶ Risk assessment and treatment
- Security policy

63

- Organization of information security
- Asset management
- Human Resources security
- Physical and environmental security
- Communications and operations management
- Access control
- ▶ Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

Tip

CISSP exam candidates should have a basic understanding of ISO standards and their purpose; however, the exam does not cover U.S. laws.

Finally, let's review a couple of European documents:

- ▶ 10 Steps to Cyber Security—Detailed cyber-security information and advice across 10 critical technical and procedural areas. Created by CESG, the information security arm of GCHQ, and the National Technical Authority for Information Assurance within the United Kingdom.
- Cybersecurity Strategy of the European Union—This document was developed by the European Union; it describes their approach to preventing and responding to cyber-security attacks.

Exam Prep Questions

- 1. Which of the following levels best represents the military classification system?
 - O A. Confidential, private, sensitive, and public
 - O B. Top secret, secret, private, sensitive, and public
 - O C. Top secret, confidential, private, sensitive, and unclassified
 - O D. Top secret, secret, confidential, sensitive, and unclassified
- 2. Which of the following standards describes how well a system or process is documented?
 - O A. ISO 27001
 - O B. ISO 9001
 - O C. ISO 27002
 - O D. ISO 17799
- **3.** Which of the following endpoint security controls could have been used to potentially prevent malware such as Stuxnet, Conficker, and Flame?
 - O A. Implementing disk encryption
 - O B. Hardening edge devices
 - O C. Blocking removable media
 - O D. Enforcing application whitelisting
- 4. Place the following in their proper order:
 - O A. Determine SLE, ARO, and ALE, then asset value.
 - O B. Determine asset value, then ARO, SLE, and ALE.
 - O C. Determine asset value, then SLE, ALE, and SLE.
 - O D. Determine asset value, then SLE, ARO, and ALE.
- 5. The downside of performing this type of assessment is that you are not working with dollar values, so it is sometimes harder to communicate the results of the assessment to management. Which of the following assessment types does this describe?
 - O A. Qualitative
 - O B. Quantitative
 - O C. Numeric mitigation
 - O D. Red team

- **6.** Which of the following categories of control can include the logical mechanisms used to control access and authenticate users?
 - O A. Administrative
 - O B. Clerical
 - O C. Technical
 - O D. Physical
- 7. Which of the following is incorrect when describing an SED?
 - O A. Eases compliance
 - O B. Slow performance
 - O C. Ease of use
 - O D. Strong security
- **8.** Which of the following is the top level of protection for commercial business classification?
 - O A. Secret
 - O B. Confidential
 - O C. Top secret
 - O D. Private
- 9. Which of the following is the most specific of security documents?
 - O A. Procedures
 - O B. Standards
 - O C. Policies
 - O **D.** Baselines
- **10.** The last thing you want in an organization is that everyone is accountable but no one is responsible. Therefore, the data owner should be in which of the following groups?
 - O A. End users
 - O B. Technical managers
 - O C. Senior management
 - O D. Everyone is responsible; therefore, all groups are owners

- **11.** Which term best describes a symbol, word, name, sound, or thing that uniquely identifies a product or service?
 - O A. Trade secret
 - O **B.** Copyright
 - O C. Patent
 - O D. Trademark
- **12.** After opening a new branch in the Midwest your company is analyzing buying patterns to determine the relationship between various items purchased. Which of the following best describes this situation?
 - O A. Data mining
 - O B. Knowledge management
 - O C. Data warehouse
 - O D. Data standards
- **13.** Which ISO document is used for a standard for information security management?
 - O A. ISO 27001
 - O B. ISO 27002
 - O C. ISO 27004
 - O **D.** ISO 27799
- **14.** Which of the following SAN solutions is fast, rides on top of Ethernet, yet is non-routable?
 - O A. SCSI
 - O B. iSCSI
 - O **C.** HBA
 - O D. FCoE
- 15. Who is ultimately responsible for the security of an asset?
 - O A. Asset owner
 - O B. Auditor
 - O C. Custodian
 - O D. Risk assessment team

Answers to Exam Prep Questions

- 1. D. The military data classification system is widely used within the Department of Defense. This system has five levels of classification: unclassified, sensitive, confidential, secret, and top secret. Each level represents an increasing level of sensitivity.
- 2. B. ISO 9001 describes how production processes are to be managed and reviewed. It is not a standard of quality; it is about how well a system or process is documented. Answers A, C, and D are incorrect: ISO 27001 describes requirements on how to establish, implement, operate, monitor, review, and maintain an information security management system; ISO 27002 is considered a code of practice that describes ways to develop a security program within the organization; ISO 17799 provides best practice guidance on information security management.
- **3. C.** Restricting removable media may have helped prevent infection from malware that is known to spread via thumb drive or removable media. Answer A is incorrect because encryption of media would not have helped. Answer B is incorrect because edge devices were not specifically targeted. Answer D is incorrect because enforcing application whitelisting would not have prevented advanced persistent threats from executing on local systems.
- **4. D.** The proper order is to determine the asset value, then SLE, ARO, and ALE. Answers A, B, and C are incorrect; they are not in the proper order.
- A. Qualitative assessment is scenario-driven and does not attempt to assign dollar values to components of the risk analysis. Quantitative assessment is based on dollar amounts; both numeric mitigation and red team are distractors.
- 6. C. Technical controls can be hardware or software. They are the logical mechanisms used to control access and authenticate users, identify unusual activity, and restrict unauthorized access. Clerical is a nonexistent category and all other answers are incorrect: administrative controls are procedural and physical controls include locks, guards, gates, and alarms.
- 7. B. Self-encrypting hard drives offer many advantages, such as easing compliance issues with items like PII. They are easy to use and offer strong encryption. Answer B is correct because SEDs do not slow down performance; they are actually integrated into the hardware and operate at full performance with no impact on user productivity.
- **8. B.** Confidential is the top level of data classification for commercial business classification. Answers A, C, and D are incorrect because secret and top secret are both part of the military classification, while private is a lower level of commercial business classification.
- 9. A. A procedure is a detailed, in-depth, step-by-step document that lays out exactly what is to be done. It's tied to specific technologies and devices. Standards are tactical documents; policies are high-level documents; and baselines are minimum levels of security that a system, network, or device must adhere to.

CHAPTER 2: Logical Asset Security

- 10. C. Senior management is the ultimate owner because these individuals are responsible for the asset and must answer if data is compromised. Although answer C is the best possible choice, it is important to realize that, in most cases, the data owner will be a member of management but might not be the most senior executive within the organization. For example, the CFO would be the data owner for all financial data, the director of human resources would be the data owner for all HR data, and so on. All other answers are incorrect because end users, technical managers, and other employees are not typically the data owners.
- **11. D.** A trademark is a symbol, word, name, sound, or thing that identifies the origin of a product or service in a particular trade. Answers A, B, and C are incorrect as they do not properly describe a trademark.
- 12. A. Data mining. It is the process of analyzing data to find and understand patterns and relationships about the data. Answers B, C, and D are incorrect. Knowledge management seeks to make intelligent use of all the knowledge in an organization. A data warehouse is a database that contains data from many different databases. Data standards provide consistent meaning to data shared among different information systems.
- **13. C.** ISO 27004 is the standard for security management. ISO 27001 is focused on requirements. ISO 27002 was developed from BS 7799, and ISO 27799 is focused on health.
- 14. D. Fiber Channel over Ethernet (FCoE) can operate at speeds of 10 GB per second and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is non-routable. Answers A, B, and C are incorrect. SCSI is used for local devices only. iSCSI is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. HBAs are used to connect a host system to an enterprise storage device.
- **15. A.** Some day-to-day responsibility may be passed down to the custodian; however, ultimately the owner is responsible.

Need to Know More?

Data valuation: www.cio.com/article/2375569/cio-role/why-cios-must-own-data-valuation.html

Understanding FIPS guidelines: www.sans.org/reading-room/whitepapers/ standards/securing-sensitive-data-understanding-federal-information-processingstandards-fips-549

ISO27002 overview: en.wikipedia.org/wiki/ISO/IEC_27002

Site security: www.faqs.org/rfcs/rfc2196.html

IT asset management: searchcio.techtarget.com/definition/ IT-asset-management-information-technology-asset-management Building effective security policies: www.sans.org/security-resources/ policies/

IT security baselines: www.securestate.com/services/minimum-security-baselines

Building effective policy: csrc.nist.gov/nissc/1997/panels/isptg/pescatore/html/

Hard drive disposal: www.semshred.com/contentmgr/showdetails.php/id/2480

This page intentionally left blank

Index

Numbers

1G, 344 2G, 345 3DES (Triple-DES), 246, 255-257 3G, 345 4G, 345 10 Steps to Cyber Security, 63 64-bit key, 246 802.1AE (MACsec), 306 802.1AR, 306 802.1X, 352 802.11 wireless networks, 346-348 Bluetooth, 350 encryption, 351 standards, 348-349 topologies, 348 wireless protection mechanisms, 352-354 802.11a, 348 802.11ac, 349 802.11b, 349 802.11g, 349 802.11i, 349, 353 802.11n, 349 802.15, 349 802.16, 349

A

AaaS (Authentication as a Service), 377 absolute addressing, 181 acceptable risk, 147 acceptable use policies (AUPs), 154, 495, 519, 523 acceptance testing and implementation, SDLC (System Development Life Cycle)

acceptance testing and implementation, SDLC (System Development Life Cycle), 551–552 access, 375 to BCP (business continuity plan), 621 controlling, managing users, 495 Kerberos, 393-396 monitoring, 408-409 network access control devices, 355 demilitarized zones, 357-358 firewall designs, 359 firewalls, 355 physical access, controlling, 524–525 remote access, 502 CHAP (Challenge Handshake Authentication Protocol), 360 EAP (Extensible Authentication Protocol), 360-361 PAP (Password Authentication Protocol), 360 PPP (Point-to-Point Protocol), 360 single sign-on (SSO), 392–393 unauthorized access, 448 access aggregation, 448-449 access control lists (ACLs), 397–398 access control models, 403 centralized access control, 403-404 Diameter, 406–407 RADIUS (remote authentication dial-in user service), 404-405 TACACS (Terminal Access Controller Access Control System), 406 decentralized access controls, 407 access control threats, 448 access aggregation, 448-449 eavesdropping, 453 identity theft, 453-454 password attacks, 449-450 shoulder surfing, 453 spoofing, 453 unauthorized access, 448

access controls

authentication, 375-376 authorization, 375-376, 397 CDAC (content-dependent access control), 403 DAC (discretionary access control), 397–398 LBAC (lattice-based access control), 403 MAC (mandatory access control), 398-400 RBAC (role-based access controls), 401-402 rule-based access controls, 402 categories of, 155–156 identification. 375-376 access logs, 434 accessibility, to facilities, 77 account management, 391 accountability, 375, 408, 518, 525. See also auditing monitoring and auditing controls, 518 accounts, managing, 493-495 clipping level, 496 accreditation, 213-214, 553 ACLs (access control lists), 397–398, 402 acoustical detection, 106 acquire, computer forensics, 475-477 active sniffing, 440 ActiveX, 564 activity blockers, 510 Address Resolution Protocol (ARP), 306 address space layout randomization (ASLR), 219-220 adhoc mode, 348 administrative controls, 154 administrative law, 124 administrative support teams, 534 ADSL (asymmetric digital subscriber line), 340

Advanced Encryption Standard (AES), 255. 257-258 advanced persistent threats (APTs, 439, 462 advisory policies, 151 AES (Advanced Encryption Standard), 255, 257-258 agent based, SIEM (security information and event management), 522 agentless, SIEM (security information and event management), 522 aggregation, databases, 567, 568-569 agile development methods, 557–558 AH (authentication header), 282, 363 AI (artificial intelligence), 570 AIC (availability, integrity, confidentiality), 29 air conditioning, facilities, 98-99 air intakes, 81 alarm systems, 106 IDS (intrusion detection systems), 106 - 107monitoring and detection, 107-108 alarms, silent hostage alarms, 95 ALE (annual loss expectancy), 139–140 algorithms, 246-247 asymmetric algorithms, 247 Diffie-Hellman, 261-262 DSA (digital signature algorithm), 271 dynamic routing, 334 hashing algorithms, 267-268 Merkle-Hellman Knapsack, 264 Rivest cipher, 258–259 RSA, 262-263 symmetric algorithms, 247, 250–251 alpha tests, 551 alphabetic cipher, 238-239 alternate routing, 607 ALU (arithmetic logic unit (ALU), 176 American Society for Testing and Materials (ASTM), 84

analysis, computer forensics, 478 analyzing, threats, 135-139 Anderson, James, 409 annual loss expectancy (ALE), 139-140 annual rate of occurrence (ARO), 139 annunciators. 87 anomaly-based IDS engines, 412 Anonymous, 437 anti-malware, 509-510 antivirus. 56 antivirus software, 577 applets, Java, 573-574 application layer OSI (Open Systems Interconnection) model, 302 TCP/IP, 314-317 application security testing, 429 application servers, 186 application switches, 330 application transactions, monitoring, 520-521 application whitelisting, 56 application-level proxy, 356 application/process layer controls, securing TCP/IP, 280 APTs (advanced persistent threats), 439.462 architecture, security architecture. See security architecture archive bits, 512 archiving, 38-39 area concerns, facilities, 77-78 arithmetic logic unit (ALU), 176 ARO (annual rate of occurrence), 139 ARP (Address Resolution Protocol), 306, 310 ARP poisoning, 446 artificial intelligence, 570-571 ASLR (address space lavout randomization), 219-220 assemblers, 564

732 assessing

assessing exam readiness, 18-19 potential loss, 595-598 risk. 130-133 asset identification. 133-135 asset management, 49-50, 497 endpoint security, 56-57 equipment lifecycle, 51-52 software licensing, 50-51 asset placement, in facilities, 82 asset security. 28 asset valuation. 133-135 assets, 49, 130 assisted password reset, 391 assurance classes, 210 **ASTM** (American Society for Testing and Materials), 84 asymmetric algorithms, 247 asymmetric cryptography, 236 asymmetric digital subscriber line (ADSL), 340 asymmetric encryption, 259-261, 272 versus symmetric encryption, 264-265 asymmetric mode, 178-179 asynchronous attacks, 220 asynchronous replication, 611 asynchronous token devices, 382-383 asynchronous transfer mode (ATM), 307 ATBASH, 237-238 ATM (asynchronous transfer mode), 307, 337 ATO (Authorization to Operate), 118 atomicity, 569 attack methodologies, 437-439 attack surface, 571 attacks, 126. See also threats availability attacks, 437 birthday attack, 287 brute force attacks, 378 chosen ciphertext, 287 chosen plaintext, 287

ciphertext-only attack, 287 covert channels, 221 cryptographic attacks, 285-288 data diddling, 435 DDoS attacks, 437, 443 dictionary attacks, 378 differential cryptanalysis, 287 directory traversal attacks, 223 DoS attacks, 442-443 VoIP (voice over IP), 344 emanations, 222-223 financial attacks, 575 hybrid attacks, 451 incremental attacks, 221-222 inference attacks, 284 injection attacks, 225 key clustering, 287 known plaintext attack, 287 linear cryptanalysis, 287 logic bombs, 575 man-in-the middle attack, 288 password attacks, 449-450 brute-force crack, 451 dictionary crack, 450-451 rainbow tables, 452 pharming attacks, 447 phishing, 454 replay attack, 288 rubber hose attack, 288 salami attacks, 575 side channel attack, 288 social engineering attacks, 454-455 spear phishing, 454 SQL injection, 224-225 state attacks, 220 viruses, 576-577 worms, 577-578 attenuation, 327 attributes, databases, 567 attribute-value pairs (AVPs), 404 audio detection, 106 audit controls, 525

audit logs, 434 audit processes, 37-38 audit reduction and correlation tools, 518 audit reduction tools, 408-409 auditing, 408. See also accountability user activities, 519 auditors, roles and responsibilities, 33 audits, 426-427 data audits, 37-38 AUPs (acceptable use policies), 154, 495, 519, 523 authentication, 375-376 computer forensics, 477 cryptography, 235, 266 something you are (Type 3), 385-390 something you have (Type 2), 381 asynchronous token devices, 382-383 cards, 383-384 certificates, 384-385 synchronous tokens, 381–382 strong authentication, 390 techniques for, 376-377 something you know (Type 1), 377-379 Authentication as a Service (AaaS), 377 authentication header (AH), 282, 363 authentication service, 394 authority, social engineering, 162 authorization, 374, 375-376 access controls, 397 CDAC (content-dependent access control), 403 DAC (discretionary access control), 397–398 LBAC (lattice-based access control), 403 MAC (mandatory access control), 398–400 RBAC (role-based access controls), 401–402 rule-based access controls, 402

Authorization to Operate (ATO), 118 automated backups, 512 availability, 29 calculating, 606 availability attacks, 437 avalanche effect, 267-268 avoiding system failures, 543 checks and application controls, 543-544 failure states, 544 AVPs (attribute-value pairs), 404 awareness BCP (business continuity plan), implementing, 619 ethics, 163-164 security awareness, 161-162 security management, 160-161

В

backdoors, 220, 458-459, 550 background checks, 156–157 social networking, 157 backup sites, 601-602 backups, 29, 511-512, 608-609 automated backups, 512 choosing methods, 613-614 cloud computing backups, 613 continuous backups, 609 data replication, 611 database shadowing, 612 differential backups, 512, 609 electronic vaulting, 612 full backups, 512, 609 incremental backups, 512-513, 609 media-rotation strategies, 611–612 on-demand backups, 512 remote journaling, 612 restoration, 609-611 SAN (storage area network), 613 tape rotation methods, 513

734 badges, employee access control

badges, employee access control, 94-95 baseband, 322 baselines, 57-58 risk management, 152 Basic Rate Interface (BRI), 338 bastion hosts, 357-358 BC (business continuity), 588 defined, 590 BCP (business continuity plan), 588, 589-591 access to, 621 assessing potential loss, 595-598 BIA (business impact analysis), 593-595 implementing, 618-619 awareness and training, 619 monitoring and maintenance, 621-622 plan design and development, 615 employee services, 617 insurance, 617-618 interacting with external groups, 616-617 personnel mobilization, 615-616 process responsibilities, 622 project management and initiation, 591-593 recovery strategies, 599-600 backup and restoration, 609-611 business process recovery, 600-601 data and information recovery, 608-609 facility and supply recovery, 601 operations recovery, 606-608 user recovery, 605 testing, 619-621 behavioral-based IDS, 412, 528-529 Bell-LaPadula model, 199-201 Berlin Wall, 83 Bernay, Mark, 465 best evidence, 482

BIA (business impact analysis), 593-595 assessing, potential loss, 595-598 questionnaires, 595-597 reputation, 599 vulnerability assessments, 595 Biba model, 202-203 Tibetan monks, 203 biometric access controls, 96-97 considerations before deploying, 389-390 usage patterns, 388 biometrics, authentication, 385-390 birthday attack, 287 blackbox testing, 428 blackbox tests, 552 blacklists, 506 blind tests, 429 block ciphers, 237, 240, 247-248 Blowfish, 250 bluejacking, 350 bluesnarfing, 350 Bluetooth, 350 Boehm, Barry, 554-555 bogon filtering, 333 bollards, 85-86 boolean operators, stream ciphers, 248 BootP (Bootstrap Protocol), 315 bot herders, 444-445 botnets, 443-446 fast-flux botnets, 445 **BPA** (Business Partnership Agreement), 119 The Brain, 456 Brewer and Nash model, 205 BRI (Basic Rate Interface), 338 bridges, 328 British Standard (BS) 7799, 216 broadband, 322 brute force attacks, 378

brute-force crack, 451

buffer overflows, 219–220, 574–575 preventing, 574–575

buffers, 574

- bulletproof hosting, 461-462
- bus, I/O bus standards, 183-184
- bus topology, 319
- **business continuity.** See BC (business continuity)
- **business continuity plan.** *See* BCP (business continuity plan)
- business impact analysis (BIA), 593–595
- business operations, threats to, 588–589
- Business Partnership Agreement (BPA), 119

business process recovery, 600-601

- business reference model, 215
- BYOD (bring your own device), 226
- BYOT (bring your own technology), 226

С

C, 564 C#, 564 C+, 564 C++, 564 CA (Certificate Authority), 272-273 CaaS (Communication as a Service), 503 Cable Internet access, 340 cable modems, 340-341 cable specifications, LAN cabling, 323-324 cabling coaxial cable, 322 fiber-optic cable, 324 LANs (local area networks), 322-324 multimode fiber, 324 plenum-grade cable, 324 single-mode fiber, 324 twisted pair, 322-323

CAC (Common Access Card), 95 Caesar's cipher, 237 CAIN (confidentiality, availability, integrity, nonrepudiation), 29 calculating, availability, 606 **CALEA** (Communications Assistance for Law Enforcement Act), 441 call trees, 615-616 CAM (content addressable memory), 329 campus area networks (CANs), 325 Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), 207 CANs (campus area networks), 325 capability lists, reference monitors, 191 Capability Maturity Model (CMM), 558-560 Capability Maturity Model Integration (CMMI), 559-560 capability tables, 402 cards authentication, 383-384 employee access control, 94-95 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), 320 carriers, steganography, 244 CASE (Computer-Aided Software Engineering), 557 CAST (Carlisle Adams/Stafford Tavares), 251 categories of access controls, 155-156 cloud computing models, 504 threats to business operations, 589 CBC (Cipher Block Chaining) mode, 253, 270 CBF (critical business function), 590 CCDs (charged coupled devices), 87 **CCMP**, 353

CCTV (closed-circuit television), 76–77 perimeter controls, 87

736 CDAC (content-dependent access control)

CDAC (content-dependent access control), 403

CDDI (Copper Distributed Data Interface), 320

CDI (constrained data items), 204

CDs (compact discs), 183

ceilings, 79–81

cell phones, 344-346

central processing unit. See CPU (central processing unit)

centralized access control, 403–404

Diameter, 406-407

RADIUS (remote authentication dial-in user service), 404–405

TACACS (Terminal Access Controller Access Control System), 406

CER (crossover error rate), 386

CERT (Computer Emergency Response Team), 467

Certificate Revocation List (CRL), 273–274

certificates authentication, 384–385 digital certificates, 274–276

certification, 18, 213-214

operations and maintenance, SDLC (System Development Life Cycle), 552–553

CFAA (Computer Fraud and Abuse Act), 123

CFB (Cipher Feedback) mode, 253–254

chain of custody, 478

chaining, 253

Challenge Handshake Authentication Protocol (CHAP), 360, 404

change control process, 561-562

change controls, 34-35

change detection, 575-576

change management, 498–500, 561–562

changeover techniques, 553

Authentication Protocol), 360, 404 charged coupled devices (CCDs), 87 charts, Gantt charts, 560 checklists, BCP (business continuity plan), 620 checks and application controls, 543-544 chief security officer, roles and responsibilities, 32 Chinese Wall model, 205 chosen ciphertext, 287 chosen plaintext, 287 CIA (confidentiality, integrity, and availability), 28 Cialdini, Robert, 162 Cipher Block Chaining mode, 253 cipher block chaining-Message Authentication Code (CBC-MAC), 270 Cipher Feedback mode, 253–254 cipher-based message authentication code (CMAC), 270 ciphers alphabetic cipher, 238-239 block ciphers, 240, 247-248 Caesar's cipher, 237 concealment ciphers, 241 polyalphabetic cipher, 238-239 Rivest cipher, 258–259 rotation cipher, 237 running key cipher, 241 stream ciphers, 240, 248 symmetric substitution ciphers, 240 transposition ciphers, 240 Vernam cipher, 241–242 Vigenere cipher, 238–239, 239 ciphertext, 236, 249 ciphertext-only attack, 287 **CIR** (committed information rate), 337

CHAP (Challenge Handshake

737

circuit switching, WANs (wide area networks), 337

cable modems, 340-341 DSL (digital subscriber line), 339-340 ISDN (Integrated Services Digital Network), 338 POTS (Plain Old Telephone Service), 338 T-carriers, 338-339 circuit-level proxy, 357 **CIRT (Computer Incident Response** Team), 467 **CISC** (Complex Instruction Set Computing), 178 Citadel, 461 civil law, 124 Clark-Wilson model, 204 classification approach, knowledge extraction, 36 classifying information, 46 data classification, 46-47 cleaning crews, 94 cleartext, 236 cleartext protocols, sniffing, 441 click-wrap license agreements, 50 client's role, in PKI (public key infrastructure), 276-277 climatology, facilities, 77 clipping level, 379, 496 cloning, 345-346 closed systems, 192 closed-circuit television (CCTV), 76-77 cloud computing, 341-342, 503-504 cloud computing backups, 613 cloud computing models, 504 cloud-based storage, 39 clouds, 185 clustering, 514, 606 CMAC (cipher-based message authentication code), 270 CMM (Capability Maturity Model), 558-560

CMMI (Capability Maturity Model Integration), 559–560 coaxial cable, 322 **COBIT** (Control Objectives for Information and related Technology), 37-38, 218, 427 **COBOL** (Common Business Oriented Language), 564 CoCOM (Coordinating Committee for Multilateral Export Controls), 285 cognitive passwords, 380 cohesion addresses, 549 COI (conflict of interest), 205 cold sites, 603 collisions, 269 hashing, 268 combination locks, 90 committed information rate (CIR), 337 Committee for Sponsoring Organizations of the Treadway Commission (COSO), 168 Common Access Card (CAC), 95 **Common Business Oriented** Language (COBOL), 564 common computer ethics fallacies, 167 Common Criteria, 210–212 common law, 123 **Common Object Request Broker** Architecture (CORBA), 566 communication cell phones, 344-346 LANs (local area networks). See LANs (local area networks) standards, 327 VoIP (voice over IP), 343 Communication as a Service (CaaS). 503 communication loss, physical security, 75 communication protocols, 318-319 Communications Assistance for Law Enforcement Act (CALEA), 441

communications attack, 126 communications teams, 534 compact discs (CDs), 183 comparative analysis, 450 comparing quantitative assessments, and qualitative assessments, 145-146 symmetric encryption, and asymmetric encryption, 250, 264-265 UDP (User Datagram Protocol), and TCP, 313 compartmentalized systems, 400 compartmented, security modes of operation, 193 compensating access controls, 155 compilers, 564 completeness check, 544 **Complex Instruction Set Computing** (CISC), 178 components of, IDS (intrusion detection systems), 413, 529 computer crimes, 125-128 **Computer Emergency Response** Team (CERT), 467 Computer Ethics Institute, 165 computer forensics, 472, 473, 474 acquire, 475-477 analysis, 478 authentication, 477 integrity, 477–478 **Computer Fraud and Abuse Act** (CFAA), 123 **Computer Security Incident Response** Team (CSIRT), 467 **Computer-Aided Software** Engineering (CASE), 557 concealment ciphers, 241 confidential military data classification, 47 public/private data classification, 48 confidentiality, 28 Bell-LaPadula model, 199-201 cryptography, 235

reciprocal agreements, 605 security models, 199 symmetric encryption, 250 confidentiality, integrity, and availability (CIA), 28 configuration lockdown, 56 configuration management, 498-500 conflict of interest (COI), 205 confusion, 248 consistency, 569 social engineering, 163 constrained data items (CDI), 204 construction of facilities, 78 doors, walls, windows, and ceilings, 79-81 contact smart cards, 383 contactless smart cards, 383 content addressable memory (CAM), 329 Content Scrambling System (CSS), 286 content switches, 330 content-dependent access control (CDAC), 403 content-services switches, 330 contingency planning, 511, 516-517 continuing professional education (CPE), 128 Continuity of Operations (COOP), 118 continuous backups, 609 continuous lighting, 88 **Control Objectives for Information** and related Technology (COBIT), 37-38, 218, 427 control units, 177 control zones, 524 controlling, physical access, 524-525 controlling access, 495 controls, 131, 154 access controls, categories of, 155 - 156administrative controls, 154

application/process layer controls, security TCP/IP, 280 biometric access controls, 96–97 change controls, 34-35 checks and application controls, 543-544 corrective controls, 550-551 data controls, 34-35 data lifecycle control, 37 detective controls, 550-551 environmental controls, 98 host to host layer controls, securing TCP/IP, 280-282 Internet layer controls, securing TCP/IP, 282–283 manual authorization input control, 520 monitoring and auditing controls, 518-519 auditing user activities, 519 controlling physical access, 524-525 emanations, 524 keystroke monitoring, 523 monitoring application transactions, 520-521 NAC (Network Access Control), 522 SIEM (security information and event management), 521-522 network access layer controls, securing TCP/IP, 283-284 output controls, 520, 521 physical controls, 155 physical port controls, 82 preventative controls, 550–551 privacy controls, 43 process controls, 520 recovery controls, 516-518 technical controls, 155 telecommunication controls, 503 blacklists, 506 cloud computing, 503-504 email, 504-506

fax, 506-507 gravlists, 506 PBX, 507–508 whitelists, 506 COOP (Continuity of Operations), 118, 531 **Coordinating Committee for** Multilateral Export Controls (CoCOM), 285 coordination teams, 534 **Copper Distributed Data Interface** (CDDI), 320 copyrights, 34 length of, 121 **CORBA** (Common Object Request Broker Architecture), 566 corporate spies, 127, 435 Corpus Juris Civilis, 125 corrective access controls, 155 corrective controls, 550-551 COSO (Committee for Sponsoring Organizations of the Treadway Commission), 168 cost, data governance policies, 31 counter measure selection, risk assessment, 146-149 Counter mode, 254-255 covering tracks, 439 covers, steganography, 244 covert channels, 220-221 covert storage channel attacks, 221 covert timing channel attacks, 221 Cowen, Fred, 456 **CPE** (continuing professional education), 128 **CPTED (Crime Prevention Through** Environmental Design), 76–77 CPU (central processing unit), 176-180 advancements, 177 cracking, password attacks, 450 cramming, 509 credentials, Kerberos, 394

740 crime

crime, 465-466 evidence life cycles, 483 evidence types, 481-482 forensics, 472-473 computer forensics, 474 procedures, 473 honeynets, 480-481 honeypots, 480-481 how computer crime has changed, 464-465 incident response, 467-468 incident response team, 468 processes, 469-470 results, 470-471 interrogations, 480 interviews, 480 investigating computer crime, 466-467 investigations, 479 jurisdiction over computer crime, 467 negligence, 483 surveillance, 479 trials, 482-483 **Crime Prevention Through** Environmental Design (CPTED), 76-77 crime triangle, 466-467 crimes, computer crimes, 125-128 crimeware kits, 461-462 criminal activities, physical security, 75 criminal law, 123-124 criminals, 465-466 critical business function (CBF), 590 criticality prioritization, 594 CRL (Certificate Revocation List), 273-274 crossover error rate (CER), 386 cross-site request forgery (CSRF), 223 cross-site scripting (XSS), 223 crosstalk, 327

cryptanalysis, 236, 285 crypters, 460 cryptographic algorithm, 236 cryptographic keys, 236 cryptography, 29, 234 3DES (Triple-DES), 255-257 **AES** (Advanced Encryption Standard), 257-258 algorithms, 246-247 asymmetric encryption, 259-261 attacks, 285-288 authentication, 235, 266 confidentiality, 235 DES (Data Encryption Standard), 252 CBC (Cipher Block Chaining) mode. 253 CFB (Cipher Feedback) mode, 253-254 Counter mode, 254-255 ECB (Electronic Cookbook) mode, 253 OFB (Output Feedback) mode, 254 Diffie-Hellman, 261–262 digital signatures, 270-271 DSA (digital signature algorithm), 271 ECC (Elliptical Curve Cryptosystem), 263 El Gamal, 263 email protection mechanisms, 277 PGP (Pretty Good Privacy), 278 encryption history of, 237-243 hybrid encryption, 265–266 Feistel Network, 242 hashing algorithms, 267-268 CBC-MAC (cipher block chaining-Message Authentication Code), 270 CMAC (cipher-based message authentication code), 270 HAVAL, 269

HMAC (Hashed Message Authentication Code), 269-270 MAC (Message Authentication Code), 269 MD algorithms, 268-269 secure hashing algorithms, 269 integrity, 235 integrity verification, 266-267 Merkle-Hellman Knapsack, 264 nonrepudiation, 235-236 NSA (National Security Agency), 242 PAIN (privacy, authentication, integrity, and nonrepudiation), 235 quantum cryptography, 242 RSA, 262-263 steganography, 243-244 digital watermarks, 245–246 steganography operations, 244-245 symmetric encryption, 249–252 TCP/IP, 279 application/process layer controls, 280 host to host layer controls, 280-282 Internet layer controls, 282–283 network access layer controls, 283 - 284**CSIRT** (Computer Security Incident Response Team), 467 CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 320 CSRF (cross-site request forgery), 223 CSS (Content Scrambling System), 286 **CTCPEC** (The Canadian Trusted **Computer Product Evaluation** Criteria), 207 customary law, 125 cut-through switches, 330 cybercriminals, 127 Cybersecurity Strategy of the European Union, 63 cyberterrorists, 127

D

DAC (discretionary access control), 397-398 damage assessment teams, 534 DARPA (Defense Advanced Research Projects Agency), 467 DASD (direct access storage device), 513 data decommissioning, 45 organizing, 35 data access, terminated employees, 33 data and information recovery, 608-609 data at rest, encryption, 52-54 data audits, 37-38 data centers. 82 temperatures of, 98 data classification, 46-47 military data classification, 47-48 public/private data classification, 48 data controls, 34-35 data custodians, roles and responsibilities, 32, 34-35 data de-duplication (DDP), SAN (storage area network), 41 data diddling, 435 data disposal, 44-45 data documentation, 35 data entry specialists, 493 data execution preventions (DEP), 219-220 data governance policies, 30-31 data in transit, 54-56 data input validation, 543 data lifecycle control, 37 data link layer, OSI (Open Systems Interconnection) model, 299-300 data management, 30 data mining, 35-36

742 Data Over Cable Service Interface Specification (DOCSIS)

Data Over Cable Service Interface Specification (DOCSIS), 340–341 data owner identification. 34 data owners, roles and responsibilities, 32 data ownership, 33-34 roles and responsibilities, 33-34 data protection, 28 Data Protection Authority, 121 data reference model, 215 data remanence, 45 data replication, 611 data retention, 44-45 data security, 41-42 encryption, 52 data at rest, 52-54 data in transit, 54-56 endpoint security, 56-57 information handling requirements, 43 privacy impact assessment, 42-43 data standards, 37-140 data storage, 38-39 cloud-based storage, 39 information handling requirements, 43 NAS (network attached storage), 38-39 SAN (storage area network), 38–39, 39-41 data warehousing, 35 database administrators, 493 database attacks, 446 database management, 566-567 artificial intelligence, 570-571 common terms, 567-568 integrity, 569 transaction processing, 569-570 database servers, 186 database shadowing, 612 databases aggregation, 568-569 inference, 569

DBMS (database management system), 566 DDoS (distributed denial of service) attacks, 443 **DDoS attacks**, 437 DDP (data de-duplication), SAN (storage area network), 41 DDR (double data rate), 182 DDR2, 182 DDR3, 182 **DDR4. 182** dead analysis, 478 decentralized access controls, 407 decommissioning, data, 45 **DeCSS**, 286 **DECT (Digital Enhanced Cordless** Communication), 354 dedicated, security modes of operation, 193 de-encapsulation, 304 default routes, 334 **Defense Advanced Research** Projects Agency (DARPA), 467 defense in depth, 72, 279 defense of breadth, 72 degaussing, 44, 502-503 delay alarms, 80 Delphi technique, 144 deluges, water sprinklers, 105 demilitarized zones, 357-358 NAT (Network Address Translation), 358 denial-of-service (DoS) attacks, 442-443 denial-of-service (DoS) testing, 429 DEP (data execution prevention), 219-220 Department of Defense security modes of operation, 193-194 standard, 177-199, 554

DES (Data Encryption Standard), 246, 250. 252 CBC (Cipher Block Chaining) mode, 253 CFB (Cipher Feedback) mode, 253-254 Counter mode, 254-255 ECB (Electronic Cookbook) mode, 253 OFB (Output Feedback) mode, 254 **DES EDE2, 256 DES EDE3, 256 DES EEE2, 256 DES EEE3. 256** destruction of data, 44-45 physical security, 74 detective access controls, 155 detective controls, 550-551 deterrent access controls, 155 developers, roles and responsibilities, 32 developing, security policies, 149-150 development methods, software development, 554 JAD (Joint Application Development), 555-556 MPM (Modified Prototype Model), 557 prototyping, 556–557 RAD (Rapid Application Development), 556 spiral model, 554-555 waterfall model, 554 **DIACAP (DoD Information Assurance Certification and Accreditation** Process), 213 Diameter, 406-407 dictionary attacks, 378 dictionary crack, 450-451 diesel fuel, 100 differential backups, 512, 609 differential cryptanalysis, 287

Diffie-Hellman, 261–262 diffusion, 248 digital certificates, 274-276, 384-385 **Digital Enhanced Cordless** Communication (DECT), 354 digital signature algorithms (DSA), 271 digital signatures, 236, 270-271, 273 DSA (digital signature algorithm), 271digital subscriber line (DSL), 339-340 digital video discs (DVDs), 183 digital watermarks, 245-246 direct access storage device (DASD), 513 direct evidence, 482 direct OS commands, 223 direct-access storage, 183 directory traversal attacks, 223 direct-sequence spread spectrum (DSSS), 347 disaster recovery, 532-533 physical security, 534 **Disaster Recovery Institute** (DRI), 588 disaster recovery life cycle, 531-532 disaster recovery managers, 532 disaster recovery plan. See DRP (disaster recovery plan) disaster recovery teams, 533-534 disasters, defined, 590 discernment, 89 discretionary access control (DAC), 397-398 discretionary security property, 201 disgruntled employees, 127 disk encryption, 56 disposal data custodians, 35 SDLC (System Development Life Cycle), 553, 554 distance-vector protocols, 334 distributed computing, 514

744 distributed denial of service (DDoS) attacks

distributed denial of service (DDoS) attacks, 443 distribution of, symmetric keys, 249-250 diverse routing, 607 DIX (Digital, Intel, and Xerox), 318 DMCA (Digital Millennium Copyright Act), 51 DMZ (demilitarized zones), 357–358 NAT (Network Address Translation), 358 DNS (Domain Name Service), 315 DNS spoofing, 447 **DNSSEC. 315 DOCSIS** (Data Over Cable Service Interface Specification), 340–341 documentation change control process, 561-562 data documentation, 35 **DoD Information Assurance Certification and Accreditation** Process (DIACAP), 213 dogs, perimeter controls, 89 Domain Name Service (DNS), 315 doors, 79-81 DoS (denial-of-service) testing, 429 DoS (denial-of-service) attacks, 442-443 VoIP (voice over IP), 344 double data rate (DDR), 182 double-blind tests, 429 drag and drop questions, 21 **DRAM (Dynamic Random Access** Memory), 181–182 Draper, John, 465 DRI (Disaster Recovery Institute), 588 drive wiping, 44, 502 DRP (disaster recovery plan), 589 dry contact switches, 106 dry pipes, water sprinklers, 104 DSA (digital signature algorithm), 271

DSD (dynamic separation of duties), 401 DSL (digital subscriber line), 339–340 DSL (very high data rate digital subscriber line), 340 Dsniff suite, 449-450 **DSSS** (direct-sequence spread spectrum), 347 dual-homed gateways, 359 dual-use kevs. 249 due care, 123, 496-497 due diligence, 123, 496-497 dumb cards, 95 duplicate check, 544 durability, 570 duress alarms, 95 **DVD CCA (DVD Copy Control** Association), 286 DVD Copy Control Association (DVD CCA), 286 DVDs (digital video discs), 183 dwell time, 347 dvnamic NAT. 358 dynamic passwords, 379-380 Dynamic Random Access Memory (DRAM), 181-182 dynamic routing, 334 dynamic separation of duties (DSD), 401

Ε

E1, 339 E3, 339 EA (enterprise architecture), 214–217 EALs (Evaluation Assurance Levels), 211 EAP (Extensible Authentication Protocol), 284, 360–361, 404 EAP-FAST, 361 EAP-Flexible Authentication via Secure Tunneling), 361 EAP-LEAP, 361

encapsulation of process or objects

EAP-MD5, 361 **EAP-PEAP, 361 EAP-SIM**, 361 EAP-Subscriber Identity Module (EAP-SIM), 361 EAP-TTLS, 361 EAP-Tunneled Transport Laver Security (EAP-TTLS), 361 earthquakes, 73 eavesdropping, 453 VoIP (voice over IP), 344 eBay, passwords, 378 ECB (Electronic Cookbook) mode, 253 ECC (Elliptical Curve Cryptosystem), 263 **Economic Espionage** Act of 1996, 123 Edmondson, Dave, 154 education, security management, 160-161 **EFF** (Electronic Frontier Foundation), 254 **EGP** (Exterior Gateway Protocol), 336 **EICER** (European Institute of Computer Anti-virus Research), 577 El Gamal, 263 electric lock pick guns, 93 electrical, physical security, 81 electrical power, 99-100 electromagnetic (EMI) chambers, 78 electro-mechanical, 106 **Electronic Cookbook** mode, 253 **Electronic Frontier Foundation** (EFF), 254 electronic serial number (ESN), 345-346 electronic vaulting, 612 elliptic curve discrete logarithm problem, 263

elliptic curves, 263 Elliptical Curve Cryptosystem (ECC), 263 email. 504-506 encryption, 55 email protection mechanisms, 277, 365 PGP (Pretty Good Privacy), 278 emanation security, 524 emanations, 222-223, 524 embedded device forensics, 472 embedded devices, 186 emergency funding, Katrina (hurricane), 617 emergency management teams, 534 emergency operations center (EOC), 601 emergency operations teams, 534 emergency power off (EPO), 100 emergency response teams, 534 emergency system restart, Orange Book, 501 EMI (electromagnetic interference) chambers, 78 employee access control, 94 badges, tokens, and cards, 94-95 biometric access controls, 96–97 RFID tags, 95-96 employee services, BCP (business continuity plan), 617 employee-awareness programs, security management, 160 employees, terminated employees, security management, 159-160 encapsulated secure payload (ESP), 282 encapsulating security payload (ESP), 363 encapsulation, 303-304 OOP (object-oriented programming), 565 encapsulation of process or objects,

179

745

746 encryption

encryption, 52, 235, 236

802.11, 351 asymmetric encryption, 259-261 authentication, 235 data at rest, 52-54 data in transit, 54-56 disk encryption, 56 end to end encryption, 56 end-to-end encryption, 284 history of, 237-243 hybrid encryption, 265-266 link encryption, 56 public key encryption, 260-261 software encryption, 54 symmetric encryption, 237, 249-252 confidentiality, 250 end to end encryption, 56 end-of-life provisions, 35 endpoint security, 56-57 endpoint-based NAC, 415, 522 end-to-end encryption, 284 enforcement, 377 Enigma machine, 242 enterprise architecture (EA), 214-215 enticement, 480, 482 entity relationship diagram (ERD), 547-548 entrapment, 482 warning banners, 510 enumeration, 438 environmental controls, facilities, 98 EOC (emergency operations center), 601 EPO (emergency power off), 100 equipment, network equipment, 328 bridges, 328 gateways, 333 hubs, 328 mirrored ports, 330 network taps, 330-331 repeaters, 328

routers, 332-333 switches, 329-330 VLANs (virtual LANs), 331 equipment failure, physical security, 75 equipment lifecycle, 51-52, 101 ERD (entity relationship diagram), 547-548 escalation, 439 escalation of privilege, 439 escrow agreements, 611 ESN (electronic serial number), 345-346 ESP (encapsulated secure payload), 282 ESP (encapsulating security payload), 363 Estonia attacks, 464 DDoS attacks, 443 Ethernet, 305, 318 Ethernet frame, 318 Ethernet II protocol, 318 ethical hackers, 430 ethics, 163-164 common computer ethics fallacies, 167 Computer Ethics Institute, 165 IAB (Internet Architecture Board), 165-166 ISC2, 164 NIST SP 800-14, 166-167 regulatory requirements, 167-168 European Institute of Computer Anti-virus Research (EICER), 577 **European Union, Data Protection** Authority, 121 Evaluation Assurance Levels (EALs), 211 event logs, 434 events, 468 evidence life cycles, crime, 483 evidence types, crime, 481-482

exam readiness, assessing, 18-19 exams. See also tests drag and drop questions, 21 hotspot question format, 22-23 multiple-choice questions, 21 strategies for taking, 24-25 strategies for taking exams, question-handling strategies, 24-25 taking, 19-20 exclusive-or (XOR), 352 execution domain switching, 189 existence check, 544 expert systems, 570 exposed risk, 138 Extensible Authentication Protocol (EAP), 284, 360-361, 404 Extensible Markup Language (XML), 565 extensions, Diameter, 407 Exterior Gateway Protocol (EGP), 336 exterior gateway protocols, 336 external groups, interacting with, 616-617 extreme programming (XP), 558

F

facial recognition, 388 facial scans, 97 **Facilitated Risk Assessment Process** (FRAP), 144 facilities, 76 area concerns, 77-78 asset placement, 82 construction, 78 doors, walls, windows, and ceilings, 79-81 **CPTED** (Crime Prevention Through Environmental Design), 76-77 electrical power, 99-100 employee access control, 94 badges, tokens, and cards, 94-95

biometric access controls, 96-97 RFID tags, 95-96 environmental controls, 98 heating, ventilating, and air conditioning, 98–99 location, 78 perimeter controls, 83 bollards, 85-86 fences, 83-84 gates, 84-85 guards and dogs, 89 lighting, 88-89 lock picking, 92-94 locks, 89–92 UPS (uninterruptible power supplies), 100 facility and supply recovery, 601 mobile sites, 604 reciprocal agreements, 604-605 redundant sites, 603-604 subscription services, 601-603 factor analysis of information risk (FAIR), 130 fail safe, 195 fail soft, 195 fail-open state, 544 fail-safe locks, 80 fail-secure, 80 failure states, 544 FAIR (factor analysis of information risk), 130 fake login screens, 455 false acceptance rate (FAR), 386 false negatives, 410, 526 false positives, 410, 526 false rejection rate (FRR), 386 FAR (false acceptance rate), 386 Farmer, Dan, 164, 427 fast infection viruses, 576-577 fast-flux botnets, 445 fault tolerance, 513-514, 606-607 fax, 506-507

748 fax activity logs

fax activity logs, 507 fax encryption, 507 fax servers, 507 FCoE (Fiber Channel over Ethernet), 40.326 FCPA (Foreign Corrupt Practices Act), 168 FEA (Federal Enterprise Architecture), 215 Federal Enterprise Architecture (FEA), 215 Federal Information Processing Standards (FIPS), 61 Federal Information Security Management Act (FISMA), 59–60, 497 Federal Sentencing Guidelines of 1991, 123 federation, 392 fees, for hot sites, 601-602 Feistel, Horst, 242 Feistel Network, 242 **FEMA (Federal Emergency** Management Administration), phreakers, 508 fences. 83-84 FHSS (frequency-hopping spread spectrum), 347 Fiber Channel over Ethernet (FCoE), 40 fiber-optic cable, 324 fields. databases. 567 file infection, 456, 576 file servers. 186 File Transfer Protocol (FTP), 314 final tests. 552 finance teams, 534 financial attacks, 575 financial audits. 37-38 fingerprint scans, 96–97 fingerprints, 388-389 FIPS (Federal Information Processing Standards), 61

fire, 74 fire detection, 101-102 fire detectors, 81 fire drills, 102 fire escapes, physical security, 81 fire prevention, 101–102 fire suppression, 101-102, 103 halon, 105–106 water sprinklers, 104-105 fire-detection equipment, 102–103 firewall designs, 359 firewalls, 355 packet filters, 355-356 proxy servers, 356-357 stateful firewalls, 356 FISMA (Federal Information Security Management Act), 59-60, 497 floods, 73 food, disaster recovery, 605 footprinting, 225, 438 Foreign Corrupt Practices Act (FCPA), 168 foreign government agents, 436 foreign keys, databases, 567 forensics, 472-473 computer forensics, 474 acquire, 475-477 analysis, 478 authenticate, 477 integrity, 477-478 procedures, 473 FORTRAN, 564 fraggle, DoS attacks, 442-443 fragment free switches, 330 fragmentation, 307 Frame Relay, 337 frameworks risk management, 129-130 Zachman Framework, 214–215 FRAP (Facilitated Risk Assessment Process), 144

Free Space Optics (FSO), 608 frequency analysis, 238 frequency-hopping spread spectrum (FHSS), 347 Fresnel lens, 88 Friedman, William, 243 FRR (false rejection rate), 386 FSO (Free Space Optics), 608 FTP (File Transfer Protocol), 314, 357 FTP Secure (FTPS), 280 FTPS (FTP Secure), 280 full backups, 512, 609 full duplex, 327 full interruption, BCP (business continuity plan), 620 fully connected topology, 322 function tests, 552 functional requirements and planning, SDLC (System Development Life Cycle), 547-548 fuzzing, 552 fuzzy solutions, 570

G

G8 (Group of Eight), 497 GANs (Global Area Networks), 325 Gantt charts, 560 GAP in WAP, 354 garbage in, garbage out testing, 552 gates, 84-85 gateways, 333 Generation 1, 563 Generation 2, 563 Generation 3, 563 Generation 4, 563 Generation 5, 563 generations of languages (GLs), 562-563 generators, 100 GFS (grandfather-father-son), 513, 612 GLBA (Gramm-Leach-Bliley Act), 59

Global Area Networks (GANs), 325 **Global System for Mobile** Communications (GSM), 192 globally unique identifier (GUID), 479 GLs (generations of languages), 562-563 gold box, phreakers, 508 Gonzalez, Albert, 466 governance, 49-50 laws, standards, mandates, 58-60 resources international resources, 61-63 United States, 60-61 security, 214-215 security governance, 116–117 government spies, 127 Graham Denning model, 205 Gramm-Leach-Bliley Act (GLBA), 59 grandfather-father-son (GFS), 513, 612 granularity, databases, 567-568 graybox testing, 428 gravlists, 506 grounding devices, 98 Group of Eight (G8), 497 GSM (Global System for Mobile Communications), 192 guards, perimeter controls, 89 GUID (globally unique identifier), 479 guidelines, 153 security, 214-215

Η

hacker insurance, 135 hacker researchers, 436 hackers, 125–128 ethical hackers, 430 skilled hackers, 436 hactivists, 435, 444 half duplex, 327 halon, 105–106 hand geometry, 97, 387 750 hard changeovers

hard changeovers, 553 hardening, 498 hardware device forensics, 472 hardware failures, 606 hardware keystroke loggers, 415-416, 523 Hardware Security Modules (HSM), 277 hardware-based NAC, 415, 522 Harrison-Ruzzo-Ullman model, 205 hash, 236 hash values, 267 Hashed Message Authentication Code (HMAC), 269-270 hashed values, 576 hashes, 379 hashing, 575 collisions, 268 hashing algorithms, 267-268, 273 CBC-MAC (cipher block chaining-Message Authentication Code), 270 CMAC (cipher-based message authentication code), 270 HAVAL, 269 HMAC (Hashed Message Authentication Code), 269–270 MAC (Message Authentication Code), 269 MD algorithms, 268-269 secure hashing algorithms, 269 **HAVAL**, 269 HBA (host bus adapter), 40, 326 HDLC (High-Level data Link Control), 341 HDSL (high data rate digital subscriber line), 340 Health Insurance Portability and Accountability Act (HIPAA), 58 hearsay evidence, 482 heating, facilities, 98-99 heuristic scanning, 509-510

HIDS (host-based intrusion detection systems), 411, 526, 527 hierarchical database management system, 567 hierarchical designs, 400 high data rate digital subscriber (HDSL), 340 High-Level Data Link Control (HDLC), 341 high-speed serial interface, 341 **HIPAA** (Health Insurance Portability and Accountability Act), 58 history of, encryption, 237-243 HMAC (Hashed Message Authentication Code), 269–270 honeynets, 480-481, 510 honeypots, 480-481, 510 horizontal privilege escalation, 439 host bus adapter (HBA) allocation, 40, 326 host to host layer controls, securing TCP/IP, 280-282 host-based firewalls, 56 host-based intrusion detection systems, 411 host-based intrusion detection systems (HIDS), 527 host-to-host layer, TCP/IP, 311 TCP (Transmission Control Protocol), 312–313 UDP (User Datagram Protocol), 313 Host-to-LAN tunnels, 55 hot fixes, 572 hot sites, 601-602 hotspot question format, 22-23 HSM (Hardware Security Modules), 277 HTML, 564 HTTP (Hypertext Transfer Protocol), 315-316, 357 hubs, 328 human safety, 590 hurricanes, 73

HVAC facilities, 98–99 security, 81 hybrid attacks, 451 hybrid designs, 400 hybrid encryption, 265–266 Hypertext Transfer Protocol (HTTP), 315–316 hypervisor, 185

I Love You virus, 464 IA (Interoperability Agreement), 118 laaS (Infrastructure-as-a-service), 341.503 IAB (Internet Architecture Board), 165-166 IAM (Information Assurance Methodology), 144 IANA (Internet Assigned Numbers Authority), 333 **ICMP**, 306 ICMP (Internet Control Message Protocol. 309-310 **IDEA** (International Data Encryption Algorithm, 251, 258 identification. 375-376 identity and access management, 374 identity management, 391-392 account management, 391 federation, 392 password management, 391 profile management, 391 identity theft, 453-454 **IDP** (Intrusion Detection and Prevention), 414, 525 IDS (intrusion detection systems), 106-107, 409-410, 525-526 anomaly-based IDS engines, 412, 528 behavioral-based IDS, 412, 528-529 components of, 413, 529

HIDS (host-based intrusion detection systems), 411, 527 NIDS (network-based intrusion detection systems), 410, 526-527 rule-based access controls, 412 rule-based IDS, 528-529 sensor placement, 413, 529 signature-based IDS engines, 411, 528 IDSL (Internet digital subscriber line), 340 IEEE (Institute of Electrical and Electronics Engineers), 297 IETF (Internet Engineering Task Force), 166, Open Systems Interconnection model **IGMP** (Internet Group Management Protocol), 310-311 **IGRP** (Internet Gateway Routing Protocol), 306 IKE (Internet Key Exchange), 363 IKE (IPSec Internet Key Exchange), 283 ILM (information lifecycle management), 33 IM (instant messaging), 364 **IMAP** (Internet Message Authentication Protocol), 316, 505 IMAPv4, 316 implementing BCP (business continuity plan), 618-619 awareness and training, 619 personnel security, 156-157 IMSI (International Mobile Subscriber Identity), 345-346 incident response, 467-468, 530-531 processes, 469-470 results, 470-471 teams, 468 incident response teams, 468, 534 incidents, 468

operational security incidents, responding to, 530

752 incremental attacks

incremental attacks, 221-222 incremental backups, 512-513, 609 Industry Standard Architecture (ISA), 183 inference, 284 databases, 569, 567 inference attacks, 284 information classifying, 46 data classification, 46-47 obsolete information, 48 Information Assurance Methodology (IAM), 144 information flow model, 199 information handling requirements, data security, 43 information lifecycle management. See ILM (information lifecycle management) Information Systems Audit and Control Association (ISACA), 37–38, 218 information technology infrastructure library (ITIL), 61, 214 Information Technology Security Evaluation Criteria (ITSEC), 210 informative policies, 151-152 Infrastructure-as-as-service (laaS), 341, 503 infrastructure-based NAC, 414, 522 initial program load (IPL), 501 initial sequence numbers (ISNs), 440 initialization vector (IV), 247 initiation, BCP (business continuity plan), 591-593 injection attacks, 225 input/output operations, 189 inputs, 520 insiders, threat actors, 435 instant messaging (IM), 364 insurance BCP (business continuity plan), 617-618 hacker insurance, 135

intangible assets, 496 Integrated Services Digital Network (ISDN). 338 integrity, 29 computer forensics, 477-478 cryptography, 235 referential integrity, 569 security models, 202 Biba model, 202-203 Clark-Wilson model, 204 semantic integrity, 569 integrity checking, 510 integrity verification, cryptography, 266-267 integrity verification procedures (IVPs), 204 intellectual property, protecting, 121 intellectual property rights, 34 software licensing, 50-51 interacting with external groups, BCP (business continuity plan), 616-617 Interconnection Security Agreement (ISA), 118 interface testing, 551 International Data Encryption Algorithm (IDEA), 258 international law, 124–125 International Organization for Standardization (ISO), 297 International Organization on Computer Evidence (IOCE), 473 international resources, for governance, 61-63 International Subscriber Identity (IMSI), 345-346 International Telecommunication **Union-Telecommunications** Standardization Sector (ITU-T), 297 Internet Architecture Board (IAB), 165-166 Internet Assigned Numbers Authority (IANA), 333

Internet Association and Key Management Protocol (ISAKMP), 283 Internet digital subscriber (IDSL), 340 Internet Engineering Task Force (IETF), 166, 297 Internet Gateway Routing Protocol. See IGRP (Internet Gateway Routing Protocol) Internet key exchange (IKE), 363 Internet layer, TCP/IP, 306 ARP (Address Resolution Protocol), 310 ICMP (Internet Control Message Protocol, 309–310 IGMP (Internet Group Management Protocol), 310–311 IP (Internet Protocol), 306–309 Internet layer controls, securing TCP/IP, 282-283 Internet Message Authentication Protocol (IMAP), 316, 505 Internet Small Computer System Interface (iSCSI), 39-40, 325 Interoperability Agreement (IA), 118 interpreters, 564 interrogations, 480 interrupt-driven I/O, 180 interrupts, 179–180 Inter-Switch Link (ISL), 331 interviews, crime, 480 intrusion detection, 409 intrusion Detection and Prevention (IDP), 414 intrusion detection systems (IDS). See IDS (intrusion detection systems) intrusion prevention systems, 414 intrusion prevention systems (IPSs), 530 investigating computer crime, 466-467, 479 invocation property, 202 I/O bus standards, 183–184 I/O using DMA, 180

IOCE (International Organization on Computer Evidence), 473 IP (Internet Protocol), 306–309 IP addresses, 332 IPL (initial program load), 501 IPS (intrusion prevention systems), 414, 530 IPSec (IP Security), 55, 362-364 **IPSec Internet Key Exchange)**, 283 IPv6, 307-309 iris recognition, 387 iris scans, 97 IS security steering committees, roles and responsibilities, 32 ISA (Industry Standard Architecture), 183 **ISA** (Interconnection Security Agreement), 118 **ISACA** (Information Systems Audit and Control Association), 37-38, 218 **ISAKMP** (The Internet Association and Key Management Protocol), 283 ISC2, ethics, 164 **iSCSI** (Internet Small Computer System Interface), 39–40, 325 ISDN (Integrated Services Digital Network), 338 ISL (Inter-Switch Link), 331 ISNs (initial sequence numbers), 440 **ISO** (International Organization for Standardization), 61-62, 297 ISO 9001, 62 ISO 17799, 41, 216 ISO 27000, 217 ISO 27001, 61, 217 ISO 27002, 61, 117, 217 ISO 27003. 62. 217 ISO 27004, 62, 217 ISO 27005, 62, 217 ISO 27799, 62 ISO-certified, 62 isolation. 570
754 IT audits

IT audits, 37-38

ITIL (information technology infrastructure library), 61, 214

ITSEC (Information Technology Security Evaluation Criteria), 210

ITU-T (International Telecommunication Union-Telecommunications Standardization Sector), 297

IV (initialization vector), 247

IVPs (integrity verification procedures), 204

J

JAD (Joint Application Development), 555-556 Japanese Purple Machine, 242, 243 Java, 196, 564, 573 mobile code, 573 Java applets, 573-574 JBOD (Just a Bunch of Disks), 516 JFK Records Act, 44 job rotation, 158 job titles, 494 Johansen, Jon Lech, 286 joins, 403 Joint Application Development (JAD), 555-556 jurisdiction over computer crime, 467 Just a Bunch of Disks (JBOD), 516

Κ

Katrina (hurricane), 600 emergency funding, 617 KDC (Key Distribution Center), 393, 394 Kerberos, 393–396 weaknesses of, 395 Kerckhoff's Principle, 286 Kerckhoff, Auguste, 286 key cards, employee access control, 94–95 key clustering, 287 Key Distribution Center (KDC), 393 key space, 246 key-bumping, 93 keys, dual-use keys, 249 keystroke monitoring, 415–416, 523 knowledge base, 570 knowledge extraction, 36–37 knowledge management, 36–37 known plaintext attack, 287 KryptoKnight, 396

L

L2F, 284 L2TP (Layer 2 Tunneling Protocol), 55. 284 land, DoS attacks, 442 languages, programming languages, 562-565 LANs (local area networks), 318 cabling, 322-324 communication protocols, 318-319 LAN-to-LAN tunnels, 55 last mile protection, 607 Lattice model. 205–206 lattice structure, 567 lattice-based access control (LBAC), 403 laws administrative law, 124 civil law, 124 common law, 123 Corpus Juris Civilis, 125 criminal law, 123-124 customary law, 125 FISMA (Federal Information Security Management Act), 59-60 GLBA (Gramm-Leach-Bliley Act), 59 governance, 58-60 HIPAA (Health Insurance Portability and Accountability Act), 58-59

international law, 124-125 keystroke monitoring, 524 mixed law, 125 Napoleonic law, 125 privacy laws, 121-122 religious law, 125 security, 123 SOX (Sarbanes-Oxley Act), 60 United States, 123-124 Layer 2 Tunneling Protocol (L2TP), 55, 284 layered protections, 72 LBAC (lattice-based access control), 403 LDAP (Lightweight Directory Access Protocol), 316, 404 LEAP (Lightweight Extensible Authentication Protocol), 361 least privilege, 158-159 legal compliance, data governance policies, 31 liability, data governance policies, 31 librarians, 493 licensing, software, 50-51 lifecycles, equipment lifecycle, 51-52, 101 lighting, perimeter controls, 88-89 Lightweight Directory Access Protocol (LDAP), 316 Lightweight directory access protocol (LDAP, 404 Lightweight Extensible Authentication Protocol (LEAP), 361 liking, social engineering, 163 limit check, 543 Line Printer Daemon, 316 linear cryptanalysis, 287 link encryption, 56 link-state protocols, 335 link-to-link encryption, 285 Lipner model, 205 live analysis, 478

LKM (loadable kernel module), 461 loadable kernel module (LKM), 461 local area networks. See LANs (local area networks) location, of facilities, 78 location redundancy, 326 SAN (storage area network), 40 lock pick sets, 93 lock picking, 92-94 lock shims, 94 locks combination locks, 90 lock picking, 92–94 mechanical locks, 91 perimeter controls, 89–92 programmable locks, 91-92 tumbler locks, 91 warded locks, 91 logging, 408-409 access logs, 434 audit logs, 434 centralized logging, 518 event logs, 434 system logs, 434 logic bombs, 457-458, 575 logic check, 544 logical attacks, 126 logs, security logs, 434 LOIC (Low Orbit Ion Cannon), 437, 444 Loki program, 221 longest running suppressed patent, 243 lookup tables, 329 loose source routing, 307 loss potential loss, assessing, 595–598 threat analysis, 136 Low Orbit Ion Cannon (LOIC), 437, 444 low-level checks, 149 LPD (Line Printer Daemon), 316 LUC, 263

756 Lucifer

Lucifer, 252 LUN masking, 326 SAN (storage area network), 40 LuzSec, 465

Μ

M of	N Control, 277
MaaS	(Monitoring as a Service), 503
MAC 398-	(mandatory access control), -400
MAC 269	(Message Authentication Code),
macr	o infections, 456, 576
magn	etic stripe readers, 383
MAID disk	(massive array of inactive (s), 608
MAID driv) (massive array of inactive hard es), 513
mail I	oombing, 447
maint plar	taining, BCP (business continuity n), 621–622
maint	enance hooks, 220, 550
malic	ious software threats, 456
AF 4	PTs (advanced persistent threats), 62
ba	ckdoors, 458–459
cri	meware kits, 461–462
log	gic bombs, 457–458
rai	nsomware, 462–463
ro	otkits, 461
Tr	ojans, 458–459
vir	ruses, 456–457
wo	orms, 457
malw	are
an	ti-malware, 509–510
Sa	lity, 578
mana	ged mode, 348
mana	iging
aco	counts, 493–495
	clipping level, 496
ass	sets. See asset management
da	ta. See data management

users, 493-495 controlling access, 495 privileged entities, 495 resource protection, 496 mandates, governance, 58-60 mandatory access control (MAC), 398-400 mandatory vacations, security management, 159 man-in-the middle attack, 288 man-made threats, physical security, 74-75 MANs (metropolitan area networks), 325 mantraps, 85 manual authorization input control, 520 Marconi, Guglielmo, 503 **MARS**, 251 maskable interrupts, 180 massive array of inactive hard drives (MAID), 513, 608 master boot record infection, 456, 576 master license agreements, 50 master mode, 348 maturity levels, CMM (Capability Maturity Model), 559 maximum tolerable downtime (MTD), 598 McCain campaign, security, 348 MD (Message Digest) algorithms, 268-269 MD5, 267-268 mean time between failure (MTBF), 101, 516-517, 606 mean time repair (MTTR), 101 mean time to repair (MTTR), 516-517, 606 mechanical locks, 91 media management, 502-503 media spokesperson, 616-617 media storage, secondary storage, 183

MOM (Means, Opportunity, and Motive)

757

media-rotation strategies, 611-612 meets, 403 Melissa virus, 464 forensics, 479 meme, 576 Memorandum of Understanding (MOU), 118 memory, 177 CAM (content addressable memory), 329 RAM (random access memory), 181 - 182ROM (read-only memory), 182 secondary storage, 183 virtual memory, 184-185 memory addressing, 181 memory cards, 384 memory leaks, 182 memory management systems, 180 memory protection, 189 memory-mapped I/O, 180 mergers, risk management, 119-120 Merkle-Hellman Knapsack, 264 mesh size, fences, 81-84 mesh topology, 321 Message Authentication Code (MAC), 269 message digest, 236 Message Digest (MD) algorithms, 268-269 message privacy, 364-365 Message Security Protocol (MSP), 278 metadata, 35-36 metropolitan area networks (MANs), 325 Microsoft Point-to-Point Encryption (MPPE), 55 The Midnight Skulker, 465 military data classification, 47-48 MIME (Object Security Services), 278 mining, data mining, 35-36 mirrored ports, 330-331

Mitnick, Kevin, 465 mixed law, 125 mobile code, 573-574 mobile devices, 186 mobile sites, 604 mobile system vulnerabilities, 225-226 models access control models. See access control models business reference model, 215 cloud computing models, 504 CMM (Capability Maturity Model), 558-560 CMMI (Capability Maturity Model Integration), 610-611 data reference model, 215 MPM (Modified Prototype Model), 557 network models, 296–297 OSI (Open Systems Interconnection) model. See OSI (Open Systems Interconnection) model, 297–303 TCP/IP. See TCP/IP, 304-317 performance reference model, 215 product security evaluation models, 206 SABSA (Sherwood Applied Business Security Architecture), 215 security models. See security models service component reference model, 215 spiral model, 554-555 SSDLC (security software development lifecycle) model, 432 technical reference model, 215 waterfall model, 554 Zachman model, 215 modes of operation DES (Data Encryption Standard), 252 security, 193-194 Modified Prototype Model (MPM), 557 MOM (Means, Opportunity, and Motive), 466

758 monitor mode

monitor mode, 348

monitoring

access and usage, 408-409 application transactions, 520-521 BCP (business continuity plan), 621-622 IDS (intrusion detection systems), 409-410 anomaly-based IDS engines, 412 behavioral-based IDS, 412 HIDS (host-based intrusion detection systems), 411 NIDS (network-based intrusion detection systems), 410 rule-based IDS, 412 sensor placement, 413 signature-based IDS engines, 411 IPS (intrusion prevention systems), 414 keystroke monitoring, 415–416, 523 NAC (Network Access Control), 414-415 surveillance, 479 monitoring and auditing controls, 518-519 auditing user activities, 519 controlling physical access, 524-525 emanations, 524 keystroke monitoring, 523 monitoring application transactions, 520-521 NAC (Network Access Control), 522 SIEM (security information and event management), 521-522 monitoring and detection, alarm systems, 107-108 Monitoring as a Service (MaaS), 503 Monsegur, Hector, 466

Morris, Robert T., 167, 457

Morris Jr., Robert, 465, 577 Morris Worm, 456, 457 MOSS (MIME Object Security Services), 278 motherboards, 176 motion detectors, 106 MOU (Memorandum of Understanding), 118 MPLS (Multiprotocol Label Switching), 329.337 MPM (Modified Prototype Model), 557 MPPE (Microsoft Point-to-Point Encryption), 55 MS-CHAPv2, 404 MSP (Message Security Protocol), 278 MTBF (mean time between failure), 101, 516-517, 606 MTD (maximum tolerable downtime), 598 MTTR (mean time to repair), 101, 516-517, 606 multifactor, 390 multi-level, security modes of operation, 193 multimode fiber, 324 multipartite virus, 457, 576 multipath solutions, SAN (storage area network), 40 multiple-choice questions, 21 multiprocessor, 178-179 multiprogramming, 178 Multiprotocol Label Switching (MPLS), 329 multistate systems, 194 multitasking, 178

Ν

NAC (Network Access Control), 414–415, 522 naming distinctions, 179 Napoleonic law, 125 NAS (Network Attached Storage), 325 NAS (network attached storage). 38-39 NAT (Network Address Translation), 358 National Computer Security Center), 207 National Information Assurance **Certification and Accreditation** Process (NIACAP), 213 National Institute of Standards and Technology (NIST), 60, 800-37, 213 National Security Agency (NSA), 207 natural disasters facilities, 77 Katrina (hurricane), 600 physical security, 73-74 natural gas, 100 NCSC (National Computer Security Center), 207 NDA (Nondisclosure Agreement), 119, 157, 495 negligence, 483 Nessus, 427-428 Network Access Control. See NAC (Network Access Control) network access control devices, 355 demilitarized zones, 357–358 NAT (Network Address Translation), 358 firewall designs, 359 firewalls, 355 Network Access Control (NAC), 522 network access layer, TCP/IP, 305-306 network access layer controls, TCP/ IP, 283-284 Network Address Translation (NAT), 358

network administrators, 494 Network Attached Storage (NAS), 325 network attached storage (NAS), 38 - 39network database management system, 567 network equipment, 328 bridges, 328 gateways, 333 hubs, 328 mirrored ports, 330 network taps, 330-331 repeaters, 328 routers, 332-333 switches, 329-330 VLANs (virtual LANs), 331 network forensics, 472 Network Information Service (NIS), 315 network layer, OSI (Open Systems Interconnection) model. 300 network models, 296-297 OSI (Open Systems Interconnection) model. 297-298 application layer, 302 data link layer, 299-300 network layer, 300 overview, 302-303 physical layer, 299 presentation layer, 301–302 session layer, 301 transport layer, 300-301 TCP/IP, 313 application layer, 314–317 host-to-host layer. See host-to-host layer Internet layer. See Internet layer network access layer, 305-306 network protection, 607

network security threats, 439

ARP poisoning, 446 botnets, 443-446 database attacks, 446 DDoS attacks, 443 DNS spoofing, 447 DoS attacks, 442-443 mail bombing, 447 pharming attacks, 447 session hijacking, 440 sniffing, 440-441 traffic analysis, 447 war dialing, 447 war driving, 447 wiretapping, 441 zero-day exploits, 447 network standards, 296-297 network storage, 325-326 network taps, 330-331 network topologies, 319 bus topology, 319 fully connected topology, 322 mesh topology, 321 ring topology, 320-321 star topology, 319-320

network-based intrusion detection systems (NIDS), 410, 526–527

networks

802.11 wireless networks. *See* 802.11 wireless networks, 346–348 CANs (campus area networks), 325 de-encapsulation, 304 encapsulation, 303–304 GANs (Global Area Networks), 325 MANs (metropolitan area networks), 325 PAN (personal area networks), 325 SANs (storage area networks), 325 SANs (storage area networks), 325–326 secure network design, 296 WANs (wide area networks). *See* WANs (wide area networks). *See* WANs (wide area networks), 325 neural networks, 570-571 new-hire agreements and policies, 157 **NIACAP** (National Information Assurance Certification and Accreditation Process), 213 NIDS (network-based intrusion detection systems), 410, 526, 526-527 Nimda, 498 NIS (Network Information Service), 315 NIST (National Institute of Standards and Technology), 60 NIST 800-37, 213 NIST 800-53, 145 NIST risk framework, 129 NIST SP 800-14, 166-167 NIST SP 800-34, 589 NIST SP 800-34s, 545 NIST-800-115, 431-432 nonce, 247 nondisclosure agreement (NDA), 119, 157, 495 noninterference model, 199 non-maskable interrupts, 180 nonrepudiation, cryptography, 235-236 NSA (National Security Agency), 207

cryptography, 242

0

OAKLEY Protocol, 283 Object Request Broker (ORB), 566 object reuse, 45 object-oriented analysis and design (OOAD), 566 object-oriented design (OOD), 566 object-oriented programming (OOP), 565–566 object-relational database system, 567

TCB (trusted computer base), 191 obsolete information, 48 OFB (Output Feedback) mode, 254 OFDM (orthogonal frequency division multiplexing), 346 OLA (Operating Level Agreement), 119 OLTP (online transaction processing), 569-570 on-demand backups, 512 one-time pad, stream ciphers, 248 one-time passwords (OTPs), 379-380, 381 online transaction processing (OLTP), 569-570 OOAD (object-oriented analysis and design), 566 OOB (out-of-band) signaling, 508-509 OOD (object-oriented design), 566 OOP (object-oriented programming), 565-566 open networks, VoIP (voice over IP), 344 **Open Source Security Testing** Methodology Manual (OSSTMM), 431 open system authentication (OSA), 352 open systems, 192 **Open Systems Interconnection** model. See OSI (Open Systems Interconnection) model **Open Web Application Security** Project, 431 Operating Level Agreement (OLA), 119 operating states, security management, 194-195 operational security incidents, responding to, 530 operations and maintenance, SDLC (System Development Life Cycle), 552-553 operations management, 553 operations recovery, 606–608

objects, 376

optical media, 183 Orange Book, 500 TCSEC (Trusted Computer System Evaluation Criteria), 207-209 trusted recovery, 500-501 orange box, phreakers, 508 ORB (Object Request Broker), 566 organization processes, risk management, 119-120 organizational unique identifier (OUI), 305 organized crime members, 436 organizing, data, 35 orthogonal frequency division multiplexing (OFDM), 346 OSA (open system authentication), 352 **OSI (Open Systems Interconnection)** model, 297-298 application layer, 302 data link layer, 299-300 network layer, 300 overview, 302-303 physical layer, 299 presentation layer, 301–302 session layer, 301 transport layer, 300-301 OSI Layer 2, 329-330 **OSPF** (Open Shortest Path First), 335 **OSSTMM** (Open Source Security Testing Methodology Manual), 431 OTPs (one-time passwords), 381 OUI (organizational unique identifier), 305 outbound dialing systems, 615-616 out-of-band, 242 output controls, 520, 521 Output Feedback mode, 254 outsider testing, 429 outsiders, threat actors, 435 ownership data governance policies, 31

data ownership, 33-34

762 PaaS (Platform-as-a-Service)

Ρ

PaaS (Platform-as-a-Service), 342, 503

packers, 459–460

packet filters, 355–356, 359 packet switching, WANs (wide area networks), 336 ATM (asynchronous transfer mode),

337 Frame Relay, 337 X.25, 336

PACs (Privilege Attribute Certificates), 396

PAIN (privacy, authentication, integrity, and nonrepudiation), 235

palm scans, 97, 387

PAN (personal area networks), 325 panic bars, 79 PAO (public affairs officer), 616 PAP (Password Authentication Protocol), 360, 404 parallel operations, 553

parallel tests, 552 BCP (business continuity plan), 620

Pass the Hash. 449–450

passive infrared sensors, 107

passive sniffing, 440

passphrases, 379

password aging, 379

password attacks, 449-450

brute-force crack, 451 dictionary crack, 450–451 rainbow tables, 452

password attempts, 379

Password Authentication Protocol (PAP), 360, 404 password complexity, 378–379 password composition, 378

password guessing, 449

password history, 379

password length, 378

password management, 391 password sharing, 449 password storage, 379 password synchronization, 374, 391 passwords, 377-379 assisted password reset, 391 cognitive passwords, 380 dynamic passwords, 379-380 password synchronization, 391 self-service password reset, 391 static passwords, 379-380 PAT (Port Address Translation), 358 patch management, 511 patches, 572 verifying, 511 patents, 34 pattern-based, signature-based IDS engines, 528 payback analysis, 546 payload, steganography, 244 Payment Card Industry Data Security Standard (PCI-DSS), 41, 218 PBX, 507-508 **PCI** (Peripheral Component Interconnect), 184 PCI-DSS (Payment Card Industry Data Security Standard), 41, 218 PCIe (Peripheral Component Interface Express), 184 PDU (protocol data unit), 303, 304 PEAP (Protected EAP), 361 peer-to-peer, 348 PEM (Privacy Enhanced Mail), 278 penetration, 439 penetration test teams, 430 penetration testing, 428-432 generic model of, 430-431 performance reference model, 215 perimeter controls, 83 bollards, 85-86 CCTV (closed-circuit television), 87 fences, 83-84

763 PID (process ID)

gates, 84-85 guards and dogs, 89 lighting, 88-89 lock picking, 92-94 locks, 89-92 perimeter intrusion and detection assessment system (PIDAS), 83 perimeters, security perimeters, 192 Peripheral Component Interconnect (PCI), 184 Peripheral Component Interface Express (PCIe), 184 permanent virtual circuits (PVCs), 337 personal area networks (PAN), 325 personal information, protecting, 121-122 personal information websites, 122 personnel mobilization, BCP (business continuity plan), 615-616 personnel security, implementing, 156-157 personnel security attacks, 126 **PERT (Program Evaluation and** Review Technique), 560 PGP (Pretty Good Privacy), 242, 278, 317 pharming attacks, 447 phased changeover, 553 phishing, 454 photoelectric sensors, 107 phreakers, 127, 345-346, 508, 508-509 FEMA (Federal Emergency Management Administration), 508 phreaking, Van Eck phreaking, 524 physical access controlling, 524-525 password attacks, 449 physical controls, 155 physical destruction, 503 physical layer, OSI (Open Systems Interconnection) model, 299

physical port controls, 82 physical security, 72 alarm systems, 106 IDS (intrusion detection systems), 106 - 107monitoring and detection, 107 - 108disaster recovery, 534 equipment lifecycle, 101 facilities, 76 area concerns, 77-78 asset placement, 82 construction, 78 **CPTED** (Crime Prevention Through Environmental Design), 76–77 electrical power, 99-100 employee access control. See employee access control environmental controls, 98 heating, ventilating, and air conditioning, 98-99 location, 78 perimeter controls. See perimeter controls UPS (uninterruptible power supplies), 100 fire prevention, 101–102 fire suppression, 103 fire-detection equipment, 102 - 103water sprinklers, 104-105 man-made threats, 74-75 natural disasters, 73-74 perimeter controls, CCTV (closed-circuit television), 87 physical port controls, 82 risks, 72-73 technical problems, 75 physical security attacks, 126 physical security testing, 429 PIA (privacy impact analysis), 42 picks, 93 PID (process ID), 178-179

764 PIDAS (perimeter intrusion and detection assessment system)

PIDAS (perimeter intrusion and detection assessment system), 83

piggybacking, 85

pilot tests, 551

ping of death, 442

PINs. 377-379

pipelining, 177

piracy, software piracy, 50

PKI (public key infrastructure, 95, 272

CA (Certificate Authority), 272–273 client's role, 276–277 CRL (Certificate Revocation List), 273–274

digital certificates, 274–276

RA (Registration Authority), 273

Plain Old Telephone Service (POTS), 337–338

plaintext, 236, 249

plan design and development, BCP (business continuity plan), 615

employee services, 617 insurance, 617–618

interacting with external groups, 616–617

personnel mobilization, 615-616

Platform-as-a-Service (PaaS), 342, 503

Please Do Not Throw Sausage Pizza Away, 297–298

plenum-grade cable, 324

Point-to-Point Protocol (PPP), 360

Point-to-Point Tunneling Protocol (PPTP), 55, 283

poison reverse, 334-335

policies

data governance policies, 30–31 new-hire agreements and policies, 157 security policies, 150–151 advisory policies, 151 developing/implementing, 149–150 informative policies, 151–152 regulatory policies, 152 polyalphabetic cipher, 238–239 polyinstantiation, OOP (object-oriented programming), 565-566 polymorphic viruses, 457, 576 polymorphism, OOP (object-oriented programming), 565 POP3, 505 Port Address Translation (PAT), 358 port mirroring, 330–331 port-mapped I/O, 180 ports application layer, TCP/IP, 314 physical port controls, 82 TCP/IP, 317 potential loss, assessing, 595-598 POTS (Plain Old Telephone Service), 337-338 power electrical power, 99-100 generators, 100 PP (Protection Profile), 212 PPP (Point-to-Point Protocol), 360 PPTP (Point-to-Point Tunneling Protocol), 55, 283 pre-action, water sprinklers, 104 presentation layer, OSI (Open Systems Interconnection) model, 301-302 pressure sensitive sensors, 106 pretexting, 454 Pretty Good Privacy (PGP), 242, 278, 317 preventative access controls, 155 preventative controls, 550-551 preventing buffer overflows, 574-575 social engineering attacks, 496 PRI (Primary Rate Interface), 338 primary images, 478 primary keys, databases, 568

Primary Rate Interface (PRI), 338

principle, Kerberos, 394 principle of least privilege, 374-375, 495 print servers, 186 priorities, criticality prioritization, 594 privacy cryptography, 235 HIPAA (Health Insurance Portability and Accountability Act), 58–59 message privacy, 364-365 privacy controls, 43 Privacy Enhanced Mail (PEM), 278 privacy impact assessment, 42-43 privacy laws, 121-122 private, public/private data classification, 48 private key cryptography, 259 Privilege Attribute Certificates (PACs), 396 privilege creep, 448-449 privileged entities, 495 privileged mode, 188 probabilistic risk assessment, 130 probalistic approach, knowledge extraction, 37 problem mode, 188 problem state, CPU (central processing unit), 177 procedures forensics, 473 risk management, 153 process activation, 189 process activity, 179 process control, 218, 520 process ID (PID), 178-179 process isolation, 195–196 process isolation techniques, 179 process spoofing, 453 processes audit processes, 37-38 change control process, 561–562

data governance policies, 31 incident response, 469-470 processor speed, 178 product security evaluation models, 206 ITSEC (Information Technology Security Evaluation Criteria), 210 Rainbow Series, 207 professional ethics, 163-164 profile management, 391 Program Evaluation and Review Technique (PERT), 560 programmable locks, 91-92 programmed I/O, 180 programming languages, 562–565 ActiveX, 564 C, 564 C#, 564 C+, 564 C++, 564 COBOL (Common Business Oriented Language), 564 FORTRAN, 564 HTML, 564 Java, 564 Ruby, 564 scripting languages, 565 Visual Basic, 564 XML (Extensible Markup Language), 565 project initiation, SDLC (System Development Life Cycle), 546–547 project management, BCP (business continuity plan), 591–593 promiscuous mode, 440 Protected EAP (PEAP), 361 protection of data, 28 intellectual property, 121 resources, 496 protection of personal information, 121-122 Protection Profile (PP), 212 protection rings, 187–189

protocol data unit (PDU), 303, 304 protocol translators, 333 protocol-based, anomaly-based IDS engines, 528 protocols ARP (Address Resolution Protocol), 306.310 BootP (Bootstrap Protocol), 315 CHAP (Challenge Handshake Authentication Protocol), 360.404 communication protocols, 318-319 distance-vector protocols, 334 DNS (Domain Name Service), 315 EAP (Extensible Authentication Protocol), 360–361, 404 EGP (Exterior Gateway Protocol), 336 Ethernet II protocol, 318 exterior gateway protocols, 336 FTP (File Transfer Protocol), 314 HTTP (Hypertext Transfer Protocol), 315-316 ICMP, 306 ICMP (Internet Control Message Protocol), 309-310 IGMP (Internet Group Management Protocol), 310-311 IGRP (Internet Gateway Routing Protocol). See IGRP (Internet Gateway Routing Protocol) IMAP (Internet Message Authentication Protocol), 316 IP (Internet Protocol), 306–309 LDAP (Lightweight Directory Access Protocol), 316, 404 Line Printer Daemon, 316 link-state protocols, 335 MS-CHAPv2, 404 OSPF (Open Shortest Path First), 335 PAP (Password Authentication Protocol), 360, 404 PGP (Pretty Good Privacy), 317 PPP (Point-to-Point Protocol), 360

RIP (Routing Information Protocol), 316 - 317RIPsplit horizon, 334–335 routed protocols, 333 routing protocols, 333-334, 335 SMTP (Simple Mail Transfer Protocol), 314-315 SNMP (Simple Network Management Protocol), 316 SSL (Secure Sockets Layer), 316 STP (Spanning Tree Protocol), 331 TCP (Transmission Control Protocol), 312-313 Telnet, 314 TFTP (Trivial File Transfer Protocol), 315 trunking protocols, 331 UDP (User Datagram Protocol), 313 prototyping, development methods, 556-557 proxy servers, 356-357 pseudorandom, 247 public, public/private data classification, 48 public affairs officer (PAO), 616 public key cryptography, 259 public key encryption, 260-261 public key infrastructure. See PKI (public key infrastructure) public-key cryptosystem, 265 public/private data classification, 48 PVCs (permanent virtual circuits), 337 Q

QoS (quality of service), VoIP (voice over IP), 343

qualitative assessment, 596-597

versus quantitative assessments, 145–146

qualitative ranking, 597

quality assurance specialists, 493

Redundant Array of Inexpensive Disks (RAID)

quantitative assessments

versus qualitative assessment, 145–146

risk assessment, 139-142

quantum cryptography, 242

question-handling strategies, 24-25

questionnaires, BIA (business impact analysis), 595–597

questions

drag and drop questions, 21 hotspot question format, 22–23 multiple-choice questions, 21

R

RA (Registration Authority), 273 race conditions, 220 RAD (Rapid Application Development), 556 radio frequency interference (RFI), 99 Radio Shack, 154 **RADIUS** (remote authentication dial-in user service), 362, 404-405 **RAID** (Redundant Array of Inexpensive Disks), 514-516, 606-607 Rainbow Series, 207 Orange Book, 207–209 Red Book. 209 rainbow tables, 452 RAIT (redundant array of independent tapes), 513 raking, 93 RAM (random access memory), 181-182 RAM-resident, 576–577 random access memory (RAM), 181-182 range check, 544 ransomware, 462-463 **Rapid Application Development** (RAD). 556 **Rapid Spanning Tree Protocol** (RSTP), 331

RAT (remote access Trojan), 458 **RBAC** (role-based access controls), 401-402 RC2. 258 RC4 (Rivest Cipher 4), 251, 258-259 WEP (Wired Equivalent Privacy), 352 RC5 (Rivest Cipher 5), 251, 259 RC6. 259 **RDBMS** (relational database management system), 567 read-only memory (ROM), 182 ready state, CPU (central processing unit), 177 realms, Kerberos, 393 reasonably prudent person rule, 497 reciprocal agreements, facility and supply recovery, 604-605 reciprocation, social engineering, 163 recovery access controls, 155 recovery controls, 516-518 recovery point objective (RPO), 613 recovery procedures, 195 recovery strategies, BCP (business continuity plan), 599-600 backup and restoration, 609-611 business process recovery, 600-601 data and information recovery, 608-609 facility and supply recovery, 601 operations recovery, 606-608 user recovery, 605 recovery time objective (RTO), 613 recovery times, 610 Red Book, 209 red box, phreakers, 508 red teams, 430 Reduced Instruction Set Computing (RISC), 178 redundancy (location), SAN (storage area network), 40 Redundant Array of Inexpensive Disks (RAID), 514-516

redundant array of independent tapes (RAIT), 513 redundant routing, 607 redundant sites, 603-604 reference monitors, TCB (trusted computer base), 189-191 referential integrity, 569 Regional Internet Registry (RIR), 333 Registration Authority (RA), 273 regression tests, 552 regulatory compliance, 218 regulatory law, 124 regulatory policies, 152 regulatory requirements, ethics, 167-168 relation, databases, 568 relational database management system (RDBMS), 567 relative addressing, 181 religious law, 125 remote access, 502 CHAP (Challenge Handshake Authentication Protocol), 360 EAP (Extensible Authentication Protocol), 360–361 PAP (Password Authentication Protocol), 360 PPP (Point-to-Point Protocol), 360 remote access Trojan (RAT), 458 remote authentication dial-in user service (RADIUS), 362 remote journaling, 612 remote meetings, 365 removable media, endpoint security, 56 repeaters, 328 replay attack, 288 reports, risk management teams, 148 reputation, 599 residual information, 554 resource protection, 496 resources, governance, 58-60

international resources, 61-63 United States, 60-61 responding to operational security incidents, 530 responsibilities BCP (business continuity plan), 622 data custodians, 34-35 data ownership, 33–34 data security, 32-33 restoration from backups, 609-611 results, incident response, 470-471 retina patterns, 388 retina scans, 97 reverse engineering, 551 **RFC** (Request for Comments), 165-166 RFI (radio frequency interference), 99 **RFID tags**, 95–96 Rijndael, 251, 257, 258 ring topology, 320-321 **RIP** (Routing Information Protocol), 316-317, 334-335 **RIR (Regional Internet Registry), 333 RISC (Reduced Instruction Set** Computing), 178 risk defined, 130 exposed risk, 138 risk acceptance, 146 risk assessment, 130-133 counter measure selection, 146-149 qualitative assessment, 142-146 quantitative assessments, 139-142 security policies, developing/ implementing, 149–150 risk avoidance, 137 risk factor analysis, 130 risk management, 117, 128 asset identification and valuation, 133-135 baselines, 152 frameworks, 129-130

guidelines, 153 organization processes, 119-120 procedures, 153 risk assessment, 130-133 counter measure selection, 146 - 149security policies, 150–151 standards, 152 threat analysis, 135-139 risk management teams, 131-132 reports, 148 risk matrix, 149 risk mitigation, 147 risk registers, 130 risk tolerance, 147 risk transference, 147 risks, physical security, 72-73 Rivest cipher, 258-259 rogue security software, 463 role-based access control (RBAC), 401-402 roles data custodians, 34-35 data ownership, 33-34 data security, 32-33 rollback plans, 499 ROM (read-only memory), 182 rootkits, 461 ROT3, 237 rotation cipher, 237 routed protocols, 333 routers, 332-333 routing, 332 alternate routing, 607 diverse routing, 607 routing by rumor, 334 Routing Information Protocol (RIP), 316-317 routing protocols, 333-334, 335 Royce, Winston, 554 RPO (recovery point objective), 613 RSA, 262–263 RSTP (Rapid Spanning Tree Protocol), 331 RTM worm, 577 RTO (recovery time objective), 613 rubber hose attack, 288 Ruby, 564 rule-based access controls, 402, 412 rule-based IDS, 528–529 running key cipher, 241

S

SA (Security Association), 282 SaaS (Software-as-a-Service), 341, 504 SABSA (Sherwood Applied Business Security Architecture), 215 SAFER (Secure and Fast Encryption Routine), 251 salami attacks, 575 Sality, 578 salvage teams, 533-534 SAML (Security Association Markup Language), 377 SAN (storage area network), 38–41, 613 SAN snapshots, 40, 326 sandboxes, 509 sanitization, 44, 502 SANs (storage area networks), 325-326, 513-514 Sarbanes-Oxley Act (SOX), 60, 168, 497 SAS 70 report, 119 SASD (sequential access storage device), 513 SATA (Serial ATA), 184 **SATAN (Security Administrator Tool** for Analyzing Networks), 164 scanning, 438 scarcity, social engineering, 162 scheduling, tasks, 560-561

770 schemas, databases

schemas, databases, 568 scoping, 58 screened host firewalls, 359 screened hosts, 357-358, 359 script kiddies, 127, 435 scripting languages, 565 scrubbing, 93 scrum, 558 SCSI (Small Computer Systems Interface), 184 scytale, 237 SDL (Security Development Lifecycle), 545 SDLC (Synchronous Data Link Control), 341 SDLC (System Development Life Cycle), 545-546 acceptance testing and implementation, 551–552 disposal, 553 functional requirements and planning, 547–548 operations and maintenance, 552-553 project initiation, 546-547 separation of duties, 550 software design specifications, 548 software development and build, 549-551 SDRAM (synchronous DRAM), 182 SDSL (symmetric digital subscriber line), 340 sealing configurations, 53 secondary evidence, 482 secondary storage, 183 secret, military data classification, 47 Secure Electronic Transaction (SET), 280 Secure European System and Applications in a Multivendor Environment (SESAME), 396 Secure FTP (SFTP), 280

secure hashing algorithms (SHA), 269 Secure Hypertext Transfer Protocol (S-HTTP), 280 Secure Multipurpose Internet Mail Extensions (S/MIME), 278 secure network design, 296 secure real-time transport protocol (SRTP), 344 Secure Shell (SSH), 280, 440 Secure Socket Tunneling Protocol (SSTP), 281 Secure Sockets Layer (SSL), 281.316 secure storage management and replication, SAN (storage area network), 40 Secure Trusted Operating Program (STOP), 194 security asset security, 28 availability, 29 baselines, 57-58 CIA (confidentiality, integrity, and availability), 28 confidentiality, 28 data governance policies, 30-31 data security. See data security governance, 214-215 guidelines, 214-215 integrity, 29 modes of operation, 193–194 operating states, 194-195 physical security, 72 facilities. See facilities man-made threats, 74-75 natural disasters, 73-74 risks, 72-73 technical problems, 75 roles and responsibilities, 32-33 security governance, third party governance, 118-119 of software environments, 571-573

Security Administrator Tool for Analyzing Networks (SATAN), 164 security advisory groups, roles and responsibilities, 32 security and risk management domains, 116 security architects, 494 security architecture, 187 closed systems, 192 open systems, 192 protection rings, 187-189 TCB (trusted computer base), 189-192 vulnerability, 218 back doors, 220 buffer overflows, 219-220 covert channels, 220-221 emanations, 222-223 incremental attacks, 221-222 mobile system vulnerabilities, 225-226 state attacks, 220 web-based vulnerabilities, 223-225 security assessments audits, 426-427 penetration testing, 428-432 vulnerability assessments, 427-428 Security Association Markup Language (SAML), 377 Security Association (SA), 282 security awareness, 161–162 security checkpoints, 88-89 Security Development Lifecycle (SDL), 545 Security DNS (DNSSEC), 315 Security Event Management (SEM), 414. 522 security governance, 116-117 third party governance, 118-119 security information and event management (SIEM), 521-522

Security Information Management (SIM), 414, 522 security kernels, 191 security labels, reference monitors, 191 security logs, 434 security management awareness, 161-162 computer crime and hackers, 125 - 128ethics, 163-164 common computer ethics fallacies, 167 Computer Ethics Institute, 165 IAB (Internet Architecture Board), 165-166 ISC2, 164 NIST SP 800-14, 166 - 167regulatory requirements, 167 - 168governance, 116-117 international law, 124-125 job rotation, 158 laws, 123 common law, 123 least privilege, 158-159 mandatory vacations, 159 new-hire agreements and policies, 157 personnel security, implementing, 156-157 privacy laws, 121–122 protection of intellectual property, 121 protection of personal information, 121-122 risk assessment, 132–133 separation of duties, 157 sexual harassment, 128 social engineering, 162-163 termination, 159-160 training, 160-161

772 security models

security models, 176, 196-197

Bell-LaPadula model, 199–201 Biba model, 202-203 Brewer and Nash model, 205 Clark-Wilson model, 204 confidentiality, 199 CPU (central processing unit), 176 - 180Graham Denning model, 205 Harrison-Ruzzo-Ullman model, 205information flow model, 199 integrity, 202 I/O bus standards, 183-184 Lattice model, 205-206 Lipner model, 205 noninterference model, 199 product security evaluation models. See product security evaluation models state machine model, 197-199 storage media, 181 Take-Grant model, 205 Security Parameter Index (SPI), 282 security perimeters, 192 security policies, 150-151 advisory policies, 151 developing/implementing, 149 - 150informative policies, 151–152 regulatory policies, 152 security software development lifecycle (SSDLC) model, 432 Security Target (ST), 212 security teams, 534 security threats. See threats Security-Enhanced Linux, 195 SEDs (self-encrypting hard drives), 53-54 self-service password reset, 391 SEM (Security Event Management), 414, 522 semantic integrity, 569

senior management BCP (business continuity plan), project management and initiation, 591-593 roles and responsibilities, 32 sensitive but unclassified or restricted military data classification, 47 public/private data classification, 48 sensitivity, 48 data governance policies, 31 sensitivity labels, 400 sensor placement, IDS (intrusion detection systems), 413, 529 separation of duties, 157-158, 401, 494 SDLC (System Development Life Cycle), 550 sequence check, 543 sequential access storage device (SASD), 513 sequential storage, 183 Serial ATA (SATA), 184 server rooms, 82 service component reference model, 215 service packs, 572 Service Provisioning Markup Language (SPML), 392 Service Set ID (SSID), 351 service-level agreements (SLAs), 75, 101, 118, 606 service-oriented architecture (SOA), 392 SESAME (Secure European System and Applications in a Multivendor Environment), 396 session hijacking, 440 session keys, 265 session layer, OSI (Open Systems Interconnection) model, 301 SET (Secure Electronic Transaction), 280 sexual harassment, 128

773 SOA (service-oriented architecture)

SFTP (Secure FTP), 280

- SHA (secure hashing algorithms), 269
- SHA-1, 269
- SHA-2, 269
- SHA-3, 269

shared key authentication (SKA), 352

Sherwood Applied Business Security Architecture (SABSA), 215

shielded twisted pair (STP), 322–323

- shoulder surfing, 453
- shrink-wrap license agreements, 51

S-HTTP (Secure Hypertext Transfer Protocol (S-HTTP), 280

- side channel attack, 288
- SIEM, 414

SIEM (security information and event management), 521–522

signature scanning, 509

signature-based, anomaly-based IDS engines, 528

signature-based IDS engines, 411, 528

signatures, 577

digital signatures. *See* digital signatures

- signing speeds, 271
- silent hostage alarms, 95

SIM (Security Information Management), 414, 522

simple integrity property, 202

Simple Key Management for Internet Protocol (SKIP), 283

Simple Mail Transfer Protocol (SMTP), 314–315, 504

Simple Network Management Protocol (SNMP), 316

simple security property (ss property), 199–200

simple tape-rotation schemes, 611

simplex, 327

simulation, BCP (business continuity plan), 620

single loss expectancy (SLE), 139

single point of failure (SPOF), 195-196. 517 single sign-on (SSO), 374, 392-393 Kerberos, 393-396 SESAME (Secure European System and Applications in a Multivendor Environment), 396 single-mode fiber, 324 single-state systems, 194 single-use passwords, 379-380 SKA (shared key authentication), 352 skilled hackers, 436 SKIP (Simple Key Management for Internet Protocol), 283 Skipjack, 251 slamming, 509 SLAs (service-level agreements), 75, 101, 118, 606 SLDC (System Development Life Cycle), 545 SLE (single loss expectancy), 139 Small Computer Systems Interface (SCSI), 184 smart cards, 95, 383 smartphones, 186 SMDS (Switched Multimegabit Data Service), 341 S/MIME (Secure Multipurpose Internet Mail Extensions), 278 smishing, 454 SMTP (Simple Mail Transfer Protocol), 314-315, 357, 504 smurf, 442 SNIA (Storage Network Industry Association), 39 sniffers, 440 sniffing, 440-441 sniffing password hashes, 449-450 **SNMP (Simple Network Management** Protocol), 316 Snowden, Edward, 286 SOA (service-oriented architecture), 392

774 sociability tests

sociability tests, 552 social engineering, 176 preventing attacks, 496 security management, 162-163 social engineering attacks, 126, 454-455 techniques for, 455 social engineering testing, 429 social networking, background checks, 157 social validation, social engineering, 163 social-based threats, 454-455 **SOCKS**, 357 software design specifications, SDLC (System Development Life Cycle), 548 software development, 542-543 agile development methods, 557-558 CASE (Computer-Aided Software Engineering), 557 change control process, 561-562 CMM (Capability Maturity Model), 558-560 CMMI (Capability Maturity Model Integration), 610-611 CORBA (Common Object Request Broker Architecture), 566 development methods, 554 JAD (Joint Application Development), 555–556 MPM (Modified Prototype Model), 557 prototyping, 556–557 RAD (Rapid Application Development), 556 spiral model, 554-555 waterfall model, 554 OOP (object-oriented programming), 565–566 programming languages, 562-565 scheduling, tasks, 560-561

SDLC (System Development Life Cycle) acceptance testing and implementation, 551-552 disposal, 553 functional requirements and planning, 547-548 operations and maintenance, 552-553 project initiation, 546-547 software design specifications, 548 software development and build phase, 549-551 security, 571-573 software development and build phase, SDLC (System Development Life Cycle), 549-551 software encryption, 54 software forensics, 472 Software IP Encryption (SwIPe), 283 software keystroke loggers, 416, 523 software licensing, 50-51, 183 software piracy, 50 Software-as-a-Service (SaaS), 341, 504 something you are (Type 3), authentication, 376, 385-390 something you have (Type 2), authentication, 376, 381 asynchronous token devices, 382-383 cards, 383-384 certificates, 384-385 synchronous tokens, 381-382 something you know (Type 1), 377-379 authentication, 376 SONET (Synchronous Optical networking), 336 SOX (Sarbanes-Oxley Act), 60, 168, 497 spam, 457 Spam over Internet Telephony (SPIT), 344 Spanning Tree Protocol (STP), 331

775 strong authentication

sparse infectors, 576-577 spear phishing, 454 SPI (Security Parameter Index), 282 spiral model, 554-555 SPIT (Spam over Internet Telephony), 344 SPML (Service Provisioning Markup Language), 392 SPOF (single point of failure), 195-196, 517 spokespersons, 616-617 spoofing, 453 spread-spectrum technology, 346 SQL injection. 224-225 SRAM (Static Random Access Memory), 181 SRTP (secure real-time transport protocol), 344 SSD (static separation of duty), 401 SSDLC (security software development lifecycle) model, 432 SSH (Secure Shell), 280, 440 SSID (Service Set ID), 351 SSL (Secure Sockets Layer), 281, 316 SSO (single sign-on), 374, 392-393 SSTP (Secure Socket Tunneling Protocol), 281 ST (Security Target), 212 standards Common Criteria, 210–212 communication, 327 data standards, 37–140 governance, 58-60 I/O bus standards, 183–184 network standards, 296–297 risk management, 152 wireless standards, 348-349 WLANs (wireless LANs), 349 standby lighting, 88 star * security property, 200 star topology, 319-320 start * integrity property, 202

state attacks, 220 state machine model, 197-199 stateful firewalls, 356 static NAT, 358 static passwords, 379-380 Static Random Access Memory (SRAM), 181 static routing, 334 static separation of duty (SSD), 401 static WEP. 352 statistical approach, knowledge extraction, 37 statistical based, anomaly-based IDS engines, 528 steganography, 243-244 digital watermarks, 245-246 steganography operations, 244-245 stegomedium, 244 Stoll, Clifford, 466 STOP (Secure Trusted Operating Program), 194 storage data storage. See data storage network storage, 325-326 storage area networks (SANs), 325-326 storage media, 181 RAM (random access memory), 181-182 ROM (read-only memory), 182 **Storage Network Industry Association** (SNIA), 39 store-and-forward switches, 330 STP (shielded twisted pair), 322–323 STP (Spanning Tree Protocol), 331 strategies for taking exams, 24-25 question-handling strategies, 24-25 stream ciphers, 237, 240, 248 boolean operators, 248 strict source routing, 307 striping, 606-607 strong authentication, 390

776 strong star * property

strong star * property, 200 structured walkthrough, BCP (business continuity plan), 620 subjects, 375 TCB (trusted computer base), 191 subscription services, 601-603 substitution box (s-box), 248 superscalar processors, 178 supervisor state, CPU (central processing unit), 177 supplicant, 362 supplies teams, 534 suppressing fires, 101–102 surveillance, 479 SVCs (switched virtual circuits), 337 swap partitions, 185 SwIPe (Software IP Encryption), 283 Switched Multimegabit Data Service (SMDS), 341 switched virtual circuits (SVCs), 337 switches, 329-330 application switches, 330 content switches, 330 content-services switches, 330 higher-layer switches, 330 symmetric algorithms, 247, 250–251 symmetric cryptography, 236 symmetric digital subscriber line (SDSL), 340 symmetric encryption, 237, 249-252, 272 versus asymmetric encryption, 264-265 block ciphers, 247-248 confidentiality, 250 stream ciphers, 248 symmetric keys, distribution of, 249-250 symmetric mode, 178-179 symmetric substitution ciphers, 240 SYN flood, 442

Synchronous Data Link Control (SDLC), 341 Synchronous DRAM (SDRAM), 182 Synchronous optical networking (SONET), 336 synchronous replication, 611 synchronous tokens, 381-382 synthetic transactions, 434 system analysts, 494 System Cold Start, 195 Orange Book, 501 System Compromise, 195 system development. See software development System Development Life Cycle (SLDC). See SDLC (System Development Life Cycle) system failures avoiding, 543, 544 checks and application controls, 543-544 recovery procedures, 195 system hardening, 497-498 system high, security modes of operation, 193 system logs, 434 System Reboot, 195 system reboot, Orange Book, 501 system resilience, 511 System Restart, 195 system testing, 551 system validation, 213 certification, 213-214 systems administrators, 493

Т

T1, 339 T3, 339 table lookups, 544 TACACS (Terminal Access Controller Access Control System), 362, 406 TACACS+, 362 tailgating, 85 tailoring, 58 Take-Grant model, 205 tamper protection, 108 tangible assets, 496 tape backups, 611 tape rotation methods, 513 Target of Evaluation (TOE), 210 task-based access control (TBAC), 402 tasks, scheduling, 560-561 TBAC (task-based access control), 402 T-carriers, 338-339 TCB (trusted computer base), 189-192 reference monitors, 189-191 TCP (Transmission Control Protocol), 311, 312-313 comparing to UDP, 313 **TCP/IP**, 313 application layer, 314–317 host-to-host layer, 311 TCP (Transmission Control Protocol), 312–313 UDP (User Datagram Protocol), 313 Internet layer, 306 ARP (Address Resolution Protocol), 310 ICMP (Internet Control Message Protocol, 309–310 IGMP (Internet Group Management Protocol), 310-311 IP (Internet Protocol), 306–309 network access layer, 305–306 ports, 317 securing with cryptography, 279 application/process layer controls, 280host to host layer controls, 280-282 Internet layer controls, 282–283 network access layer controls, 283-284

TCSEC (Trusted Computer System Evaluation Criteria), 207, 500 Orange Book, 207-209 teams administrative support teams, 534 BCP (business continuity plan) teams, 591-593 communications teams, 534 coordination teams, 534 damage assessment teams, 534 disaster recovery teams, 533-534 emergency management teams, 534 emergency operations teams, 534 emergency response teams, 534 finance teams, 534 incident response, 468 incident response teams, 534 penetration test teams, 430 risk management teams, 131–132 reports, 148 security teams, 534 supplies teams, 534 transportation teams, 534 teardrop, 442 technical controls, 155 technical problems, physical security, 75 technical reference model, 215 technical support, equipment lifecycle, 52 Tejon Crypter, 460 Telco gear, 472 telecommunication controls, 503 blacklists, 506 cloud computing, 503-504 email, 504-506 fax, 506-507 gravlists, 506 whitelists, 506

778

telecommunications equipment

telecommunications equipment, 328

bridges, 328 gateways, 333 hubs, 328 mirrored ports, 330 network taps, 330–331 repeaters, 328 routers, 332–333 switches, 329–330 VLANs (virtual LANs), 331

Telnet, 305, 314

temperatures, data centers, 98

TEMPEST, 222, 524

Temporal Key Integrity Protocol (TKIP), 353

tension wrenches, 93

Terminal Access Controller Access Control System (TACACS), 362

terminated employees

data access, 33 security management, 159–160

terrorism, physical security, 74

test classifications, 550-551

test types, 551-552

testing

application security testing, 429 BCP (business continuity plan), 619-621 blackbox testing, 428 blind tests, 429 denial-of-service (DoS) testing, 429 garbage in, garbage out testing, 552 graybox testing, 428 importance of, 435 interface testing, 551 outsider testing, 429 penetration testing, 428-432 physical security testing, 429 social engineering testing, 429 system testing, 551 unit testing, 551 war dialing, 429

whitebox testing, 428 wireless network testing, 429 testing techniques, 432-435 tests alpha tests, 551 blackbox tests, 552 double-blind tests, 429 final tests, 552 function tests, 552 parallel tests, 552 pilot tests, 551 regression tests, 552 sociability tests, 552 whitebox tests, 552 TFTP (Trivial File Transfer Protocol), 315 TGTs (ticket-granting tickets), 394 theft, physical security, 74 thin clients, 393 third party governance, 118-119 thread, 178-179 threat actors, 435-437 threat agents, 136 threat modeling, 448, 571 threats, 130, 131, 138, 435 access control threats, 448 access aggregation, 448-449 eavesdropping, 453 identity theft, 453-454 password attacks, 449-450 shoulder surfing, 453 spoofing, 453 unauthorized access, 448 analyzing, 135-139 attack methodologies, 437-439 to business operations, 588-589 malicious software threats, 456 APTs (advanced persistent threats), 462 backdoors, 458-459 crimeware kits, 461-462 logic bombs, 457-458

ransomware, 462-463 rootkits, 461 Trojans, 458–459 viruses, 456-457 worms, 457 network security threats, 439 ARP poisoning, 446 botnets, 443-446 database attacks, 446 DDoS (distributed denial of service) attacks, 443 DNS spoofing, 447 DoS attacks, 442-443 mail bombing, 447 pharming attacks, 447 session hijacking, 440 sniffing, 440-441 traffic analysis, 447 war dialing, 447 war driving, 447 wiretapping, 441 zero-day exploits, 447 to physical security, 72-73 social-based threats, 454-455 threat actors, 435-437 Tibetan monks, Biba model, 203 ticket-granting service, KDC (Key Distribution Center), 394 ticket-granting tickets (TGTs), 394 tickets, Kerberos, 393 tidal waves, 73 time multiplexing, 179 time of check (TOC), 220 time of use (TOU), 220 **TKIP** (Temporal Key Integrity Protocol), 353 TLS (Transport Layer Security), 281, 354 **TNI (Trusted Network Interpretation),** 209 TOC (time of check), 220 TOE (Target of Evaluation), 210

token ring, 318-319 tokens, 318-319 asynchronous token devices, 382-383 employee access control, 94-95 reference monitors, 191 synchronous tokens, 381-382 top secret, military data classification, 47 topologies, network topologies, 319 bus topology, 319 fully connected topology, 322 mesh topology, 321 ring topology, 320-321 star topology, 319-320 tornadoes, 73 TOU (time of use), 220 Tower of Hanoi, 612 TP (transformation procedures), 204 TPM (trusted platform module), 53 trace evidence, 482 trade secrets, 34 trademarks, 34 traffic analysis, 447 traffic padding, 285 traffic-based, anomaly-based IDS engines, 528 training BCP (business continuity plan), implementing, 619 ethics. 163-164 security management, 160–161 transaction processing, 569-570 transformation procedures (TP), 204 Transmission Control Protocol. See TCP (Transmission Control Protocol) transport and tunnel modes, 283 transport layer, OSI (Open Systems Interconnection) model, 300-301 Transport Layer Security (TLS), 281 transport layer security (TLS), 354 transport mode, IPSec, 363 transportation teams, 534

780 transposition ciphers

transposition ciphers, 240 trap doors, 260-261 trials, for crimes, 482-483 Triangle Shirtwaist factory, 79 Triple-DES (3DES), 255-257 Trivial File Transfer Protocol (TFTP), 315 Trojans, 458-459 tropical cyclones, 73 trunking protocols, 331 trusted computer base (TCB), 189-192 **Trusted Computer System Evaluation** Criteria (TCSEC), 207, 500 Trusted Network Interpretation (TNI), 209 trusted platform modules (TPM), 53 trusted recovery, 500-501 TrustedBSD, 195 tsunamis, 73 tubular picks, 93-94 tumbler locks, 91 tumbling, 345-346 tunnel mode, IPSec, 363 tunnels Host-to-LAN tunnels, 55 LAN-to-LAN tunnels, 55 tuple, databases, 568 turnstiles. 85 twisted pair, 322-323 Twofish. 250 Type I errors, 386 Type II errors, 386 typhoons, 73

U

UA (Uptime Agreement), 119 UDIs (unconstrained data items), 204 UDP (User Datagram Protocol), 311, 313 comparing to TCP, 313 **UEFI (Unified Extensible Firmware** Interface), 182 unauthorized access. 448 unauthorized phone use, VoIP (voice over IP), 344 uncappers, 340 unclassified or official, military data classification, 47 unconstrained data items (UDIs), 204 unicode encoding, 223 **Unified Extensible Firmware Interface** (UEFI). 182 uninterruptible power supply (UPS), 100 unit testing, 551 United States laws, 123-124 methods government can use to defeat encryption, 286 privacy laws, 122 United States resources, 60-61 United States Securities Act of 1933, 496-497 unshielded twisted pair (UTP), 322-323 UPS (uninterruptible power supplies), 100 Uptime Agreement (UA), 119 URL encoding, 223 U.S. Child Pornography Prevention Act of 1996, 123 U.S. Patriot Act of 2001, 123 usage patterns, monitoring, 408-409 **USB**, 82 user activities, auditing, 519 User Datagram Protocol. See UDP (User Datagram Protocol) user mode, 188

user provisioning, 391 user recovery, 605 user spoofing, 453 users managing, 493-495 controlling access, 495 privileged entities, 495 resource protection, 496 roles and responsibilities, 32 terminated employees, data access, 33 utilities, facilities, 77 utility loss, physical security, 75 UTP (unshielded twisted pair), 322-323

V

vacations, mandatory vacations, 159 validity check, 544 Van Eck phreaking, 222, 524 vandalism, physical security, 74 Venema, Wietse, 427 ventilating, facilities, 98-99 verifying, patches, 511 Vernam, Gilbert, 241-242 Vernam cipher, 241-242 vertical privilege escalation, 439 very high data rate digital subscriber line (VDSL), 340 vibration sensors, 106 views, databases, 568 Vigenere cipher, 238–239 virtual LANs (VLANs), 329 virtual machines, 184-185 virtual mapping, 179 virtual memory, 184-185 virtual private networks (VPNs), 55 virtual SAN (VSAN), 39

virtualization, 185 viruses, 456-457, 576-577 fast infection viruses, 576-577 I Love You virus, 464 Melissa virus, 464 forensics, 479 RAM-resident, 576–577 visibility, facilities, 77-78 Visual Basic, 564 VLAN hopping, 331 VLANs (virtual LANs), 329, 331 voice communication recovery, 607 voice recognition, 388 VoIP (voice over IP), 343 QoS (quality of service), 343 UDP (User Datagram Protocol), 313 vulnerability, 343-344 VPNs (virtual private networks), 55 VSAN (virtual SAN), 39 vulnerability, 130, 131, 138 security architecture, 218 back doors, 220 buffer overflows, 219-220 covert channels, 220-221 emanations, 222-223 incremental attacks, 221-222 mobile system vulnerabilities, 225-226 state attacks, 220 web-based vulnerabilities. 223-225 VoIP (voice over IP), 343-344 vulnerability assessments, 427-428 BIA (business impact analysis), 595 vulnerability scanners, 427-428

W

wait state, CPU (central processing unit), 177 walls, 79–81

WANs (wide area networks), 325, 336

circuit switching, 337 cable modems, 340-341 DSL (digital subscriber line), 339-340 ISDN (Integrated Services Digital Network), 338 POTS (Plain Old Telephone Service), 338 T-carriers, 338-339 HDLC (High-Level data Link Control), 341 high-speed serial interface, 341 packet switching, 336 ATM (asynchronous transfer mode), 337 Frame Relay, 337 X.25, 336 SDLC (Synchronous Data Link Control), 341 SMDS (Switched Multimegabit Data Service), 341 WAP (Wireless Application Protocol), 354 war chalking, 354 war dialing, 429, 447 war driving, 354, 447 warded locks, 91 warm sites, 602 warning banners, 510, 519 Wassenaar Arrangement, 285 water sprinklers, 104-105 waterfall model, 554 watermarks, digital watermarks, 245-246 Watson, 570 web conferencing, 364 web servers, 186 Web Services Security, 392 web-based vulnerabilities, 223-225 websites, personal information websites, 122

Weev, 436 WEP (Wired Equivalent Privacy), 258-259.352 static WEP, 352 Wesson, Rick, 444-445 wet pipes, water sprinklers, 104 whaling, 454 whitebox testing, 428 whitebox tests, 552 whitelists, 506 wide area networks (WANs), 325 Wi-Fi Protected Access (WPA), 353 windows of facilities, 79-81 physical security, 81 wire area networks. See WANs (wide area networks) Wired Equivalent Privacy (WEP), 258-259, 352 static WEP, 352 wireless access points, 351 Wireless Application Protocol (WAP), 354 wireless devices, 347 wireless LANs (WLANs), 347 components of, 351 standards, 349 wireless markup language (WML), 354 wireless network testing, 429 wireless networking cards, 351 wireless networks, topologies, 348 wireless PANs (WPANs), 325, 349 wireless protection mechanisms, 352-354 wireless sniffers, 351 wireless standards, 348-349 wireless topologies, 348 Wireless Transport Layer Security (WTLS), 281-282

wiretapping, 441 WLANs (wireless LANs), 347 components of, 351 standards, 349 WML (wireless markup language), 354 work factor, 286, 288 work recovery time (WRT), 615 workflow, business process recovery, 600-601 worms, 457, 577-578 WPA (Wi-Fi Protected Access), 353 WPA2-Enterprise, 284 WPANs (wireless PANs), 325, 349 wrappers, 459 WRT (work recovery time), 615 WTLS (Wireless Transport Layer Security), 281-282, 354

X-Y

X.25, 336 X.509 certificate, 275, 385 XML (Extensible Markup Language), 392, 565 XOR (exclusive-or), 352 XP (extreme programming), 558 XSS (cross-site scripting), 223 XTACACS (Extended TACACS), 406 XTR, 263 XTS-400, 194

Z

Zachman Framework, 214–215 Zachman model, 215 zero knowledge proof, 260 zero-day exploits, 447 zeroization, 44, 502 ZigBee, 350 Zimmermann, Phil, 278