

EXAM ✓ CRAM

CISSP[®]

Fifth Edition



Cram
Sheet



Flash
Cards



Practice
Tests



MICHAEL GREGG

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



EXAM ✓ **CRAM**

**CISSP[®] Exam
Cram**

Fifth Edition

Michael Gregg

CISSP® Exam Cram, Fifth Edition

Copyright © 2021 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

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: 978-0-13-741955-5

ISBN-10: 0-13-741955-4

Library of Congress Control Number: 2021907884

ScoutAutomatedPrintCode

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

Director, ITP Product Management

Brett Bartow

Executive Editor

James Manly

Development Editor

Christopher A.
Cleveland

Managing Editor

Sandra Schroeder

Project Editor

Mandie Frank

Copy Editor

Kitty Wilson

Indexer

Ken Johnson

Proofreader

Donna Mulder

Technical Editor

Dr. Dwayne Hodges

Publishing Coordinator

Cindy Teeters

Designer

Chuti Prasertsith

Page Layout

codeMantra

Credits

Figure	Attribution/Credit Line
Figure 3-2	Screenshot of World's Biggest Data Breaches © 2021 Information is Beautiful
Figure 4-13	Screenshot of The Burp Proxy Attack Tool © 2021 PortSwigger Ltd
Figure 4-21	Screenshot of X.509 Certificate © Google LLC
Figure 5-5	Courtesy of Cisco Systems, Inc.
Figure 5-6	Courtesy of Cisco Systems, Inc.
Figure 5-8	Courtesy of Cisco Systems, Inc.
Figure 5-9	Courtesy of Cisco Systems, Inc.
Figure 5-10	Courtesy of Cisco Systems, Inc.
Figure 5-13	Courtesy of Unified IT Services Pvt Ltd
Figure 6-5	Courtesy of Cisco Systems, Inc.
Figure 6-6	Courtesy of Cisco Systems, Inc.
Figure 7-1	Courtesy of Cisco Systems, Inc.
Figure 7-8	Screenshot of Tejon Crypter © Rdgsoft.net
Figure 7-9	Screenshot of Ransomware © 2016 Malware Removal Guides
Figure 8-2	Courtesy of Cisco Systems, Inc.

Contents at a Glance

	Introduction	1
CHAPTER 1	The CISSP Certification Exam	19
CHAPTER 2	Understanding Asset Security	29
CHAPTER 3	Security and Risk Management	69
CHAPTER 4	Security Architecture and Engineering	151
CHAPTER 5	Communications and Network Security	249
CHAPTER 6	Identity and Access Management	341
CHAPTER 7	Security Assessment and Testing	411
CHAPTER 8	Security Operations	467
CHAPTER 9	Software Development Security	559
	Practice Exam I	607
	Practice Exam II	621
	Answers to Practice Exam I	635
	Answers to Practice Exam II	651
	Glossary	667
	Index	705

Table of Contents

Introduction	1
CHAPTER 1:	
The CISSP Certification Exam	19
Introduction	20
Assessing Exam Readiness	20
Exam Topics	21
Taking the Exam	22
Examples of CISSP Test Questions	24
Answer to Multiple-Choice Question	26
Answer to Drag and Drop Question	26
Answer to Hotspot Question	26
Question-Handling Strategies	27
Mastering the Inner Game.	27
Need to Know More?	28
CHAPTER 2:	
Understanding Asset Security	29
Introduction	30
Basic Security Principles	30
Data Management: Determining and Maintaining Ownership	32
Data Governance Policies	32
Roles and Responsibilities	34
Data Ownership.	35
Data Custodians.	36
Data Documentation and Organization	36
Data Warehousing	37
Data Mining	37
Knowledge Management.	38
Data Standards.	38
Data Lifecycle Control	38
Data Audits	39
Data Storage and Archiving	39
Data Security, Protection, Sharing, and Dissemination.	42
Privacy Impact Assessment	43
Information Handling Requirements	44

Record Retention and Destruction	45
Data Remanence and Decommissioning	46
Classifying Information and Supporting Asset Classification	47
Data Classification	49
Asset Management and Governance	51
Software Licensing	52
The Equipment Lifecycle	54
Determining Data Security Controls	55
Data at Rest	55
Data in Transit	57
Endpoint Security	59
Baselines	60
Exam Prep Questions	63
Answers to Exam Prep Questions	66
Need to Know More?	67

CHAPTER 3:

Security and Risk Management	69
Introduction	70
Security Governance	70
U.S. Legal System and Laws	71
Relevant U.S. Laws and Regulations	72
International Legal Systems and Laws	72
International Laws to Protect Intellectual Property	73
Global Legal and Regulatory Issues	74
Computer Crime and Hackers	76
Sexual Harassment	79
U.S. Governance	79
International Governance	82
Risk Management Concepts	86
Risk Management Frameworks	87
Risk Assessment	88
Risk Management Team	89
Selecting Countermeasures	104
Threat Modeling Concepts and Methodologies	107
Threat Modeling Steps	107
Threat Modeling Tools and Methodologies	108
Managing Risk with the Supply Chain and Third Parties	110
Reducing Risk in Organization Processes	112

Identifying and Prioritizing Business Continuity	
Requirements Based on Risk	113
Project Management and Initiation	116
Business Impact Analysis	117
Developing and Implementing Security Policy	123
Security Policy	124
Standards	126
Baselines	126
Guidelines	127
Procedures	127
Types of Controls	127
Administrative Controls	128
Technical Controls	129
Physical Controls	129
Access Control Categories	129
Implementing Personnel Security	130
New-Hire Agreements and Policies	131
Separation of Duties	131
Job Rotation	132
Least Privilege	132
Mandatory Vacations	133
Termination	133
Security Education, Training, and Awareness	134
Security Awareness	136
Social Engineering	136
Professional Ethics Training and Awareness	137
(ISC) ² Code of Ethics	138
Computer Ethics Institute	139
Internet Architecture Board	140
NIST SP 800-14	141
Common Computer Ethics Fallacies	141
Regulatory Requirements for Ethics Programs	142
Exam Prep Questions	144
Answers to Exam Prep Questions	148
Need to Know More?	150

CHAPTER 4:

Security Architecture and Engineering	151
Introduction	152
Secure Design Guidelines and Governance Principles	152
Enterprise Architecture	155
Regulatory Compliance and Process Control	157
Fundamental Concepts of Security Models	158
Central Processing Unit	158
Storage Media	163
I/O Bus Standards	166
Virtual Memory and Virtual Machines	167
Computer Configurations	168
Security Architecture	170
Protection Rings	170
Trusted Computing Base	172
Open and Closed Systems	175
Security Modes of Operation	176
Operating States	177
Recovery Procedures	178
Process Isolation	179
Common Formal Security Models	179
State Machine Model	180
Information Flow Model	182
Noninterference Model	182
Confidentiality	182
Integrity	185
Other Models	188
Product Security Evaluation Models	189
The Rainbow Series	189
Information Technology Security Evaluation Criteria (ITSEC)	191
Common Criteria	192
System Validation	194
Certification and Accreditation	194
Vulnerabilities of Security Architectures	195
Buffer Overflows	196
Backdoors	197
State Attacks	197

Covert Channels	197
Incremental Attacks	198
Emanations	198
Web-Based Vulnerabilities	199
Mobile System Vulnerabilities	202
Cryptography	203
Algorithms	206
Cipher Types and Methods	207
Symmetric Encryption	208
Data Encryption Standard (DES)	211
Triple DES (3DES)	215
Advanced Encryption Standard (AES)	217
International Data Encryption Algorithm (IDEA)	218
Rivest Cipher Algorithms	218
Asymmetric Encryption	218
Diffie-Hellman	220
RSA	222
El Gamal	223
Elliptical Curve Cryptosystem (ECC)	223
Merkle-Hellman Knapsack	223
Review of Symmetric and Asymmetric Cryptographic Systems	223
Hybrid Encryption	224
Public Key Infrastructure and Key Management	225
Certificate Authorities	226
Registration Authorities	226
Certificate Revocation Lists	227
Digital Certificates	227
The Client's Role in PKI	229
Integrity and Authentication	230
Hashing and Message Digests	231
Digital Signatures	235
Cryptographic System Review	236
Cryptographic Attacks	237
Site and Facility Security Controls	240
Exam Prep Questions	242
Answers to Exam Prep Questions	246
Need to Know More?	248

CHAPTER 5:
Communications and Network Security 249

- Introduction 250
- Secure Network Design. 250
- Network Models and Standards 250
 - OSI Model 251
 - Encapsulation/De-encapsulation 257
- TCP/IP. 258
 - Network Access Layer. 259
 - Internet Layer 260
 - Host-to-Host (Transport) Layer 264
 - Application Layer 267
- LANs and Their Components 271
 - LAN Communication Protocols. 271
 - Network Topologies 272
 - LAN Cabling. 275
 - Network Types 278
 - Network Storage 278
- Communication Standards. 280
- Network Equipment 281
 - Repeaters 281
 - Hubs 281
 - Bridges 282
 - Switches 282
 - Mirrored Ports and Network Taps 284
 - VLANs. 284
 - Routers 285
 - Gateways. 287
- Routing. 287
- WANs and Their Components. 289
 - Packet Switching 290
 - Circuit Switching 291
- Cloud Computing. 294
- Software-Defined WAN (SD-WAN). 296
- Securing Email Communications 296
 - Pretty Good Privacy (PGP). 297
 - Other Email Security Applications 297

Securing Voice and Wireless Communications	298
Secure Communications History	298
Voice over IP (VoIP).	304
Cell Phones	306
802.11 Wireless Networks and Standards	308
Securing TCP/IP with Cryptographic Solutions	316
Application/Process Layer Controls	317
Host-to-Host Layer Controls	318
Internet Layer Controls	319
Network Access Layer Controls	320
Link and End-to-End Encryption.	320
Network Access Control Devices	321
Firewalls	322
Demilitarized Zone (DMZ).	324
Remote Access	326
Point-to-Point Protocol (PPP).	326
Remote Authentication Dial-in User Service (RADIUS)	328
Terminal Access Controller Access Control System (TACACS)	328
Internet Protocol Security (IPsec).	329
Message Privacy and Multimedia Collaboration	331
Exam Prep Questions	333
Answers to Exam Prep Questions	337
Need to Know More?	338

CHAPTER 6:
Identity and Access Management. 341

Introduction	342
Perimeter Physical Control Systems	344
Fences	344
Gates	345
Bollards	346
Additional Physical Security Controls	347
CCTV Cameras	348
Lighting	349
Guards and Dogs	350
Locks	351

Employee Access Control	355
Badges, Tokens, and Cards	355
Biometric Access Controls	358
Identification, Authentication, and Authorization	358
Authentication Techniques	359
Identity Management Implementation	376
Single Sign-On (SSO)	378
Kerberos	378
SESAME	381
Authorization and Access Control Techniques	382
Discretionary Access Control (DAC)	382
Mandatory Access Control (MAC)	383
Role-Based Access Control (RBAC)	385
Attribute-Based Access Control	387
Rule-Based Access Control	388
Other Types of Access Control	389
Centralized and Decentralized Access Control Models	390
Centralized Access Control	390
Decentralized Access Control	393
Audits and Monitoring	394
Monitoring Access and Usage	395
Intrusion Detection Systems (IDSs)	396
Intrusion Prevention Systems (IPSS)	401
Network Access Control (NAC)	401
Keystroke Monitoring	402
Exam Prep Questions	404
Answers to Exam Prep Questions	408
Suggesting Reading and Resources	410

CHAPTER 7:

Security Assessment and Testing	411
Introduction	412
Security Assessments and Penetration Test Strategies	412
Audits	412
Root Cause Analyses	415
Log Reviews	415
Network Scanning	418
Vulnerability Scans and Assessments	419
Penetration Testing	420

Test Techniques and Methods	424
Security Threats and Vulnerabilities	427
Threat Actors	428
Attack Methodologies	430
Network Security Threats and Attack Techniques	431
Session Hijacking	431
Sniffing	432
Wiretapping	433
DoS and DDoS Attacks	433
Botnets	434
Other Network Attack Techniques	436
Access Control Threats and Attack Techniques	438
Unauthorized Access	438
Access Aggregation	438
Password Attacks	439
Spoofing	442
Eavesdropping and Shoulder Surfing	442
Identity Theft	443
Social-Based Threats and Attack Techniques	443
Malicious Software Threats and Attack Techniques	444
Viruses	445
Worms	446
Logic Bombs	446
Backdoors and Trojans	447
Rootkits	449
Exploit Kits	450
Advanced Persistent Threats (APTs)	450
Ransomware	450
Investigating Computer Crime	452
Computer Crime Jurisdiction	452
Incident Response	453
Disaster Recovery and Business Continuity	458
Investigations	459
Search, Seizure, and Surveillance	459
Interviews and Interrogations	459
Exam Prep Questions	461
Answers to Exam Prep Questions	464
Need to Know More?	465

CHAPTER 8:

Security Operations 467

- Introduction 468
- Foundational Security Operations Concepts 468
 - Managing Users and Accounts 469
 - Privileged Entities 470
 - Controlling Access 471
 - Clipping Levels 471
- Resource Protection 472
 - Due Care and Due Diligence 472
 - Asset Management 473
 - System Hardening 473
 - Change and Configuration Management 474
 - Trusted Recovery 475
 - Remote Access 476
 - Media Management, Retention, and Destruction 476
- Telecommunication Controls 477
 - Cloud Computing 477
 - Email 478
 - Whitelisting, Blacklisting, and Graylisting 480
 - Firewalls 481
 - Phone, Fax, and PBX 482
 - Anti-malware 483
 - Honeypots and Honeynets 484
 - Patch Management 485
- System Resilience, Fault Tolerance, and Recovery Controls 486
 - Recovery Controls 486
- Monitoring and Auditing Controls 487
 - Auditing User Activity 488
 - Monitoring Application Transactions 489
 - Security Information and Event Management (SIEM) 490
 - Network Access Control 491
 - Keystroke Monitoring 491
 - Emanation Security 492
- Perimeter Security Controls and Risks 493
 - Natural Disasters 493
 - Human-Caused Threats 494
 - Technical Problems 495

Facility Concerns and Requirements	495
CPTED	496
Area Concerns	497
Location	498
Construction	498
Doors, Walls, Windows, and Ceilings	498
Asset Placement	501
Environmental Controls	502
Heating, Ventilating, and Air Conditioning	502
Electrical Power	503
Uninterruptible Power Supplies (UPSs)	504
Equipment Lifecycle	505
Fire Prevention, Detection, and Suppression	505
Fire-Detection Equipment	506
Fire Suppression	507
Alarm Systems	509
Intrusion Detection Systems (IDSs)	510
Monitoring and Detection	511
Intrusion Detection and Prevention Systems	512
Investigations and Incidents	513
Incident Response	514
Digital Forensics, Tools, Tactics, and Procedures	514
Standardization of Forensic Procedures	516
Digital Forensics	516
The Disaster Recovery Lifecycle	521
Teams and Responsibilities	523
Recovery Strategy	524
Fault Tolerance	532
Backups	534
Plan Design and Development	541
Implementation	544
Testing	546
Monitoring and Maintenance	547
Exam Prep Questions	549
Answers to Exam Prep Questions	555
Need to Know More?	558

CHAPTER 9:
Software Development Security 559

- Introduction 560
- Integrating Security into the Development Lifecycle. 560
 - Avoiding System Failure 561
 - The Software Development Lifecycle 563
- Development Methodologies 573
 - The Waterfall Model 573
 - The Spiral Model. 574
 - Joint Application Development (JAD) 575
 - Rapid Application Development (RAD). 575
 - Incremental Development 575
 - Prototyping 575
 - Modified Prototype Model (MPM). 576
 - Computer-Aided Software Engineering (CASE). 576
 - Agile Development Methods 577
 - Maturity Models 578
 - Scheduling 580
- Change Management 580
- Database Management 582
 - Database Terms 583
 - Integrity 585
 - Transaction Processing 585
 - Database Vulnerabilities and Threats 586
 - Artificial Intelligence and Expert Systems 587
- Programming Languages, Secure Coding Guidelines, and Standards. . . 588
 - Object-Oriented Programming 591
 - CORBA 592
 - Security of the Software Environment. 592
 - Mobile Code 595
 - Buffer Overflow 595
 - Financial Attacks 596
 - Change Detection 597
 - Viruses and Worms. 597
- Exam Prep Questions 599
- Answers to Exam Prep Questions 603
- Need to Know More? 605

Practice Exam I	607
Practice Exam II	621
Answers to Practice Exam I	635
Answers to Practice Exam II	651
Glossary	667
Index	705

About the Author

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 performing security management, audits, and assessments, Gregg has authored or coauthored more than 25 books, including *Certified Ethical Hacker Exam Prep* (Que), *CISSP Exam Cram 2* (Que), and *Security Administrator Street Smarts* (Sybex). He has testified before the 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 leading, building, and managing security programs is where he spends the bulk of his time, contributing to the written body of IT security knowledge is how Michael believes he can give something back to the community that has given him so much.

About the Technical Reviewer

Dr. Dwayne Hodges is a retired U.S. Army officer and combat Iraq War veteran with over 25 years' experience. He is the founder and owner of Wellspring Services, a service disabled veteran-owned small business, and he is a senior cybersecurity executive with extensive education, training, and experience working in commercial, government, and military agencies. Dr. Hodges is a university professor, consultant, and board member in higher education with over 17 years' experience with teaching, course development, and curriculum design. He holds a doctorate in education and organizational leadership, a master's degree in information systems technologies and management information systems security, a master's degree in public administration, and a bachelor's degree in sociology and criminal justice. He is a graduate of the U.S. Army Signal Communications School: School of Information Technology, U.S. Army Signal Center, and U.S. Army Command and General College. Dr. Hodges holds several industry certifications and certificates, including (ISC)² CISSP, CCISO, and CEH; CompTIA Information Security+; Certified Network Defense Architect; Information Technology Infrastructure Library (ITIL); and Certified Encryption Specialist. Dr. Hodges has been a featured TEDx speaker, he is a published author, and he has been a featured speaker for the State of Cyber Security discussions. He has testified in front of the National Academy of Sciences on cybersecurity threats. He is also an author, instructor, and course developer for advanced cryptography concepts on Udemy.

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 the entire Pearson crew, as they have allowed me to maintain this book over 15 years and 5 editions. It's been a great pleasure to help thousands of individuals prepare for and pass the CISSP exam.

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@informit.com

Reader Services

CHAPTER 2

Understanding Asset Security

Terms you'll need to understand:

- ▶ Confidentiality
- ▶ Integrity
- ▶ Availability
- ▶ Personally identifiable information
- ▶ Information lifecycle management (ILM)
- ▶ Data retention
- ▶ 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 with local, state, and federal laws
- ▶ The implementation of encryption and its use for the protection of data
- ▶ How to use data security controls

Introduction

Understanding asset security is a key requirement of a CISSP candidate. 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 lifecycle phase. This chapter starts by reviewing the basic security principles of confidentiality, integrity, and availability and moves on to data management and governance.

The CISSP exam requires you to understand data security and how information is protected while it is in transit, in storage, and at rest. You must understand that protection of data is much more important today than it was years ago because data is no longer isolated in standalone servers. Today data often resides in the cloud; data can also be found on laptops, in RAID arrays, or even in paper form. Regardless of its storage location, data must have adequate protection and must be properly disposed of at the end of its useful life.

Basic Security Principles

Confidentiality, integrity, and availability (CIA) are the basic building blocks of any good security program. When defining the goals for network, asset, information, and/or information system security, the term *CIA triad* is commonly used to refer to these concepts. Although the abbreviation CIA might not be as intriguing as the U.S. 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. A number of controls are 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 plaintext information. The Organization for Economic Co-operation and Development (OECD) specifies that personal data should be limited and provides guidelines for ensuring privacy and confidentiality.

Integrity has to do with accuracy of information and offering users a high degree of confidence that the information they are viewing has not been tampered with. The integrity of data must be protected while the data is in storage, at rest, and in transit. It is important to ensure that unauthorized users have not made any changes and authorized users have not made inappropriate changes. Data in storage can be protected through the use of access controls and audit controls. Cryptography and hashing algorithms can enhance this protection. Cryptography tools include programs such as HashTools, HashCheck, and PowerShell. Likewise, integrity in transit can be ensured primarily through the use of these tools in combination with protocols and frameworks such as public key infrastructure (PKI), digital signatures, and asymmetric algorithms.

Availability refers to the need for information and systems to 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 have an availability problem. Availability in the world of electronics can manifest in many ways. 24x7 access to a backup facility does little good if there are no updated backups to restore from and the original copies have been encrypted with ransomware.

Keeping backups is a good way to ensure availability. A backup provides a copy of critical information that can be reinstated if data is destroyed or equipment fails. Using failover equipment is another way to ensure availability. Systems such as redundant arrays of independent disks (RAID) and redundant sites (which can be hot, cold, or warm sites) are two other examples. Disaster recovery is tied closely to availability because it's all about getting critical systems up and running quickly.

Which part of the security triad is considered most important? It depends. In different organizations with different priorities, one part might be more important than the other two. For example, your local bank might consider integrity the most important, an organization responsible for data processing might see availability as the primary concern, and an organization such as a healthcare records clearing agency might value confidentiality the most.

Even though this book refers to the triad 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.

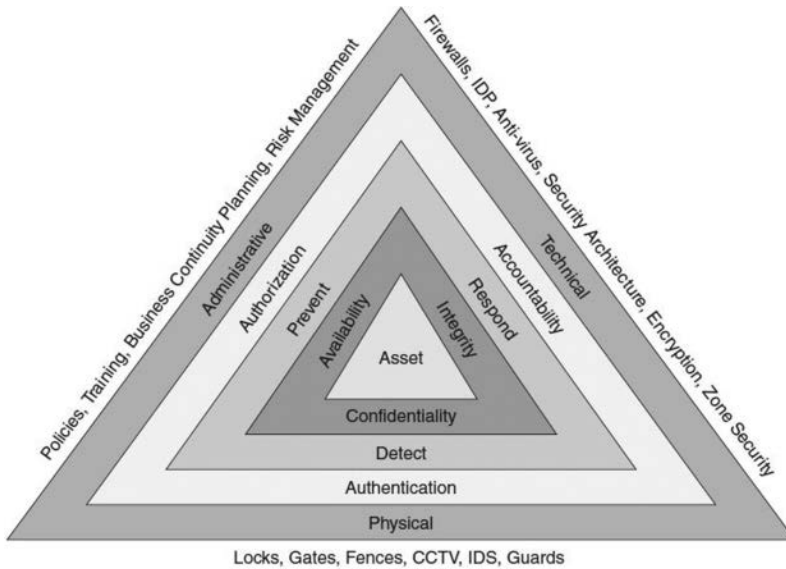


FIGURE 2.1 Asset Protection Triad

Data Management: Determining and Maintaining Ownership

Data management is not easy, and it has in fact become more complex recently. 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, and in a public cloud.

Data Governance Policies

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 goals of data governance include the following:

- ▶ Establish appropriate responsibility for the management of data
- ▶ Improve ease of access to data
- ▶ Ensure that once data is located, users have enough information about the data to interpret it correctly and consistently
- ▶ Improve the security of data, including confidentiality, integrity, and availability

Issues to consider include the following:

- ▶ **Cost:** This can include the cost of providing access to the data as well as the cost of protecting it.
- ▶ **Ownership:** This includes concerns about who owns the data or who might be a custodian. For example, you might be the custodian of 50 copies of Microsoft Windows Server 2019, yet the code is owned by Microsoft. Users pay for a software license and not ownership of the software itself, and they typically have only the compiled .exe file and not the source code for a program.
- ▶ **Liability:** This refers to the financial and legal costs an organization would bear if data were lost, stolen, or hacked.
- ▶ **Sensitivity:** This includes issues related to the sensitivity of data that should be protected against unwarranted disclosure (for example, Social Security numbers, date of birth, medical history information).
- ▶ **Ensuring law/legal compliance:** This includes items related to legal compliance. For example, you must retain tax records for a minimum number of years, but you might be required to retain personally identifiable information (PII) customer information for only the time it takes to process a single transaction.
- ▶ **Process:** This includes methods and tools used to transmit or modify data.

Roles and Responsibilities

Data security requires responsibility. A clear division of roles and responsibility is 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. 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 the head of that department. The data owner is responsible for setting the security classification of the data. The data owner can delegate some day-to-day responsibility.
- ▶ **Data custodian:** The data custodian, who is usually a member of the IT department, does not decide what controls are needed but implements controls on behalf of the data owner. Other responsibilities include handling 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.
- ▶ **Information security steering committee:** Individuals on this committee are from various levels of management and 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 are also responsible for reviewing security plans and procedures.
- ▶ **Chief security officer:** This individual is responsible for the day-to-day security of the organization and its critical assets.
- ▶ **Users:** End users in an organization 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.

- ▶ **Auditor:** This individual is responsible for examining the organization's security procedures and mechanisms. The auditor must provide an independent and objective opinion about the effectiveness of the organization's security controls. How often this process is performed depends on the industry and its related regulations. For example, the healthcare industry in the United States is governed by Health Insurance Portability and Accountability Act (HIPAA) regulations and requires yearly reviews.

ExamAlert

The CISSP exam might test you 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. However, this type of 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 potential for damage.

Data Ownership

Every data object within an organization must have an owner. Any object 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. ILM 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 are times when it is static. For example, after this book has been published, it will stay in a fixed format until the next edition is released.

For the purposes of business records, the lifecycle process includes five phases:

1. Creation and receipt
2. Distribution
3. Use
4. Maintenance
5. Disposition

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 must be formally appointed. 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

Organizing and structuring data can help ensure that that it is better understood and interpreted by users. Data documentation should detail 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. It allows for trend analysis and marketing decisions through data analytics (discussed later in this chapter). Data warehousing enables 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). Many things must be in place for data mining to occur, including 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 data. *Metadata* is best described as being data about data. For example, the number 212 has no meaning by itself. But qualifications can be added to give it meaning; for example, if you learn that 212 is an area code, then you understand that the number represents an area code in Manhattan.

Organizations treasure data and the relationships that can be deduced between individual data elements. These relationships can help companies understand their competitors and the usage patterns of their customers and can help them target their marketing. For example, diapers may be located in the back of the store, near the beer case, because data mining shows that after 10 p.m., more men than women buy diapers, and they tend to buy beer at the same time.

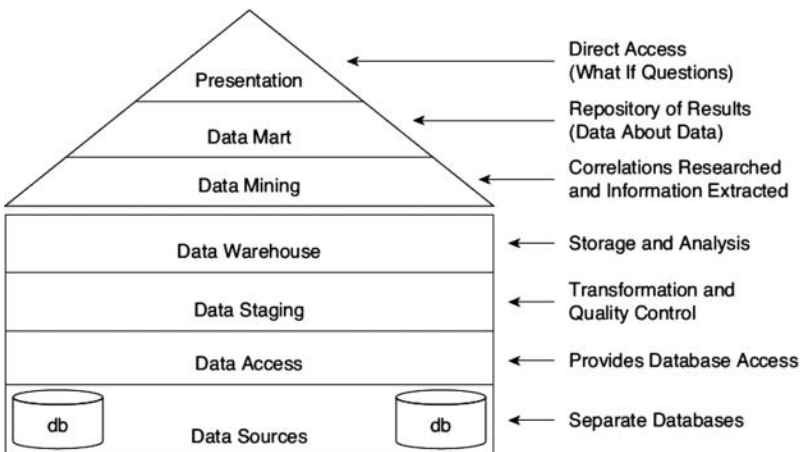


FIGURE 2.2 Data Mining

Knowledge Management

Knowledge management seeks to make intelligent use of the data in an organization by applying wisdom to it. This involves turning data into intelligence through analytics by tying 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.

There are three main approaches to knowledge extraction:

- ▶ **Classification:** This approach is used to discover patterns and 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 a data warehouse.)
- ▶ **Probabilistic:** This approach is used to permit statistical analysis, often in planning and control systems or in applications that involve uncertainty.
- ▶ **Statistical:** This is a number-crunching approach in which rules are constructed to identify generalized patterns in the data.

Data Standards

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

Tip

To see an example of a data standard, check out FDA Resources for Data Standards, at www.fda.gov/industry/fda-resources-data-standards. The FDA provides this site to ensure that common data standards are used throughout the FDA.

Data Lifecycle Control

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

Data Audits

After all the tasks discussed so far in this chapter have been performed, the organization's security management practices 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. For example, financial audits can be performed using the 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 that helps provide governance and assurance. COBIT was designed for performance management and IT management, and it is considered a system of best practices. COBIT was created by the ISACA and the IT Governance Institute (ITGI) in 1992.

Auditors can use COBIT, and this framework is also useful for IT users and managers designing controls and optimizing processes.

Audits make it possible 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 employees actually works. To learn more about COBIT, see www.isaca.org/cobit/. Another set of documents that can be used to benchmark the infrastructure is the ISO 27000 family of standards; for details, see www.27000.org.

Data Storage and Archiving

Organizations have a never-ending need for increased storage. Whereas thumb drives were revolutionary and initially provided in the range of 10 MB of storage, today they can provide terabytes of storage. Data storage options in organizations typically include the following:

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

Organizations should fully define their security requirements for data storage before deploying a technology. 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 can a NAS. Cloud-based storage offers yet another option but also presents concerns, including the following:

- ▶ 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.

The Storage Networking 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.

For the CISSP exam, it is important to know the following terms related to SANs:

- ▶ **Virtual SAN:** A virtual SAN (VSAN) is a SAN that offers isolation for devices that are physically connected to the same SAN fabric. The use of VSANs 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 allows a resource on any individual VSAN to be shared by other users on a different VSAN without requiring the SAN fabrics to be merged.
- ▶ **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 Fibre

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

- ▶ **Fibre Channel over Ethernet (FCoE):** FCoE, a transport protocol that is similar to iSCSI, can operate at speeds of 10 Gbps and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is non-routable. By contrast, iSCSI is routable because it operates higher up the stack, on top of the TCP and UDP protocols.
- ▶ **Host bus adapter (HBA) allocation:** A host bus adapter is used to connect a host system to an enterprise storage device. HBAs can be allocated either through soft zoning or 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 system that makes LUNs available to some HBAs but not to others. LUN masking implemented at this level is vulnerable to any attack that compromises the local adapter.
- ▶ **Location redundancy:** Location redundancy makes contents 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. A 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 a 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.

- ▶ **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 medium, such as disk or tape.

Data Security, Protection, Sharing, and Dissemination

Data security involves protecting 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 importance of data security, consider that according to the Privacy Rights Clearinghouse (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 2020 is 11,717,011,063.

The international standard ISO/IEC 17799 covers data security on a global level. ISO 17799 makes clear the fact that all data should have a data owner and data custodian so that it is clear who is responsible for securing and protecting access to that data.

An example of a proprietary international information security standard is the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS sets standards for any entity that handles cardholder information for credit cards, prepaid cards, and POS cards. PCI-DSS comprises 6 control objectives and 12 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 antivirus software.

Requirement 6: Develop and maintain secure systems and applications.

4. Implement strong access control measures.

Requirement 7: Restrict access to cardholder data based on 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 PII 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 overlook 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.

Privacy controls tend to be overlooked for the same reason many security controls are overlooked. Management might have a preconceived idea that security controls will reduce the efficiency or speed of business processes. To overcome such 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 related to the loss of personal information of clients and customers. These costs can include fines, lawsuits, lost customers, reputation, and, ultimately, the viability of the company.

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. You can think of policies as high-level documents and procedures as step-by-step instructions. Many organizations are in industries that are subject to 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: May 1, 2021
Author: Christine Gregg
Classification: Top Secret
Retention Period: 3 Years
Title and Description: Project X



FIGURE 2.3 Data Labeling

Note

Unless you're a classic car enthusiast like I am, it might have been a while since you have seen a working in-dash cassette player. Technology changes, and the requirement to be able to read and access old media is something to consider. Stored media—including older options such as cassette tapes, laser discs, Zip drives, and PATA hard drives—must be readable in order to be useful.

Record Retention and Destruction

All data has a lifetime. Eventually data should either be purged, released, or unclassified. Record retention involves maintaining important information as long as it is needed and destroying or declassifying it when it isn't needed.

Some record retention guidelines are legally mandated by governments. For example, companies typically cannot legally delete potential evidence after a lawsuit is filed and must maintain these assets and records until the court case has concluded. In addition, the JFK Records Act was a record retention act put in place to eventually declassify all records dealing with the assassination of President John F. Kennedy and make these records public by 2018.

The steps in creating a record retention policy include the following:

1. Understand the business needs and any existing regulatory requirements.
2. Classify assets or records.
3. Create retention periods and specify data destruction methods.
4. Develop the policy and determine the impact should the policy not be followed.
5. Conduct training, education, and awareness about the policy.
6. Audit the policy and procedures.
7. Review the policy and procedures regularly.
8. Record the implementation and audit results.

ExamAlert

Two key aspects of data retention are categorization and classification. *Categorization* defines the impact should the asset be exposed. *Classification* defines the value. The CISSP exam is likely to test you on your understanding of these terms.

The Problem of Data Disposal

While hard drive size and performance have continued to grow rapidly, most hard drives and thumb drives are still shipped without encryption enabled. This means, for example, 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 gain access to the data on the drive. While many of us have used a paper 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 drives cannot be recovered.

To find out whether organizations are doing a good job of ensuring that their data is unrecoverable, two researchers from MIT bought 158 used hard drives from eBay. Out of these hard drives, 129 drives still functioned, and 69 of these drives contained data that the researchers were able to copy. The data on these drives included personal information, company HR records, medical information, a pharmacy database, and another database containing several thousand credit card numbers.

Data Remanence and Decommissioning

Object reuse must be carefully considered because information may remain on a hard disk or any other type of media. Even when data has been sanitized, there may be some remaining information. *Data remanence* is the residual data that remains after data has been erased from a storage device. *Sanitization* is the process of clearing all identified content such that no data remnants can be recovered. The CISSP exam will expect you to understand the differences between various types of sanitization methods.

Asset disposal must be handled in an approved manner and must be part of the systems development lifecycle. For 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.

Clearing and purging are two ways to decommission hardware. *Zeroization* is a type of clearing. Purging is considered a stronger, permanent form of sanitization. Degaussing and drive wiping are types of purging. The details of these methods are as follows:

- ▶ **Zeroization:** This process, which is a type of clearing, is usually associated with cryptographic processes. The term was originally used with mechanical cryptographic devices, which 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 in ANSI X9.17. Data may be recoverable with this method.

- ▶ **Degaussing:** This process is used to permanently destroy the contents of a hard drive or magnetic media. Degaussing involves using 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.
- ▶ **Drive wiping:** This is the act of overwriting all information on a drive. Drive wiping, which is covered in National Institute of Standards and Technology (NIST) 800-88 and U.S. Department of Defense (DoD) 5200.28, allows a drive to be reused. One form of drive wiping (specified in DoD 5200.28) is overwriting a drive with a special digital pattern through seven passes.

It is common for a storage device to have some remaining amount of information left on it after it has been erased. If the media is going to be reused rather than destroyed, the best practice is to overwrite it with a minimum of seven passes of random ones and zeros.

For information deemed too sensitive, assets such as hard drives, media, and other storage devices may need to be destroyed rather than reused. Destruction, which is the strongest form of sanitization, can include acid baths and physical destruction. If records that are no longer needed are held on a newer non-magnetic drive, such as a solid-state drive (SSD), Curie temperature may be used to heat the drive to the point where it loses its magnetic properties.

ExamAlert

The CISSP exam will expect you to understand the different ways you can dispose of data. One easy way to memorize this is to think of the phrase “Cow, Pig, Sow,” or “CP SOW,” which stands for **clearing can be recovered**, **purging is permanent**, **sanitizing is the same**, **overwriting o’s**, and **wiping is writing**.

Classifying Information and Supporting Asset Classification

Asset classification involves assigning assets to groups, based on a number of common characteristics. Before you can classify assets, however, you must know what you have. You determine this through an asset inventory. Modern organizations rely heavily on asset inventories and the use of tools such as Asset

Panda, AssetCloud, and ManagerPlus. These applications (and others) assist organizations in identifying, locating, and classifying their assets. The components of an asset inventory include items such as the following:

- ▶ Asset name
- ▶ Asset location
- ▶ Asset cost
- ▶ Asset owner
- ▶ Asset classification
- ▶ Data protection level required

The standard or process used to classify and manage assets is typically left to the discretion of an individual organization. Two things to consider are the size and structure of the organization and what is considered common in the country or industry in which the organization operates. Regardless of the particular approach, the asset classification process consists of five steps:

1. Create an asset inventory.
2. Assign ownership.
3. Classify based on value.
4. Protect based on classification.
5. Assess and review.

Note

To memorize the asset classification process for the CISSP exam, think of CACPA, which rhymes with “Cat Paw” and refers to the steps listed above.

In addition to protecting its assets, an organization must protect the information maintained in those assets that is proprietary or confidential. 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 the importance of the data. For 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.

Index

Numbers

- 1G cell phone technology, 306
- 2G cell phone technology, 306
- 3DES (3Data Encryption Standard), 206, 215–216
- 3G cell phone technology, 306
- 4G cell phone technology, 306
- 5G cell phone technology, 307
- 10 Commandments of Computer Ethics, 139–140
- 10 Steps to Cyber Security, 86
- 802.1AE (MACsec) security standard, 259–260
- 802.1AR security standard, 260
- 802.11 wireless networks/standards
 - 802.11a wireless standard, 310
 - 802.11ac wireless standard, 310
 - 802.11b wireless standard, 310
 - 802.11g wireless standard, 310
 - 802.11i wireless standard, 310
 - 802.11n wireless standard, 310
 - 802.16 wireless standard, 310
- 1998 Directive on Data Protection, 76

A

- AAL (Authenticator Assurance Levels), 360
- ABAC (Attribute-Based Access Control), 387–388
- absolute addressing, 163
- acceptable risk, 104, 105
- acceptance testing/implementation, SDLC, 569–571

access controls, 129–130

- attacks/threats, 438
 - access aggregation, 438–439
 - password attacks, 439–442
 - unauthorized access, 438
- networks, 321–322
 - DMZ, 324–325
 - firewalls, 322, 481
 - NAT, 325
 - packet filters, 322
 - proxy servers, 322–324
 - stateful firewalls, 322
 - zero trust, 325
- operational security, 471
- physical, 240, 495–497
- remote access, 326, 476
 - CHAP, 326
 - EAP, 326–328
 - IPsec, 329–330
 - PAP, 326
 - PPP, 326
 - RADIUS, 328
 - TACACS, 328–329
- restricted access/work area security, 241

access/identity management, 342, 358–359, 377

- accountability, 343
- authentication, 342–343, 358–361
 - AAL, 360
 - biometrics, 370–375
 - card-based authentication, 369–370
 - CHAP, 390
 - digital certificates, 370
 - EAP, 390
 - FIM, 358–360
 - IAL, 360
 - IDaaS, 358–360
 - MS-CHAPv2, 390
 - multifactor authentication, 375
 - OAuth, 362
 - OpenID, 362

- PAP, 390
- passwords, 363–367
- SAML, 361–362
- strong authentication, 375
- tokens, 367–368
- two-factor authentication, 375
- authorization, 343, 382
 - ABAC, 387–388
 - audits, 394–396
 - CDAC, 389
 - centralized access control, 390–393
 - DAC, 382–383
 - decentralized access control, 393–394
 - IDS, 396–401, 510–511, 512–513
 - IPS, 384, 401
 - keystroke monitoring, 402–403
 - LBAC, 389
 - MAC, 383–385
 - monitoring access, 394–396
 - NAC, 401–402
 - RBAC, 385–387
 - rule-based access control, 388
 - SIEM, 401
- employee access control, 355
 - biometrics, 358, 370–375
 - card keys/badges, 355–356
 - RFID tags, 342, 357
 - silent hostage (duress) alarms, 356
 - smart/dumb cards, 356
- federation, 377
- Kerberos, 378–381
- least privilege, 343
- lifecycles, 376
- perimeter physical control systems, 344
 - bollards, 346–347
 - CCTV cameras, 348–349, 496
 - deadman doors, 346
 - dogs, 350
 - fences, 343

- gates, 345–346
 - guards, 350
 - lighting, 349–350
 - locks, 351–355
 - mantraps, 346
 - turnstiles, 346
 - physical access controls, 342–343, 344–348
 - profile management, 377
 - SESAME, 381
 - SPML, 378
 - SSO, 343, 378
 - user provisioning, 376
 - WS-Security, 377
 - XML, 377
- access logs, 416**
- account management, 469**
- access controls, 471
 - clipping levels, 471–472
 - database administrators, 469
 - job rotation, 471
 - least privilege, 471
 - network administrators, 469
 - privileged entities, 470–471
 - quality assurance specialists, 469
 - reasonably prudent person rule, 472–473
 - security architects, 469
 - separation of duties, 469–470, 471
 - system administrators, 469
 - systems analysts, 469
- accountability, 343, 487–489**
- accreditation, 195, 571**
- ace locks, 352**
- ACL (Access Control Lists), 382–383, 388**
- acquisition, digital forensics, 516, 517–519**
- active sniffing, 432**
- ActiveX programming language, 590**
- activity blockers, 484**
- adhesion, contracts of, 53**
- administrative controls, 128**
- administrative (regulatory) law, U.S. legal system/laws, 71**
- administrators, system, 469**
- advisor groups, security, data management, 34**
- advisory policies, 125**
- AES (Advanced Encryption Standard), 217**
- aggregation**
- access, 438–439
 - databases, 583, 584
- agile development, software, 577–578**
- aging, passwords, 364**
- AH (Authentication Headers), 329**
- AI (Artificial Intelligence), 587–588**
- AIC. See CIA triad**
- alarms, 509–510**
- IDS, 510–511, 512–513
 - monitoring/detection, 511–512
 - silent hostage (duress) alarms, 356
- ALE (Annual Loss Expectancy), 97, 98–99, 106**
- algorithms**
- cryptographic, 204, 206–207
 - asymmetric cryptography, 207
 - symmetric algorithms, 207
 - DSA, 236, 237
 - hashing algorithms, 205, 231–233, 237
 - CBC-MAC, 234
 - CMAC, 235
 - HVAL, 234
 - HMAC, 234
 - MAC, 234–235
 - SHA-1, 233
 - SHA-2, 233
 - SHA-3, 234
 - IDEA, 210
 - LUC algorithm, 222
 - MD algorithms, 233
 - Rivest cipher algorithms, 210–211, 218
 - RSA algorithm, 222

alpha testing

alpha testing, 570

ALU (Arithmetic Logic Units), 158

analytics

- BIA, 117–119
 - MTD, 122
 - potential loss assessments, 119–122
 - qualitative ranking, 120–121
 - quantitative ranking, 121–122
 - questionnaires, 119–121
 - risk reduction process, 121–122
- comparative analysis, passwords, 439
- cost-benefit analysis of risk management, 106
- data analytics, 37
- digital forensics, 517, 520–521
- FRAP, 102
- frequency analysis, 299
- MITRE Risk Matrix, 106
- payback analysis, 564
- risk factor analysis, 87
- root causes analyses, 415
- threats, 93–96
- traffic analysis, 437

anomaly-based IDS, 399–400

answers, CISSP exams

- drag-and-drop questions, 26
- hotspot questions, 26
- multiple-choice questions, 26
- strategies for answering, 27

anti-malware, telecommunications control, 483–484

antivirus software, 60

applets, 595

application controls, 561–562

application layer

- OSI network model, 256
- TCP/IP network model, 267–271, 316–320

application-level proxies, 323–324

application servers, 169

applications

- logs, 416
- security testing, 420
- transaction monitoring, 489–490
- whitelisting, 60

APT (Advanced Persistent Threats), 450

architecture security and engineering, 152, 170

- accreditation, 195
- certification, 194–195
- computer/device configurations, 168–170
- CPU, 158–163
- cryptography, 203
 - 3DES, 215–216
 - AES, 217
 - algorithms, 204, 206–207
 - asymmetric encryption, 205, 207, 218–224, 237
 - attacks, 237–240
 - authentication, 203–204, 230–231
 - block ciphers, 205, 207–208
 - ciphertext, 204
 - confidentiality, 203
 - cryptanalysis, 205
 - CSS, 238
 - DES, 211–215
 - digital signatures, 205, 235–236, 237
 - DRM, 205
 - encryption, 203, 204
 - hashing algorithms, 205, 231–236, 237
 - hybrid encryption, 224–225
 - integrity, 204, 230–231
 - Kerckhoff's Principle, 238
 - key management, 205
 - keys, 204
 - MD algorithms, 233
 - nonces, 206–207
 - nonrepudiation, 204

- plaintext, 204
- pseudorandom numbers, 206–207
- s-boxes, 208
- steganography, 205
- stream ciphers, 205, 208
- symmetric encryption, 205, 208–211, 223–224, 237
- defense in depth design process, 152–153
- design guidelines, 152–155
- EA, 155–157
- frameworks, 154–155
- fundamentals, overview, 158
- I/O bus standards, 166–167
- open/closed systems, 175
- operating states, 177–178
- PKI, 153, 225–226
 - CA, 226
 - client's role, 229–230
 - CRL, 227
 - digital certificates, 227–229
 - RA, 226–227
- process control, 157–158
- process isolation, 179
- product security evaluation models, 189
 - Common Criteria (ISO 15408), 192–194
 - CTCPEC, 190
 - ITSEC, 191–192
 - Rainbow Series, The, 189–191
 - TCSEC, 189–190, 191–192
- protection rings, 170–172
- recovery procedures, 178, 486–487
- regulatory compliance, 157–158
- security models, 179, 189
 - Bell-LaPadula model, 182–184
 - Biba model, 185–186
 - Brewer and Nash model, 188
 - Clark-Wilson model, 187
 - Graham-Denning model, 188
 - Harrison-Ruzzo-Ullman model, 188
 - information flow model, 182
 - Lattice model, 188
 - Lipner model, 188
 - noninterference model, 182
 - state machine model, 180–181
 - Take-Grant model, 188
- security modes of operation, 176–177
- site/facility controls, 240–241
- storage media, 163
 - CD, 165
 - direct-access storage, 165
 - DVD, 166
 - flash memory storage, 166
 - I/O bus standards, 166–167
 - optical media, 165
 - RAM, 163–164, 167–168
 - ROM, 164–165
 - secondary storage, 165–166
 - sequential storage, 165
 - software, 165
 - SSD, 166
- swap partitions, 167–168
- system validation, 194
- TCB, 172–175
- TPM chips, 154
- virtual memory, 167–168
- VM, 168
- vulnerabilities, 195–196
 - backdoors, 197
 - buffer overflows, 196, 200, 595–596
 - covert channels, 197–198
 - data diddling, 198
 - database attacks, 201–202
 - emanations, 198–199
 - incremental attacks, 198
 - maintenance hooks, 197
 - mobile system vulnerabilities, 202–203

architecture security and engineering

- salami attacks, 198
- SQL injections, 201–202, 586
- state attacks, 197
- Van Eck Phreaking, 199, 492
- web-based vulnerabilities, 199–202
- wireless vulnerabilities, 202

architectures

- CORBA, 592
- OS, 174–175

archive bits, 536–537**area concerns, facility/site security controls, 497****ARO (Annual Rate of Occurrence), 97, 98–99****ARP (Address Resolution Protocol), 260**

- poisoning, 436
- TCP/IP network model, 263–264

assemblers, 589**assessing**

- exam readiness, 20–21
- potential loss, 119–122
- risk. *See* separate entry
- security, 412
 - application security testing, 420
 - audits, 412–415
 - blackbox testing, 420
 - code reviews, 425
 - coverage, 413–414
 - DAST, 425
 - DoS testing, 420
 - Fagan inspections, 426
 - fuzz testing, 426
 - graybox testing, 420
 - IAST, 425
 - integer overflow, 426–427
 - KPI, 414–415
 - KRI, 415
 - log reviews, 415–418
 - misuse case testing, 426

- outsider testing, 420
- penetration testing, 257–263
- physical security testing, 420
- RASP, 425
- root causes analyses, 415
- sampling plans, 413–414
- SAST, 425
- scanning networks, 418–419
- social engineering testing, 421
- stress testing, 420
- synthetic transactions, 426
- techniques/methods, 424–427
- vulnerability scanning, 419
- war dialing, 420–421
- whitebox testing, 420
- wireless network testing, 420
- vulnerabilities, 419

assessing risk, 88

- assets, 88, 91–93
- controls, 95–96
- hacker insurance, 93
- high-impact assets, 92–93
- high-risk assets, 92–93
- identifying assets, 91–93
- losses, 94
- probabilistic risk assessment, 87
- qualitative assessments, 102, 103–104
 - Delphi technique, 102
 - FRAP, 102
 - IAM, 102
 - impact scale, 100–101
 - NIST 800–53, 102–103
 - performing, 103
 - results, 101–102
 - steps of, 101
- quantitative assessments, 97, 103–104
 - ALE, 97, 98–99, 106
 - ARO, 97, 98–99
 - calculations, 97–99
 - formulas, 99–100
 - SLE, 97, 98–100

- SATAN vulnerability assessment tool, 138–139
- steps of assessment, 90
- threat analysis, 93–96
- threats, 89
- vulnerabilities, 89, 95–96
- Asset Protection Triad (CIA triad), 30, 31–32**
 - availability, 31
 - confidentiality, 30
 - integrity, 31
- assets**
 - governance, 51–52
 - high-impact assets, 92–93
 - high-risk assets, 92–93
 - identifying, 91–93, 107
 - management, 51–52, 473
 - “CACPA”, 48
 - change management, change management, 474–475
 - classifying, 47–48
 - cloud computing, 477–478
 - configuration management, 474–475
 - inventories, 47–48
 - media management, 476–477
 - remote access, 476
 - software licensing, 52–54
 - system hardening, 473–474
 - trusted recovery, 475–476
 - placement, facility/site security controls, 501–502
 - risk assessments, 88
 - valuation, 91–93
- assisted password resets, 365**
- asymmetric encryption, 205, 207, 218–220, 237**
 - Diffie-Hellman key exchanges, 220–222
 - ECC, 223
 - El Gamal, 223
 - Knapsack, 223
 - LUC algorithm, 222
 - RSA algorithm, 222
 - XTR public key cryptosystem, 222
- asymmetric mode, processors, 160**
- asynchronous tokens, 367–368**
- ATA (Advanced Technology Attachments), 166**
- ATBASH, 299**
- ATM (Asynchronous Transfer Mode), 291**
- ATO (Authorization To Operate), 111**
- attacks/threats, 431**
 - access controls, 438
 - access aggregation, 438–439
 - password attacks, 439–442
 - unauthorized access, 438
 - APT, 450
 - ARP poisoning, 436
 - backdoors, 447–449
 - booters, 434
 - botnets, 434–436
 - brute-force cracking, 441
 - buffer overflows, 595–596
 - crypters, 448–449
 - database attacks, 437
 - DDoS attacks, 433–434
 - DNS spoofing, 437
 - DoS attacks, 433
 - dumpster diving, 444
 - eavesdropping, 442
 - email bombing, 437
 - exploit kits, 450
 - financial attacks, 596–597
 - human-caused threats, 494–495
 - hybrid attacks, 440
 - identity theft, 443
 - impersonation attacks, 444
 - IOC, 597
 - logic bombs, 446–447, 596–597
 - malicious software, 444–445

attacks/threats

- APT, 450
- backdoors, 447–449
- crypters, 448–449
- exploit kits, 450
- logic bombs, 446–447
- packers, 448
- ransomware, 450–451
- rootkits, 449–450
- success attacks, 450
- Trojans, 447–449
- viruses, 445–446
- worms, 446
- wrappers, 448
- methodologies of attacks, 430–431
- packers, 448
- pharming attacks, 437
- phishing, 443
- phreaking, 492
- piggybacking, 444
- pretexting, 443–444
- rainbow tables, 441–442
- ransomware, 450–451
- rootkits, 449–450
- session hijacking, 431–432
- shoulder surfing, 442, 444
- smishing, 308, 443
- sniffing, 432
- social engineering attacks, 443–444
- spear phishing, 443
- spoofing attacks, 442, 444
- success attacks, 450
- tailgating, 444
- traffic analysis, 437
- Trojans, 447–449
- Van Eck Phreaking, 199, 492
- vectors, computer crime/hackers, 77
- virus hoaxes, 444
- viruses, 445–446, 597–598
- war driving, 437
- whaling, 443
- wiretapping, 433, 437

- worms, 446, 597–598
- wrappers, 448
- zero-day vulnerabilities, 437

attenuation, cabling, 280**attributes, databases, 583****auditors, data management, 35****audits**

- auditing controls, 487–489
- data, 39
- employees, 548
- identity/access management, 394–396
- logs, 416
- penetration testing/assessments, 412–415
- SAS 70, 112

AUP (Acceptable Use Policies), 128, 471**authentication, 342–343, 358–361**

- AAL, 360
- AH, 329
- biometrics, 370–371, 374–375
 - CER, 372
 - facial recognition, 373
 - FAR, 371
 - fingerprint recognition, 373–374
 - FRR, 371
 - hand geometry recognition, 372
 - iris recognition, 373
 - retina pattern recognition, 373
 - Type I errors, 371
 - Type II errors, 371
 - voice recognition, 373
- card-based authentication, 369–370
- CHAP, 326, 390
- cryptography, 203–204, 230–231
- digital certificates, 370
- digital forensics, 516–517, 520
- EAP, 320, 326–328, 390
- encryption, 58
- FIM, 358–360
- IAL, 360

- IDaaS, 358–360
- IMAP, 269
- MAC, 234–235
 - CBC-MAC, 234
 - CMAC, 235
 - HMAC, 234
- MFA, 202
- MS-CHAPv2, 390
- OAuth, 362
- OpenID, 362
- PAP, 326, 390
- passwords, 363–364, 367
 - aging, 364
 - assisted password resets, 365
 - attempts, 364
 - clipping levels, 364
 - cognitive passwords, 366–367
 - complexity, 364
 - composition, 364
 - cracking, 366
 - dynamic passwords, 365–366
 - history, 364
 - length, 364
 - OTP, 367
 - passphrases, 365
 - self-service password resets, 365
 - session management, 364
 - single-use passwords, 365–366
 - static passwords, 365–366
 - storing, 364
 - synchronization, 365
 - threshold levels, 364
- SAML, 361–362
- strong authentication, 375
- tokens, 367
 - asynchronous tokens, 367–368
 - synchronous tokens, 367–368
- authorization, 343, 382**
 - ABAC, 387–388
 - audits, 394–396
 - CDAC, 389
 - centralized access control, 390
 - CHAP, 390
 - Diameter, 393
 - EAP, 390
 - MS-CHAPv2, 390
 - PAP, 390
 - RADIUS, 391–392
 - TACACS, 392
 - DAC, 382–383
 - decentralized access control, 393–394
 - IDS, 396–397, 510–511, 512–513
 - anomaly-based IDS, 399–400
 - HIDS, 398, 512
 - NIDS, 397–398, 512
 - rule-based IDS, 400
 - sensor placement, 400–401
 - signature-based IDS, 399
 - IPS, 384, 401
 - keystroke monitoring, 402–403
 - LBAC, 389
 - MAC, 383–385
 - monitoring access, 394–396
 - NAC, 401–402
 - RBAC, 385–387
 - rule-based access control, 388
 - SIEM, 401
- AS (Autonomous Systems), 289**
- availability**
 - backups, 31
 - CIA triad, 31
- avoiding risk, 105**
- awareness, employees, 134–136**
 - disaster recovery plans, 545
 - ethics training/awareness, 137–138
 - 10 Commandments of Computer Ethics, 139–140
 - common fallacies, 141–142
 - Computer Ethics Institute, 139–140
 - IAB, 140–141
 - (ISC)2 Code of Ethics, 138–139

awareness, employees

ISOC, 140–141
 NIST SP 80–14, 141
 regulatory requirements, 142–143
 RFC 1087, 140–141

B

backdoors, 197, 447–449

background checks, 131

backups, 31

choosing, 539–541
 cloud computing, 539
 continuous backups, 538
 data replication, 538
 database shadowing, 538
 differential backups, 536–537
 disaster recovery, 534–541
 electronic vaulting, 539
 full backups, 536
 incremental backups, 537
 remote journaling, 539
 RPO, 539–541
 RTO, 539–541
 SAN, 539
 tape rotation schemes, 537–538
 validating, 458

badges, employee access control, 355–356

banners, warning, 489

baseband transmissions, cabling, 275

baselines

NIST-800–52, 61–62
 NIST-800–53, 60–61
 risk management, 126
 scoping, 60–61, 62
 supplementation, 62
 tailoring, 61–62

bastion hosts, 324

bathhtub curves, 486–487

BCP (Business Continuity Plans)

BIA, 117–119
 MTD, 122
 potential loss assessments, 119–122

qualitative ranking, 120–121
 quantitative ranking, 121–122
 questionnaires, 119–121
 risk reduction process, 121–122
 corrective controls, 117
 detective controls, 117
 DRP, 113–115
 preventive controls, 117
 project management/initiation, 116–117
 reputations, 122–123

BEAST cryptographic attack, 240

Bell-LaPadula security model, 182–184

beta/pilot testing, 570

BIA (Business Impact Analysis), 117–119

MTD, 122
 potential loss assessments, 119–122
 qualitative ranking, 120–121
 quantitative ranking, 121–122
 questionnaires, 119–121
 risk reduction process, 121–122

Biba security model, 185–186

biometrics, 358, 370–371, 374–375

CER, 372
 facial recognition, 373
 FAR, 371
 fingerprint recognition, 373–374
 FRR, 371
 hand geometry recognition, 372
 iris recognition, 373
 retina pattern recognition, 373
 Type I errors, 371
 Type II errors, 371
 voice recognition, 373

birthday attacks, 239

blackbox testing, 420, 570

blacklists, 480

block ciphers, 205, 207–208

blockers, activity, 484

Blowfish, 210

blue boxes, 482
BlueBorne, 312
Bluejacking, 312
Bluetooth technologies, 311–312
bollards, perimeter physical control systems, 346–347
bombing email, 437
book ciphers, 302–303
Boolean operators, 208
booters, 434
BootP (Bootstrap Protocol), 269
bot herders, 435
botnets, 434–436
BPA (Business Partnership Agreements), 112
BREACH cryptographic attack, 240
breaches, data, 76–77
Brewer and Nash security model, 188
bridges, 282
broadband transmissions, cabling, 275
broken configuration management, database vulnerabilities, 586
browsers, unpatched browsers, mobile system vulnerabilities, 203
brute-force cracking, 441
buffer overflows, 196, 200, 586, 595–596
bulletproof hosting, 450
Bullrun, 331
bump keys, 354
Burp Proxy Attack tool, 200
bus topologies, 272
buses

- FireWire (IEEE 1394) interfaces, 167
- HBA, 41
- I/O bus standards, 166–167
- ISA, 166
- northbridges, 166
- PCI, 166
- PCIe, 166

SATA, 166
 SCSI, 167
 southbridges, 166
 Thunderbolt interfaces, 167
 USB, 167

business continuity, 458–459
business process recovery strategies, 524–525
business reference model, FEA frameworks, 156
BYOD policies, 169
BYOT controls, 202–203
bytecode, 595

C

C programming language, 590
C# programming language, 590
C+ programming language, 590
C++ programming language, 590
CA (Certificate Authorities), 226
CaaS (Communication-as-a-Service), 477
cable Internet access, 293–294
cabling

- attenuation, 280
- baseband transmissions, 275
- broadband transmissions, 275
- coaxial cables, 275–277
- fiber-optic cables, 277
- LAN, 275–278
- multimode fiber cables, 277
- plenum-grade cables, 277
- single-mode cables, 277

“CACPA”, 48
Caesar’s cipher, 298–299
CAIN. See CIA triad
CALEA (Communications Assistance for Law Enforcement Act), 433
call trees, 542
caller ID spoofing, 308
CAM (Content-Addressable Memory), 283

Camellia, 211**cameras, CCTV, 348–349, 496****CAN (Campus Area Networks), 278****capability tables, 388****card keys, employee access control, 355–356****card-based authentication, 369–370****CASE model, software development, 576–577****CAST (Carlisle Adams/Stafford Tavares), 211****categorization**

record retention policies, 45

threats, 107

CBC mode, DES, 213**CBC-MAC (Cipher Block Chaining-MAC), 234****CBK (Common Body of Knowledge), 21****CCTV cameras, perimeter physical control systems, 348–349****CD (Compact Discs), 165****CDAC (Content-Dependent Access Control), 389****CDN (Content Delivery Networks), 324****ceilings, facility/site security controls, 498–501****cell phones, 306–308****centralized access control, 390**

CHAP, 390

Diameter, 393

EAP, 390

MS-CHAPv2, 390

PAP, 390

RADIUS, 391–392

TACACS, 392

CER (Crossover Error Rates), 372**certificates, digital, 227–229, 370****certification**

architecture security and engineering, 194–195

CISSP exams, 20

(ISC)² website, 28

software development, 571

X.509 certificates, 370

CFAA (Computer Fraud and Abuse Act) of 1986, 72**CFB mode, DES, 213****change control, 36****change detection, 597****change management, 474–475, 580–582****changeovers, software, 572****channels, ISDN, 291–292****CHAP (Challenge-Handshake Authentication Protocol), 326, 390****checklists, disaster recovery, 521–522****checks, software, 561–562****chief security officers, data management, 34****chosen ciphertext, 238****chosen plaintext, 238****CIA triad, 30, 31–32**

availability, 31

confidentiality, 30

integrity, 31

cipher locks, 352–353**ciphers, 205**

block ciphers, 205, 207–208

s-boxes, 208

stream ciphers, 205, 208

ciphertext, 204

chosen ciphertext, 238

ciphertext-only attacks, 238

CIR (Committed Information Rates), 290**circuit switching, WAN, 291–294****circuit-level proxies, 323****CISC (Complex Instruction Set Computers), 160****CISSP exams**

answering

drag-and-drop questions, 26

hotspot questions, 26

multiple-choice questions, 26

strategies for answering, 27

assessing readiness, 20–21

- CBK, 21
- certification, 20
- fees, 20
- (ISC)2 website, 21–22, 23
- mastering, 27–28
- online resources, 28
- passing score, 20
- questions, types of, 24
 - answer strategies, 27
 - drag-and-drop questions, 24, 26
 - hotspot questions, 25, 26
 - multiple-choice questions, 24, 26
- taking exams, 22–23
- terminology, 28
- topics, 21
- civil law, U.S. legal system/laws, 71**
- Clark-Wilson security model, 187**
- classification approach, knowledge management, 38**
- classification, record retention policies, 45**
- classifying**
 - assets, 47–48
 - data, 49–50
 - commercial data, 51
 - military data, 50, 51
 - private data, 51
 - public data, 51
 - sensitivity, 50
- click-wrap license agreements, 53**
- clipping levels, 364, 365, 471–472**
- clock speeds, CPU, 159**
- cloning cell phones, 307**
- closed/open systems, 175**
- cloud computing, 294–295**
 - asset management, 477–478
 - backups, 539
 - cloud-based storage, 39–40
 - CSA, STAR ratings, 85
- clustering**
 - keys, 239
 - servers, 530, 533
- CMAC (Cipher-based MAC), 235**
- CMMI model, software development, 578–579**
- coaxial cables, 275, 277**
- COBIT (Control Objectives for Information and Related Technologies), 39, 413**
- coding**
 - assemblers, 589
 - compilers, 589
 - interpreters, 590
 - mobile code, 595
 - OOP, 591–592
 - programming languages, 588–590
 - reviewing, 425
 - scripting languages, 590
- cognitive passwords, 366–367**
- cold sites, disaster recovery, 527**
- collaboration, multimedia, 331–332**
- combination locks, 351–352**
- commercial data classification, 51**
- Common Criteria (ISO 15408), product security evaluation models, 192–194**
- common law, 71**
- communications**
 - attacks, 77
 - CaaS, 477
 - email security, 296–297
 - frequency analysis, 299
 - full duplex communication, 280
 - half duplex communication, 280
 - LAN protocols, 271–272
 - loss, 495
 - security, 298
 - 802.11 wireless networks/standards, 308–316
 - ATBASH, 299
 - Bluetooth technologies, 311–312
 - book ciphers, 302–303
 - Caesar’s cipher, 298–299
 - cell phones, 306–308
 - concealment ciphers, 302

communications

- DECT, 315
- Enigma machine, 303
- Feistel network, 303
- frequency analysis, 299
- history, 298–304
- polyalphabetic ciphers, 299–300
- Purple machine, 303, 304
- quantum cryptography, 304
- running key ciphers, 302–303
- substitution ciphers, 301–302
- TCP/IP network model, 316–320
- Vernam ciphers, 303
- Vigenere ciphers, 300–301
- VoIP, 304–306
- WAP, 315–316
- WEP, 313–315
- simplex communication, 280
- telecommunications equipment, 281

community clouds, 478**comparative analysis, passwords, 439****compartmentalized systems, MAC, 385****compartmented operation mode, 176****compilers, 589****completeness checks, 562****compliance, data governance policies, 33****computer crime/hackers, 76**

- attack methodologies, 430–431
- attack vectors, 77
- communications attacks, 77
- corporate spies, 78
- crackers, 77–78
- cyberterrorists/cybercriminals, 78
- data breaches, 76–77
- disgruntled employees, 78
- hacker researchers, 428, 429
- hactivism, 142, 428
- insurance, 93
- investigating computer crimes, 452, 459, 513
 - business continuity, 458–459

- digital forensics, 461–465
- disaster recovery, 458–459
- incident response, 453–458, 514
- interviews/interrogations, 459–460
- jurisdictions, 452–453
 - search and seizure/surveillance, 459

IOCE, 516

law enforcement/security conferences, 79

logical attacks, 77

nation-state hackers, 78

organized crime, 428

personnel security attacks, 77

phreakers, 308, 430, 482, 492

physical security attacks, 77

script kiddies, 78

skilled hackers, 428

social engineering attacks, 77

threat actors, 78

computer/device configurations, 168–170**Computer Ethics Institute, 139–140****computer forensics, 515****continuous lighting, 349****concealment ciphers, 302****conferences**

- security conferences, computer crime/hackers, 79
- web conferencing, 331

confidentiality

- CIA triad, 30

- cryptography, 203

- security models, 182

configurations

- broken configuration management, database vulnerabilities, 586

- computers/devices, 168–170

- email, 479–480

- lockdowns, 60

- managing, 474–475

- sealing, 56

construction, facility/site security controls, 498

contact smart cards, 369

contactless smart cards, 369

continuity plans, 458–459

BCP

BIA, 117–123

corrective controls, 117

detective controls, 117

DRP, 113–115

preventive controls, 117

project management/initiation, 116–117

reputations, 122–123

DRP, 113–115

continuous backups, 538

contracts of adhesion, 53

control units, 158

control zones, 198–199, 492

controls, 127–128, 130

access controls, 129–130

administrative controls, 128

application controls, 561–562

BYOT controls, 202–203

corrective controls, 568

data center controls, 241

detective controls, 568

employee access control, 355

biometrics, 358, 370–375

card keys/badges, 355–356

RFID tags, 342, 357

silent hostage (duress) alarms, 356

smart/dumb cards, 356

environmental controls/HVAC, 241, 501

fire prevention/detection/suppression controls, 241, 501, 505–506

fire suppression, 507–509

fire-detection equipment, 506–507

logical security controls, 152

perimeter physical control systems, 344, 493

bollards, 346–347

CCTV cameras, 348–349, 496

deadman doors, 346

dogs, 350

fences, 343

gates, 345–346

guards, 350

lighting, 349–350

locks, 351–355

mantraps, 346

turnstiles, 346

physical access controls, 240, 342–343, 495–496

CPTED, 496–497

perimeter physical control systems, 344–348, 493

physical controls, 129, 152

preventive controls, 568

risk assessments, 95–96

security policies, levels of control, 124

server room controls, 241

site/facility security controls, 240–241

software, 561–562

technical controls, 129

convergence, network, 304

COOP (Continuity Of Operations Plan), 111

copyrights

DMCA, 53–54

intellectual property, 74

CORBA (Common Object Request Broker Architecture), 592

cordless phones, 308

corporate spies, 78, 428

Corpus Juris Civilis, 73

corrective controls, 117, 568

COSO (Committee for Sponsoring Organizations of Treadway Commission), 142

costs

cost-benefit analysis, risk management, 106

- data governance policies, 33
- risk versus levels of control, 105–106

countermeasures, risk management

- acceptable risk, 103–105
- avoiding risk, 105
- cost of risk versus levels of control, 105–106
- mitigating risk, 105
- residual risk, 105–106
- risk reports, 106
- tolerating risk, 103–104, 105

coverage, penetration testing, 413–414**covert channels, 197–198****“CP SOW”, 47****CPTED (Crime Prevention Through Environmental Design), 496–497****CPU (Central Processing Units), 158**

- advancements, 159
- ALU, 158
- categorizing, 160
- CISC, 160
- clock speeds, 159
- control units, 158
- input, 160
- interrupts, 162
- I/O bus standards, 166–167
- memory, 159
- MIPS, 159
- multiprocessor systems, 160
- multithreaded programs, 161
- PID, 161
- problem state, 159, 160
- processes, 161
- ready state, 159
- RISC, 160
- scalar processors, 160
- superscalar processors, 160
- supervisor state, 159, 160
- threads, 161
- transistors, 159
- wait state, 159

crackers, 77–78**cracking passwords, 366, 439–442****credential stuffing, 439****credit/debit cards, PCI-DSS, 42–43****CRIME cryptographic attack, 240****crime triangles, 452****criminal law, U.S. legal system/laws, 71****CRL (Certificate Revocation Lists), 227****Cross-Site Scripting (XSS), 199, 200****cryptanalysis, 205**

- differential cryptanalysis, 238
- linear cryptanalysis, 238

crypters, 448–449**cryptography, 153, 203**

- 3DES, 215–216
- AES, 217
- algorithms, 204, 206–207
 - asymmetric cryptography, 207
 - symmetric algorithms, 207
- asymmetric encryption, 205, 207, 218–220, 237
 - Diffie-Hellman key exchanges, 220–222
 - ECC, 223
 - El Gamal, 223
 - Knapsack, 223
 - LUC algorithm, 222
 - RSA algorithm, 222
 - XTR public key cryptosystem, 222

ATBASH, 299**attacks, 237–240****authentication, 203–204, 230–231****block ciphers, 205, 207–208****book ciphers, 302–303****Caesar’s cipher, 298–299****ciphertext, 204****concealment ciphers, 302****confidentiality, 203****cryptanalysis, 205**

- CSS, 238
- DES, 211–212
 - CFB mode, 213
 - CTR mode, 214–215
 - ECB mode, 212–213
 - OFB mode, 214
- digital signatures, 205, 235–236, 237
- DRM, 205
- encryption, 203, 204, 298–304
 - 3DES, 215–216
 - AES, 217
 - asymmetric encryption, 207, 218–224, 237
 - DES, 211–215
 - end-to-end encryption, 320–321
 - hybrid encryption, 224–225
 - IDEA, 210, 218
 - link-to-link encryption, 321
 - OSI network model, 256
 - RC2, 218
 - RC4, 210, 218
 - RC5, 210–211, 218
 - Rijndael, 210, 217
 - swIPe, 320
 - symmetric encryption, 205, 208–211, 223–224, 237
 - tunneling protocols, 57–58, 319, 320
 - U.S. Government, 237
- Enigma machine, 303
- Feistel network, 303
- frequency analysis, 299
- hashing algorithms, 205, 231–233, 237
 - CBC-MAC, 234
 - CMAC, 235
 - HVAL, 234
 - HMAC, 234
 - MAC, 234–235
 - SHA-1, 233
 - SHA-2, 233
 - SHA-3, 234
- hybrid encryption, 224–225
- integrity, 204, 230–231
- Kerckhoff's Principle, 238
- key management, 205
- keys, 204
- MD algorithms, 233
- nonces, 206–207
- nonrepudiation, 204
- PKI, 153, 225–226
 - CA, 226
 - client's role, 229–230
 - CRL, 227
 - digital certificates, 227–229
 - RA, 226–227
- plaintext, 204
- polyalphabetic ciphers, 299–300
- pseudorandom numbers, 206–207
- Purple machine, 303, 304
- quantum cryptography, 304
- running key ciphers, 302–303
- s-boxes, 208
- steganography, 205
- stream ciphers, 205, 208
- substitution ciphers, 301–302
- symmetric cryptography, 207
- symmetric encryption, 205, 208–211, 223–224, 237
- TCP/IP network model, 316–320
- TPM chips, 154
- Vernam ciphers, 303
- Vigenere ciphers, 300–301
- Cryptolocker cryptographic attack, 240**
- CSA (Cloud Security Alliance), STAR ratings, 85**
- CSMA/CA (Carrier-Sense Multiple Access/Collision Avoidance), 273**
- CSMA/CD (Carrier-Sense Multiple Access/Collision Detection), 273–274**
- CSRF (Cross-Site Request Forgery), 199, 200**

CSS (Content Scrambling System), 238
CTCPEC (Canadian Trusted Computer Product Evaluation Criteria), 190
CTR mode, DES, 214–215
custodians, data, 34, 36, 136
customary law, 73
Cyber Security, 10 Steps to, 86
Cybersecurity Strategy of the European Union, 86
cyberterrorists/cybercriminals, 78

D

DAC (Discretionary Access Control), 382–383
DASD (Direct Access Storage Devices), 532
DAST (Dynamic Application Security Testing), 425
data analytics, 37
data and information recovery strategies, 534
data at rest, encryption, 55–57
data audits, 39
data breaches, 76–77
data center controls, 241
data classification, 49–50
 commercial data, 51
 military data, 50, 51
 private data, 51
 public data, 51
 sensitivity, 50
data controls, 36
data custodians, 34, 36, 136
data diddling, 198
data disposal, 46
data documentation, 36
data governance policies, 32–33
data in transit, encryption, 57–59
data labeling, 44
data lifecycle control, 38
data link layer, OSI network model, 253–254
data management, 32
 auditors, 35
 chief security officers, 34
 data audits, 39
 data custodians, 34, 36
 data documentation, 36
 data governance policies, 32–33
 data lifecycle control, 38
 data mining, 37
 data organization, 36
 data owners, 34
 data ownership, 35, 36
 data standards, 38
 data storage, 39–42
 data warehouses, 37
 developers, 34
 information security steering committees, 34
 knowledge management, 38
 responsibilities, 34–35
 roles, 34–35
 security advisor groups, 34
 senior management, 34
 users, 34
data mining, 37
data organization, 36
data owners
 data management, 34
 identification, 36
 ILM, 35
data ownership, 35
data privacy, PIA, 43–44
Data Protection Authority, 75
data purges, 46
data recovery procedures, 178, 486–487
data reference model, FEA frameworks, 156
data remanence, 46–47
data replication, 538

data sanitization, 46–47, 476–477**data security**

- authentication, 58
- defense in depth, 56
- email protocols, 58
- encryption, 55
 - authentication, 58
 - data at rest, 55–57
 - data in transit, 57–59
 - end-to-end encryption, 59
 - IPsec, 57–58
 - keys, 56–57
 - link encryption, 58–59
 - SED, 56
 - TPM chips, 55–56
 - tunneling protocols, 57–58
 - VPN, 57–58
- endpoint security, 59–60
- FTP, 57
- HTTP, 57
- insecure protocols, 57
- IPsec, 57–58
- ISO/IEC 17799, 42
- PCI-DSS, 42–43
- Privacy Rights Clearinghouse, 42
- SMTP, 57
- Telnet, 57
- tunneling protocols, 57–58
- VPN, 57–58
- zero-trust environments, 59

data standards, 38**data storage, 364**

- cloud-based storage, 39–40
- DASD, 532
- data disposal, 46
- data sanitization, 46–47
- evidence storage controls, 241
- information handling requirements, 44–45
- labeling data, 44
- MAID, 532–533
- NAS, 39–40

- record retention policies, 45
- SAN, 39–42, 278–280
- SASD, 532

data warehouses, 37**database servers, 169****databases, 580–582**

- administrators, 469
- aggregation, 583, 584
- attacks, 201–202, 437
- attributes, 583
- development security, 583–585
 - AI, 587–588
 - buffer overflows, 595–596
 - change detection, 597
 - CORBA, 592
 - expert systems, 587–588
 - integrity, 585
 - mobile code, 595
 - OOB, 591–592
 - programming languages, 588–590
 - transaction processing, 585
 - vulnerabilities, 586–587
- fields, 583
- foreign keys, 583
- granularity, 583
- hierarchical database management systems, 582
- inference, 583, 584–585
- knowledge bases, 587
- managing, 582–583
- network database management systems, 582
- object-relational database systems, 583
- primary keys, 584
- RDBMS, 582–583
- relations, 583
- shadowing, 538
- schemas, 584
- scripting languages, 590
- tuples, 583
- unpatched databases, 586

- views, 584
- vulnerabilities, 586–587
- DCS (Distributed Control Systems), 169**
- DDoS attacks, 433–434**
- DDP (Data De-Duplication), 42**
- DDR (Double Data Rates), 164**
- deadman doors, perimeter physical control systems, 346**
- debit/credit cards, PCI-DSS, 42–43**
- decentralized access control, 393–394**
- decommissioning hardware, 46–47**
- DECT (Digital Enhanced Cordless Telecommunication), 315**
- dedicated (single-state) operating systems, 177**
- dedicated operation mode, 176**
- de-encapsulation, OSI network model, 258**
- default routes, 288**
- defense in depth, 56, 152–153**
- degaussing, 46–47, 477**
- Delphi technique, qualitative assessments, 102**
- deprovisioning/provisioning, identity/access management, 376**
- DES (Data Encryption Standard), 206, 210, 211–212**
 - CBC mode, 213
 - CFB mode, 213
 - CTR mode, 214–215
 - ECB mode, 212–213
 - OFB mode, 214
- DES EDE2, 216**
- DES EDE3, 216**
- DES EEE2, 216**
- DES EEE3, 216**
- design guidelines, architecture security, 152–155**
- design specifications, software, 566**
- destroying media/hardware, 477**
- detection, alarms, 511–512**
- detective controls, 414, 568**
- detective controls, BCP, 117**
- developers, data management, 34**
- development methodologies, software**
 - agile development, 577–578
 - CASE model, 576–577
 - CMMI model, 578–579
 - IDEAL model, 579
 - incremental development, 575
 - JAD model, 575
 - maturity models, 578–579
 - MPM model, 576
 - prototyping, 575–576
 - RAD model, 575
 - spiral model, 574
 - waterfall model, 573
- development security, databases, 583–585**
 - AI, 587–588
 - buffer overflows, 595–596
 - change detection, 597
 - CORBA, 592
 - expert systems, 587–588
 - integrity, 585
 - mobile code, 595
 - OOP, 591–592
 - programming languages, 588–590
 - transaction processing, 585
 - vulnerabilities, 586–587
- development security, software, 560**
 - buffer overflows, 595–596
 - change detection, 597
 - change management, 580–582
 - CORBA, 592
 - database management, 582–583
 - environment security, 592–595
 - lifecycles, 560–561
 - mobile code, 595
 - OOP, 591–592
 - programming languages, 588–590
 - scheduling, 580

- SDLC, 563
 - acceptance testing/implementation, 569–571
 - building/development, 567–569
 - design specifications, 566
 - development methodologies, 573–579
 - disposal, 572
 - ERD, 565–566
 - functional requirements/planning, 565–566
 - operations/maintenance, 571–572
 - project initiation, 564–565
 - reverse engineering, 569
 - stages of, 563–564
 - system failure, avoiding, 561–562
 - application controls, 561–562
 - avoiding system failure, 562
 - checks, 561–562
- device/computer configurations, 168–170**
- device locks, 353**
- diagramming, potential attacks, 107**
- dialing, war, 420–421**
- dialing systems, outband, 542**
- Diameter, centralized access control, 393**
- dictionary cracking, 439–440**
- differential backups, 536–537**
- differential cryptanalysis, 238**
- Diffie-Hellman key exchanges, 220–222**
- digital certificates, 227–229, 370**
- digital forensics, 515–516**
 - acquisition, 516, 517–519
 - analytics, 517, 520–521
 - authentication, 516–517, 520
 - procedures, 516
 - stages of, 515
 - types of, 514–515
- digital signatures, 205, 235–236, 237**
- direct OS commands, web-based vulnerabilities, 199**
- direct-access storage, 165**
- Directive on Data Protection, 1998, 76**
- directory traversal attacks, 199**
- disaster recovery, 458–459, 493–494**
 - awareness, 545
 - backups, 534–541
 - business process recovery strategies, 524–525
 - checklists, 521–522
 - cold sites, 527
 - data and information recovery strategies, 534
 - employee services, 543–544
 - facility recovery strategies, 525–528
 - fault tolerance, 530–534
 - flat tires, 522–523
 - hot sites, 525–526
 - implementing plans, 544–545
 - insurance, 544
 - interfacing with external groups, 542–543
 - lifecycle of, 521–523
 - maintaining plans, 547–548
 - mobile sites, 527–528
 - monitoring recovery plans, 547–548
 - operations recovery strategies, 529–532
 - organizational functions and recovery times, 535–536
 - personnel mobilization, 542
 - plan design/development, 541–544
 - reciprocal agreements, 528
 - redundant sites, 527
 - strategies, 524–532
 - subscription services, 525–527
 - supply recovery strategies, 525–528
 - teams/responsibilities, 523
 - tertiary sites, 525
 - testing recovery plans, 546–547
 - user recovery strategies, 528–529
 - warm sites, 526

discovery scans, networks

discovery scans, networks, 418

disgruntled employees, computer crime/hackers, 78

disk encryption, 60

disposal

data, 36, 46

software, 572

distance-vector protocols, 288–289

distributed computing, 533–534

diving, dumpster, 444

DMA, I/O using DMA, 162

DMCA (Digital Millennium Copyright Act), 53–54

DMZ (Demilitarized Zones), 324–325

DNS (Domain Name System), 268

DNS spoofing, 437

DNSSEC (Domain Name System Security), 268

documentation

ATO, 111

BCP

BIA, 117–123

corrective controls, 117

detective controls, 117

DRP, 113–115

preventive controls, 117

project management/initiation, 116–117

reputations, 122–123

BIA questionnaires, 119–121

BPA, 112

COOP, 111

data, 36

DRP, 113–115

IA, 111

ISA, 110

MOU, 111

NDA, 112

OLA, 111

risk reports, 106

SAS 70, 112

security policies, 124

SLA, 111, 495

UA, 111

dogs, perimeter physical control systems, 350

doors, facility/site security controls, 498–501

DoS (Denial of Service)

attacks, 305, 433, 586

testing, 420

doxing, 428

drag-and-drop questions, CISSP exams, 24, 26

DRAM (Dynamic Random-Access Memory), 163–164

DREAD, threat modeling, 109

drive wiping, 47, 477

driving, war, 437

DRM (Digital Rights Management), 205

DROWN cryptographic attack, 240

DRP (Disaster Recovery Plans), 113–115

DSA (Digital Signature Algorithms), 236, 237

DSL (Digital Subscriber Line), 293

DSSS (Direct-Sequence Spread Spectrum), 308

due care, 72, 472–473

due diligence, 72, 472–473

dumb cards, employee access control, 356

dumpster diving, 444

duplicate checks, 562

duress (silent hostage) alarms, 356

duties, separation of, 131–132, 469–470, 471

DVD (Digital Video Discs), 166

dwelling time, 308

dynamic NAT, 325

dynamic passwords, 365–366

dynamic routing, 288

E**EA (Enterprise Architectures), 155**

- FEA frameworks, 156
- ISO 27000 series standards, 157
- SABSA, 156–157
- Zachman Framework, 155–156

EAL (Evaluation Assurance Levels), 192–193**EAP (Extensible Authentication Protocol), 320, 326–328, 390****EAP-FAST, 327****EAP-LEAP, 327****EAP-MD5, 327****EAP-PEAP, 327****EAP-SIM, 327****EAP-TTLS, 327****eavesdropping, 306, 442****ECB mode, DES, 212–213****ECC (Elliptical Curve Cryptosystem), 223****Economic Espionage Act of 1996, 72****educating employees, 134–135****EGP (Exterior Gateway Protocol), 289****Ei Gamal, 223****electric lock pick guns, 355****electrical power, facility/site security controls, 503–504****electronic vaulting, 539****email**

- asset management, 478
- bombing attacks, 437
- configurations, 479–480
- IMAP, 479
- message privacy, 331–332
- POP, 479
- security, 296–297
- SMTP, 268, 479
- standard email protocols, data security, 58

emanations, 198–199, 492**embedded devices, 169–170****EMI (Electromagnetic Interference), 503****employees**

- access control, 355
 - biometrics, 358, 370–375
 - card keys/badges, 355–356
 - RFID tags, 342, 357
 - silent hostage (duress) alarms, 356
 - smart/dumb cards, 356
- audits, 548
- awareness, disaster recovery, 545
- disaster recovery services, 543–544
- disgruntled employees, computer crime/hackers, 78
- HIPAA, 79–80
- job descriptions, 547
- performance reviews, 548
- personnel security, 130
 - background checks, 131
 - educating employees, 134–135
 - employee awareness, 134–136
 - ethics training/awareness, 137–143
 - job rotation, 132
 - least privilege, 132–133
 - mandatory vacations, 133
 - NDA, 131
 - new-hire agreements/policies, 131
 - separation of duties, 131–132
 - social engineering, 136–137
 - social networking, 131
 - termination of employees, 133–134
 - training employees, 134–135
- training, disaster recovery, 545

enabled features (unnecessary), database vulnerabilities, 586**encapsulation**

- OOP, 591
- OSI network model, 256, 257–258

encryption, 55, 203, 204

- 3DES, 206, 215–216
- AES, 217

encryption

- asymmetric encryption, 207, 218–220, 237
 - Diffie-Hellman key exchanges, 220–222
 - ECC, 223
 - El Gamal, 223
 - Knapsack, 223
 - LUC algorithm, 222
 - RSA algorithm, 222
 - XTR public key cryptosystem, 222
 - ATBASH, 299
 - authentication, 58
 - Blowfish, 210
 - book ciphers, 302–303
 - Caesar's cipher, 298–299
 - Camellia, 211
 - CAST, 211
 - concealment ciphers, 302
 - data at rest, 55–57
 - data in transit, 57–59
 - DES, 206, 210, 211–212
 - CBC mode, 213
 - CFB mode, 213
 - CTR mode, 214–215
 - ECB mode, 212–213
 - OFB mode, 214
 - disk encryption, 60
 - end-to-end encryption, 59, 320–321
 - Enigma machine, 303
 - Feistel network, 303
 - frequency analysis, 299
 - hybrid encryption, 224–225
 - IDEA, 210, 218
 - IPsec, 57–58
 - keys, 56–57
 - link encryption, 58–59
 - link-to-link encryption, 321
 - MARS, 211
 - OSI network model, 256
 - polyalphabetic ciphers, 299–300
 - Purple machine, 303, 304
 - RC2, 218
 - RC4, 210, 218
 - RC5, 210–211, 218
 - Rijndael, 210, 217
 - running key ciphers, 302–303
 - SAFER, 211
 - SED, 56
 - Skipjack, 211
 - substitution ciphers, 301–302
 - swIPE, 320
 - symmetric encryption, 205, 208–211, 223–224, 237
 - TPM chips, 55–56
 - tunneling protocols, 57–58
 - L2TP, 320
 - PPTP, 320
 - SSTP, 319
 - Twofish, 210
 - U.S. Government, 237
 - Vernam ciphers, 303
 - Vigenere ciphers, 300–301
 - VPN, 57–58
- end-of-life provisions, 36**
- endpoint security, 59–60**
- end-to-end encryption, 59, 320–321**
- engineering and architecture security, 152, 170, 172–175**
- accreditation, 195
 - certification, 194–195
 - computer/device configurations, 168–170
 - CPU, 158–163
 - cryptography, 203
 - 3DES, 215–216
 - AES, 217
 - algorithms, 204, 206–207
 - asymmetric encryption, 205, 207, 218–224, 237
 - attacks, 237–240
 - authentication, 203–204, 230–231
 - block ciphers, 205, 207–208
 - ciphertext, 204

- confidentiality, 203
- cryptanalysis, 205
- CSS, 238
- DES, 211–215
- digital signatures, 205, 235–236, 237
- DRM, 205
- encryption, 203, 204
- hashing algorithms, 205, 231–236, 237
- hybrid encryption, 224–225
- integrity, 204, 230–231
- Kerckhoff's Principle, 238
- key management, 205
- keys, 204
- MD algorithms, 233
- nonces, 206–207
- nonrepudiation, 204
- plaintext, 204
- pseudorandom numbers, 206–207
- s-boxes, 208
- steganography, 205
- stream ciphers, 205, 208
- symmetric encryption, 205, 208–211, 223–224, 237
- defense in depth design process, 152–153
- design guidelines, 152–155
- EA, 155–157
- frameworks, 154–155
- fundamentals, overview, 158
- I/O bus standards, 166–167
- open/closed systems, 175
- operating states, 177–178
- PKI, 153, 225–226
 - CA, 226
 - client's role, 229–230
 - CRL, 227
 - digital certificates, 227–229
 - RA, 226–227
- process control, 157–158
- process isolation, 179
- product security evaluation models, 189
 - Common Criteria (ISO 15408), 192–194
 - CTCPEC, 190
 - ITSEC, 191–192
 - Rainbow Series, The, 189–191
 - TCSEC, 189–190, 191–192
- protection rings, 170–172
- recovery procedures, 178, 486–487
- regulatory compliance, 157–158
- security models, 179, 189
 - Bell-LaPadula model, 182–184
 - Biba model, 185–186
 - Brewer and Nash model, 188
 - Clark-Wilson model, 187
 - Graham-Denning model, 188
 - Harrison-Ruzzo-Ullman model, 188
 - information flow model, 182
 - Lattice model, 188
 - Lipner model, 188
 - noninterference model, 182
 - state machine model, 180–181
 - Take-Grant model, 188
- security modes of operation, 176–177
- site/facility controls, 240–241
- storage media, 163
 - CD, 165
 - direct-access storage, 165
 - DVD, 166
 - flash memory storage, 166
 - I/O bus standards, 166–167
 - optical media, 165
 - RAM, 163–164, 167–168
 - ROM, 164–165
 - secondary storage, 165–166
 - sequential storage, 165
 - software, 165
 - SSD, 166
- swap partitions, 167–168
- system validation, 194

- TPM chips, 154
- virtual memory, 167–168
- VM, 168
- vulnerabilities, 195–196
 - backdoors, 197
 - buffer overflows, 196, 200, 595–596
 - covert channels, 197–198
 - data diddling, 198
 - database attacks, 201–202
 - emanations, 198–199
 - incremental attacks, 198
 - maintenance hooks, 197
 - mobile system vulnerabilities, 202–203
 - salami attacks, 198
 - SQL injections, 201–202, 586
 - state attacks, 197
 - Van Eck Phreaking, 199, 492
 - web-based vulnerabilities, 199–202
 - wireless vulnerabilities, 202
- Enigma machine, 303**
- environmental controls/HVAC, 241, 501, 502–503**
- EPO (Emergency Power Off), 504**
- equipment failure, 495**
- equipment lifecycles, 54–55, 505**
- ERD (Entity Relationship Diagrams), 565–566**
- escalation of privilege, 431, 586**
- ESP (Encapsulating Security Payloads), 329**
- Ethernet**
 - FCoE, 41
 - frames, 271–272
- ethics training/awareness, 137–138**
 - 10 Commandments of Computer Ethics, 139–140
 - common fallacies, 141–142
 - Computer Ethics Institute, 139–140
 - IAB, 140–141
 - (ISC)2 Code of Ethics, 138–139
 - ISOC, 140–141
 - NIST SP 80–14, 141
 - regulatory requirements, 142–143
 - RFC 1087, 140–141
- EU (European Union)**
 - 1998 Directive on Data Protection, 76
 - Cybersecurity Strategy of the European Union, 86
 - Data Protection Authority, 75
 - right to be forgotten, 75
- event logs, 416**
- evidence**
 - hearsay evidence, U.S. legal system/laws, 72
 - storage controls, 241
- exams, CISSP**
 - answer strategies, 24–27
 - assessing readiness, 20–21
 - CBK, 21
 - certification, 20
 - drag-and-drop questions, 24, 26
 - fees, 20
 - hotspot questions, 25, 26
 - (ISC)2 website, 21–22, 23
 - mastering, 27–28
 - multiple-choice questions, 24, 26
 - online resources, 28
 - passing score, 20
 - taking exams, 22–23
 - terminology, 28
 - topics, 21
 - types of questions, 24
- existence checks, 562**
- expert systems, 587–588**
- exploit kits, 450**
- extensive privileges, database vulnerabilities, 586**
- exterior gateway protocols, 289**
- external audits, 413**
- external groups (disaster recovery), interfacing with, 542–543**

F

- facial recognition, 373**
- facility recovery strategies, 525–528**
- facility/site security controls, 240–241, 495–496**
 - area concerns, 497
 - asset placement, 498–501
 - ceilings, 498–501
 - construction, 498
 - CPTED, 496–497
 - doors, 498–501
 - electrical power, 503–504
 - environmental controls/HVAC, 502–503
 - equipment lifecycles, 505
 - location, 498
 - UPS, 504–505
 - walls, 498–501
 - windows, 498–501
- Fagan inspections, 426**
- failure states, 562**
- failures (system), avoiding, 561–562**
- FAIR (Factor Analysis of Information Risk), 87**
- FAR (False Acceptance Rates), 371**
- Fast-Flux botnets, 435**
- fast-injection viruses, 597–598**
- fault tolerance, 486**
 - disaster recovery, 530–534
 - RAID, 530–532
- faxes, operational security, 482**
- FCoE (Fibre Channel over Ethernet), 41**
- FCPA (Foreign Corrupt Practices Act), 142**
- FDA Resources of Data Management, 38**
- FEA frameworks, 156**
- Federal Sentencing Guidelines of 1991, 72**
- federation, identity/access management, 377**
- fees, CISSP exam, 20**
- Feistel network, 303**
- fences, perimeter physical control systems, 344–345**
- FHSS (Frequency-Hopping Spread Spectrum), 308**
- fiber-optic cables, 277**
- field devices, 169**
- fields, databases, 583**
- file servers, 168–169**
- filters, packet, 322**
- FIM (Federated Identity Management), 361**
- final testing, 570**
- financial attacks, 596–597**
- fingerprint recognition, 373–374**
- FIPS (Federal Information Processing Standards), 82**
 - FIPS 199, 82
 - FIPS 200, 82
- fire detectors, 501**
- fire escapes, 501**
- fire prevention/detection/suppression controls, 241, 501, 505–506**
 - fire suppression, 507–509
 - fire-detection equipment, 506–507
- firewalls, 322, 481**
- FireWire (IEEE 1394) interfaces, 167**
- firing employees, 133–134**
- FISMA (Federal Information Security Management Act), 81**
- flash memory storage, 166**
- flat tires, disaster recovery, 522–523**
- foot-candles, 349**
- foreign government agents, threat actors, 429**
- foreign keys, databases, 583**
- forensics, digital, 515–516**
 - acquisition, 516, 517–519
 - analytics, 517, 520–521
 - authentication, 516–517, 520
 - procedures, 516

- stages of, 515
- types of, 514–515

FOUO, data classification, 50

frame relays, 290

frames, 258, 271–272

frameworks

- governance frameworks, 154–155
- ISO/IEC 19249, 154–155
- ITIL, 155
- NIST Risk Management Framework, 87
- Protection of Information in Computing Systems, The [ital]154
- Zachman Framework, 155–156

FRAP (Facilitated Risk Analysis Process), 102

fraud, CFAA of 1986, 72

FREAK cryptographic attack, 240

frequency analysis, 299

Fresnel lenses, 349

Friedman, William, 304

FRR (False Rejection Rates), 371

FSTP (FTP Secure), 317

FTP (File Transfer Protocol), 57, 267–268, 324

full backups, 536

full duplex communication, 280

fully connected topologies, 275

function testing, 570

functional requirements/planning, SDLC, 565–566

fuzz testing, 426

G

G8 (Group of Eight), 473

GAN (Global Area Networks), 278

Gantt chart, 580

gates, perimeter physical control systems, 345–346

gateways, 287

gateway-to-gateway architectures, 330

gateway-to-gateway tunneling protocols, 58

generic smart cards, 369

GFS tape-rotation schemes, 537

glare protection, 350

GLBA (Gramm-Leach-Bliley Act), 80

global legal/regulatory issues, 74–75

- Data Protection Authority, 75
- right to be forgotten, 75

governance, security, 70

- computer crime/hackers, 76
 - attack vectors, 77
 - communications attacks, 77
 - corporate spies, 78
 - crackers, 77–78
 - cyberterrorists/cybercriminals, 78
 - data breaches, 76–77
 - disgruntled employees, 78
 - hactivism, 142
 - law enforcement/security conferences, 79
 - logical attacks, 77
 - nation-state hackers, 78
 - personnel security attacks, 77
 - physical security attacks, 77
 - script kiddies, 78
 - social engineering attacks, 77
 - threat actors, 78
- global legal/regulatory issues, 74–75
 - Data Protection Authority, 75
 - right to be forgotten, 75
- holistic enterprise security systems, 71

international legal system/laws, 72–73

- 1998 Directive on Data Protection, 76
- Corpus Juris Civilis, 73
- customary law, 73
- halakha law, 73
- intellectual property, 73–74
- mixed law systems, 73

- Napoleonic law, 73
 - religious law, 73
 - sharia law, 73
 - policies, assets, 51–52
 - privacy laws, 75–76
 - sexual harassment, 79
 - U.S. legal system/laws
 - administrative (regulatory) law, 71
 - CFAA (Computer Fraud and Abuse Act) of 1986, 72
 - civil law, 71
 - common law, 71
 - criminal law, 71
 - due care, 72
 - due diligence, 72
 - Economic Espionage Act of 1996, 72
 - Federal Sentencing Guidelines of 1991, 72
 - hearsay evidence, 72
 - Identity Theft and Assumption Deterrence Act of 1998, 76
 - personal information websites, 76
 - Privacy Act of 1974, The, 75
 - privacy laws, 75–76
 - stare decisis, 71
 - U.S. Child Pornography Prevention Act of 1996, 72
 - U.S. Patriot Act of 2001, 72
 - governance frameworks, 154**
 - ISO/IEC 19249, 154–155
 - ITIL, 155
 - Protection of Information in Computing Systems, The [ital]154
 - governance policies, data, 32–33**
 - Graham-Denning security model, 188**
 - granularity, databases, 583**
 - graybox testing, 420**
 - graylists, 480**
 - grid computing, 533–534**
 - guards, perimeter physical control systems, 350**
 - guidelines, risk management, 127**
- ## H
-
- hackers/computer crime, 76**
 - attack methodologies, 430–431
 - attack vectors, 77
 - communications attacks, 77
 - corporate spies, 78
 - crackers, 77–78
 - cyberterrorists/cybercriminals, 78
 - data breaches, 76–77
 - disgruntled employees, 78
 - hacker researchers, 428, 429
 - hactivism, 142, 428
 - insurance, 93
 - investigating computer crimes, 452, 459, 513
 - business continuity, 458–459
 - digital forensics, 461–465
 - disaster recovery, 458–459
 - incident response, 453–458, 514
 - interviews/interrogations, 459–460
 - jurisdictions, 452–453
 - search and seizure/surveillance, 459
 - IOCE, 516
 - law enforcement/security conferences, 79
 - logical attacks, 77
 - nation-state hackers, 78
 - organized crime, 428
 - personnel security attacks, 77
 - phreakers, 308, 430, 482, 492
 - physical security attacks, 77
 - script kiddies, 78
 - skilled hackers, 428
 - social engineering attacks, 77
 - threat actors, 78
- halakha law, 73**
 - half duplex communication, 280**
 - halon fire suppression, 508–509**
 - hand geometry recognition, 372**
 - Hanoi, Tower of, 538**

hard changeovers, software

hard changeovers, software, 572

hard drives, SED, 56

hardware

bridges, 282

configuration lockdowns, 60

data sanitization, 476–477

decommissioning, 46–47

degaussing, 477

destroying, 477

disk encryption, 60

drive wiping, 47, 477

equipment lifecycles, 54–55, 505

forensics, 515

gateways, 287

hubs, 281

keystroke loggers, 403

mirrored ports, 284

network taps, 284

repeaters, 281

routers, 285–286

routine maintenance, 54

SED, 56

switches, 282–283

technical support, 54–55

zeroization, 477

zero-trust environments, 59

Harrison-Ruzzo-Ullman security model, 188

hashing algorithms, 205, 231–233, 237

HAVAL, 234

MAC, 234–235

CBC-MAC, 234

CMAC, 235

HMAC, 234

SHA-1, 233

SHA-2, 233

SHA-3, 234

HAVAL, 234

HBA (Hot Bus Adapters), 41

HDLC (Hugh-Level Data Link Control), 294

headers, 257

AH, 329

UDP, 266–267

hearsay evidence, U.S. legal system/laws, 72

heuristic scanning, 483

HIDS (Host-Based Intrusion Detection Systems), 398, 512

hierarchical database management systems, 582

hierarchical designs, MAC, 385

high-impact assets, 92–93

high-risk assets, 92–93

hijacking sessions, 431–432

HIPAA (Health Insurance Portability and Accountability Act), 79–80

HMAC (Hash-based Message Authentication Code), 234

hoaxes, virus, 444

holistic enterprise security systems, 71

honeypots/honeynets, operational security, 484–485

hopping, VLAN, 285

host-to-gateway architectures, 330

host-to-host architectures, 330

host-to-host (transport) layer, TCP/IP network model, 259–260, 318–319

TCP, 264–266, 267

UDP, 264–265, 266–267

Host-to-LAN tunneling protocols, 58

hot fixes, 595

hot sites, disaster recovery, 525–526

hotspot questions, CISSP exams, 25, 26

HR, need for, 128

HSSI (High-Speed Serial Interface), 294

HTML programming language, 590

HTTP (HyperText Transfer Protocol), 269, 324

data security, 57

S-HTTP, 317

hubs, 281

human-caused threats, 494–495

HVAC/environmental controls, 241, 501, 502–503

hybrid attacks, 440

hybrid clouds, 478

hybrid designs, MAC, 385

hybrid encryption, 224–225

I

IA (Interoperability Agreements), 111

laaS (Infrastructure-as-a-Service), 294–295, 478

IAB (Internet Architecture Board), ethics training/awareness, 140–141

IAL (Identity Assurance Levels), 360

IAM (INFOSEC Assessment Methodology), 102

IAST (Interactive Application Security Testing), 425

ICMP (Internet Control Message Protocol), TCP/IP network model, 263

ICS (Industrial Control Systems), 169

IDaaS (Identity as a Service), 362–363

IDEA (International Data Encryption Algorithm), 210, 218

IDEAL model, software development, 579

identifying assets, 91–93, 107

identity theft, 443

Identity Theft and Assumption Deterrence Act of 1998, 76

identity/access management, 342, 358–359, 377

accountability, 343

authentication, 342–343, 358–361

AAL, 360

biometrics, 370–375

card-based authentication, 369–370

CHAP, 390

digital certificates, 370

EAP, 390

FIM, 358–360

IAL, 360

IDaaS, 358–360

MS-CHAPv2, 390

multifactor authentication, 375

OAuth, 362

OpenID, 362

PAP, 390

passwords, 363–367

SAML, 361–362

strong authentication, 375

tokens, 367–368

two-factor authentication, 375

authorization, 343, 382

ABAC, 387–388

audits, 394–396

CDAC, 389

centralized access control, 390–393

DAC, 382–383

decentralized access control, 393–394

IDS, 396–401, 510–511, 512–513

IPS, 384, 401

keystroke monitoring, 402–403

LBAC, 389

MAC, 383–385

monitoring access, 394–396

NAC, 401–402

RBAC, 385–387

rule-based access control, 388

SIEM, 401

employee access control, 355

biometrics, 358, 370–375

card keys/badges, 355–356

RFID tags, 342, 357

silent hostage (duress) alarms, 356

smart/dumb cards, 356

federation, 377

Kerberos, 378–381

least privilege, 343

- lifecycles, 376
- perimeter physical control systems, 344
 - bollards, 346–347
 - CCTV cameras, 348–349, 496
 - deadman doors, 346
 - dogs, 350
 - fences, 343
 - gates, 345–346
 - guards, 350
 - lighting, 349–350
 - locks, 351–355
 - mantraps, 346
 - turnstiles, 346
- physical access controls, 342–343, 344–348
- profile management, 377
- SESAME, 381
- SPML, 378
- SSO, 343, 378
- user provisioning, 376
- WS-Security, 377
- XML, 377
- IDS (Intrusion Detection Systems), 396–397, 510–511**
 - anomaly-based IDS, 399–400
 - HIDS, 398, 512
 - NIDS, 397–398, 512
 - rule-based IDS, 400
 - sensor placement, 400–401
 - signature-based IDS, 399
- IEEE 1394 (FireWire) interfaces, 167**
- IGMP (Internet Group Management Protocol), TCP/IP network model, 264**
- IKE (Internet Key Exchange), 329–330**
- ILM (Information Lifecycle Management), 35**
- IM (Instant Messaging), 331**
- images, digital forensics**
 - primary images, 520
 - working images, 520
- IMAP (Internet Message Authentication Protocol), 269, 479**
- impact scale, qualitative assessments, 100–101**
- impersonation attacks, 444**
- implementing disaster recovery plans, 544–545**
- incident response, computer crime investigations, 453–458, 514**
- incremental attacks, 198**
- incremental backups, 537**
- incremental development, software, 575**
- inference**
 - attacks, 321
 - databases, 583, 584–585
- information flow security model, 182**
- information handling requirements, data storage, 44–45**
- information security steering committees, data management, 34**
- informative policies, 125–126**
- insecure protocols, data security, 57**
- insecure/jailbroken devices, 203**
- insiders/disgruntled employees, 428**
- insurance**
 - disaster recovery, 544
 - hackers/computer crime, 93
- integer overflow, 426–427**
- integrity**
 - checking, 483
 - CIA triad, 31
 - cryptography, 204, 230–231
 - databases, 585
 - digital forensics, authentication, 520
 - security models, 185–188
- intellectual property**
 - copyrights, 74
 - international legal system/laws, 73–74
 - service marks, 73
 - trade secrets, 73–74
 - trademarks, 73
- interface testing, 569**

- interfacing with external groups, disaster recovery, 542–543**
- internal audits, 413**
- international governance standards, 86**
 - 10 Steps to Cyber Security, 86
 - Cybersecurity Strategy of the European Union, 86
 - ISO, 83–85
 - ITIL, 82–83
 - OECD, 85–86
 - STAR ratings, CSA, 85
- international legal system/laws, 72–73**
 - 1998 Directive on Data Protection, 76
 - Corpus Juris Civilis, 73
 - customary law, 73
 - halakha law, 73
 - intellectual property, 73–74
 - IOCE, 516
 - mixed law systems, 73
 - Napoleonic law, 73
 - religious law, 73
 - sharia law, 73
- Internet layer, TCP/IP network model, 260, 319–320**
 - ARP, 263–264
 - ICMP, 263
 - IGMP, 264
 - IP, 260–262
- interpreters, 590**
- interrogations/interviews, investigating computer crimes, 459–460**
- interrupt-driven I/O, 162**
- interrupts, CPU, 162**
- interviews/interrogations, investigating computer crimes, 459–460**
- intrusion detection, IDS, 396–397, 510–511**
 - anomaly-based IDS, 399–400
 - HIDS, 398, 512
 - NIDS, 397–398, 512
 - rule-based IDS, 400
 - sensor placement, 400–401
 - signature-based IDS, 399
- inventories, assets, 47–48**
- investigating computer crimes, 452**
 - digital forensics, 461–465
 - incident response, 453–458, 514
 - IOCE, 516
 - jurisdictions, 452–453
 - operational security, 513
- I/O**
 - bus standards, 166–167
 - interrupt-driven I/O, 162
 - I/O using DMA, 162
 - memory-mapped I/O, 162
 - port-mapped I/O, 162
 - programmed I/O, 162
- IOC (Indicators of Compromise), 597**
- IOCE (International Organization of Computer Evidence), 516**
- IoT (Internet of Things), 169–170**
- IP (Internet Protocol)**
 - SKIP, 319
 - swIPE, 320
 - TCP/IP network model, 260–262
 - VoIP, 304–306
- IPS (Intrusion Prevention Systems), 384, 401**
- IPsec (IP Security), 57–58, 329–330**
- iris recognition, 373**
- ISA (Interconnection Security Agreements), 110, 166**
- (ISC)2**
 - Code of Ethics, 138–139
 - website, 21–22, 23, 28
- iSCSI (Internet Small Computer System Interface), 40–41**
- ISDN (Integrated Services Digital Network), 291–292**
- ISO (International Organization for Standardization)**
 - ISO 9001, 84
 - ISO 15408 (Common Criteria), 192–194

ISO (International Organization for Standardization)

ISO 27001, 84–85, 157
 ISO 27002, 83, 157
 ISO 27003, 157
 ISO 27004, 84, 157
 ISO 27005, 84, 157
 ISO 27799, 84
 ISO/IEC 17799, 42
 ISO/IEC 19249, 154–155
 ISO/IEC 27002, sexual harassment, 79

ISOC (Internet Society), ethics training/awareness, 140–141

isolating processes, 179

ITIL (Information Technology Infrastructure Library), 82–83, 155

ITSEC (Information Technology Security Evaluation Criteria), 191–192

J

JAD model, software development, 575

jailbroken/insecure devices, 203

Java programming language, 590, 595

JFK Records Act, 45

jobs

descriptions, 547
 rotation, 132, 471

joins, LBAC, 389

journaling, remote, 539

jurisdictions, computer crime investigations, 452–453

K

kanban, 578

Kerberos, 378–381

Kerckhoff's Principle, 238

kernels, security, 174

key cards, employee access control, 355–356

keys

bumping, 354
 clustering, 239

cryptographic keys, 204

Diffie-Hellman key exchanges, 220–222

encryption keys, 56–57

foreign keys, databases, 583

IKE, 329–330

managing, 205

primary keys
 databases, 584
 ERD, 565

SKIP, 319

space, 206

symmetric encryption, 210

XTR public key cryptosystem, 222

keystroke monitoring, 402–403, 491–492

Knapsack, 223

knowledge bases, 587

knowledge management, 38

classification approach, 38
 probabilistic approach, 38
 statistical approach, 38

known plaintext attacks, 238

KPI (Key Performance Indicators), 414–415

KRI (Key Risk Indicators), 415

L

L2TP (Layer 2 Tunneling Protocol), 320

labeling data, 44

LAN (Local Area Networks), 271, 278

cabling, 275–278
 communication protocols, 271–272
 Ethernet frames, 271–272
 tokens, 272
 VLAN, 282, 284–285
 VXLAN, 284–285
 WLAN, 309, 312–313

LAN-to-LAN tunneling protocols, 58

laptops, 169

Lattice security model, 188

**law enforcement, computer crime/
hackers, 79****law/legal compliance, data
governance policies, 33****laws/legal systems**

- global legal/regulatory issues, 74–75

- Data Protection Authority, 75

- right to be forgotten, 75

- international legal system/laws, 72–73

- 1998 Directive on Data Protection, 76

- Corpus Juris Civilis, 73

- customary law, 73

- halakha law, 73

- intellectual property, 73–74

- IOCE, 516

- mixed law systems, 73

- Napoleonic law, 73

- religious law, 73

- sharia law, 73

- privacy laws, 75–76

- U.S. legal system/laws

- administrative (regulatory) law, 71

- CALEA, 433

- CFAA (Computer Fraud and Abuse Act) of 1986, 72

- civil law, 71

- common law, 71

- criminal law, 71

- due care, 72

- due diligence, 72

- Economic Espionage Act of 1996, 72

- FCPA, 142

- Federal Sentencing Guidelines of 1991, 72

- FIPS, 82

- FISMA, 81

- GLBA, 80

- hearsay evidence, 72

- HIPAA, 79–80

- Identity Theft and Assumption Deterrence Act of 1998, 76

- keystroke monitoring, 492

- NIST, 82

- personal information websites, 76

- Privacy Act of 1974, The, 75

- privacy laws, 75–76

- SOX, 81, 142, 472

- stare decisis, 71

- U.S. Child Pornography Prevention Act of 1996, 72

- U.S. Patriot Act of 2001, 72

- U.S. Securities Act of 1933, 472

LBAC (Lattice-Based Access Controls), 389**LDAP (Lightweight Directory Access Protocol), 270****leaks, memory, 164****least privilege, 132–133, 343, 468, 471****levels of control, security policies, 124****liability, data governance policies, 33****licensing software, 52–53**

- click-wrap license agreements, 53

- contracts of adhesion, 53

- DMCA, 53–54

- master license agreements, 53

- shrink-wrap license agreements, 53

lifecycles

- equipment, 54–55, 505

- software, 560–561, 563

- acceptance testing/
implementation, 569–571

- building/development, 567–569

- design specifications, 566

- ERD, 565–566

- functional requirements/planning, 565–566

- operations/maintenance, 571–572

- project initiation, 564–565

- reverse engineering, 569

- stages of, 563–564

lifestyle control, data, 38**lifetimes, session, 202**

lighting, perimeter physical control systems

lighting, perimeter physical control systems, 349–350

limit checks, 562

linear cryptanalysis, 238

link encryption, 58–59

link-state protocols, 289

link-to-link encryption, 321

Lipner security model, 188

location

facility/site security controls, 498

redundancy, 41

lock pick sets, 355

lock shims, 355

lockdowns, configuration, 60

locks, perimeter physical control systems, 351–355

log reviews, 415–418

logic bombs, 446–447, 596–597

logic checks, 562

logical attacks, 77

logical security controls, 152

lookups, table, 562

losses

ALE, 97, 98–99, 106

potential loss assessments, 119–122

threat analysis, 94

LPD (Line Printer Daemon), 270

LUC algorithm, 222

lumens, 349

LUN masking, 41

lux, 349

M

MaaS (Monitoring-as-a-Service), 477

MAC (Mandatory Access Control), 177, 383–385

MAC (Message Authentication Code), 234

CBC-MAC, 234

CMAC, 235

HMAC, 234

magnetic stripe cards, 370

MAID (Massive Array of Inactive Disks), 532–533

maintenance

disaster recovery plans, 547–548

hooks, 197

routine maintenance, equipment lifecycles, 54, 505

SDLC, 571–572

malicious software threats/attacks, 444–445

APT, 450

backdoors, 447–449

crypters, 448–449

exploit kits, 450

logic bombs, 446–447

packers, 448

ransomware, 450–451

rootkits, 449–450

success attacks, 450

Trojans, 447–449

viruses, 445–446

worms, 446

wrappers, 448

malware

anti-malware, 483–484

removable media, 59–60

MAN (Metropolitan Area Networks), 278

management, senior, security awareness, 136

managing, keys, 205

managing

assets, 51–52, 473

“CACPA”, 48

change management, change management, 474–475

classification, 47–48

cloud computing, 477–478

configuration management, 474–475

inventories, 47–48

media management, 476–477

- remote access, 476
- software licensing, 52–54
- system hardening, 473–474
- trusted recovery, 475–476
- change, 474–475, 580–582
- configurations, 474–475
- data, 32
 - auditors, 35
 - chief security officers, 34
 - data audits, 39
 - data custodians, 34, 36
 - data documentation, 36
 - data governance policies, 32–33
 - data lifecycle control, 38
 - data mining, 37
 - data organization, 36
 - data owners, 34
 - data ownership, 35, 36
 - data standards, 38
 - data storage, 39–42
 - data warehouses, 37
 - developers, 34
 - information security steering committees, 34
 - knowledge management, 38
 - responsibilities, 34–35
 - roles, 34–35
 - security advisor groups, 34
 - senior management, 34
 - users, 34
- databases, 582–583
- knowledge, 38
 - classification approach, 38
 - probabilistic approach, 38
 - statistical approach, 38
- media, 476–477
- patches, 485
- profiles, identity/access management, 377
- projects, BCP, 116–117
- risk. *See* separate entry
- sessions, 364
- users/accounts, 469
 - access controls, 471
 - audits, 488–489
 - clipping levels, 471–472
 - database administrators, 469
 - job rotation, 471
 - least privilege, 471
 - network administrators, 469
 - privileged entities, 470–471
 - quality assurance specialists, 469
 - reasonably prudent person rule, 472–473
 - security architects, 469
 - separation of duties, 469–470, 471
 - system administrators, 469
 - systems analysts, 469
- managing risk, 70**
 - acceptable risk, 104, 105
 - assessing risk, 88
 - asset valuation, 91–93
 - assets, 88
 - controls, 95–96
 - hacker insurance, 93
 - high-impact assets, 92–93
 - high-risk assets, 92–93
 - identifying assets, 91–93
 - losses, 94
 - probabilistic risk assessment, 87
 - qualitative assessments, 100–104
 - quantitative assessments, 97–100, 103–104
 - steps of assessment, 90
 - threat analysis, 93–96
 - threats, 89
 - vulnerabilities, 89, 95–96
- ATO, 111
- avoiding risk, 105
- baselines, 126
- BCP
 - BIA, 117–123
 - corrective controls, 117
 - detective controls, 117

managing risk

- DRP, 113–115
 - preventive controls, 117
 - project management/initiation, 116–117
 - reputations, 122–123
 - BPA, 112
 - concepts, 86–87
 - controls, 127–128, 130
 - access controls, 129–130
 - administrative controls, 128
 - physical controls, 129
 - technical controls, 129
 - COOP, 111
 - cost of risk versus levels of control, 105–106
 - cost-benefit analysis, 106
 - countermeasures
 - acceptable risk, 104, 105
 - avoiding risk, 105
 - cost of risk versus levels of control, 105–106
 - mitigating risk, 105
 - residual risk, 105–106
 - risk reports, 106
 - tolerating risk, 104, 105
 - transferring risk, 104–105
 - DRP, 113–115
 - FAIR, 87
 - frameworks, 87
 - guidelines, 127
 - HR, need for, 128
 - IA, 111
 - international governance standards, 86
 - 10 Steps to Cyber Security, 86
 - Cybersecurity Strategy of the European Union, 86
 - ISO, 83–85
 - ITIL, 82–83
 - OECD, 85–86
 - STAR ratings, CSA, 85
 - ISA, 110
 - mitigating risk, 105
 - MITRE Risk Matrix, 106
 - MOU, 111
 - NDA, 112
 - NIST Risk Management Framework, 87
 - OLA, 111
 - organization processes, 112–113
 - personnel security, 130
 - background checks, 131
 - educating employees, 134–135
 - employee awareness, 134–136
 - ethics training/awareness, 137–143
 - job rotation, 132
 - least privilege, 132–133
 - mandatory vacations, 133
 - NDA, 131
 - new-hire agreements/policies, 131
 - separation of duties, 131–132
 - social engineering, 136–137
 - social networking, 131
 - termination of employees, 133–134
 - training employees, 134–135
- procedures, 127
 - residual risk, 105–106
 - risk factor analysis, 87
 - risk registers, 88
 - risk reports, 106
 - SAS 70, 112
 - SCRM, 110
 - security governance, 70
 - computer crime/hackers, 76–79
 - global legal/regulatory issues, 74–76
 - holistic enterprise security systems, 71
 - international legal system/laws, 72–74
 - sexual harassment, 79
 - U.S. legal system/laws, 71–72
 - security policies
 - advisory policies, 125
 - AUP, 128

- control levels, 124–125
- developing, 123–124
- documentation, 124
- informative policies, 125–126
- purpose of, 124–125
- regulatory policies, 126, 142–143
- structure of, 124–125
- SLA, 111, 495
- standards, 126
- strategies, 91
- teams, 89–90
 - asset valuation, 91–93
 - controls, 95–96
 - hacker insurance, 93
 - high-impact assets, 92–93
 - high-risk assets, 92–93
 - identifying assets, 91–93
 - losses, 94
 - qualitative assessments, 100–104
 - quantitative assessments, 97–100, 103–104
 - steps of risk assessment, 90
 - tasks, 90
 - threat analysis, 93–96
 - vulnerabilities, 95–96
- third-party risk management, 110–112
- threat modeling, 107, 108
 - categorizing threats, 107
 - DREAD, 109
 - identifying threats, 107
 - mapping/diagramming potential attacks, 107
 - mitigating threats, 108
 - OCTAVE, 109
 - PASTA, 109
 - STRIDE, 108
 - threat intelligence, 107
 - Trike, 109–110
 - VAST, 109
- tolerating risk, 104, 105
- transferring risk, 104–105
- UA, 111
- U.S. legal system/laws
 - FCPA, 142
 - FIPS, 82
 - FISMA, 81
 - GLBA, 80
 - HIPAA, 79–80
 - NIST, 82
 - security governance, 70–72, 75–76, 79–82
 - SOX, 81, 142
- mandatory vacations, 133**
- man-in-the-middle attacks, 59, 239**
- mantraps, perimeter physical control systems, 346**
- mapping, potential attacks, 107**
- MARS, 211**
- maskable interrupts, 162**
- masking, LUN, 41**
- master license agreements, 53**
- maturity models, software development, 578–579**
- MD algorithms, 233**
- MDM (Mobile Device Management), 203**
- mechanical locks, 351**
- media management, 476–477**
- Meltdown cryptographic attack, 240**
- memory**
 - absolute addressing, 163
 - CAM, 283
 - cards, 369
 - CPU, 159
 - DDR, 164
 - DRAM, 163–164
 - hierarchy of, 162–163
 - leaks, 164
 - physical addressing, 163
 - RAM, 163–164, 167–168
 - relative addressing, 163
 - ROM, 164–165
 - SDRAM, 164

memory

- SRAM, 163–164
- virtual memory, 167–168
- memory-mapped I/O, 162**
- mergers, 112**
- Merkle-Hellman Knapsack, 223**
- mesh topologies, 274**
- message digest/hash, 205**
- message privacy, 331–332**
- methodologies of attacks, 430–431**
- MFA (Multifactor Authentication), 202**
- military data classification, 50, 51**
- mining data, 37**
- MIPS (Million Instructions Per Second), 159**
- mirrored ports, 284**
- mission-critical operations, 458**
- misuse case testing, 426**
- mitigating**
 - risk, 105
 - threats, 108
- MITRE Risk Matrix, 106**
- mixed law systems, 73**
- mobile code, 595**
- mobile sites, disaster recovery, 527–528**
- mobile system vulnerabilities, 202–203**
- mobilizing personnel, disaster recovery, 542**
- modeling threats, 107, 108**
 - categorizing threats, 107
 - DREAD, 109
 - identifying threats, 107
 - mapping/diagramming potential attacks, 107
 - mitigating threats, 108
 - OCTAVE, 109
 - PASTA, 109
 - software, 593
 - STRIDE, 108
 - threat intelligence, 107
 - Trike, 109–110
 - VAST, 109

- modes of operation, security, 176–177**

monitoring

- access, 394–396
- alarms, 511–512
- application transactions, 489–490
- controls, 487–488
- disaster recovery plans, 547–548
- keystrokes, 402–403, 491–492
- MaaS, 477
- MOSS (MIME Object Security Services), 297**
- MOU (Memorandum of Understanding), 111**
- MPLS (Multiprotocol Label Switching), 282, 291**
- MPM model, software development, 576**
- MS-CHAPv2, 390**
- MSP (Message Security Protocol), 297**
- MTBF (Mean Time Between Failures), 486–487, 529–530**
- MTD (Maximum Tolerable Downtime), 122**
- MTTR (Mean Time To Repair), 486–487, 529–530**
- multifactor authentication, 375
- multilevel operation mode, 176
- multimedia collaboration, 331–332
- multimode fiber cables, 277
- multipath solutions, SAN, 41
- multiple-choice questions, CISSP exams, 24, 26
- multiplexing, 291
- multiprocessor systems, CPU, 160
- multistate operating systems, 177–178
- multithreaded programs, 161

N

- NAC (Network Access Control), 401–402, 491**
- Napoleonic law, 73**
- NAS (Network Archived Storage), 39–40**

- NAT (Network Address Translation), 325**
- nation-state hackers, 78**
- natural access control, 496**
- natural disasters, operational security, 493–494**
- NDA (Nondisclosure Agreements), 112, 131, 471**
- network access layer, TCP/IP network model, 259–260, 320**
- network cards, promiscuous mode, 432**
- network layer, OSI network model, 254**
- networks, 250–251**
 - 802.1AE (MACsec) security standard, 259–260
 - 802.1AR security standard, 260
 - 802.11 wireless networks/standards, 308–316
 - access controls, 321–322
 - DMZ, 324–325
 - firewalls, 322, 481
 - NAT, 325
 - packet filters, 322
 - proxy servers, 322–324
 - remote access, 326–330
 - stateful firewalls, 322
 - zero trust, 325
 - administrators, 469
 - bridges, 282
 - cabling
 - attenuation, 280
 - baseband transmissions, 275
 - broadband transmissions, 275
 - coaxial cables, 275–277
 - fiber-optic cables, 277
 - multimode fiber cables, 277
 - plenum-grade cables, 277
 - single-mode cables, 277
 - CAN, 278
 - CDN, 324
 - cloud computing, 294–295
 - communication
 - full duplex communication, 280
 - half duplex communication, 280
 - simplex communication, 280
 - telecommunications equipment, 281
 - convergence, 304
 - database management systems, 582
 - de-encapsulation, 258
 - discovery scans, 418
 - encapsulation, 257–258
 - Feistel network, 303
 - forensics, 514
 - frames, 258
 - GAN, 278
 - gateways, 287
 - headers, 257
 - hubs, 281
 - ISDN, 291–292
 - LAN, 271, 278
 - cabling, 275–278
 - communication protocols, 271–272
 - Ethernet frames, 271–272
 - tokens, 272
 - VLAN, 282, 284–285
 - VXLAN, 284–285
 - WLAN, 309, 312–313
 - MAN, 278
 - mirrored ports, 284
 - NAC, 401–402
 - NAS, 39–40
 - neural networks, 587–588
 - open networks, VoIP, 305
 - OSI model, 251–252
 - application layer, 256
 - data link layer, 253–254
 - de-encapsulation, 258
 - encapsulation, 256, 257–258
 - encryption, 256
 - network layer, 254
 - physical layer, 253, 257

- presentation layer, 255
- protocols summary, 256–257
- session layer, 255
- SSL, 257
- transport layer, 254–255
- PAN, 278
- PDU, 257, 258
- remote access, 326
 - CHAP, 326
 - EAP, 326–328
 - IPsec, 329–330
 - PAP, 326
 - PPP, 326
 - RADIUS, 328
 - TACACS, 328–329
- removable media, malware, 59–60
- repeaters, 281
- routed protocols, 287
- routers, 285–286
- routing protocols, 287–289
- SAN, 39–40, 278–280, 533, 539
 - DDP, 42
 - FCoE, 41
 - HBA, 41
 - iSCSI, 40–41
 - location redundancy, 41
 - LUN masking, 41
 - multipath solutions, 41
 - secure storage management/replication, 41
 - snapshots, 41
 - VSAN, 40
- scanning, 418–419
- SD-WAN, 296
- switches, 282–283
- taps, 284
- TCP/IP model, 258–259
 - application layer, 267–271
 - cryptographic security, 316–320
 - host-to-host (transport) layer, 264–267
 - Internet layer, 260–264
 - network access layer, 259–260
 - telecommunications equipment, 281
 - topologies, 272
 - bus topologies, 272
 - fully connected topologies, 275
 - mesh topologies, 274
 - ring topologies, 273–274
 - star topologies, 273
 - VLAN, 282, 284–285
 - VPN, 57–58
 - VXLAN, 284–285
 - WAN, 278, 289–290
 - circuit switching, 291–294
 - packet switching, 290–291
 - SD-WAN, 296
 - wireless network testing, 420
 - WLAN, 309, 312–313
 - WPAN, 278
 - zero-trust environments, 59
- neural networks, 587–588**
- new-hire agreements/policies, 131**
- NIDS (Network-Based Intrusion Detection Systems), 397–398, 512**
- NIS (Network Information Service), 268**
- NIST (National Institute of Standards and Technology), 82**
 - NIST 800–37, 82
 - NIST 800–52 baselines, 61–62
 - NIST 800–53, 60–61, 82, 102–103
 - NIST 800–60, 82
 - NIST 800–115, 424
 - NIST 800–207, 429
 - NIST-SP 80–14, 141
 - NIST-SP 800–92, 416–417
 - NIST-SP 800–137, 417–418
 - penetration testing, 423–424
 - Risk Management Framework, 87
- nonces, 206–207**
- noninterference security model, 182**
- non-maskable interrupts, 162**
- nonrepudiation, cryptography, 204**
- northbridges, 166**

O

-
- Oakley protocol, 329**
 - OAuth, 362**
 - object-relational database systems, 583**
 - OCTAVE, threat modeling, 109**
 - OECD (Organization for Economic Co-operation and Development), 85–86**
 - OFB mode, DES, 214**
 - OFDM (Orthogonal Frequency-Division Multiplexing), 308**
 - OLA (Operating-Level Agreements), 111**
 - OLTP (Online Transaction Processing), 585**
 - online resources, CISSP exams, 28**
 - OOP (Object-Oriented Programming), 591–592**
 - open networks, VoIP, 305**
 - open/closed systems, 175**
 - OpenID, 362**
 - operation, security modes of, 176–177**
 - operational security, 468–469**
 - account management, 469
 - access controls, 471
 - clipping levels, 471–472
 - database administrators, 469
 - job rotation, 471
 - least privilege, 471
 - network administrators, 469
 - privileged entities, 470–471
 - quality assurance specialists, 469
 - reasonably prudent person rule, 472–473
 - security architects, 469
 - separation of duties, 469–470, 471
 - system administrators, 469
 - systems analysts, 469
 - alarms, 509–510
 - IDS, 510–511, 512–513
 - monitoring/detection, 511–512
 - asset management, 473
 - change management, 474–475
 - configuration management, 474–475
 - media management, 476–477
 - remote access, 476
 - system hardening, 473–474
 - trusted recovery, 475–476
 - auditing controls, 487–489
 - digital forensics, 515–516
 - acquisition, 516, 517–519
 - analytics, 517, 520–521
 - authentication, 516–517, 520
 - procedures, 516
 - stages of, 515
 - types of, 514–515
 - disaster recovery
 - awareness, 545
 - backups, 534–541
 - business process recovery strategies, 524–525
 - checklists, 521–522
 - cold sites, 527
 - data and information recovery strategies, 534
 - employee services, 543–544
 - facility recovery strategies, 525–528
 - fault tolerance, 530–534
 - flat tires, 522–523
 - hot sites, 525–526
 - implementing plans, 544–545
 - insurance, 544
 - interfacing with external groups, 542–543
 - lifecycle of, 521–523
 - maintaining plans, 547–548
 - mobile sites, 527–528
 - monitoring recovery plans, 547–548
 - operations recovery strategies, 529–532
 - organizational functions and recovery times, 535–536

operational security

- personnel mobilization, 542
- plan design/development, 541–544
- reciprocal agreements, 528
- redundant sites, 527
- strategies, 524–532
- subscription services, 525–527
- supply recovery strategies, 525–528
- teams/responsibilities, 523
- tertiary sites, 525
- testing recovery plans, 546–547
- user recovery strategies, 528–529
- warm sites, 526
- emanation security, 492
- facility/site security controls, 495–496
 - area concerns, 497
 - asset placement, 498–501
 - ceilings, 498–501
 - construction, 498
 - CPTED, 496–497
 - doors, 498–501
 - electrical power, 503–504
 - environmental controls/HVAC, 502–503
 - equipment lifecycles, 505
 - location, 498
 - UPS, 504–505
 - walls, 498–501
 - windows, 498–501
- fault tolerance, 486
- fire prevention/detection/suppression controls, 505–506
 - fire suppression, 507–509
 - fire-detection equipment, 506–507
- human-caused threats, 494–495
- incident response, 514
- investigating computer crimes, 513
- keystroke monitoring, 491–492
- monitoring application transactions, 489–490
- monitoring controls, 487–488
- NAC, 491
- natural disasters, 493–494
- perimeter physical control systems, 493
- recovery controls, 486–487
- resource protection, 472
 - due care, 472–473
 - due diligence, 472–473
- SIEM, 490–491
- system resilience, 486
- technical problems, 495
- telecommunications control, 477
 - anti-malware, 483–484
 - blacklists, 480
 - cloud computing, 477–478
 - email, 478–479
 - faxes, 482
 - firewalls, 481
 - graylists, 480
 - honeypots/honeynets, 484–485
 - patch management, 485
 - PBX, 482
 - phones, 482
 - sandboxing, 480
 - whitelists, 480
- user management, 469
 - access controls, 471
 - clipping levels, 471–472
 - database administrators, 469
 - job rotation, 471
 - least privilege, 471
 - network administrators, 469
 - privileged entities, 470–471
 - quality assurance specialists, 469
 - reasonably prudent person rule, 472–473
 - security architects, 469
 - separation of duties, 469–470, 471
 - system administrators, 469
 - systems analysts, 469

operations

- recovery strategies, 529–532
- SDLC, 571–572

optical media, 165

Orange Book (The Rainbow Series), 190

organization processes, risk management, 112–113

organizational functions and recovery times, 535–536

organized crime, threat actors, 428

organizing data, 36

OS (Operating Systems)

- architectures, 174–175
- direct OS commands, web-based vulnerabilities, 199
- multistate operating systems, 177–178
- single-state (dedicated) operating systems, 177
- unpatched OS, mobile system vulnerabilities, 203

OSI network model, 251–252

- application layer, 256
- data link layer, 253–254
- de-encapsulation, 258
- encapsulation, 256, 257–258
- encryption, 256
- network layer, 254
- physical layer, 253, 257
- presentation layer, 255
- protocols summary, 256–257
- session layer, 255
- SSL, 257
- transport layer, 254–255

OSPF (Open Shortest Path First), 289

OTP (One-Time Passwords), 367

outbound dialing systems, 542

outsider testing, 420

outsiders, threat actors, 428

ownership, data

- governance policies, 33
- identification, 36
- ILM, 35

P

PaaS (Platform-as-a-Service), 295, 478

packers, 448

packets

- filters, 322
- sniffing, 432
- switching, WAN, 290–291

padding traffic, 321

PAN (Personal Area Networks), 278

PAP (Password Authentication Protocol), 326, 390

PAP (Policy Administration Points), 387

parallel operations, software, 572

parallel testing, 570

passing score, CISSP exams, 20

passphrases, 365

passwords, 363–364, 367

- aging, 364
- assisted password resets, 365
- attacks, 439–442
- attempts, 364
- brute-force cracking, 441
- BYOT controls, 202
- clipping levels, 364, 365
- cognitive passwords, 366–367
- comparative analysis, 439
- complexity, 364
- composition, 364
- cracking, 366, 439–442
- database vulnerabilities, 586
- dynamic passwords, 365–366
- history, 364
- impersonation attacks, 444
- length, 364
- OTP, 367
- PAP, 326, 390
- passphrases, 365
- plaintext, 440
- rainbow tables, 441–442

passwords

- resetting, 365
- self-service password resets, 365
- session management, 364
- single-use passwords, 365–366
- spoofing attacks, 442, 444
- static passwords, 365–366
- storing, 364
- synchronization, 343, 365
- threshold levels, 364

PASTA, threat modeling, 109**PAT (Port Address Translation), 325****patch management, 485****payback analysis, 564****PBX, operational security, 482****PCI (Peripheral Component Interconnect), buses, 166****PCI-DSS (Payment Card Industry-Data Security Standard), 42–43****PCIe (Peripheral Component Interconnect Express), 166****PDP (Policy Decision Points), 387****PDU (Protocol Data Units), 257, 258****PEM (Privacy Enhanced Mail), 297****penetration testing, 420–424****PEP (Policy Enforcement Points), 387****performance reference model, FEA frameworks, 156****performance reviews, 548****perimeter physical control systems, 344, 493**

- bollards, 346–347
- CCTV cameras, 348–349, 496
- deadman doors, 346
- dogs, 350
- fences, 343
- gates, 345–346
- guards, 350
- lighting, 349–350
- locks, 351–355
- mantraps, 346
- turnstiles, 346

perimeters, security, 174–175**personal information websites, 76****personnel mobilization, disaster recovery, 542****personnel security, 130**

- attacks, 77
- background checks, 131
- educating employees, 134–135
- employee awareness, 134–136
- ethics training/awareness, 137–138
 - 10 Commandments of Computer Ethics, 139–140, 141–142
 - Computer Ethics Institute, 139–140
 - IAB, 140–141
 - (ISC)2 Code of Ethics, 138–139
 - ISOC, 140–141
 - NIST SP 80–14, 141
 - regulatory requirements, 142–143
 - RFC 1087, 140–141
- job rotation, 132
- least privilege, 132–133
- mandatory vacations, 133
- NDA, 131
- new-hire agreements/policies, 131
- separation of duties, 131–132
- social engineering, 136–137
- social networking, 131
- termination of employees, 133–134
- training employees, 134–136

PERT (Program Evaluation and Review Technique), 580**PGP (Pretty Good Privacy), 270, 297****pharming attacks, 437****phased changeovers, software, 572****phishing, 443****phone use, unauthorized, 306****phones**

- cell phones, 306–308
- cordless phones, 308
- operational security, 482

phreakers, 308, 430, 482, 492

physical access controls, 240, 342–343, 495–496

CPTED, 496–497

perimeter physical control systems, 344–348, 493

physical addressing, 163**physical controls, 129****physical layer, OSI network model, 253****physical security**

attacks, 77

controls, 152

testing, 420

PIA (Privacy Impact Assessments), 43–44**picking locks, 354–355****PID (Process IDs), 161****piggybacking, 346, 444****pilot/beta testing, software, 570****PIP (Policy Information Points), 387****PKI (Public Key Infrastructures), 153, 225–226**

CA, 226

client's role, 229–230

CRL, 227

digital certificates, 227–229

RA, 226–227

plaintext, 204

chosen plaintext, 238

known plaintext attacks, 238

passwords, 440

plan design/development, disaster recovery, 541–544**plenum-grade cables, 277****policies**

advisory policies, 125

AUP, 128

BYOD policies, 169

informative policies, 125–126

new-hire agreements/policies, 131

PAP, 387

PDP, 387

PEP, 387

PIP, 387

regulatory policies, 126

architecture security and engineering, 157–158

ethics training/awareness, 142–143

security policies

advisory policies, 125

AUP, 128

control levels, 124

developing, 123–124

documentation, 124

informative policies, 125–126

purpose of, 124–125

regulatory policies, 126, 142–143

structure of, 124–125

XACML, 387

polyalphabetic ciphers, 299–300**polyinstantiation, OOP, 591****polymorphism, OOP, 591****POODLE cryptographic attack, 240****POP (Post Office Protocol), 479****port-mapped I/O, 162****ports**

applications/protocols, 267–270

common ports, 270–271

mirrored ports, 284

PAT, 325

ranges, 267

POS cards, PCI-DSS, 42–43**potential attacks, mapping, 107****POTS (Plain Old Telephone Service), 291****power supplies, facility/site security controls, 504–505****PPP (Point-to-Point Protocol), 326****PPTP (Point-to-Point Tunneling Protocol), 320****presentation layer, OSI network model, 255****pretexting, 80, 443–444**

preventive controls

preventive controls, 117, 568

primary images, digital forensics, 520

primary keys

databases, 584

ERD, 565

principle of least privilege, 132–133, 343, 468, 471

print servers, 168

privacy, message privacy, 331–332

Privacy Act of 1974, The, 75

privacy, data, PIA, 43–44

privacy laws, 75–76

personal information websites, 76

Privacy Rights Clearinghouse, 42

private clouds, 478

private data, classifying, 51

privilege

database vulnerabilities, 586

escalation of privileges, 431, 586

least privilege, 132–133, 343, 468, 471

privileged entities, 470–471

probabilistic approach, knowledge management, 38

probabilistic risk assessment, 87

problem state, CPU, 159, 160

procedures, risk management, 127

process control, architecture security and engineering, 157–158

processes

CPU, 161

data governance policies, 33

isolation, 179

spoofing, 442

process layer, TCP/IP network model, 317–318

processing database transactions, 585

processors

asymmetric mode, 160

multiprocessor systems, 160

scalar processors, 160

superscalar processors, 160

symmetric mode, 160

product security evaluation models, 189

Common Criteria (ISO 15408), 192–194

CTCPEC, 190

ITSEC, 191–192

Rainbow Series, The, 189–190

Orange Book, 190

Red Book, 191

TCSEC, 189–190, 191–192

profile management, 377

programmable locks, 352–353

programmed I/O, 162

programming languages, 588–590

project initiation, SDLC, 564–565

project management, BCP, 116–117

promiscuous mode, network cards, 432

Protection of Information in Computing Systems, The [ital]154

protection rings, 170–172

prototyping, software development, 575–576

provisioning/deprovisioning, identity/access management, 376

proxy servers, 322–324

prudent person rule, reasonably, 472–473

pseudorandom numbers, 206–207

public clouds, 478

public data, classifying, 51

purging data, 46

Purple machine, 303, 304

PVC (Permanent Virtual Circuits), 290

Q

QoS, VoIP, 304–305

qualitative assessments, 102, 103–104

Delphi technique, 102

FRAP, 102

- IAM, 102
 - impact scale, 100–101
 - NIST 800–53, 102–103
 - performing, 103
 - results, 101–102
 - steps of, 101
 - qualitative ranking, BIA, 120–121**
 - quality assurance specialists, 469**
 - quantitative assessments, 97, 103–104**
 - ALE, 97, 98–99, 106
 - ARO, 97, 98–99
 - calculations, 97–99
 - formulas, 99–100
 - SLE, 97, 98–100
 - quantitative ranking, BIA, 121–122**
 - quantum cryptography, 304**
 - questionnaires, BIA, 119–121**
 - questions, CISSP exams, 24**
 - answer strategies, 27
 - drag-and-drop questions, 24, 26
 - hotspot questions, 25, 26
 - multiple-choice questions, 24, 26
-
- R**
- RA (Registration Authorities), 226–227**
 - RAD model, software development, 575**
 - RADIUS (Remote Authentication Dial-In User Service), 328, 391–392**
 - RAID (Redundant Array of Independent Disks), 530–532**
 - Rainbow Series, The, 189–190**
 - Orange Book, 190
 - Red Book, 191
 - rainbow tables, 441–442**
 - RAIT (Redundant Array of Independent Tapes), 532**
 - RAM (Random-Access Memory), 163–164, 167–168**
 - range checks, 562**
 - ransomware, 450–451**
 - RARP (Reverse ARP), 263**
 - RASP (Runtime Application Self-Protection), 425**
 - RBAC (Role-Based Access Controls), 385–387**
 - RC2 (Rivest Cipher 2), 218**
 - RC4 (Rivest Cipher 4), 210, 218**
 - RC5 (Rivest Cipher 5), 210–211, 218**
 - RDBMS (Relational Database Management Systems), 582–583**
 - readiness assessments, CISSP exams, 20–21**
 - ready state, CPU, 159**
 - reasonably prudent person rule, 472–473**
 - reciprocal agreements, disaster recovery, 528**
 - record retention policies, 45**
 - recovery, disaster, 458–459, 493–494**
 - awareness, 545
 - backups, 534–541
 - business process recovery strategies, 524–525
 - checklists, 521–522
 - cold sites, 527
 - data and information recovery strategies, 534
 - employee services, 543–544
 - facility recovery strategies, 525–528
 - fault tolerance, 530–534
 - flat tires, 522–523
 - hot sites, 525–526
 - implementing plans, 544–545
 - insurance, 544
 - interfacing with external groups, 542–543
 - lifecycle of, 521–523
 - maintaining plans, 547–548
 - mobile sites, 527–528
 - monitoring recovery plans, 547–548
 - operations recovery strategies, 529–532
 - organizational functions and recovery times, 535–536
 - personnel mobilization, 542

recovery, disaster

- plan design/development, 541–544
- reciprocal agreements, 528
- redundant sites, 527
- strategies, 524–532
- subscription services, 525–527
- supply recovery strategies, 525–528
- teams/responsibilities, 523
- tertiary sites, 525
- testing recovery plans, 546–547
- user recovery strategies, 528–529
- warm sites, 526

recovery controls, 486–487**recovery procedures, 178****recovery, trusted, 475–476****Red Book (The Rainbow Series), 191****redundancy**

- location, 41
- sites, disaster recovery, 527

reference monitors, TCB, 172–174**referential integrity, 585****regression testing, 570****regulatory (administrative) law, U.S. legal system/laws, 71****regulatory policies, 126**

- architecture security and engineering, 157–158
- ethics training/awareness, 142–143

relations, databases, 583**relative addressing, 163****religious law, 73****remanence, data, 46–47****remote access, 326, 476**

- CHAP, 326
- EAP, 326–328
- IPsec, 329–330
- PAP, 326
- PPP, 326
- RADIUS, 328
- TACACS, 328–329

remote journaling, 539**removable media, malware, 59–60****repeaters, 281****replay attacks, 239****replicating data, 538****replication/secure storage management, 41****reporting risk, 106****reputations, BCP, 122–123****researchers, hacker, 428, 429****resetting passwords, self-service password resets, 365****residual risk, 105–106****resource protection, 472**

- due care, 472–473
- due diligence, 472–473

responsibilities, disaster recovery, 523**rest (encryption), data at, 55–57****restricted access/work area security, 241****retina pattern recognition, 373****reverse engineering, 569****reviews**

- code, 425
- performance, 548

RFC 1087, 140–141**RFI (Radio Frequency Interference), 503****RFID tags, 342, 357****right to be forgotten, global legal/regulatory issues, 75****Rijndael, 210, 217****ring topologies, 273–274****RIP (Routing Information Protocol), 270, 288****RISC (Reduced Instruction Set Computers), 160****risk factor analysis, 87****risk management, 70**

- acceptable risk, 104, 105
- assessing risk, 88
 - asset valuation, 91–93
 - assets, 88
 - controls, 95–96

- hacker insurance, 93
- high-impact assets, 92–93
- high-risk assets, 92–93
- identifying assets, 91–93
- losses, 94
- probabilistic risk assessment, 87
- qualitative assessments, 100–104
- quantitative assessments, 97–100, 103–104
- steps of assessment, 90
- threat analysis, 93–96
- threats, 89
- vulnerabilities, 89, 95–96
- ATO, 111
- avoiding risk, 105
- baselines, 126
- BCP
 - BIA, 117–123
 - corrective controls, 117
 - detective controls, 117
 - DRP, 113–115
 - preventive controls, 117
 - project management/initiation, 116–117
 - reputations, 122–123
- BPA, 112
- concepts, 86–87
- controls, 127–128, 130
 - access controls, 129–130
 - administrative controls, 128
 - physical controls, 129
 - technical controls, 129
- COOP, 111
- cost of risk versus levels of control, 105–106
- cost-benefit analysis, 106
- countermeasures
 - acceptable risk, 104, 105
 - avoiding risk, 105
 - cost of risk versus levels of control, 105–106
 - mitigating risk, 105
 - residual risk, 105–106
 - risk reports, 106
 - tolerating risk, 104, 105
 - transferring risk, 104–105
- DRP, 113–115
- FAIR, 87
- frameworks, 87
- guidelines, 127
- HR, need for, 128
- IA, 111
- international governance standards, 86
 - 10 Steps to Cyber Security, 86
 - Cybersecurity Strategy of the European Union, 86
 - ISO, 83–85
 - ITIL, 82–83
 - OECD, 85–86
 - STAR ratings, CSA, 85
- ISA, 110
- KRI, 415
- mitigating risk, 105
- MITRE Risk Matrix, 106
- MOU, 111
- NDA, 112
- NIST Risk Management Framework, 87
- OLA, 111
- organization processes, 112–113
- personnel security, 130
 - background checks, 131
 - educating employees, 134–135
 - employee awareness, 134–136
 - ethics training/awareness, 137–143
 - job rotation, 132
 - least privilege, 132–133
 - mandatory vacations, 133
 - NDA, 131
 - new-hire agreements/policies, 131
 - separation of duties, 131–132
 - social engineering, 136–137

risk management

- social networking, 131
 - termination of employees, 133–134
 - training employees, 134–135
 - procedures, 127
 - reduction process, BIA, 121–122
 - residual risk, 105–106
 - risk factor analysis, 87
 - risk registers, 88
 - risk reports, 106
 - SAS 70, 112
 - SCRM, 110
 - security governance, 70
 - computer crime/hackers, 76–79
 - global legal/regulatory issues, 74–76
 - holistic enterprise security systems, 71
 - international legal system/laws, 72–74
 - sexual harassment, 79
 - U.S. legal system/laws, 71–72
 - security policies
 - advisory policies, 125
 - AUP, 128
 - control levels, 124
 - developing, 123–124
 - documentation, 124
 - informative policies, 125–126
 - purpose of, 124–125
 - regulatory policies, 126, 142–143
 - structure of, 124–125
 - SLA, 111, 495
 - standards, 126
 - strategies, 91
 - teams, 89–90
 - asset valuation, 91–93
 - controls, 95–96
 - hacker insurance, 93
 - high-impact assets, 92–93
 - high-risk assets, 92–93
 - identifying assets, 91–93
 - losses, 94
 - qualitative assessments, 100–104
 - quantitative assessments, 97–100, 103–104
 - steps of risk assessment, 90
 - tasks, 90
 - threat analysis, 93–96
 - vulnerabilities, 95–96
 - third-party risk management, 110–112
 - threat modeling, 107, 108
 - categorizing threats, 107
 - DREAD, 109
 - identifying threats, 107
 - mapping/diagramming potential attacks, 107
 - mitigating threats, 108
 - OCTAVE, 109
 - PASTA, 109
 - STRIDE, 108
 - threat intelligence, 107
 - Trike, 109–110
 - VAST, 109
 - tolerating risk, 104, 105
 - transferring risk, 104–105
 - UA, 111
 - U.S. legal system/laws
 - FCPA, 142
 - FIPS, 82
 - FISMA, 81
 - GLBA, 80
 - HIPAA, 79–80
 - NIST, 82
 - security governance, 70–72, 75–76, 79–82
 - SOX, 81, 142
- Rivest cipher algorithms, 210–211, 218**
- ROM (Read-Only Memory), 164–165**
- root causes analyses, 415**
- rootkits, 449–450**
- rotating jobs, 132**
- routed protocols, 287**
- routers, 285–286**

routine maintenance, equipment lifecycles, 54, 505

routing

by rumor, 288

protocols, 287–289

RPO (Recovery Point Objective), 539–541

RSA algorithm, 222

RTO (Recovery Time Objective), 539–541

rubber hose attacks, 239

Ruby programming language, 590

rule-based access control, 388

rule-based IDS, 400

rumor, routing by, 288

running key ciphers, 302–303

S

SA (Security Association), 329

SaaS (Software-as-a-Service), 295, 478

SABSA (Sherwood Applied Business Security Architecture), 156–157

SAFER (Secure and Fast Encryption Routine), 211

salami attacks, 198

SAML (Security Assurance Markup Language), 361–362

sampling plans, 413–414

SAN (Storage Area Networks), 39–40, 278–280, 533, 539

DDP, 42

FCoE, 41

HBA, 41

iSCSI, 40–41

location redundancy, 41

LUN masking, 41

multipath solutions, 41

secure storage management/
replication, 41

snapshots, 41

VSAN, 40

sandboxing, 480

sanitizing data, 46–47, 476–477

SAS 70 (Statement of Auditing Standards 70), 112

SASD (Sequential Access Storage Devices), 532

SAST (Static Application Security Testing), 425

SATA (Serial ATA), 166

SATAN vulnerability assessment tool, 138–139

s-boxes (Substitution Boxes), 208

SCADA systems, 169

scalar processors, CPU, 160

scanning

heuristic scanning, 483

networks, 418–419

signature scanning, 483

vulnerabilities, 419

scheduling, software development, 580

schemas, databases, 584

scoping, baselines, 60–61, 62

scores (CISP exams), passing, 20

screened hosts, 324

script kiddies, 78, 428

scripting languages, 590

scripts, XSS, 199, 200

SCRM (Supply Chain Risk Management), 110

scrums, 578

SCSI (Small Computer Systems Interface), 167

SDLC (Software Development Lifecycle), 563

acceptance testing/implementation, 569–571

building/development, 567–569

design specifications, 566

ERD, 565–566

functional requirements/planning, 565–566

operations/maintenance, 571–572

SDLC (Software Development Lifecycle)

- project initiation, 564–565
- reverse engineering, 569
- stages of, 563–564
- SDLS (Synchronous Data Link Control), 294**
- SDRAM (Synchronous Dynamic Random-Access Memory), 164**
- SD-WAN (Software-Defined Wide Area Networks), 296**
- sealing configurations, 56**
- search and seizure/surveillance, 459**
- secondary storage, 165–166**
- secure storage management/replication, 41**
- security advisor groups, data management, 34**
- security architects, 469**
- security architecture and engineering, 152, 170**
 - accreditation, 195
 - certification, 194–195
 - computer/device configurations, 168–170
 - CPU, 158–163
 - cryptography, 203
 - 3DES, 215–216
 - AES, 217
 - algorithms, 204, 206–207
 - asymmetric encryption, 205, 207, 218–224, 237
 - attacks, 237–240
 - authentication, 203–204, 230–231
 - block ciphers, 205, 207–208
 - ciphertext, 204
 - confidentiality, 203
 - cryptanalysis, 205
 - CSS, 238
 - DES, 211–215
 - digital signatures, 205, 235–236, 237
 - DRM, 205
 - encryption, 203, 204
 - hashing algorithms, 205, 231–236, 237
 - hybrid encryption, 224–225
 - integrity, 204, 230–231
 - Kerckhoff's Principle, 238
 - key management, 205
 - keys, 204
 - MD algorithms, 233
 - nonces, 206–207
 - nonrepudiation, 204
 - plaintext, 204
 - pseudorandom numbers, 206–207
 - s-boxes, 208
 - steganography, 205
 - stream ciphers, 205, 208
 - symmetric encryption, 205, 208–211, 223–224, 237
 - defense in depth design process, 152–153
 - design guidelines, 152–155
 - EA, 155–157
 - frameworks, 154–155
 - fundamentals, overview, 158
 - I/O bus standards, 166–167
 - open/closed systems, 175
 - operating states, 177–178
 - PKI, 153, 225–226
 - CA, 226
 - client's role, 229–230
 - CRL, 227
 - digital certificates, 227–229
 - RA, 226–227
 - process control, 157–158
 - process isolation, 179
 - product security evaluation models, 189
 - Common Criteria (ISO 15408), 192–194
 - CTCPEC, 190
 - ITSEC, 191–192
 - Rainbow Series, The, 189–191
 - TCSEC, 189–190, 191–192
 - protection rings, 170–172
 - recovery procedures, 178, 486–487
 - regulatory compliance, 157–158

- security models, 179, 189
 - Bell-LaPadula model, 182–184
 - Biba model, 185–186
 - Brewer and Nash model, 188
 - Clark-Wilson model, 187
 - Graham-Denning model, 188
 - Harrison-Ruzzo-Ullman model, 188
 - information flow model, 182
 - Lattice model, 188
 - Lipner model, 188
 - noninterference model, 182
 - state machine model, 180–181
 - Take-Grant model, 188
 - security modes of operation, 176–177
 - site/facility controls, 240–241
 - storage media, 163
 - CD, 165
 - direct-access storage, 165
 - DVD, 166
 - flash memory storage, 166
 - I/O bus standards, 166–167
 - optical media, 165
 - RAM, 163–164, 167–168
 - ROM, 164–165
 - secondary storage, 165–166
 - sequential storage, 165
 - software, 165
 - SSD, 166
 - swap partitions, 167–168
 - system validation, 194
 - TCB, 172–175
 - TPM chips, 154
 - virtual memory, 167–168
 - VM, 168
 - vulnerabilities, 195–196
 - backdoors, 197
 - buffer overflows, 196, 200, 595–596
 - covert channels, 197–198
 - data diddling, 198
 - database attacks, 201–202
 - emanations, 198–199
 - incremental attacks, 198
 - maintenance hooks, 197
 - mobile system vulnerabilities, 202–203
 - salami attacks, 198
 - SQL injections, 201–202, 586
 - state attacks, 197
 - Van Eck Phreaking, 199, 492
 - web-based vulnerabilities, 199–202
 - wireless vulnerabilities, 202
- security assessment/testing**
- application security testing, 420
 - audits, 412–415
 - blackbox testing, 420
 - code reviews, 425
 - coverage, 413–414
 - DAST, 425
 - DoS testing, 420
 - Fagan inspections, 426
 - fuzz testing, 426
 - graybox testing, 420
 - IAST, 425
 - integer overflow, 426–427
 - KPI, 414–415
 - KRI, 415
 - log reviews, 415–418
 - misuse case testing, 426
 - outsider testing, 420
 - penetration testing, 257–263
 - physical security testing, 420
 - RASP, 425
 - root causes analyses, 415
 - sampling plans, 413–414
 - SAST, 425
 - scanning networks, 418–419
 - social engineering testing, 421
 - stress testing, 420
 - synthetic transactions, 426
 - techniques/methods, 424–427
 - vulnerability scanning, 419

security assessment/testing

- war dialing, 420–421
- whitebox testing, 420
- wireless network testing, 420

security awareness, 134–136**security conferences, computer crime/hackers, 79****security controls**

- logical security controls, 152
- physical security controls, 152

security, data

- authentication, 58
- defense in depth, 56
- email protocols, 58
- encryption, 55
 - authentication, 58
 - data at rest, 55–57
 - data in transit, 57–59
 - end-to-end encryption, 59
 - IPsec, 57–58
 - keys, 56–57
 - link encryption, 58–59
 - SED, 56
 - TPM chips, 55–56
 - tunneling protocols, 57–58
 - VPN, 57–58
- endpoint security, 59–60
- FTP, 57
- HTTP, 57
- insecure protocols, 57
- IPsec, 57–58
- ISO/IEC 17799, 42
- PCI-DSS, 42–43
- Privacy Rights Clearinghouse, 42
- SMTP, 57
- Telnet, 57
- tunneling protocols, 57–58
- VPN, 57–58
- zero-trust environments, 59

security, endpoint, 59–60**security governance, 70**

- computer crime/hackers, 76
 - attack vectors, 77

- communications attacks, 77
- corporate spies, 78
- crackers, 77–78
- cyberterrorists/cybercriminals, 78
- data breaches, 76–77
- disgruntled employees, 78
- hactivism, 142
- law enforcement/security conferences, 79
- logical attacks, 77
- nation-state hackers, 78
- personnel security attacks, 77
- physical security attacks, 77
- script kiddies, 78
- social engineering attacks, 77
- threat actors, 78

global legal/regulatory issues, 74–75

- Data Protection Authority, 75
- right to be forgotten, 75

holistic enterprise security systems, 71

international legal system/laws, 72–73

- 1998 Directive on Data Protection, 76
- Corpus Juris Civilis, 73
- customary law, 73
- halakha law, 73
- intellectual property, 73–74
- mixed law systems, 73
- Napoleonic law, 73
- religious law, 73
- sharia law, 73

policies, assets, 51–52

privacy laws, 75–76

sexual harassment, 79

U.S. legal system/laws

- administrative (regulatory) law, 71
- CFAA (Computer Fraud and Abuse Act) of 1986, 72
- civil law, 71
- common law, 71
- criminal law, 71

- due care, 72
- due diligence, 72
- Economic Espionage Act of 1996, 72
- Federal Sentencing Guidelines of 1991, 72
- hearsay evidence, 72
- Identity Theft and Assumption Deterrence Act of 1998, 76
- personal information websites, 76
- Privacy Act of 1974, The, 75
- privacy laws, 75–76
- stare decisis, 71
- U.S. Child Pornography Prevention Act of 1996, 72
- U.S. Patriot Act of 2001, 72
- security kernels, 174**
- security logs, 416**
- security models, 179, 189**
 - Bell-LaPadula model, 182–184
 - Biba model, 185–186
 - Brewer and Nash model, 188
 - Clark-Wilson model, 187
 - confidentiality, 182–184
 - Graham-Denning model, 188
 - Harrison-Ruzzo-Ullman model, 188
 - information flow model, 182
 - integrity, 185–188
 - Lattice model, 188
 - Lipner model, 188
 - noninterference model, 182
 - state machine model, 180–181
 - Take-Grant model, 188
- security modes of operation, 176–177**
- security operations, 468–469, 496**
 - account management, 469
 - access controls, 471
 - clipping levels, 471–472
 - database administrators, 469
 - job rotation, 471
 - least privilege, 471
 - network administrators, 469
 - privileged entities, 470–471
 - quality assurance specialists, 469
 - reasonably prudent person rule, 472–473
 - security architects, 469
 - separation of duties, 469–470, 471
 - system administrators, 469
 - systems analysts, 469
 - alarms, 509–510
 - IDS, 510–511, 512–513
 - monitoring/detection, 511–512
 - asset management, 473
 - change management, 474–475
 - configuration management, 474–475
 - media management, 476–477
 - remote access, 476
 - system hardening, 473–474
 - trusted recovery, 475–476
 - auditing controls, 487–489
 - digital forensics, 515–516
 - acquisition, 516, 517–519
 - analytics, 517, 520–521
 - authentication, 516–517, 520
 - procedures, 516
 - stages of, 515
 - types of, 514–515
 - disaster recovery
 - awareness, 545
 - backups, 534–541
 - business process recovery strategies, 524–525
 - checklists, 521–522
 - cold sites, 527
 - data and information recovery strategies, 534
 - employee services, 543–544
 - facility recovery strategies, 525–528
 - fault tolerance, 530–534
 - flat tires, 522–523
 - hot sites, 525–526
 - implementing plans, 544–545

security operations

- insurance, 544
- interfacing with external groups, 542–543
- lifecycle of, 521–523
- maintaining plans, 547–548
- mobile sites, 527–528
- monitoring recovery plans, 547–548
- operations recovery strategies, 529–532
- organizational functions and recovery times, 535–536
- personnel mobilization, 542
- plan design/development, 541–544
- reciprocal agreements, 528
- redundant sites, 527
- strategies, 524–532
- subscription services, 525–527
- supply recovery strategies, 525–528
- teams/responsibilities, 523
- tertiary sites, 525
- testing recovery plans, 546–547
- user recovery strategies, 527
- warm sites, 526
- emanation security, 492
- facility/site security controls, 495–496
 - area concerns, 497
 - asset placement, 498–501
 - ceilings, 498–501
 - construction, 498
 - CPTED, 496–497
 - doors, 498–501
 - electrical power, 503–504
 - environmental controls/HVAC, 502–503
 - equipment lifecycles, 505
 - location, 498
 - UPS, 504–505
 - walls, 498–501
 - windows, 498–501
- fault tolerance, 486
- fire prevention/detection/suppression controls, 505–506
 - fire suppression, 507–509
 - fire-detection equipment, 506–507
- human-caused threats, 494–495
- incident response, 514
- investigating computer crimes, 513
- keystroke monitoring, 491–492
- monitoring application transactions, 489–490
- monitoring controls, 487–488
- NAC, 491
- natural disasters, 493–494
- perimeter physical control systems, 493
- recovery controls, 486–487
- resource protection, 472
 - due care, 472–473
 - due diligence, 472–473
- SIEM, 490–491
- system resilience, 486
- technical problems, 495
- telecommunications control, 477
 - anti-malware, 483–484
 - blacklists, 480
 - cloud computing, 477–478
 - email, 478–479
 - faxes, 482
 - firewalls, 481
 - graylists, 480
 - honeypots/honeynets, 484–485
 - patch management, 485
 - PBX, 482
 - phones, 482
 - sandboxing, 480
 - whitelists, 480
- user management, 469
 - access controls, 471
 - clipping levels, 471–472
 - database administrators, 469
 - job rotation, 471

- least privilege, 471
- network administrators, 469
- privileged entities, 470–471
- quality assurance specialists, 469
- reasonably prudent person rule, 472–473
- security architects, 469
- separation of duties, 469–470, 471
- system administrators, 469
- systems analysts, 469
- security perimeters, 174–175**
- security policies**
 - advisory policies, 125
 - AUP, 128
 - controls, levels of control, 124
 - developing, 123–124
 - documentation, 124
 - informative policies, 125–126
 - purpose of, 124–125
 - regulatory policies, 126, 142–143
 - structure of, 124–125
- SED (Self-Encrypting Hard Drives), 56**
- self-service password resets, 365**
- semantic integrity, 585**
- senior management**
 - data management, 34
 - security awareness, 136
- sensitivity**
 - data
 - classification, 50
 - database vulnerabilities, 586
 - governance policies, 33
 - labels, MAC, 385
- sensor placement, IDS, 400–401**
- separation of duties, 131–132, 469–470, 471**
- sequence checks, 562**
- sequential storage, 165**
- server room controls, 241**
- servers**
 - application servers, 169
 - clustering, 530, 533
 - database servers, 169
 - farms, 533
 - file servers, 168–169
 - print servers, 168
 - proxy servers, 322–324
 - web servers, 169
- service component reference model, FEA frameworks, 156**
- service marks, 73**
- service packs, 595**
- SESAME (Secure European System for Applications in a Multivendor Environment), 381**
- session layer, OSI network model, 255**
- sessions**
 - hijacking, 431–432
- lifetimes, 202**
 - management, 364
- SET (Secure Electronic Transaction), 317–318**
- sexual harassment, 79**
- SFTP (Secure File Transfer Protocol), 317**
- SHA-1 (Secure Hashing Algorithm-1), 233**
- SHA-2 (Secure Hashing Algorithm-2), 233**
- SHA-3 (Secure Hashing Algorithm-3), 234**
- sharia law, 73**
- shims, lock, 355**
- shoulder surfing, 442, 444**
- shrink-wrap license agreements, 53**
- S-HTTP (Secure HTTP), 317**
- side-channel attacks, 239**
- SIEM (Security Information and Event Management), 401, 490–491**
- signatures**
 - digital, 205, 235–236, 237
 - IDS, 399
 - scanning, 483
- silent hostage (duress) alarms, 356**

simple tape-rotation schemes

simple tape-rotation schemes, 537

simplex communication, 280

single-mode cables, 277

single-state (dedicated) operating systems, 177

single-use passwords, 365–366

site/facility security controls, 240–241

skilled hackers, 428

SKIP (Simple Key-Management for Internet Protocol), 319

Skipjack, 211

SLA (Service-Level Agreements), 111, 495, 530

SLE (Single Loss Expectancy), 97, 98–100

smart cards

contact smart cards, 369

contactless smart cards, 369

employee access control, 356

generic smart cards, 369

magnetic stripe cards, 370

memory cards, 369

smart locks, 352–353

smartphones, 169

SMDS (Switched Multimegabit Data Service), 294

S/MIME (Secure/Multipurpose Internet Mail Extensions), 297

smishing, 308, 443

SMTP (Simple Mail Transfer Protocol), 57, 268, 324, 479

snapshots, SAN, 41

sniffing, 432

SNMP (Simple Network Management Protocol), 269

social engineering

attacks, 77, 443–444

personnel security, 136–137

testing, 421

social networking, background checks, 131

sociability testing, 570

SOCKS, 324

software

accreditation, 571

alpha testing, 570

antivirus software, 60

blackbox testing, 570

building/development, 567–569

certification, 571

checks, 561–562

completeness checks, 562

controls, 561–562

corrective controls, 568

design specifications, 566

detective controls, 568

development methodologies

agile development, 577–578

CASE model, 576–577

CMMI model, 578–579

IDEAL model, 579

incremental development, 575

JAD model, 575

maturity models, 578–579

MPM model, 576

prototyping, 575–576

RAD model, 575

scheduling, 580

spiral model, 574

waterfall model, 573

development security, 560

application controls, 561–562

avoiding system failure, 561–562

buffer overflows, 595–596

change detection, 597

change management, 580–582

checks, 561–562

CORBA, 592

database management, 582–583

mobile code, 595

OOP, 591–592

programming languages, 588–590

scheduling, 580

SDLC, 563–572

software lifecycles, 560–561

- disposal, 572
 - duplicate checks, 562
 - environment security, 592–595
 - existence checks, 562
 - final testing, 570
 - forensics, 514
 - function testing, 570
 - Gantt chart, 580
 - hard changeovers, 572
 - keystroke loggers, 403
 - licensing, 52–53
 - click-wrap license agreements, 53
 - contracts of adhesion, 53
 - DMCA, 53–54
 - master license agreements, 53
 - shrink-wrap license agreements, 53
 - lifecycles, 560–561, 563
 - acceptance testing/
implementation, 569–571
 - building/development, 567–569
 - design specifications, 566
 - ERD, 565–566
 - functional requirements/planning, 565–566
 - operations/maintenance, 571–572
 - project initiation, 564–565
 - reverse engineering, 569
 - stages of, 563–564
 - limit checks, 562
 - logic checks, 562
 - lookups, table, 562
 - malicious software threats/attacks, 444–445
 - APT, 450
 - backdoors, 447–449
 - crypters, 448–449
 - exploit kits, 450
 - logic bombs, 446–447
 - packers, 448
 - ransomware, 450–451
 - rootkits, 449–450
 - success attacks, 450
 - Trojans, 447–449
 - viruses, 445–446
 - worms, 446
 - wrappers, 448
 - parallel operations, 572
 - parallel testing, 570
 - PERT, 580
 - phased changeovers, 572
 - pilot/beta testing, 570
 - preventive controls, 568
 - range checks, 562
 - regression testing, 570
 - SaaS, 478
 - scripting languages, 590
 - SDLC, 563
 - acceptance testing/
implementation, 569–571
 - building/development, 567–569
 - design specifications, 566
 - ERD, 565–566
 - functional requirements/planning, 565–566
 - operations/maintenance, 571–572
 - project initiation, 564–565
 - reverse engineering, 569
 - stages of, 563–564
 - sequence checks, 562
 - sociability testing, 570
 - storage media, 165
 - system testing, 569
 - table lookups, 562
 - threat modeling, 593
 - unit testing, 569
 - unpatched software, mobile system vulnerabilities, 203
 - validity checks, 562
 - vulnerabilities, 592
 - whitebox testing, 570
 - whitelisting, 60
- SONET (Synchronous Optical Networks), 290**
- southbridges, 166**

- SOX (Sarbanes-Oxley Act), 81, 142, 472**
- sparse infectors, 597–598**
- spear phishing, 443**
- Spectre cryptographic attack, 240**
- SPI (Security Parameter Index), 329**
- spies, corporate, 428**
- spiral model, software development, 574**
- SPIT (Spam over Internet Telephony), 306**
- SPML (Service Provisioning Markup Language), 378**
- spoofing**
 - attacks, 442, 444
 - DNS, 437
- spread-spectrum technologies, 308**
- sprinklers, water, 508–509**
- SQL injections, 201–202, 586**
- SRAM (Static Random-Access Memory), 163–164**
- SRTP (Secure Real-Time Transport Protocol), 306**
- SSD (Solid-State Drives), 166**
- SSH (Secure Shell), 317**
- SSL (Secure Sockets Layer), 257, 269, 318**
- SSO (Single Sign-On), 343, 378**
- SSTP (Secure Socket Tunneling Protocol), 319**
- standard email protocols, data security, 58**
- standards**
 - data, 38
 - risk management, 126
 - wireless standards, 310
- standby lighting, 349**
- STAR ratings, CSA, 85**
- star topologies, 273**
- stare decis, 71**
- state attacks, 197**
- state machine security model, 180–181**
- stateful firewalls, 322**
- static NAT, 325**
- static passwords, 365–366**
- static routing, 287**
- statistical approach, knowledge management, 38**
- steering committees, information security, data management, 34**
- steganography, 205**
- storage media, 163**
 - CD, 165
 - DASD, 532
 - direct-access storage, 165
 - DVD, 166
 - flash memory storage, 166
 - I/O bus standards, 166–167
 - MAID, 532–533
 - optical media, 165
 - RAM, 163–164, 167–168
 - ROM, 164–165
 - SASD, 532
 - secondary storage, 165–166
 - sequential storage, 165
 - software, 165
 - SSD, 166
- storing data**
 - cloud-based storage, 39–40
 - DASD, 532
 - data disposal, 46
 - data sanitization, 46–47
 - evidence storage controls, 241
 - information handling requirements, 44–45
 - labeling data, 44
 - MAID, 532–533
 - NAS, 39–40
 - passwords, 364
 - record retention policies, 45
 - SAN, 39–42, 278–280
 - SASD, 532

STP (Spanning Tree Protocol), 284

strategies

- answering questions, CISSP exams, 27
- disaster recovery, 524–532

stream ciphers, 205, 208

stress testing, 420

STRIDE, threat modeling, 108

strong authentication, 375

stuffing credentials, 439

subscription services, disaster recovery, 525–527

Substitution Boxes (s-boxes), 208

substitution ciphers, 301–302

success attacks, 450

superscalar processors, 160

supervisor (privileged) mode, protection rings, 171

supervisor state, CPU, 159, 160

supplementation, baselines, 62

supply chains, SCRM, 110

supply recovery strategies, 525–528

surfing, shoulder, 442, 444

surveillance/search and seizure, 459

swap partitions, 167–168

swiPe (Software IP encryption), 320

switches, 282–283

- circuit switching, 291–294
- packet switching, 290–291

symmetric cryptography, 207

symmetric encryption, 205, 208–211, 223–224, 237

symmetric mode, processors, 160

synchronization, passwords, 343, 365

synchronous tokens, 367–368

synthetic transactions, 426

system administrators, 469

system failure, avoiding, 561–562

system hardening, 473–474

system high operation mode, 176

system logs, 416

system resilience, 486

system testing, 569

system validation, architecture security and engineering, 194

systems analysts, 469

T

tables

- capability tables, 388
- lookups, 562

tablets, 169

TACACS (Terminal Access Controller Access Control System), 328–329, 392

tailgating, 346, 444

tailoring, baselines, 61–62

Take-Grant security model, 188

taking CISSP exam, 22–23

tape rotation schemes, 537–538

taps, network, 284

T-carrier service, 292

TCB (Trusted Computing Bases), 172–175

TCP (Transmission Control Protocol), 254, 264–266, 267

TCP/IP network model, 258–259

- application layer
 - applications/protocols, 267–270
 - common ports, 270–271
 - port ranges, 267
- application layer controls, 317–318
- cryptographic security, 316–317
- host-to-host (transport) layer, 259–260, 318–319
 - TCP, 264–266, 267
 - UDP, 264–265, 266–267
- Internet layer, 260
 - ARP, 263–264
 - ICMP, 263
 - IGMP, 264
 - IP, 260–262
- Internet layer controls, 319–320
- network access layer, 259–260

TCP/IP network model

- network access layer controls, 320

- process layer controls, 317–318

TCSEC (Trusted Computer System Evaluation Criteria), 189–190, 191–192

teams/responsibilities, disaster recovery, 523

technical controls, 129

technical problems, operational security, 495

technical reference model, FEA frameworks, 156

technical support, equipment lifecycles, 54–55

telecommunications control, 477

- anti-malware, 483–484

- blacklists, 480

- cloud computing, 477–478

- email, 478–479

- faxes, 482

- firewalls, 481

- graylists, 480

- honeypots/honeynets, 484–485

- patch management, 485

- PBX, 482

- phones, 482

- sandboxing, 480

- whitelists, 480

telecommunications equipment, 281

Telnet, 57, 268

TEMPEST, 198–199, 492

tension wrenches, 354

termination of employees, 133–134

terminology, CISSP exams, 28

tertiary sites, disaster recovery, 525

testing

- disaster recovery plans, 546–547

- interface testing, interface testing, 569

- security, 412

- audits, 412–415

- blackbox testing, 420

- code reviews, 425

- coverage, 413–414

- DAST, 425

- DoS testing, 420

- Fagan inspections, 426

- fuzz testing, 426

- graybox testing, 420

- IAST, 425

- integer overflow, 426–427

- KPI, 414–415

- KRI, 415

- log reviews, 415–418

- misuse case testing, 426

- outsider testing, 420

- penetration testing, 257–263

- RASP, 425

- root causes analyses, 415

- sampling plans, 413–414

- SAST, 425

- scanning networks, 418–419

- social engineering testing, 421

- stress testing, 420

- synthetic transactions, 426

- techniques/methods, 424–427

- vulnerability scanning, 419

- war dialing, 420–421

- whitebox testing, 420

- wireless network testing, 420

software

- alpha testing, 570

- blackbox testing, 570

- final testing, 570

- function testing, 570

- interface testing, 569

- parallel testing, 570

- pilot/beta testing, 570

- regression testing, 570

- sociability testing, 570

- system testing, 569

- unit testing, 569

- whitebox testing, 570

TFTP (Trivial File Transfer Protocol), 269

thin clients, 378**third-party risk management, 110–112****threads, CPU, 161****threat actors, 78, 429–430**

- attack methodologies, 430–431
- corporate spies, 428
- doxing, 428
- foreign government agents, 429
- hacker researchers, 428, 429
- hactivism, 428
- insiders/disgruntled employees, 428
- organized crime, 428
- outsiders, threat actors, 428
- phreakers, 308, 430, 482, 492
- script kiddies, 428
- skilled hackers, 428
- zero trust, 429

threats/attacks, 431

- access controls, 438
 - access aggregation, 438–439
 - password attacks, 439–442
 - unauthorized access, 438
- APT, 450
- ARP poisoning, 436
- backdoors, 447–449
- booters, 434
- botnets, 434–436
- brute-force cracking, 441
- buffer overflows, 595–596
- crypters, 448–449
- database attacks, 437
- DDoS attacks, 433–434
- DNS spoofing, 437
- DoS attacks, 433
- dumpster diving, 444
- eavesdropping, 442
- email bombing, 437
- exploit kits, 450
- financial attacks, 596–597
- human-caused threats, 494–495
- hybrid attacks, 440
- identity theft, 443

impersonation attacks, 444

- intelligence, conducting, 107

IOC, 597

logic bombs, 446–447, 596–597

malicious software, 444–445

- APT, 450

- backdoors, 447–449

- crypters, 448–449

- exploit kits, 450

- logic bombs, 446–447

- packers, 448

- ransomware, 450–451

- rootkits, 449–450

- success attacks, 450

- Trojans, 447–449

- viruses, 445–446

- worms, 446

- wrappers, 448

methodologies of attacks, 430–431

mitigating, 108

modeling, 107, 108

- categorizing threats, 107

- DREAD, 109

- identifying threats, 107

- mapping/diagramming potential attacks, 107

- mitigating threats, 108

- OCTAVE, 109

- PASTA, 109

- software, 593

- STRIDE, 108

- threat intelligence, 107

- Trike, 109–110

- VAST, 109

packers, 448

pharming attacks, 437

phishing, 443

phreaking, 492

piggybacking, 444

pretexting, 443–444

rainbow tables, 441–442

ransomware, 450–451

threats/attacks

- risk assessments, 89, 93–96
- rootkits, 449–450
- session hijacking, 431–432
- shoulder surfing, 442, 444
- smishing, 308, 443
- sniffing, 432
- social engineering attacks, 443–444
- spear phishing, 443
- spoofing attacks, 442, 444
- success attacks, 450
- tailgating, 444
- traffic analysis, 437
- Trojans, 447–449
- Van Eck Phreaking, 199, 492
- virus hoaxes, 444
- viruses, 445–446, 597–598
- war driving, 437
- whaling, 443
- wiretapping, 433, 437
- worms, 446, 597–598
- wrappers, 448

threshold levels, 364**Thunderbolt interfaces, 167****Tibetan monks, Biba security model, 186****tires (flat), disaster recovery, 522–523****TLS (Transport Layer Security), 318–319****TNI (Trusted Network Interpretation), 191****tokens, 367**

- asynchronous tokens, 367–368
- LAN, 272
- synchronous tokens, 367–368

tolerating risk, 104, 105**topologies**

- network, 272
 - bus topologies, 272
 - fully connected topologies, 275
 - mesh topologies, 274
 - ring topologies, 273–274
 - star topologies, 273
 - wireless topologies, 309–310

Tower of Hanoi tape-rotation schemes, 538**TPM chips, 55–56, 154****trade secrets, 73–74****trademarks, 73****traffic analysis, 437****traffic padding, 321****training employees, 134–135**

- disaster recovery, 545
- ethics training/awareness, 137–138
 - 10 Commandments of Computer Ethics, 139–140
 - common fallacies, 141–142
 - Computer Ethics Institute, 139–140
 - IAB, 140–141
 - (ISC)2 Code of Ethics, 138–139
 - ISOC, 140–141
 - NIST SP 80–14, 141
 - regulatory requirements, 142–143
 - RFC 1087, 140–141

transactions

- processing, databases, 585
- synthetic, 426

transferring risk, 104–105**transistors, CPU, 159****transit (encryption), data in, 57–59****transport (host-to-host) layer, TCP/IP network model, 259–260, 318–319**

- TCP, 264–266, 267
- UDP, 264–265, 266–267

transport layer, OSI network model, 254–255**transport mode, IPsec, 330****Trike, threat modeling, 109–110****Triple DES (3DES), 206****Trojans, 447–449****trunks, VLAN, 285****trusted recovery, 475–476****tubular locks, 352, 355****tumbler locks, 352****tumbling attacks, 307–308**

tunnel mode, IPsec, 330
tunneling protocols, encryption, 57–58
 L2TP, 320
 PPTP, 320
 SSTP, 319
tuples, databases, 583
turnstiles, perimeter physical control systems, 346
twisted pair cables, 275–277
two-factor authentication, 375
Twofish, 210
Type I errors, 371
Type II errors, 371

U

UA (Uptime Agreements), 111
UDP (User Datagram Protocol), 255, 264–265, 266–267
unauthorized access, 438
unauthorized phone use, 306
unencrypted sensitive data, database vulnerabilities, 586
Unicode encoding, web-based vulnerabilities, 200
unit testing, 569
unnecessary enabled features, database vulnerabilities, 586
unpatched databases, 586
unpatched OS/software/browsers, mobile system vulnerabilities, 203
UPS, facility/site security controls, 504–505
URL encoding, web-based vulnerabilities, 200
USB (Universal Serial Buses), 167
user management, audits, 488–489
user mode, protection rings, 171
user provisioning, 376
users
 data management, 34
 managing, 469
 access controls, 471
 clipping levels, 471–472
 database administrators, 469
 job rotation, 471
 least privilege, 471
 network administrators, 469
 privileged entities, 470–471
 quality assurance specialists, 469
 reasonably prudent person rule, 472–473
 security architects, 469
 separation of duties, 469–470, 471
 system administrators, 469
 systems analysts, 469
 recovery strategies, 528–529
 security awareness, 136
 spoofing, 442

U.S. Government, encryption, 237

U.S. legal system/laws

administrative (regulatory) law, 71
 CALEA, 433
 CFAA of 1986, 72
 civil law, 71
 common law, 71
 criminal law, 71
 due care, 72
 due diligence, 72
 Economic Espionage Act of 1996, 72
 FCPA, 142
 Federal Sentencing Guidelines of 1991, 72
 FIPS, 82
 FISMA, 81
 GLBA, 80
 hearsay evidence, 72
 HIPAA, 79–80
 Identity Theft and Assumption Deterrence Act of 1998, 76
 keystroke monitoring, 492
 NIST, 82
 personal information websites, 76
 Privacy Act of 1974, The, 75
 privacy laws, 75–76

U.S. legal system/laws

- SOX, 81, 142, 472
- stare decisis, 71
- U.S. Child Pornography Prevention Act of 1996, 72
- U.S. Patriot Act of 2001, 72
- U.S. Securities Act of 1933, 472

utility loss, 495**V****vacations, mandatory, 133****validating**

- backups, 458
- systems, architecture security and engineering, 194

validity checks, 562**valuing assets, 91–93****Van Eck Phreaking, 199, 492****VAST, threat modeling, 109****vaulting, electronic, 539****Vernam ciphers, 303****views, databases, 584****Vignere ciphers, 300–301****virtual memory, 167–168****virus hoaxes, 444****viruses, 445–446, 597–598****Visual Basic programming language, 590****VLAN (Virtual Local Area Networks), 282, 284–285****VM (Virtual Machines), 168****voice recognition, 373****voice/wireless communications security, 298**

- 802.11 wireless networks/standards, 308–316
- ATBASH, 299
- Bluetooth technologies, 311–312
- book ciphers, 302–303
- Caesar's cipher, 298–299
- cell phones, 306–308
- concealment ciphers, 302

DECT, 315

end-to-end encryption, 320–321

Enigma machine, 303

Feistel network, 303

frequency analysis, 299

history, 298–304

link-to-link encryption, 321

message privacy, 331–332

multimedia collaboration, 331–332

network access control, 321–330

polyalphabetic ciphers, 299–300

Purple machine, 303, 304

quantum cryptography, 304

running key ciphers, 302–303

substitution ciphers, 301–302

TCP/IP network model, 316–320

- application layer controls, 317–318

- host-to-host (transport) layer, 318–319

- Internet layer controls, 319–320

- network access layer controls, 320

- process layer controls, 317–318

Vernam ciphers, 303

Vignere ciphers, 300–301

VoIP, 304–306

WAP, 315–316

WEP, 313–315

VoIP (Voice over IP), 304–306**VPN (Virtual Private Networks), 57–58****VSAN (Virtual SAN), 40****vulnerabilities**

- architecture security, 195–196
 - backdoors, 197
 - buffer overflows, 196, 200, 595–596
 - covert channels, 197–198
 - data diddling, 198
 - database attacks, 201–202
 - emanations, 198–199
 - incremental attacks, 198

- maintenance hooks, 197
 - mobile system vulnerabilities, 202–203
 - salami attacks, 198
 - SQL injections, 201–202, 586
 - state attacks, 197
 - Van Eck Phreaking, 199, 492
 - web-based vulnerabilities, 199–202
 - wireless vulnerabilities, 202
 - assessing, 419
 - cell phones, 307–308
 - databases, 586–587
 - IOC, 597
 - mobile system vulnerabilities, 202–203
 - risk assessments, 89, 95–96
 - SATAN vulnerability assessment tool, 138–139
 - scanning, 419
 - software, 592
 - viruses, 597–598
 - VoIP, 305–306
 - web-based vulnerabilities, 199
 - Burp Proxy Attack tool, 200
 - CSRF, 199, 200
 - direct OS commands, 199
 - directory traversal attacks, 199
 - SQL injections, 201–202, 586
 - Unicode encoding, 200
 - URL encoding, 200
 - XSS, 199, 200
 - wireless vulnerabilities, 202
 - worms, 597–598
 - zero-day vulnerabilities, 239, 401, 437
- VXLAN (Virtual Extensible Local Area Networks), 284–285**
- W**
-
- wait state, CPU, 159**
 - walls, facility/site security controls, 498–501**
 - WAN (Wide Area Networks), 278, 289–290**
 - circuit switching, 291–294
 - packet switching, 290–291
 - SD-WAN, 296
 - WAP (Wireless Application Protocol), 315–316**
 - war dialing, 420–421**
 - war driving, 437**
 - warded locks, 351**
 - warehouses, data, 37**
 - warm sites, disaster recovery, 526**
 - warning banners, 489**
 - water sprinklers, 508–509**
 - waterfall model, software development, 573**
 - web-based vulnerabilities, 199**
 - Burp Proxy Attack tool, 200
 - CSRF, 199, 200
 - direct OS commands, 199
 - directory traversal attacks, 199
 - SQL injections, 201–202, 586
 - Unicode encoding, 200
 - URL encoding, 200
 - XSS, 199, 200
 - web browsers (unpatched), mobile system vulnerabilities, 203**
 - web conferencing, 331**
 - web servers, 169**
 - websites, personal information websites, 76**
 - Weev, hacker researchers, 429**
 - WEP (Wired Equivalent Privacy), 313–315**
 - whaling, 443**
 - white noise, 198–199**
 - whitebox testing, 420, 570**
 - whitelists, 60, 480**
 - windows, facility/site security controls, 498–501**
 - wiping drives, 47, 477**
 - wireless network testing, 420**

wireless standards, 310**wireless topologies, 309–310****wireless/voice communications security, 298**

802.11 wireless networks/standards, 308–316

ATBASH, 299

Bluetooth technologies, 311–312

book ciphers, 302–303

Caesar's cipher, 298–299

cell phones, 306–308

concealment ciphers, 302

DECT, 315

end-to-end encryption, 320–321

Enigma machine, 303

Feistel network, 303

frequency analysis, 299

history, 298–304

link-to-link encryption, 321

message privacy, 331–332

multimedia collaboration, 331–332

network access control, 321–330

polyalphabetic ciphers, 299–300

Purple machine, 303, 304

quantum cryptography, 304

running key ciphers, 302–303

substitution ciphers, 301–302

TCP/IP network model, 316–320

application layer controls, 317–318

host-to-host (transport) layer, 318–319

Internet layer controls, 319–320

network access layer controls, 320

process layer controls, 317–318

Vernam ciphers, 303

Vigenere ciphers, 300–301

VoIP, 304–306

WAP, 315–316

WEP, 313–315

wireless vulnerabilities, 202**wiretapping, 433****WLAN (Wireless Local Area Networks), 309, 312–313****work area security/restricted access, 241****work factors, cryptographic attacks, 239–240****working images, digital forensics, 520****worms, 446, 597–598****WPA2 Enterprise, 320****WPAN (Wireless Personal Area Networks), 278****wrappers, 448****WS-Security, 377****WTLS (Wireless Transport Layer Security), 319**

X**X.25, 290****X.509 certificates, 228, 370****XACML (Extensible Access Control Markup Language), 387–388****XML programming language, 377, 590****XP (Extreme Programming), 577****XSS (Cross-Site Scripting), 199, 200****XTR public key cryptosystem, 222**

Y - Z**Zachman Framework, 155–156****zero trust, 325, 429****zero-day vulnerabilities, 239, 401, 437****zeroization, 46, 477****zero-trust environments, 59**