Cert Guide
Learn, prepare, and practice for exam success

CISA
Certified Information Systems Auditor® (CISA)

FREE SAMPLE CHAPTER
Certified Information Systems Auditor® (CISA®) Cert Guide

Michael Gregg
Rob Johnson
Contents at a Glance

Introduction xxiii

CHAPTER 1 The CISA Certification 3
CHAPTER 2 The Information Systems Audit 23
CHAPTER 3 The Role of IT Governance 71
CHAPTER 4 Maintaining Critical Services 137
CHAPTER 5 Information Systems Acquisition and Development 181
CHAPTER 6 Auditing and Understanding System Controls 231
CHAPTER 7 Systems Maintenance and Service Management 269
CHAPTER 8 Protection of Assets 333
CHAPTER 9 Asset Threats, Response, and Management 387
CHAPTER 10 Final Preparation 437
GLOSSARY 445

APPENDIX A Answers to the “Do I Know This Already” Quizzes and Review Questions 467

Index 484

Online Elements:

APPENDIX B Memory Tables
APPENDIX C Memory Tables Answer Key
# Table of Contents

**Introduction**  xxiii

**Chapter 1 The CISA Certification  3**

Exam Intent  3

Why the CISA Certification Is So Important  4

CISA: The Gold Standard  5

Exam Requirements  6

CISA Exam Windows  6

Scheduling to Take the Exam  7

Deadline to Apply for the CISA Certification  7

ISACA Agreements  9

CISA Exam Domains  10

Question Format and Grading  13

*Exam Grading*  13

*Exam Questions*  14

Getting Exam Results and Retests  15

Maintaining CISA Certification  16

*Reporting CPE Hours Earned*  16

*Earning CPE Hours*  17

Top 10 Tips and Tricks  18

Chapter Summary  19

Define Key Terms  20

Suggested Readings and Resources  20

**Chapter 2 The Information Systems Audit  23**

“Do I Know This Already?” Quiz  23

Foundation Topics  27

Skills and Knowledge Required to Be an IS Auditor  27

Work-Related Skills  27

Knowledge of Ethical Standards  28
ISACA Standards, Procedures, Guidelines, and Baselines

Knowledge of Regulatory Standards
Guidance Documents
Auditing Compliance with Regulatory Standards
Knowledge of Business Processes
Types of Audits
Risk Assessment Concepts

Risk Management
Auditing and the Use of Internal Controls
The Auditing Life Cycle
Audit Methodology
The Auditing Life Cycle Steps
Chain of Custody and Evidence Handling
Automated Work Papers
CAATs
Audit Closing
Report Writing

The Control Self-Assessment Process
Continuous Monitoring
Quality Assurance
The Challenges of Audits
Communicating Results
Negotiation and the Art of Handling Conflicts

Chapter Summary
Exam Preparation Tasks
Review All the Key Topics
Complete Tables from Memory
Define Key Terms
Exercises

2.1 Network Inventory
Review Questions
Suggested Readings and Resources
Chapter 3  The Role of IT Governance  71

“Do I Know This Already?” Quiz  71

Foundation Topics  75

The IT Steering Committee  75

Corporate Structure  77

IT Governance Frameworks  77

COBIT  78

ITIL  78

COBIT Versus ITIL  79

Enterprise Risk Management  80

The Risk Management Team  81

Asset Identification  82

Threat Identification  82

Quantitative Risk Assessment  84

Qualitative Risk Assessment  86

The Three Lines of Defense Model  87

Policy Development  90

Policy  91

Policy, Standards, Procedures, and Baselines  92

Auditing Policies, Standards, Procedures, and Baselines  93

Data Classification  96

Security Policy  98

Management Practices of Employees  100

Forced Vacations, Rotation of Assignments, and Dual Control  102

Separation Events  102

Roles and Responsibilities  103

Segregation of Duties (SoD)  105

Compensating Controls  106

Key Employee Controls  106

Performance Management  107

Key Performance Terms  108
Final Plan Design and Implementation 151
Training and Awareness 152
Implementation and Testing 153
Paper Tests 155
Preparedness Tests 155
Full Operation Tests 156
Monitoring and Maintenance 156
Understanding BCP Metrics 157
Recovery Strategies 159
Alternate Processing Sites 159
Alternate Processing Options 160
Hardware Recovery 163
Redundant Array of Independent Disks 164
Software and Data Recovery 165
Backup and Restoration 167
Telecommunications Recovery 169
Verification of Disaster Recovery and Business Continuity Process Tasks 170
The Disaster Life Cycle 172
Chapter Summary 174
Exam Preparation Tasks 174
Review All the Key Topics 175
Define Key Terms 175
Exercises 175
4.1 Business Impact and Risk 175
Review Questions 177
Suggested Readings and Resources 179

Chapter 5 Information Systems Acquisition and Development 181
“Do I Know This Already?” Quiz 181
Foundation Topics 185
IT Acquisition and Project Management 185
IT Acquisition 185
Software Escrow Agreements 185
Software Licensing 185
Contents

Project Management 187

Roles, Responsibility, and Structure of Project Management 188

Project Culture and Objectives 189

Making the Business Case for Investment 190

Return on Investment 191

Project Management Activities and Practices 192

Project Initiation 193

Project Planning 193

Project Control and Execution 199

Project Closing 199

Business Application Development 200

Systems-Development Methodology 200

Phase 1: Initiation phase 202

Phase 2: Development 204

Phase 3: Implementation 208

Phase 4: Operation and Maintenance 210

Phase 5: Disposal 211

Tools and Methods for Software Development 212

Information Systems Maintenance 213

Outsourcing and Alternative System Development 214

Cloud Computing 216

Cloud Threats 218

Application-Development Approaches 219

N-tier 220

Virtualization 221

Chapter Summary 222

Exam Preparation Tasks 223

Review All the Key Topics 223

Complete Tables from Memory 223

Define Key Terms 224

Exercises 224

5.1 Project Management 224

5.2 Project Management 225

Review Questions 226

Suggested Readings and Resources 229
<table>
<thead>
<tr>
<th>Exercises</th>
<th>262</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-1 Software Application Audit</td>
<td>262</td>
</tr>
<tr>
<td>Review Questions</td>
<td>263</td>
</tr>
<tr>
<td>Suggested Readings and Resources</td>
<td>266</td>
</tr>
<tr>
<td><strong>Chapter 7 Systems Maintenance and Service Management</strong></td>
<td>269</td>
</tr>
<tr>
<td>“Do I Know This Already?” Quiz</td>
<td>269</td>
</tr>
<tr>
<td>Foundation Topics</td>
<td>273</td>
</tr>
<tr>
<td>Service Management Frameworks</td>
<td>273</td>
</tr>
<tr>
<td>COBIT</td>
<td>273</td>
</tr>
<tr>
<td>FitSM</td>
<td>274</td>
</tr>
<tr>
<td>ISO 20000</td>
<td>274</td>
</tr>
<tr>
<td>eTOM</td>
<td>275</td>
</tr>
<tr>
<td>Fundamental Technologies</td>
<td>275</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>275</td>
</tr>
<tr>
<td>Secondary Storage</td>
<td>277</td>
</tr>
<tr>
<td>Utility Software</td>
<td>277</td>
</tr>
<tr>
<td>Database-Management Systems</td>
<td>278</td>
</tr>
<tr>
<td>Database Structure</td>
<td>279</td>
</tr>
<tr>
<td>Software Licensing Issues</td>
<td>282</td>
</tr>
<tr>
<td>Digital Rights Management</td>
<td>283</td>
</tr>
<tr>
<td>Network Infrastructure</td>
<td>283</td>
</tr>
<tr>
<td>Network Types</td>
<td>284</td>
</tr>
<tr>
<td>Network Standards and Protocols</td>
<td>285</td>
</tr>
<tr>
<td>The OSI Reference Model</td>
<td>286</td>
</tr>
<tr>
<td><strong>The Application Layer</strong></td>
<td>287</td>
</tr>
<tr>
<td><strong>The Presentation Layer</strong></td>
<td>287</td>
</tr>
<tr>
<td><strong>The Session Layer</strong></td>
<td>288</td>
</tr>
<tr>
<td><strong>The Transport Layer</strong></td>
<td>288</td>
</tr>
<tr>
<td><strong>The Network Layer</strong></td>
<td>288</td>
</tr>
<tr>
<td><strong>The Data Link Layer</strong></td>
<td>289</td>
</tr>
<tr>
<td><strong>The Physical Layer</strong></td>
<td>289</td>
</tr>
<tr>
<td>Network Services and Applications</td>
<td>290</td>
</tr>
</tbody>
</table>
Chapter 8  Protection of Assets  333

“Do I Know This Already?” Quiz  333

Foundation Topics  336

Access Control  336

Identification and Authentication (I&A)  336

Authentication by Knowledge  336
Authentication by Ownership  338
Authentication by Characteristic  338

Single Sign-on  340

Federation  343
Remote Access  345

RADIUS  345
Diameter  346
TACACS  346

Additional Remote Access Options  346

SSH  347
VPNs  348

Physical and Environmental Access Controls  349

Fences, Gates, and Bollards  349

Other Physical and Environmental Controls  351

Using Guards to Restrict Access  352

Locks  353
Lighting  354
CCTV  355

Heating, Ventilation, and Air Conditioning (HVAC)  356

Security Controls for Hardware and Software  356

Securing Voice Communications  356

Encryption’s Role as a Security Control  357

Private Key Encryption  359

Data Encryption Standard (DES)  361

Advanced Encryption Standard (AES)  362

Public Key Encryption  362

RSA Encryption  363

Elliptic Curve Cryptography (ECC)  363
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantum Cryptography</td>
<td>364</td>
</tr>
<tr>
<td>Hashing and Digital Signatures</td>
<td>364</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td>365</td>
</tr>
<tr>
<td>Using Cryptography to Secure Assets</td>
<td>367</td>
</tr>
<tr>
<td>Internet Security Protocols</td>
<td>368</td>
</tr>
<tr>
<td>Protection of Information Assets</td>
<td>369</td>
</tr>
<tr>
<td>Information Life Cycle</td>
<td>369</td>
</tr>
<tr>
<td>Access Restriction</td>
<td>370</td>
</tr>
<tr>
<td>Laws Related to the Protection of Information</td>
<td>370</td>
</tr>
<tr>
<td>Maintaining Compliance</td>
<td>371</td>
</tr>
<tr>
<td>Protection of Privacy</td>
<td>372</td>
</tr>
<tr>
<td>Using Data Classification to Secure Critical Resources</td>
<td>373</td>
</tr>
<tr>
<td>Data Leakage and Attacks</td>
<td>374</td>
</tr>
<tr>
<td>Attacks Against Encryption</td>
<td>374</td>
</tr>
<tr>
<td>Threats from Unsecured Devices</td>
<td>375</td>
</tr>
<tr>
<td>Threats from Improper Destruction</td>
<td>378</td>
</tr>
<tr>
<td>Threats to the Infrastructure</td>
<td>378</td>
</tr>
<tr>
<td>Chapter Summary</td>
<td>380</td>
</tr>
<tr>
<td>Exam Preparation Tasks</td>
<td>381</td>
</tr>
<tr>
<td>Review All the Key Topics</td>
<td>381</td>
</tr>
<tr>
<td>Complete Tables from Memory</td>
<td>382</td>
</tr>
<tr>
<td>Define Key Terms</td>
<td>382</td>
</tr>
<tr>
<td>Review Questions</td>
<td>382</td>
</tr>
<tr>
<td>Suggested Reading and Resources</td>
<td>384</td>
</tr>
<tr>
<td><strong>Chapter 9</strong> Asset Threats, Response, and Management</td>
<td>387</td>
</tr>
<tr>
<td>“Do I Know This Already?” Quiz</td>
<td>387</td>
</tr>
<tr>
<td>Foundation Topics</td>
<td>391</td>
</tr>
<tr>
<td>Security Controls</td>
<td>391</td>
</tr>
<tr>
<td>Technical Controls</td>
<td>391</td>
</tr>
<tr>
<td>Cloud Computing</td>
<td>391</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>391</td>
</tr>
<tr>
<td>Databases</td>
<td>393</td>
</tr>
<tr>
<td>Virtualization</td>
<td>395</td>
</tr>
<tr>
<td>Administrative Controls</td>
<td>396</td>
</tr>
</tbody>
</table>
## Attack Methods and Techniques  399
- Social Engineering and Nontechnical Attacks  399
- Sniffing  400
- Man-in-the-Middle Attacks and Hijacking  401
- Denial of Service  402
- Botnets  403
- Malware  404
- Wireless and Bluetooth  405
- SQL Injection  408
- Buffer Overflow  409
- XSS and XSRF  411
- Logic Bombs, Rounding Down, and Asynchronous Attacks  411
- Integer Overflow  412
- Password Attacks  412

## Prevention and Detection Tools and Techniques  414
- Audit and Log Review  414
- Security Testing Techniques  415
  - *Vulnerability Scanning*  416
  - *Penetration Testing*  416

## Problem and Incident Management Practices  418
- Tracking Change  418
- Fraud Risk Factors  419
- *Insiders*  419
- *Outsiders*  419
- Incident Response  420
  - *Emergency Incident Response Team*  422
  - *Incident Response Process*  422
  - *Incident Response and Results*  424
  - *Forensic Investigation*  425
  - *Forensics Steps*  426
  - *Other Forensic Types*  427
  - Computer Crime Jurisdiction  429

## Chapter Summary  430

## Exam Preparation Tasks  430
Review All the Key Topics 430
Complete Tables from Memory 431
Define Key Terms 431
Review Questions 431
Suggested Reading and Resources 433

Chapter 10 Final Preparation 437
Tools for Final Preparation 437
Pearson Test Prep Practice Test Software and Questions on the Website 437
Accessing the Pearson Test Prep Software Online 438
Accessing the Pearson Test Prep Software Offline 438
Customizing Your Exams 439
Updating Your Exams 440
Premium Edition 440
Memory Tables 441
Chapter-Ending Review Tools 441
Suggested Plan for Final Review/Study 441
Summary 442

Glossary 445
Appendix A Answers to the “Do I Know This Already” Quizzes and Review Questions 467
Index 484

Online Elements:
Appendix B Memory Tables
Appendix C Memory Tables Answer Key
About the Authors

Michael Gregg (CISSP, SSCP, CISA, MCSE, MCT, CTI+, A+, N+, Security+, CCNA, CASP, CISA, CISM, CEH, CHFI, and GSEC) works for a Houston, Texas-based IT security consulting firm.

Michael is responsible for working with organizations to develop cost-effective and innovative technology solutions to security issues and for evaluating the security of emerging technologies. He has more than 20 years of experience in the IT field and holds two associate’s degrees, a bachelor’s degree, and a master’s degree. In addition to co-authoring the first, second, and third editions of Security Administrator Street Smarts, Michael has written or co-authored 15 other books, including The Network Security Test Lab: A Step-by-Step Guide (Wiley, 2015); CompTIA Security+ Rapid Review (Microsoft, 2013); Certified Ethical Hacker Cert Guide (Pearson, 2017); and CISSP Exam Cram (Que, 2016).

Michael has been quoted in newspapers such as the New York Times and featured on various television and radio shows, including NPR, ABC, CBS, Fox News, CNN, and others, discussing cybersecurity and ethical hacking. He has created more than a dozen IT security training classes, and he has created and performed video instruction on many security topics, such as cybersecurity, CISSP, CASP, Security+, and others.

When not consulting, teaching, or writing, Michael enjoys 1960s muscle cars and has a slot in his garage for a new project car.

Rob Johnson (CISSP, CISA, CISM, CGEIT, and CRISC) is experienced in information risk, IT audit, privacy, and security management. He has a diverse background that includes hands-on operational experience as well as providing strategic risk assessment and support to leadership and board-level audiences.

Rob currently serves as a senior vice president and technology executive with global teams and responsibilities at Bank of America. He has held various technology and executive positions throughout his career, including chief information security officer for a global insurance company, head of IT audit for a major domestic bank, chief information security officer for a large midwestern bank, chief cybersecurity architect and product owner for a major software house where he led deployments across 15 countries, and senior partner at a consulting firm.
Rob is well known across a number of industry groups. He is a published author and frequent speaker at conferences. Rob has served on a number of ISACA global committees; for example, he was formerly the chair of the ISACA Education Committee and a member of the ISACA Assurance Committee to name a few. In addition, Rob was one of the 12 members of the prestigious ISACA COBIT 5 Task Force, which led to the creation of the COBIT 5 global standard.

Rob holds a Bachelor of Science Degree in Interdisciplinary Studies from the University of Houston. He lives a quiet life, where he enjoys his children, watches his amazing son Donald win chess tournaments, and spends time with his wonderful wife, Lin.
Dedication

In memory of Debbie Dablin, who served as a technical editor for several of my books and fought a year-long battle against cancer. Cancer does not have a face until it’s someone you know.—M.G.

To my extraordinary father, who always gives of himself to others and taught us the importance of how to live a simple life through family and country and to give of one’s self.—R.J.
Acknowledgments

I would like to offer a big thank-you to Christine for her help and understanding during the long hours that a book project entails. I also want to thank my parents. A special thanks to the people of Pearson IT Certification, who helped make this project a reality.—Michael Gregg

I would like to thank Ellie Bru for her professional support in making this book happen and her keen ability to keep up with my never-ending travel schedule. She has the rare ability to track me down anywhere in the world to keep my edits on course. Thank you! I also thank Michelle and the team at Pearson IT Certification for the opportunity to make this book possible and the belief in its important contribution.—Rob Johnson
About the Technical Reviewer

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

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

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

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

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

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
      ATTN: Reader Feedback
      800 East 96th Street
      Indianapolis, IN 46240 USA

Reader Services

Register your copy of Certified Information Systems Auditor (CISA) Cert Guide at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789758446 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

The ISACA CISA exam has become the leading ethical hacking certification available today. CISA is recognized by both employers and the industry as providing candidates with a solid foundation of auditing and technical network assessment review. The CISA exam covers a broad range of IT auditing concepts to prepare candidates for roles in both audit and non-audit capacities, including IT risk management, IT compliance, and IT controls analysis.

This book offers you a one-stop shop for what you need to know to pass the CISA exam. To pass the exam, you do not have to take a class in addition to reading this book. However, depending on your personal study habits or learning style, you might benefit from buying this book and taking a class.

Cert Guides are meticulously crafted to give you the best possible learning experience for the particular characteristics of the technology covered and the certification exam. The instructional design implemented in the Cert Guides reflects the nature of the CISA certification exam. The Cert Guides provide you with the factual knowledge base you need for the exams and then take it to the next level with exercises and exam questions that require you to engage in the analytic thinking needed to pass the CISA exam.

ISACA recommends that a candidate for this exam have a minimum of 5 years of experience in audit and IT security. In addition, ISACA requires that candidates have that experience within the 10-year period preceding the application date for certification or within 5 years.

This book’s goal is to prepare you for the CISA exam, and it reflects the vital and evolving responsibilities of IT auditors. It provides basics to get you started in the world of IT audit and prepare you for the exam. Those wanting to become experts in this field should be prepared for additional reading, training, and practical experience.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the CISA exam. In fact, if the primary objective of this book was different, the book’s title would be misleading; however, the methods used in this book to help you pass the CISA exam are designed to also make you much more knowledgeable about how IT auditors do their job. This book and the accompanying online practice exams together have more than enough questions to help you prepare for the exam.
One key methodology used in this book is to help you discover the exam topics and tools that you need to review in more depth. The CISA exam will expect you to understand not only IT auditing concepts but common frameworks such as COBIT. This book does not try to help you pass the exam by memorization alone but helps you truly learn and understand the topics and know when specific approaches should be used. This book will help you pass the CISA exam by using the following methods:

- Helping you discover which test topics you still need to master
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions online

Who Should Read This Book?

This book is not designed to be a general IT book or a book that teaches financial audits. This book looks specifically at how IT auditors assess networks, examine controls, and test defenses to determine their adequacy. Overall, this book is written with one goal in mind: to help you pass the exam.

So, why should you want to pass the CISA exam? Because it’s one of the leading IT audit certifications. It is also featured as part of DoDD 8140, and having the certification might mean a raise, a promotion, or other recognition. It’s also a chance to enhance your resume and to demonstrate that you are serious about continuing the learning process and are not content to rest on your laurels.

Strategies for Exam Preparation

Although this book is designed to prepare you to take and pass the CISA certification exam, there are no guarantees. Read this book, work through the questions and exercises, and when you feel confident, take the practice exams provided online. Your results should tell you whether you are ready for the real thing.

When taking the actual certification exam, make sure that you answer all the questions before your time limit expires. Do not spend too much time on any one question. If you are unsure about the answer to a question, answer it as best you can and then mark it for review.

Remember that the primary objective is not to pass the exam but to understand the material. When you understand the material, passing the exam should be simple.
Knowledge is similar to a pyramid in that to build upward, you need a solid foundation. This book and the CISA certification are designed to ensure that you have that solid foundation.

Regardless of the strategy you use or the background you have, the book is designed to help you get to the point where you can pass the exam in the least amount of time possible. Several book features will help you gain the confidence you need to be convinced that you know some material already and to help you know what topics you need to study more.

**How This Book Is Organized**

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need to work with further. Chapter 1, “The CISA Certification,” provides an overview of the CISA certification and reviews some basics about exam preparation. Chapters 2 through 9 are the core chapters. If you intend to read them all, the order in the book is an excellent sequence to use.

The core chapters, Chapters 2 through 9, cover the following topics:

- **Chapter 2, “The Information Systems Audit”:** This chapter discusses basic audit techniques and the skills that are required of an auditor. This chapter reviews guidance documents and auditing standards.

- **Chapter 3, “The Role of IT Governance”:** This chapter discusses the basic ideas behind governance and steering committees. The chapter reviews management and control frameworks and process optimization.

- **Chapter 4, “Maintain Critical Services”:** This chapter covers issues related to business continuity and disaster recovery. Maintaining critical services requires an understanding of criticality and maximum tolerable downtime.

- **Chapter 5, “Information Systems Acquisition and Development”:** This chapter examines IT acquisition and the decision to build or buy. Project management and application development methodologies are discussed. Emerging technologies such as cloud computing are also covered.

- **Chapter 6, “Auditing and Understanding System Controls”:** This chapter covers auditing and business controls.

- **Chapter 7, “System Maintenance and Service Management”:** This chapter covers the basics of system maintenance and service management, including service management frameworks and networking infrastructure.
Chapter 8, “Protection of Assets”: This chapter examines the controls used to protect assets. These controls can be administrative, physical, or technical. The concept is to layer controls to provide reasonable assurance.

Chapter 9, “Asset Threats, Response, and Management”: This chapter discusses incident management and the response to threats from both insiders and outsiders.

How to Use This Book

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Therefore, this book does not try to help you pass the exams only by memorization but by truly learning and understanding the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it but do not study it any further, you probably will not be ready to pass the exam with confidence. The following features in this book give you tools that help you determine what you know, review what you know, better learn what you don’t know, and be well prepared for the exam:

- **“Do I Know This Already?” quizzes**: Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter.

- **Foundation Topics**: This section provides the core content of each chapter. In it you learn about the protocols, concepts, and configuration for the topics in the chapter.

- **Exam Preparation Tasks**: This section lists a series of study activities that should be done after reading the Foundation Topics section. Each chapter includes the activities that make the most sense for studying the topics in that chapter. This section includes the following activities:
  - **Key Topics Review**: The Key Topic icon appears next to the most important items in the Foundation Topics section of the chapter. The Key Topics Review activity lists the key topics from the chapter and their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic. Review these topics carefully.
  - **Definition of Key Terms**: Although certification exams might be unlikely to ask you to define terms, the CISA exam requires you to learn and know a lot of terminology. This section lists some of the most important terms.
from the chapter and asks you to write a short definition and compare your answer to the Glossary.

- **Memory Tables:** Like most other certification guides from Pearson IT Certification, this book purposefully organizes information into tables and lists for easier study and review. Rereading these tables can be very useful before the exam. However, it is easy to skim over the tables without paying attention to every detail, especially when you remember having seen the table’s contents when reading the chapter.

Instead of simply reading the tables in the various chapters, you can use Appendix B, “Memory Tables,” and Appendix C, “Memory Tables Answer Key,” as another review tool. Appendix B lists partially completed versions of many of the tables from the book. You can open Appendix B (a PDF on the companion website page that comes with this book) and print the appendix. For review, attempt to complete the tables.

Appendix C, also a PDF located on the companion website page, lists the completed tables so you can check yourself. You can also just refer to the tables as printed in the book.

- **Exercises:** At the end of each chapter are sample exercises that list a series of tasks for you to practice to apply the lessons from the chapter in a real-world setting.

- **Review Questions:** These questions help you confirm that you understand the content just covered.

- **Answers and Explanations:** We provide the answer to each of the Review Questions, as well as explanations about why each possible answer is correct or incorrect.

- **Suggested Readings and Resources:** Each chapter provides a list of links to further information on topics related to the chapter you’ve just read.

**Companion Website**

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


2. Respond to the challenge questions.

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

4. Click on the Access Bonus Content link under the product listing.
Pearson Test Prep Practice Test Software

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

Accessing the Pearson Test Prep Software Online

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

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

Accessing the Pearson Test Prep Software Offline

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

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

Step 2. Correctly answer the challenge questions.
Step 3. Go to your account page and select the Registered Products tab.
Step 4. Click the **Access Bonus Content** link under the product listing.

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

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

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

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

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

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

Step 11. Click **Next** and then click **Finish** to download the exam data to your application.

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

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

**Customizing Your Exams**

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

- **Study Mode**: Study Mode allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you use first, to assess your knowledge and identify information gaps.

- **Practice Exam Mode**: Practice Exam Mode locks certain customization options and presents a realistic exam experience. Use this mode when you are preparing to test your exam readiness.

- **Flash Card Mode**: Flash Card Mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers.
without the benefit of seeing multiple choice options. This mode will not provide the detailed score reports that the other two modes will, so it should not be used if you are trying to identify knowledge gaps.

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

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

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

Updating Your Exams

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

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

To update a particular exam you have already activated and downloaded, simply select the Tools tab and click the Update Products button. Again, this is only an issue with the desktop Windows application.
If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the **Tools** tab and click the **Update Application** button to ensure that you are running the latest version of the software engine.

**Premium Edition eBook and Practice Tests**

This book includes an exclusive offer for 70 percent off the Premium Edition eBook and Practice Tests edition of this title. See the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

**End-of-Chapter Review Tools**

Chapters 1 through 9 each have several features in the “Exam Preparation Tasks” and “Review Questions” sections at the end of the chapter. You might have already worked through these in each chapter. However, you might also find it helpful to use these tools again as you make your final preparations for the exam.
The following exam domain is partially covered in this chapter:

Domain 4—Information Systems Operations, Maintenance and Service Management

This chapter covers the following topics:

- **Threats to Business Operations**: Businesses face many threats and must have the proper controls and countermeasures to deal with them.

- **The Business Continuity Planning (BCP) Process**: One of the key activities of business continuity is the measurement of the performance of the program. Good governance presumes analysis of ongoing business processes to ensure that they are fulfilling company objectives.

- **Recovery Strategies**: Many different recovery strategies exist to deal with potential outages. An organization must choose the right one to ensure that critical activities can continue.
CHAPTER 4

Maintaining Critical Services

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 4-1 lists the major headings in this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers at the bottom of the page following the quiz and in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions Covered in This Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats to Business Operations</td>
<td>1, 10</td>
</tr>
<tr>
<td>The Business Continuity Planning (BCP) Process</td>
<td>2–5</td>
</tr>
<tr>
<td>Recovery Strategies</td>
<td>6–9</td>
</tr>
</tbody>
</table>

**CAUTION** The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as incorrect for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following is the highest level of incident classification?
   a. Major
   b. Minor
   c. Defined
   d. Crisis
2. From an audit perspective, what best defines how current the data must be or how much data an organization can afford to lose?
   a. RTO
   b. RPO
   c. MTD
   d. WRT

3. Which of the following specifies the maximum elapsed time to recover an application at an alternate site?
   a. RTO
   b. RPO
   c. MTD
   d. WRT

4. Which of the following defines the maximum amount of time the organization can provide services at the alternate site? This value can be determined by items such as contractual values.
   a. SDO
   b. SLA
   c. MTD
   d. WRT

5. Which of the following activities are specifically required for critical processes and produce revenue?
   a. Core processing
   b. Non-discretionary processes
   c. Maximum acceptable outage
   d. Supporting processes

6. Which version of RAID offers no fault tolerance?
   a. RAID 0
   b. RAID 1
   c. RAID 10
   d. RAID 15
7. This tape-rotation scheme is named after a mathematical puzzle.
   a. Grandfather, Father, Son
   b. Complex
   c. Simple
   d. Tower of Hanoi

8. This recovery option is sometimes referred to as a gentleman’s agreement.
   a. Hot site
   b. Redundant site
   c. Reciprocal
   d. Grandfather, father, son

9. Which of the following would be used to describe a non-repairable item that has reached end of life?
   a. MTTR
   b. MTTF
   c. MTBF
   d. SLA

10. Which of the following is the lowest level of incident classification?
    a. Major
    b. Minor
    c. Negligible
    d. Crisis
There is no shortage of events that can endanger business operations. Such events can come from inside or outside the organization and are typically categorized as either human-caused, technical, or natural threats, as shown in Figure 4-1. Natural threats are high on the list. In 2016, events such as Hurricane Matthew in the Caribbean, earthquakes in Ecuador, and catastrophic flooding in China topped the list. Such events highlight the need to be adequately prepared. Companies tend to seriously underestimate how long it would take to restore operations. In 2017, many companies were hit with ransomware because of flaws in their backup and offsite storage programs; other companies suffered because they had no workstation recovery plans for end users.

Figure 4-1  Sources of Security Threats

Answers to the “Do I Know This Already?” Quiz:

A company may not always update its plans as the company grows, changes, or modifies existing processes, even though the results of poor planning can be disastrous for the company. Some estimates indicate that only a small percentage of businesses are required by regulation to have a disaster recovery plan. Disaster recovery must compete for limited funds. Companies might be lulled into thinking that these funds might be better spent on more immediate needs. Some businesses might simply underestimate the risk and hope that adverse events don’t happen to them. Disaster recovery planning requires a shift of thinking from reactive to proactive.

Many of us would prefer not to plan for disasters. Many see it as an unpleasant exercise or would just prefer to ignore it. Sadly, we all must deal with disasters and incidents. They are dynamic by nature. For example, mainframes face a different set of threats than distributed systems, just as users connected to free wireless networks face a different set of threats than those connected to wired networks inside an organization. This means that management must be dynamic and must be able to change with time. Regardless of the source of a threat, each one has the potential to cause an incident. Incident management and disaster recovery are closely related. Incidents might or might not cause disruptions to normal operations. From the perspective of an auditor, a review of incident management should be performed to determine whether problems and incidents are prevented, detected, analyzed, reported, and resolved in a timely manner. This means the auditor should review existing incident response plans. The auditor also plays a critical role after an incident in that there should be a review of what worked and what did not so the plan can be optimized to be better prepared for the next incident.

An organization needs to have a way to measure incidents and quantify their damage. Table 4-2 lists the incident classification per ISACA. An auditor should have knowledge of problem and incident management practices.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crisis</td>
<td>A crisis is considered a major problem. It is of sufficient impact that it adversely affects the organization’s ability to continue business functions.</td>
</tr>
<tr>
<td>Major</td>
<td>A major incident is of sufficient strength to negatively impact one or more departments, or it might even affect external clients.</td>
</tr>
<tr>
<td>Minor</td>
<td>Although these events are noticeable, they cause little or no damage.</td>
</tr>
<tr>
<td>Negligible</td>
<td>These detectable events cause no damage or have no longer-term effect.</td>
</tr>
</tbody>
</table>
Disruptive incidents such as a crisis or major or minor events should be tracked and analyzed so that corrective actions can be taken to prevent these events from occurring in the future.

The Business Continuity Planning (BCP) Process

The BCP process can be described as the process of creating systems of prevention and recovery to deal with potential threats to a company. One of the best sources of information about the BCP process is the Disaster Recovery Institute International (DRII), which you can find online at www.drii.org. The process that DRII defines for BCP is much broader in scope than the ISACA process. DRII breaks down the disaster recovery process into 10 domains:

- Project initiation and management
- Risk evaluation and control
- Business impact analysis
- Developing business continuity management strategies
- Emergency response and operations
- Developing and implementing business continuity plans
- Awareness and training programs
- Exercising and maintaining business continuity plans
- Crisis communications
- Coordination with external agencies

The BCP process as defined by ISACA has a much narrower scope and focuses on the following seven steps, each of which is discussed in greater detail in the following sections:

1. Project management and initiation
2. Business impact analysis
3. Development and recovery strategy
4. Final plan design and implementation
5. Training and awareness
6. Implementation and testing
7. Monitoring and maintenance
NOTE The auditors role in the business continuity process is to evaluate resilience and to determine whether the BCP process is controlled effectively and continue to support the organization’s objectives.

Project Management and Initiation

Before the BCP process can begin, management must be on board. Management is ultimately responsible and must be actively involved in the process. Management sets the budget, determines the team leader, and gets the process started. The BCP team leader determines who will be on the BCP team. The team’s responsibilities include the following:

- Identifying regulatory and legal requirements
- Identifying all possible threats and risks
- Estimating the possibilities of these threats and their loss potential and ranking them based on the likelihood of the event occurring
- Performing a business impact analysis (BIA)
- Outlining which departments, systems, and processes must be up and running first
- Developing procedures and steps in resuming business after a disaster
- Assigning tasks to individuals that they should perform during a crisis situation
- Documenting, communicating with employees, and performing training and drills

One of the first steps the team is tasked with is meeting with senior management. The purpose of this meeting is to define goals and objectives, discuss a project schedule, and discuss the overall goals of the BCP process. This should give everyone present some idea of the scope of the final BCP policy.

It’s important for everyone involved to understand that the BCP is the most important corrective control the organization will have an opportunity to shape. Although the BCP process is primarily corrective, it also has the following elements:

- **Preventive:** Controls to identify critical assets and develop ways to prevent outages
- **Detective:** Controls to alert the organization quickly in case of outages or problems
- **Corrective:** Controls to return to normal operations as quickly as possible
Business Impact Analysis

Chance and uncertainty are part of the world we live in. We cannot predict what tomorrow will bring or whether a disaster will occur—but this doesn’t mean we cannot plan for it. As an example, the city of Galveston, Texas, is in an area prone to hurricanes. Just because the possibility of a hurricane in winter in Galveston is extremely low doesn’t mean that planning can’t take place to reduce the potential negative impact of such an event actually occurring. This is what BIA is about. Its purpose is to think through all possible disasters that could take place, assess the risk, quantify the impact, determine the loss, and develop a plan to deal with the incidents that seem most likely to occur.

As a result, BIA should present a clear picture of what is needed to continue operations if a disaster occurs. The individuals responsible for BIA must look at the organization from many different angles and use information from a variety of inputs. For BIA to be successful, the BIA team must know what the key business processes are. This is something that businesses may already know but don’t recognize it as such. As an example, a computer company that places a priority on selling computers over the service and repair of computers has determined the key activity. It’s the selling of the product. As such, this activity needs to have controls in place to continue in the face of negative events. Questions the team must ask when determining critical processes might include the following:

- **Does the process support health and safety?** Items such as the loss of an air traffic control system at a major airport or the loss of power in a hospital operating room could be devastating to those involved and result in loss of life.

- **Does the loss of the process have a negative impact on income?** For example, a company such as eBay would find the loss of Internet connectivity devastating, whereas a small nonprofit organization might be able to live without connectivity for days.

- **Does the loss of the process violate legal or statutory requirements?** For example, a coal-powered electrical power plant might be using scrubbers to clean the air before emissions are released. Loss of these scrubbers might lead to a violation of federal law and result in huge regulatory fines.

- **How does the loss of the process affect users?** Returning to the example of the coal-powered electrical power plant, it is easy to see how problems with the steam-generation process would shut down power generation and leave many residential and business customers without power. This loss of power in the Alaskan winter or in the Houston summer would have a large impact.

As you might be starting to realize, performing BIA is no easy task. It requires not only knowledge of business processes but also a thorough understanding of the
organization. This includes IT resources and individual business units, as well as the interrelationships between these pieces. This task requires the support of senior management and the cooperation of IT personnel, business unit managers, and end users. The general steps of BIA are as follows:

1. Determine data-gathering techniques.
2. Gather business impact analysis data.
3. Identify critical business functions and resources.
4. Verify completeness of data.
5. Establish recovery time for operations.
6. Define recovery alternatives and costs.

**TIP** For the CISA exam, you should understand that many BIA programs look no further than the traditional network. It is important that BIA also look at systems and information that might normally be overlooked, such as information stored on end-user systems that are not backed up and laptops used by the sales force or management.

BIA typically includes both quantitative and qualitative components:

- **Quantitative analysis** deals with numbers and dollar amounts. It involves attempting to assign a monetary value to the elements of risk assessment and to place dollar amounts on the potential impact, including both loss of income and expenses. Quantitative impacts can include all associated costs, including these:
  - Lost productivity
  - Delayed or canceled orders
  - Cost of repair
  - Value of the damaged equipment or lost data
  - Cost of rental equipment
  - Cost of emergency services
  - Cost to replace the equipment or reload data
Qualitative assessment is scenario driven and does not involve assigning dollar values to components of the risk analysis. A qualitative assessment ranks the seriousness of impacts into grades or classes, such as low, medium, and high. These are usually associated with items to which no dollar amount can be easily assigned:

- **Low**: Minor inconvenience; customers might not notice.
- **Medium**: Some loss of service; might result in negative press or cause customers to lose some confidence in the organization.
- **High**: Will result in loss of goodwill between the company and a client or an employee; negative press also reduces the outlook for future products and services.

Although different approaches for calculating loss exist, one of the most popular methods of acquiring data is using a questionnaire. A team may develop a questionnaire for senior management and end users and might hand it out or use it during an interview process. This form might include items such as the recovery point objective (RPO), the recovery time objective (RTO), or even the mean time to recover (MTTR). Figure 4-2 provides an example of a typical BIA questionnaire.

The questionnaire can even be used in a round-table setting. This method of performing information gathering requires the BIA team to bring the required key individuals into a meeting and discuss as a group what impact specific types of disruptions would have on the organization. Auditors play a key role because they might be asked to contribute information such as past transaction volumes or the impact to the business of specific systems becoming unavailable.

**NOTE** The BIA must typically determine criticality, downtime estimates, and resource requirements. Criticality can be determined by performing risk calculations such as annualized loss and its impact. Downtime estimates can be evaluated by examining the RTO. Determining the resource requirements requires an analysis of the inputs and outputs of systems. As an example, a generator is needed for backup, yet fuel is needed as a resource to keep the generator running.
Key Business Processes

Identify and describe the key business processes of the unit/division. For each process, identify its Recovery Time Objective (RTO). RTO is defined as how quickly the process must be restored following a disaster. The Recovery Time Objective is an estimate of how long the process can be unavailable. Also identify a Recovery Point Objective (RPO) for each process. RPO is the determination of how much data loss, in terms of time, is tolerable before a process is significantly impacted. If the process can be performed manually, please use Attachment A to explain. Use multiple pages if needed.

<table>
<thead>
<tr>
<th>Key Business Process</th>
<th>Recovery Time Objective</th>
<th>Recovery Point Objective</th>
<th>Can This Be Performed Manually? For How Long?</th>
<th>Computer Systems/Applications Required to Perform This Process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4-2  BIA Questionnaire

Criticality Analysis

How do you classify systems and resources according to their value or order of importance? You determine the estimated loss in the event of a disruption and calculate the likelihood that the disruption will occur. The quantitative method for this process involves three steps:

1. **Estimate potential losses (SLE):** This step involves determining the single loss expectancy (SLE), which is calculated as follows:

   \[
   \text{Single loss expectancy} = \text{Asset value} \times \text{Exposure factor}
   \]

   Items to consider when calculating the SLE include the physical destruction of human-caused events, the loss of data, and threats that might cause a delay or disruption in processing. The exposure factor is the measure or percentage of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO):** The purpose of a threat analysis is to determine the likelihood that an unwanted event will happen. The goal is to estimate the annual rate of occurrence (ARO). Simply stated, how many times is this event expected to happen in one year?
3. **Determine annual loss expectancy (ALE):** This third and final step of the quantitative assessment seeks to combine the potential loss and rate/year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

\[
\text{Annualized loss expectancy (ALE)} = \text{Single loss expectancy (SLE)} \times \text{Annualized rate of occurrence (ARO)}
\]

For example, suppose that the potential loss due to a hurricane on a business based in Tampa, Florida, is $1 million. An examination of previous weather patterns and historical trends reveals that there has been an average of one hurricane of serious magnitude to hit the city every 10 years, which translates to 1/10, or 0.1% per year. This means the assessed risk that the organization will face a serious disruption is $100,000 (= $1 million × 0.1) per year. That value is the annualized loss expectancy and, on average, is the amount per year that the disruption will cost the organization. Placing dollar amounts on such risks can aid senior management in determining what processes are most important and should be brought online first. Qualitatively, these items might be categorized not by dollar amount but by a risk-ranking scale. According to ISACA, the scale shown in Table 4-3 is used to classify systems according to their importance to the organization.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>These extremely important functions cannot be performed with duplicate systems or processes. These functions are extremely intolerant to disruptions, and any disruption is very costly.</td>
</tr>
<tr>
<td>Vital</td>
<td>Although these functions are important, they can be performed by a backup manual process—but not for a long period of time. These systems can tolerate disruptions for typically five days or less.</td>
</tr>
<tr>
<td>Sensitive</td>
<td>Although these tasks are important, they can be performed manually at a reasonable cost. However, this is inconvenient and requires additional resources or staffing.</td>
</tr>
<tr>
<td>Noncritical</td>
<td>These services are not critical and can be interrupted. They can be restored later with little or no negative effects.</td>
</tr>
</tbody>
</table>

After addressing all these questions, the BCP team can start to develop recommendations and look at some potential recovery strategies. The BCP team should report these findings to senior management as a prioritized list of key business resources and the order in which restoration should be processed. The report should also offer potential recovery scenarios. Many times it will be the network operations center
(NOC) or help desk that first hears of a problem via end users. It’s important to have processes that tie these reports back to BCP teams so that potential problems can be addressed quickly.

Before presenting the report to senior management, however, the team should distribute it to the various department heads. These individuals were interviewed, and the plan affects them and their departments; therefore, they should be given the opportunity to review it and note any discrepancies. The BIA information must be correct and accurate because all future decisions will be based on those findings.

**NOTE**  Interdependencies can make criticality analysis very complex. For example, you might have two assets that on their own are noncritical but in certain contexts or situations become critical!

### Development and Recovery Strategy

At this point, the team has completed both the project initiation and BIA. Now it must determine the most cost-effective recovery mechanisms to be implemented based on the critical processes and threats determined during the BIA. An effective recovery strategy should apply preventive, detective, and corrective controls to meet the following objectives:

- Remove identified threats.
- Reduce the likelihood of identified risks.
- Reduce the impact of identified risks.

The recovery strategies should specify the best way to recover systems and processes in case of interruption. Operations can be interrupted in several different ways:

- **Data interruptions**: Caused by the loss of data. Solutions to data interruptions include backup, offsite storage, and remote journaling.

- **Operational interruptions**: Caused by the loss of equipment. Solutions to this type of interruption include hot sites, redundant equipment, and redundant array of independent disks (RAID).

- **Facility and supply interruptions**: Caused by interruptions due to fire, loss of inventory, transportation problems, HVAC problems, and telecommunications. Solutions to this type of interruption include redundant communication and transporting systems.
Business interruptions: Caused by interruptions due to loss of human resources, strikes, critical equipment, supplies, and office space. Solutions to this type of interruption include redundant sites, alternate locations, and temporary staff.

The selection of a recovery strategy is based on several factors, including cost, criticality of the systems or process, and the time required to recover. To determine the best recovery strategy, follow these steps:

1. Document all costs for each possible alternative.
2. Obtain cost estimates for any outside services that might be needed.
3. Develop written agreements with the chosen vendor for such services.
4. Evaluate what resumption strategies are possible if there is a complete loss of the facility.
5. Document your findings and report your chosen recovery strategies to management for feedback and approval.

Normally, any IT system that runs a mission-critical application needs a recovery strategy. There are many to choose from; the appropriate choice is based on the impact to the organization of the loss of the system or process. Recovery strategies include the following:

- Continuous processing
- Standby processing
- Standby database shadowing
- Remote data journaling
- Electronic vaulting
- Mobile site
- Hot site
- Warm site
- Cold site
- Reciprocal agreements

All of these options are discussed later in the chapter, in the section “Recovery Strategies.” To get a better idea of how each of these options compares to the cost of implementation, take a moment to review Figure 4-3. At this point, it is
important to realize that there must be a balance between the level of service needed and the recovery method.

![Diagram showing recovery options and costs](image)

**Figure 4-3** Recovery Options and Costs

**TIP** Exam candidates should understand that recovery strategies should be based on the disruptive cost versus the recovery costs. Finding a balance between the two enables recovery to occur at the minimized cost.

**Final Plan Design and Implementation**

In the final plan design and implementation phase, the team prepares and documents a detailed plan for recovering critical business systems. This plan should be based on information gathered during the project initiation, the BIA, and the recovery strategies phase. The plan should be a guide for implementation. The plan should address factors and variables such as these:

- Selecting critical functions and priorities for restoration
- Determining support systems that critical functions need
- Estimating potential disasters and calculating the minimum resources needed to recover from the catastrophe
- Determining the procedures for declaring a disaster and under what circumstances this will occur
- Identifying individuals responsible for each function in the plan
- Choosing recovery strategies and determining what systems and equipment will be needed to accomplish the recovery
- Determining who will manage the restoration and testing process
- Calculating what type of funding and fiscal management is needed to accomplish these goals

The plan should be written in easy-to-understand language that uses common terminology that everyone will understand. The plan should detail how the organization will interface with external groups such as customers, shareholders, the media, and community, region, and state emergency services groups during a disaster. Important teams should be formed so that training can be performed. The final step of the phase is to combine all this information into the business continuity plan and then interface it with the organization’s other emergency plans.

**NOTE**  Copies of the business continuity plan should be kept both onsite and offsite.

**Training and Awareness**

The goal of training and awareness is to make sure all employees know what to do in case of an emergency. Studies have shown that training improves response time and helps employees be better prepared. Employees need to know where to call or how to maintain contact with the organization if a disaster occurs. Therefore, the organization should design and develop training programs to make sure each employee knows what to do and how to do it. Training can include a range of specific programs, such as CPR, fire drills, crisis management, and emergency procedures. Employees assigned to specific tasks should be trained to carry out needed procedures. Cross-training of team members should occur, if possible, so that team members are familiar with a variety of recovery roles and responsibilities. Some people might not be able to lead under the pressure of crisis command; others might not be able to report to work. Table 4-4 describes some of the key groups involved in the BCP process and their responsibilities.
Table 4-4  BCP Process Responsibilities

<table>
<thead>
<tr>
<th>Person or Department</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior management</td>
<td>Project initiation, ultimate responsibility, overall approval and support</td>
</tr>
<tr>
<td>Middle management or business unit managers</td>
<td>Identification and prioritization of critical systems</td>
</tr>
<tr>
<td>BCP committee and team members</td>
<td>Planning, day-to-day management, implementation, and testing of the plan</td>
</tr>
<tr>
<td>Functional business units</td>
<td>Plan implementation, incorporation, and testing</td>
</tr>
<tr>
<td>IT audit</td>
<td>Business continuity plan review, test results evaluation, offsite storage facilities, alternate processing contracts, and insurance coverage</td>
</tr>
</tbody>
</table>

**TIP** For the CISA exam you should know that the number-one priority of any business continuity plan or disaster recovery plan is to protect the safety of employees.

**Implementation and Testing**

During the implementation and testing phase, the BCP team ensures that the previously agreed-upon steps are implemented. No demonstrated recovery exists until a plan has been tested. Before examining the ways in which the testing can occur, look at some of the teams that are involved in the process:

- **Incident response team**: Team developed as a central clearinghouse for all incidents.
- **Emergency response team**: The first responders for the organization. They are tasked with evacuating personnel and saving lives.
- **Emergency management team**: Executives and line managers who are financially and legally responsible. They must also handle the media and public relations.
- **Damage assessment team**: The estimators. They must determine the damage and estimate the recovery time.
- **Salvage team**: Those responsible for reconstructing damaged facilities. This includes cleaning up, recovering assets, creating documentation for insurance filings or legal actions, and restoring paper documents and electronic media.
- **Communications team**: Those responsible for installing communications (data, voice, phone, fax, radio) at the recovery site.

- **Security team**: Those who manage the security of the organization during a time of crisis. They must maintain order after a disaster.

- **Emergency operations team**: Individuals who reside at the alternative site and manage systems operations. They are primarily operators and supervisors who are familiar with system operations.

- **Transportation team**: Those responsible for notifying employees that a disaster has occurred. They are also in charge of providing transportation, scheduling, and lodging for those who will be needed at the alternative site.

- **Coordination team**: Those tasked with managing operations at different remote sites and coordinating the recovery efforts.

- **Finance team**: Individuals who provide budgetary control for recovery and accurate accounting of costs.

- **Administrative support team**: Individuals who provide administrative support and also handle payroll functions and accounting.

- **Supplies team**: Individuals who coordinate with key vendors to maintain needed supplies.

- **Relocation team**: Those in charge of managing the process of moving from the alternative site to the restored original location.

- **Recovery test team**: Individuals deployed to test the business continuity plan/disaster recovery plan and determine their effectiveness.

Did you notice that the last team listed is the recovery test team? This team consists of individuals who test the business continuity plan; this should be done at least once a year. Without testing, there is no guarantee that the plan will work. Testing helps bring theoretical plans into reality. To build confidence, the BCP team should start with easier parts of the plan and build to more complex items. The initial tests should focus on items that support core processing and should be scheduled during a time that causes minimal disruption to normal business operations. Tests should be observed by an auditor who can witness the process and record accurate test times. Having an auditor is not the only requirement: Key individuals who would be responsible in a real disaster must play a role in the testing process. Testing methods vary among organizations and range from simple to complex. Regardless of the method or types of testing performed, the idea is to learn from the practice and
improve the process each time a problem is discovered. As a CISA exam candidate, you should be aware of the three different types of BCP testing, as defined by the ISACA:

- Paper tests
- Preparedness tests
- Full operation tests

The following sections describe these basic testing methods.

**TIP** ISACA defines three types of BCP tests: paper tests, preparedness tests, and full operation tests.

**Paper Tests**

The most basic method of BCP testing is the *paper test*. Although it is not considered a replacement for a full interruption or parallel test, it is a good start. A paper test is an exercise that can be performed by sending copies of the plan to different department managers and business unit managers for review. Each of these individuals can review the plan to make sure nothing has been overlooked and that everything that is being asked of them is possible.

A paper test can also be performed by having the members of the team come together and discuss the business continuity plan. This is sometimes known as *walk-through testing*. The plans are laid out across the table so that attendees have a chance to see how an actual emergency would be handled. By reviewing the plan in this way, some errors or problems should become apparent. With either method—sending the plan around or meeting to review the plan—the next step is usually a preparedness test.

**Preparedness Tests**

A *preparedness test* is a simulation in which team members go through an exercise that reenacts an actual outage or disaster. This type of test is typically used to test a portion of the plan. The preparedness test consumes time and money because it is an actual test that measures the team’s response to situations that might someday occur. This type of testing provides a means of incrementally improving the plan.
TIP  During preparedness tests, team leaders might want to use the term exercise because the term test denotes passing or failing, which can add pressure on team members and can be detrimental to the goals of continual improvement. For example, during one disaster recovery test, the backup media was to be returned from the off-site location to the primary site. When the truck arrived with the media, it was discovered that the tapes had not been properly secured, and they were scattered around the bed of the truck. Even though the test could not continue, it was not a failure because it uncovered a weakness in the existing procedure.

Full Operation Tests

The full operation test is as close to an actual service disruption as you can get. The team should have performed paper tests and preparedness tests before attempting this level of interruption. This test is the most detailed, time-consuming, and thorough of all the tests discussed. A full interruption test mimics a real disaster, and all steps are performed to start up backup operations. It involves all the individuals who would be involved in a real emergency, including internal and external organizations. Goals of a full operation test include the following:

- Verifying the business continuity plan
- Evaluating the level of preparedness of the personnel involved
- Measuring the capability of the backup site to operate as planned
- Assessing the ability to retrieve vital records and information
- Evaluating the functionality of equipment
- Measuring overall preparedness for an actual disaster

TIP  The disaster recovery and continuity plan should be tested at least once yearly. Environments change; each time the plan is tested, more improvements might be uncovered.

Monitoring and Maintenance

When the testing process is complete, individuals tend to feel that their job is done. If someone is not made responsible for this process, the best plans in the world can start to become outdated in six months or less. Don’t be surprised to find out that
no one really wants to take on the task of documenting procedures and processes. The responsibility of performing periodic tests and maintaining the plan should be assigned to a specific person. While you might normally think of change-management practices being used to determine whether changes made to systems and applications are adequately controlled and documented, these same techniques should be used to address issues that might affect the business continuity plan.

A few additional items must be done to finish the business continuity plan. The primary remaining item is to put controls in place to maintain the current level of business continuity and disaster recovery. This is best accomplished by implementing change-management procedures. If changes to the approved plans are required, you will then have a documented structured way to accomplish this. A centralized command and control structure will ease this burden. Life is not static, and the organization’s business continuity plans shouldn’t be either.

### Understanding BCP Metrics

Reviewing the results of the information obtained is the next step of the BIA process. During this step, the BIA team should ask questions such as these:

- **Are the systems identified critical?** All departments like to think of themselves as critical, but that is usually not the case. Some departments can be offline longer than others.

- **What is the required recovery time for critical resources?** If the resource is critical, costs will mount the longer the resource is offline. Depending on the service and the time of interruption, these times will vary.

All this information might seem a little overwhelming; however, it is needed because at the core of the BIA are two critical items:

- **Recovery point objective (RPO):** The RPO defines how current the data must be or how much data an organization can afford to lose. The greater the RPO, the more tolerant the process is to interruption.

- **Recovery time objective (RTO):** The RTO specifies the maximum elapsed time to recover an application at an alternate site. The greater the RTO, the longer the process can take to be restored.

The lower the time requirements are, the higher the cost will be to reduce loss or restore the system as quickly as possible. For example, most banks have a very low RPO because they cannot afford to lose any processed information. Think of the recovery strategy calculations as being designed to meet the required recovery time frames: Maximum tolerable downtime (MTD) = RTO + Work recovery time
(WRT). (The WRT is the remainder of the MTD used to restore all business operations.) Figure 4-4 presents an overview of how RPO and RTO are related.

![Recovery Point Objective vs. Recovery Time Objective](image)

**Figure 4-4  RPO and RTO**

**NOTE** The RTO specifies the maximum elapsed time to recover an application at an alternate site. The greater the RTO, the longer the process can take to be restored.

These items must be considered in addition to RTO and RPO:

- **Maximum acceptable outage**: This value is the time that systems can be offline before causing damage. This value is required in creating RTOs and is also known as maximum tolerable downtime (MTD).
- **Work recovery time (WRT)**: The WRT is the time it takes to get critical business functions back up and running once the systems are restored.
- **Service delivery objective (SDO)**: This defines the level of service provided by alternate processes while primary processing is offline. This value should be determined by examining the minimum business need.
- **Maximum tolerable outages**: This is the maximum amount of time the organization can provide services at the alternate site. This value can be determined using contractual values.
- **Core processes**: These activities are specifically required for critical processes and produce revenue.
- **Supporting processes**: These activities are required to support the minimum services needed to generate revenue.
■ **Discretionary processes:** These include all other processes that are not part of the core or supporting processes and that are not required for any critical processes or functions.

### Recovery Strategies

Recovery alternatives are the choices an organization has for restoring critical systems and the data in those systems. Recovery strategies can include the following:

- Alternate processing sites
- Hardware recovery
- Software and data recovery
- Backup and restoration
- Telecommunications recovery

The goal is to create a recovery strategy that balances the cost of downtime, the criticality of the system, and the likelihood of occurrence. As an example, if you have an RTO of less than 12 hours and the resource you are trying to recover is a mainframe computer, a cold-site facility would never work—because you can’t buy a mainframe, install it, and get the cold site up and running in less than 12 hours. Therefore, although cost is important, so are criticality and the time to recover. The total outage time that the organization can endure is referred to as **maximum tolerable downtime** (MTD). Table 4-5 shows some MTDs used by many organizations.

#### Table 4-5  Required Recovery Times

<table>
<thead>
<tr>
<th>Item</th>
<th>Required Recovery Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Minutes to hours</td>
</tr>
<tr>
<td>Urgent</td>
<td>24 hours</td>
</tr>
<tr>
<td>Important</td>
<td>72 hours</td>
</tr>
<tr>
<td>Normal</td>
<td>7 days</td>
</tr>
<tr>
<td>Nonessential</td>
<td>30 days</td>
</tr>
</tbody>
</table>

### Alternate Processing Sites

For disasters that have the potential to affect the primary facility, plans must be made for a backup process or an alternate site. Some organizations might opt for a
redundant processing site. Redundant sites are equipped and configured just like the primary site. They are owned by the organization, and their cost is high. After all, the company must spend a large amount of funds to build and equip a complete, duplicate site. Although the cost might seem high, it must be noted that organizations that choose this option have done so because they have a very short (if any) RPO. A loss of services for even a very short period of time would cost the organization millions. The organization also might be subjected to regulations that require it to maintain redundant processing. Before choosing a location for a redundant site, it must be verified that the site is not subject to the same types of disasters as the primary site. Regular testing is also important to verify that the redundant site still meets the organization’s needs and that it can handle the workload to meet minimum processing requirements.

Alternate Processing Options

Mobile sites are another alternate processing alternative. Mobile sites are usually tractor-trailer rigs that have been converted into data-processing centers. They contain all the necessary equipment and can be transported to a business location quickly. They can be chained together to provide space for data processing and can provide communication capabilities. Used by the military and large insurance agencies, mobile sites are a good choice in areas where no recovery facilities exist.

Another type of recovery alternative is subscription services, such as hot sites, warm sites, and cold sites.

A hot site facility is ready to go. It is fully configured and equipped with the same system as the production network. It can be made operational within just a few hours. A hot site merely needs staff, data files, and procedural documentation. Hot sites are a high-cost recovery option, but they can be justified when a short recovery time is required. Because a hot site is typically a subscription-based service, a range of fees is associated with it, including a monthly cost, subscription fees, testing costs, and usage or activation fees. Contracts for hot sites need to be closely examined; some might charge extremely high activation fees to prevent users from utilizing the facility for anything less than a true disaster.

Regardless of what fees are involved, the hot site needs to be periodically tested. Tests should evaluate processing abilities as well as security. The physical security of a hot site should be at the same level or greater than the physical security at the primary site. Finally, it is important to remember that the hot site is intended for short-term use only. With a subscriber service, other companies might be competing for the same resource. The organization should have a plan to recover primary services quickly or move to a secondary location.
Hot sites should not be externally identifiable to decrease the risk of sabotage and other potential disruptions.

For a slightly less expensive alternative, an organization can choose a warm site. A warm site has data equipment and cables and is partially configured. It could be made operational in anywhere from a few hours to a few days. The assumption with a warm site is that computer equipment and software can be procured in case of a disaster. Although the warm site might have some computer equipment installed, it typically has lower processing power than the equipment at the primary site. The costs associated with a warm site are slightly lower than those of a hot site. The warm site is the most popular subscription alternative.

For organizations that are looking for a cheaper alternative and that have determined that they can tolerate a longer outage, a cold site might be the right choice. A cold site is basically an empty room with only rudimentary electrical, power, and computing capability. It might have a raised floor and some racks, but it is nowhere near ready for use. It might take several weeks to a month to get the site operational. A common misconception with cold sites is that the organization will be able to get the required equipment after a disaster. This might not be true with large disasters. For example, with Hurricanes Katrina, Sandy, and Irma, vendors sold out of equipment and could not meet demand. It is possible that backorders could push out the operation dates of a cold site to much longer than planned. Cold sites offer the least of the three subscription services discussed. Table 4-6 shows some examples of functions and their recovery times.

**TIP** For the exam, you should understand that cold sites are a good choice for the recovery of noncritical services.

<table>
<thead>
<tr>
<th>Process</th>
<th>Recovery Time</th>
<th>Recovery Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>15 minutes to 1 hour</td>
<td>Database shadowing at a redundant site</td>
</tr>
<tr>
<td>Applications</td>
<td>12–24 hours</td>
<td>Hot site</td>
</tr>
<tr>
<td>Help desk</td>
<td>24–48 hours</td>
<td>Hot site</td>
</tr>
<tr>
<td>Purchasing</td>
<td>24–48 hours</td>
<td>Hot site</td>
</tr>
<tr>
<td>Payroll</td>
<td>1–3 days</td>
<td>Redundant site</td>
</tr>
<tr>
<td>Process</td>
<td>Recovery Time</td>
<td>Recovery Strategy</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Asset inventory</td>
<td>5–7 days</td>
<td>Warm site</td>
</tr>
<tr>
<td>Nonessential services</td>
<td>30 days</td>
<td>Cold site</td>
</tr>
<tr>
<td>Emergency services (for example, for companies that need to set up operations quickly in areas that have been hit by disasters, such as insurance companies, governmental agencies, military, and so on)</td>
<td>Hours to a few days</td>
<td>Mobile site</td>
</tr>
</tbody>
</table>

*With reciprocal agreements*, two organizations pledge assistance to one another in the event of a disaster. These agreements are carried out by sharing space, computer facilities, and technology resources. On paper, this appears to be a cost-effective solution because the primary advantage is its low cost. However, reciprocal agreements have drawbacks and are infrequently used. The parties to such an agreement must trust each other to aid in the event of a disaster. However, the nonvictim might be hesitant to follow through if such a disaster occurs, based on concerns such as the realization that the damaged party might want to remain on location for a long period of time or that the victim company’s presence will degrade the helping company’s network services. Even concerns about the loss of competitive advantage can drive this hesitation. The issue of confidentiality also arises: The damaged organization is placed in a vulnerable position and must entrust the other party with confidential information. Finally, if the parties to the agreement are near each other, there is always the danger that disaster could strike both parties and thereby render the agreement useless. The legal departments of both firms need to look closely at such an agreement. ISACA recommends that organizations considering reciprocal agreements address the following concerns before entering into them:

- What amount of time will be available at the host computer site?
- Will the host site’s employees be available for help?
- What specific facilities and equipment will be available?
- How long can emergency operations continue at the host site?
- How frequently can tests be scheduled at the host site?
- What type of physical security is available at the host site?
- What type of logical security is available at the host site?
- Is advance notice required for using the site? If so, how much?
- Are there any blocks of time or dates when the facility is not available?
NOTE Although reciprocal agreements are not usually appropriate for organizations with large databases, some organizations, such as small banks, have been known to sign reciprocal agreements for the use of a shared hot site.

When reviewing alternative processing options, subscribers should look closely at any agreements and at the actual facility to make sure it meets the needs of the organization. One common problem is oversubscription. If situations such as Hurricane Harvey occur, there could be more organizations demanding a subscription service than the vendor can supply. The subscription agreement might also dictate when the organization may inhabit the facility. Thus, even though an organization might be in the path of a deadly storm, it might not be able to move into the facility yet because the area has not been declared a disaster area. Procedures and documentation should also be kept at the offsite location, and backups must be available. It’s important to note that backup media should be kept in an area that is not subject to the same type of natural disaster as the primary site. For example, if the primary site is in a hurricane zone, the backup needs to be somewhere less prone to those conditions. If backup media is at another location, agreements should be in place to ensure that the media will be moved to the alternate site so it is available for the recovery process. A final item is that organizations must also have prior financial arrangements to procure needed equipment, software, and supplies during a disaster. This might include emergency credit lines, credit cards, or agreements with hardware and software vendors.

Hardware Recovery

Recovery alternatives are just one of the items that must be considered to cope with a disaster. Hardware recovery is another. Remember that an effective recovery strategy involves more than just corrective measures; it is also about prevention. Hardware failures are some of the most common disruptions that can occur. It is therefore important to examine ways to minimize the likelihood of occurrence and to reduce the effect if it does occur. This process can be enhanced by making well-informed decisions when buying equipment. At purchase time, you should know three important items associated with the reliability:

- **Mean time between failures (MTBF):** The MTBF calculates the expected lifetime of a device that can be repaired. A higher MTBF means the equipment should last longer.

- **Mean time to failure (MTTF):** The MTTF calculates the expected lifetime of a one-time-use item that is typically not repaired.
Mean time to repair (MTTR): The MTTR estimates how long it would take to repair the equipment and get it back into use. For MTTR, lower numbers mean the equipment takes less time to repair and can be returned to service sooner.

For critical equipment, an organization might consider some form of service level management. This is simply an agreement between an IT service provider and a customer. The most common example is a service level agreement (SLA), which is a contract with a hardware vendor that provides a certain level of protection. For a fee, the vendor agrees to repair or replace the equipment within the contracted time.

Fault tolerance can be used at the server level or the drive level. At the server level is clustering, technology that groups several servers together yet allows them to be viewed logically as a single server. Users see the cluster as one unit, although it is actually many. The advantage is that if one server in the cluster fails, the remaining active servers will pick up the load and continue operation.

Redundant Array of Independent Disks

Fault tolerance on the drive level is achieved primarily with redundant array of independent disks (RAID), which is used for hardware fault tolerance and/or performance improvements and is achieved by breaking up the data and writing it to multiple disks. RAID has humble beginnings that date back to the 1980s at the University of California. To applications and other devices, RAID appears as a single drive. Most RAID systems have hot-swappable disks, which means the drives can be removed or added while the computer systems are running. If a RAID system uses parity and is fault tolerant, the parity date is used to rebuild the newly replaced drive. Another RAID technique is striping, which means the data is divided and written over several drives. Although write performance remains almost constant, read performance drastically increases. According to ISACA, these are the most common levels of RAID used today:

- RAID 0
- RAID 3
- RAID 5

RAID level descriptions are as follows:

- **RAID 0: Striped disk array without fault tolerance:** Provides data striping and improves performance but provides no redundancy.

- **RAID 1: Mirroring and duplexing:** Duplicates the information on one disk to another. It provides twice the read transaction rate of single disks and the same write transaction rate as single disks yet effectively cuts disk space in half.
Chapter 4: Maintaining Critical Services

- **RAID 2: Error-correcting coding**: Rarely used because of the extensive computing resources needed. It stripes data at the bit level instead of the block level.

- **RAID 3: Parallel transfer with parity**: Uses byte-level striping with a dedicated disk. Although it provides fault tolerance, it is rarely used.

- **RAID 4: Shared parity drive**: Similar to RAID 3 but provides block-level striping with a parity disk. If a data disk fails, the parity data is used to create a replacement disk. Its primary disadvantage is that the parity disk can create write bottlenecks.

- **RAID 5: Block interleaved distributed parity**: Provides data striping of both data and parity. Level 5 has good performance and fault tolerance. It is a popular implementation of RAID. It requires at least three drives.

- **RAID 6: Independent data disks with double parity**: Provides high fault tolerance with block-level striping and parity data distributed across all disks.

- **RAID 10: A stripe of mirrors**: Known to have very high reliability. It requires a minimum of four drives.

- **RAID 0+1: A mirror of stripes**: Not one of the original RAID levels. RAID 0+1 uses RAID 0 to stripe data and creates a RAID 1 mirror. It provides high data rates.

- **RAID 15**: Creates mirrors (RAID 1) and distributed parity (RAID 5). This is not one of the original RAID levels.

One final drive-level solution worth mentioning is just a bunch of disks (JBOD). JBOD is similar to RAID 0 but offers few of the advantages. What it does offer is the capability to combine two or more disks of various sizes into one large partition. It also has an advantage over RAID 0: In case of drive failure, only the data on the affected drive is lost; the data on surviving drives remains readable. This means that JBOD has no fault tolerance. JBOD does not provide the performance benefits associated with RAID 0.

**Software and Data Recovery**

Because data processing is essential to most organizations, having the software and data needed to continue this operation is critical to the recovery process. The objectives are to back up critical software and data and be able to restore them quickly. Policy should dictate when backups are performed, where the media is stored, who has access to the media, and what its reuse or rotation policy is. Backup media can include tape reels, tape cartridges, removable hard drives, disks, and cassettes. The organization must determine how often backups should be performed and what type of backup should be performed. These operations will vary depending on the cost of
the media, the speed of the restoration needed, and the time allocated for backups. Typically, the following four backup methods are used:

- **Full backup:** All data is backed up. No data files are skipped or bypassed. All items are copied to one tape, set of tapes, or backup medium. If restoration is needed, only one tape or set of tapes is needed. A full backup requires the most time and space on the storage medium but takes the least time to restore.

- **Differential backup:** A full backup is done typically once a week, and a daily differential backup is done only to those files that have changed since the last full backup. If you need to restore, you need the last full backup and the most recent differential backup. This method takes less time per backup but takes longer to restore because both the full and differential backups are needed.

- **Incremental backup:** This method backs up only those files that have been modified since the previous incremental backup. An incremental backup requires additional backup media because the last full backup, the last incremental backup, and any additional incremental backups are required to restore the media.

- **Continuous backup:** Some backup applications perform a continuous backup that keeps a database of backup information. These systems are useful because if a restoration is needed, the application can provide a full restore, a point-in-time restore, or a restore based on a selected list of files.

**NOTE**  
Tape continues to be a viable option for backup. One current backup format is linear tape-open (LTO). LTO provides high-capacity storage, and in its latest iteration, LTO-6, it offers 2.5TB of storage per tape cartridge. If compression is used an enterprise can store up to 6.25TB of data on a single tape.

Although tape and optical systems still have significant market share for backup systems, hardware alternatives and cloud based options are making inroads. One of these technologies is massive array of inactive disks (MAID). MAID offers a hardware storage option for the storage of data and applications. It was designed to reduce the operational costs and improve long-term reliability of disk-based archives and backups. MAID is similar to RAID, except that it provides power management and advanced disk monitoring. The MAID system powers down inactive drives, reduces heat output, reduces electrical consumption, and increases the drive's life expectancy. This represents real progress over using hard disks to back up data. Storage area networks (SANs) are another alternative. SANs are designed as a subnetwork of high-speed, shared storage devices. Cloud backup is gaining in
popularity as it offers several benefits. These value-added functions include geographical redundancy, advanced search, content management and automatic offsite storage.

**Backup and Restoration**

Where backup media are stored can have a big impact on how quickly data can be restored and brought back online. The media should be stored in more than one physical location to reduce the possibility of loss. A tape librarian should manage these remote sites by maintaining the site, controlling access, rotating media, and protecting this valuable asset. Unauthorized access to the media is a huge risk because it could impact the organization’s ability to provide uninterrupted service. Encryption can help mitigate this risk. Transportation to and from the remote site is also an important concern. Consider the following important items:

- Secure transportation to and from the site must be maintained.
- Delivery vehicles must be bonded.
- Backup media must be handled, loaded, and unloaded in an appropriate way.
- Drivers must be trained on the proper procedures to pick up, handle, and deliver backup media.
- Access to the backup facility should be 24×7 in case of emergency.

*Offsite storage* should be contracted with a known firm that has control of the facility and is responsible for its maintenance. Physical and environmental controls should be equal to or better than those of the organization’s facility. A letter of agreement should specify who has access to the media and who is authorized to drop off or pick up media. There should also be an agreement on response time that is to be met in times of disaster. *Onsite storage* should be maintained to ensure the capability to recover critical files quickly. Backup media should be secured and kept in an environmentally controlled facility that has physical control sufficient to protect such a critical asset. This area should be fireproof, with controlled access so that anyone depositing or removing media is logged. Although most backup media is rather robust, it will not last forever and will fail over time. This means that tape rotation is another important part of backup and restoration.

Backup media must be periodically tested. Backups will be of little use if they malfunction during a disaster. Common media-rotation strategies include the following:

- **Simple**: A simple backup rotation scheme is to use one tape for every day of the week and then repeat the next week. One tape can be for Mondays, one for Tuesdays, and so on. You would add a set of new tapes each month and then
archive the monthly sets. After a predetermined number of months, you would put the oldest tapes back into use.

- **Grandfather-father-son**: This rotation method includes four tapes for weekly backups, one tape for monthly backups, and four tapes for daily backups. It is called *grandfather-father-son* because the scheme establishes a kind of hierarchy. Grandfathers are the one monthly backup, fathers are the four weekly backups, and sons are the four daily backups.

- **Tower of Hanoi**: This tape-rotation scheme is named after a mathematical puzzle. It involves using five sets of tapes, each set labeled A through E. Set A is used every other day; set B is used on the first non-A backup day and is used every fourth day; set C is used on the first non-A or non-B backup day and is used every eighth day; set D is used on the first non-A, non-B, or non-C day and is used every 16th day; and set E alternates with set D.

**NOTE** An organization’s backups are a complete mirror of the organization’s data. Although most backups are password protected, this really offers only limited protection. If attackers have possession of the backup media, they are not under any time constraints and have ample time to crack passwords and access the data. Encryption can offer an additional layer of protection and help protect the confidentiality of the data.

SANs are an alternative to traditional backup. SANs support disk mirroring, backup and restore, archival and retrieval of archived data, and data migration from one storage device to another. SANs can be implemented locally or can use storage at a redundant facility. Another option is a virtual SAN (VSAN), a SAN that offers isolation among devices that are physically connected to the same SAN fabric. A VSAN is sometimes called *fabric virtualization*.

Traditionally, SANs used Small Computer System Interface (SCSI) for connectivity, but there are more current options in use today. One is iSCSI, which is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. Fiber Channel over Ethernet (FCoE) is another SAN interface standard. FCoE is similar to iSCSI; it can operate at speeds of 10Gbps and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is nonroutable.

One important issue with SAN and backups is location redundancy. This is the concept that content should be accessible from more than one location. An extra measure of redundancy can be provided by means of a replication service so that data is available even if the main storage backup system fails.
Another important item is security of the backups. This is where secure storage management and replication are important. The idea is that systems must be designed to allow a company to manage and handle all corporate data in a secure manner, with a focus on the confidentiality, integrity, and availability of the information. The replication service allows for the data to be duplicated in real time so that additional fault tolerance is achieved.

When you need to make point-in-time backups, you can use SAN snapshots. SAN snapshot software is typically sold with a SAN solution and offers a way to bypass typical backup operations. The snapshot software has the ability to temporarily stop writing to physical disk and make a point-in-time backup copy.

If budget is an issue, an organization can opt for electronic vaulting, which involves transferring data by electronic means to a backup site, as opposed to physical shipment. With electronic vaulting, an organization contracts with a vaulting provider. The organization typically loads a software agent onto systems to be backed up, and the vaulting service accesses these systems and copies the selected files. Moving large amounts of data can slow WAN service.

Another backup alternative is standby database shadowing. A standby database is an exact duplicate of a database maintained on a remote server. In case of disaster, it is ready to go. Changes are applied from the primary database to the standby database to keep records synchronized.

As an alternative to traditional backup techniques, using cloud services for backup may offer a cost-saving alternative. These services should be carefully evaluated, as there are many concerns when using them. Cloud backups can be deployed in a variety of configurations—for example, as an on-premises private cloud or as an offsite public or private cloud.

**Telecommunications Recovery**

Telecommunications recovery should play a key role in recovery. After all, the telecommunications network is a critical asset and should be given a high priority for recovery. Although these communications networks can be susceptible to the same threats as data centers, they also face some unique threats. Protection methods include redundant WAN links and bandwidth on demand. Whatever the choice, the organization should verify capacity requirements and acceptable outage times. The following are the primary methods for telecommunications network protection:

- **Redundancy**: This involves exceeding what is required or needed. Redundancy can be added by providing extra capacity, providing multiple routes, using dynamic routing protocols, and using failover devices to allow for continued operations.
- **Diverse routing**: This is the practice of routing traffic through different cable facilities. Organizations can obtain both diverse routing and alternate routing, but the cost is not low. Most of these systems use facilities that are buried, and they usually emerge through the basement and can sometimes share space with other mechanical equipment. This adds risk. Many cities have aging infrastructures, which is another potential point of failure.

- **Alternate routing**: This is the ability to use another transmission line if the regular line is busy or unavailable. This can include using a dial-up connection in place of a dedicated connection, a cell phone instead of a land line, or microwave communication in place of a fiber connection.

- **Long-haul diversity**: This is the practice of having different long-distance communication carriers. This recovery facility option helps ensure that service is maintained; auditors should verify that it is present.

- **Last-mile protection**: This is a good choice for recovery facilities in that it provides a second local loop connection and can add to security even more if an alternate carrier is used.

- **Voice communication recovery**: Many organizations are highly dependent on voice communications. Some of these organizations have started making the switch to VoIP because of the cost savings. Some land lines should be maintained to provide recovery capability.

**NOTE** Recovery strategies have historically focused on computing resources and data. Networks are susceptible to many of the same problems, but often they are not properly backed up. This can be a real problem because there is a heavy reliance on networks to deliver data when needed.

**Verification of Disaster Recovery and Business Continuity Process Tasks**

As an auditor, you will be tasked with understanding and evaluating business continuity/disaster recovery strategy. An auditor should review a plan and make sure it is current and up-to-date. The auditor should also examine last year’s test to verify the results and look for any problem areas. The business continuity coordinator is responsible for maintaining previous tests. Upon examination, an auditor should confirm that a test met targeted goals or minimum standards. The auditor should also inspect the offsite storage facility and review its security, policies, and configuration. This should include a detailed inventory that includes checking data files, applications, system software, system documentation, operational documents, consumables, supplies, and a copy of the business continuity plan.
Contracts and alternative processing agreements should also be reviewed. Any off-site processing facilities should be audited, and the owners should have a reference check. All agreements should be made in writing. The offsite facility should meet the same security standards as the primary facility and should have environmental controls such as raised floors, HVAC controls, fire prevention and detection, filtered power, and uninterruptible power supplies (UPSs). A UPS allows a computer to keep running for at least a short time when the primary power source is lost.

If the location is a shared site, the rules that determine who has access and when they have access should be examined. Another area of concern is the business continuity plan itself. An auditor must make sure the plan is written in easy-to-understand language and that users have been trained. This can be confirmed by interviewing employees.

Finally, insurance should be reviewed. An auditor should examine the level and types of insurance the organization has purchased. Insurance can be obtained for each of the following items:

- IS equipment
- Data centers
- Software recovery
- Business interruption
- Documents, records, and important papers
- Errors and omissions
- Media transportation

Insurance is not without drawbacks, which include high premiums, delayed claim payouts, denied claims, and problems proving financial loss. Finally, most policies pay for only a percentage of actual loss and do not pay for lost income, increased operating expenses, or consequential loss.

The purpose of disaster recovery is to get a damaged organization restarted so that critical business functions can resume. When a disaster occurs, the process of progressing from the disaster back to normal operations includes the following:

- Crisis management
- Recovery
- Reconstitution
- Resumption
An auditor should be concerned with all laws, mandates, and policies that govern the organization in a disaster situation. As an example, federal and state government entities typically use a Continuity of Operations (COOP) site, which is designed to take on operational capabilities when the primary site is not functioning. The length of time the COOP site is active and the criteria used to determine when the COOP site is enabled depend on the business continuity and disaster recovery plans. An example of the Disaster Lifecycle is shown in Figure 4-5.

![Figure 4-5: The Disaster Life Cycle](image)

The Disaster Life Cycle

Both governmental and nongovernmental entities typically use a checklist to manage continuity of operations. Table 4-7 shows a sample disaster recovery checklist.
### Table 4-7 Disaster Recovery Checklist

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>When disaster occurs</td>
<td>Notify disaster recovery manager and recovery coordinator</td>
</tr>
<tr>
<td>Under 2 hours</td>
<td>Assess damage, notify senior management, and determine immediate course of action</td>
</tr>
<tr>
<td>Under 4 hours</td>
<td>Contact offsite facility, recover backups, and replace equipment as needed</td>
</tr>
<tr>
<td>Under 8 hours</td>
<td>Provide management with updated assessment and begin recovery at updated site</td>
</tr>
<tr>
<td>Under 36 hours</td>
<td>Reestablish full processing at alternative site and determine a timeline for return to the primary facility</td>
</tr>
</tbody>
</table>

**NOTE** An auditor should verify that the disaster recovery manager directs short-term recovery actions immediately following a disaster and has the approval and resources to do so.

Protection of life is a priority while working to mitigate damage. The areas impacted the most need attention first. Recovery from a disaster entails sending personnel to the recovery site. Individuals responsible for emergency management need to assess damage and perform triage. When employees and materials are at the recovery site, interim functions can resume operations. This might require installing software and hardware. Backup data or copies of configurations might need to be loaded, and systems might require setup.

When operations are moved from the alternative operations site back to the restored site, the efficiency of the new site must be tested. In other words, processes should be sequentially returned from least critical to most critical. In the event that a few glitches need to be worked out in the new facility, you can be confident that your most critical processes are still in full operation at the alternative site. When those processes are complete, normal operations can resume.

**TIP** When migrating from the backup site to the primary site, always move from least critical to most critical.
Chapter Summary

This chapter discusses the process of business continuity planning—preparing for the worst possible events that could happen to an organization. Many organizations give BCP a low priority for a host of reasons, including cost, inability to quantify some potential threats, and the belief that the organization can somehow escape these events.

The first step, initiation, requires that senior management establish business continuity as a priority. Developing and carrying out a successful business continuity plan takes much work and effort and should be done in a modular format. The business impact analysis is the next step. Although auditors are unlikely to be directly involved in this process, they can be of help here in providing data on the impact to the business if specific systems are unavailable. The goal of business impact analysis is to determine which processes need to happen first, second, third, and so on. Each step of the business continuity process builds on the last; the BCP team members must know the business and need to work with other departments and management to determine critical processes.

Recovery strategies must also be determined. For example, in case of loss of power, will a generator be used, or might the process continue at another location that has power? With these decisions made, a written plan must be developed that locks into policy whatever choices have been made. When the plan is implemented, the process is still not complete; the team must test the plan. During the test, an IS auditor should be present to observe the results. No demonstrated recovery exists until the plan has been tested. Common test methods include paper tests, preparedness tests, and full operation tests. To make sure these plans and procedures do not grow old or become obsolete, disaster recovery should become part of the decision-making process so that when changes are made, issues that may affect the policies can be updated. Business continuity and disaster recovery plans can also be added to job responsibilities and to yearly performance reviews.

Exam Preparation Tasks

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple choices for exam preparation: the exercises here; Chapter 10, “Final Preparation;” and the exam simulation questions on the book’s companion web page (www.informit.com/title/9780789758446).
Review All the Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 4-8 lists these key topics and the page number on which each is found.

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 4-1</td>
<td>Sources of security threats</td>
<td>140</td>
</tr>
<tr>
<td>Table 4-4</td>
<td>BCP process responsibilities</td>
<td>153</td>
</tr>
<tr>
<td>Figure 4-4</td>
<td>RPO and RTO</td>
<td>158</td>
</tr>
<tr>
<td>Section</td>
<td>Hardware recovery</td>
<td>163</td>
</tr>
<tr>
<td>List</td>
<td>The primary methods for network protection</td>
<td>169</td>
</tr>
</tbody>
</table>

Define Key Terms

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

- business impact analysis
- cold site
- hot site
- JBOD
- massive array of inactive disks (MAID)
- paper test
- protocol
- recovery point objective (RPO)
- recovery testing
- recovery time objective (RTO)
- redundant array of inexpensive disks (RAID)
- resilience
- software
- storage area network (SAN)
- telecommunications
- transaction
- uninterruptible power supply (UPS)

Exercises

4.1 Business Impact and Risk

Estimated time: 10 minutes

For this exercise, you need to walk through the profile and then answer the following questions.

**Kerney, Cleveland, and Glass Law Firm**

**Driving concern:** This law firm, located in the Washington, D.C., area has serviced a who’s who of individuals inside and outside the Beltway. The firm recently suffered a major network outage after a key server failed, and it was determined that the backup media was corrupt. Management has existing business continuity plans
but could not contact the person in charge of cloud backups during this late-night problem. They are now worried that the plans are not adequate.

**Overview:** The firm has two offices: one in the D.C. area and the other on the West Coast. The firm handles many confidential documents, often of high monetary value. The firm is always looking for ways to free up the partners from administrative tasks so that they can have more billable hours. Partners access their data from wireless LANs and remotely through a corporate VPN.

The two offices are connected by a T1 leased line. Each office has a connection to the Internet. The West Coast office connects to the Internet through the D.C. office. The wireless network supports Windows servers in the D.C. office. Partners also carry laptop computers that contain many confidential documents needed at client sites. The law firm has a bring-your-own-device (BYOD) policy and allows users to connect almost any device to the network. No encryption is used, and there is no insurance to protect against downtime or disruptions.

1. Which of the following items would you consider a priority if you were asked to audit the law firm’s business continuity plan?
   - Verify that the business continuity plan provides for the recovery of all systems? Yes/No
   - Require that you or another auditor is present during a test of the business continuity plan? Yes/No
   - Verify that the notification directory is being maintained and is current? Yes/No
   - Verify that the IS department is responsible for declaring a disaster if such a situation occurred? Yes/No
   - Suggest that the law firm increase its recovery time objective? Yes/No
   - Determine the most critical finding?

2. Examine the list from Question 1 and compare your answers with the following:
   - Verify that the business continuity plan provides for the recovery of all systems? Yes/No (Typically, only 50% of information is critical.)
   - Require that you or another auditor is present during a test of the business continuity plan? Yes/No (The auditor should be present to make sure the test meets required targets.)
   - Verify that the notification directory is being maintained and is current? Yes/No (Without a notification system, there is no easy way to contact employees or for them to check in case of disaster.)
Verify that the IS department is responsible for declaring a disaster if such a situation occurred? Yes/No (Senior management should designate someone for that task.)

Suggest that the law firm increase its recovery time objective? Yes/No (This would increase recovery time, not decrease it.)

Determine the most critical finding? Lack of insurance/Loss of data (The most vital asset for an organization is its data.)

Review Questions

1. Which of the following should be the primary objective when using tape backup as a recovery strategy?
   a. That the RPO is high
   b. That the RPO is low
   c. That the RTO is low
   d. That fault tolerance is low

2. When performing an audit, which of the following is the best reason to use a hot site?
   a. It can be used for long-term processing.
   b. It is not a subscription service.
   c. There is no additional cost for using it or periodic testing.
   d. It is ready for service.

3. Which of the following is the greatest advantage of JBOD?
   a. In case of drive failure, only the data on the affected drive is lost.
   b. It is superior to disk mirroring.
   c. It offers greater performance gains than RAID.
   d. It offers greater fault tolerance than RAID.

4. Which of the following processes is most critical in terms of revenue generation?
   a. Discretionary
   b. Supporting
   c. Core
   d. Critical
5. As an auditor, how often would you say that a business continuity plan should be updated?
   a. Every five years
   b. Every year or as required
   c. Every six months
   d. Upon any change or modification

6. During an audit, you have been asked to review the disaster recovery and backup processes. When maintaining data backups at offsite locations, which of the following is the best way to control concern?
   a. The storage site should be as secure as the primary site.
   b. A suitable tape-rotation plan should be in use.
   c. That backup media should be tested regularly.
   d. That copies of current critical information should be kept offsite.

7. Which of the following is the most important purpose of BIA?
   a. Identifying countermeasures
   b. Prioritizing critical systems
   c. Developing recovery strategies
   d. Determining potential test strategies

8. Which of the following is not a valid BCP test type?
   a. Paper test
   b. Structured walk-through
   c. Full operation test
   d. Preparedness test

9. Which of the following is the practice of routing traffic through different cable facilities?
   a. Alternate routing
   b. Long-haul diversity
   c. Diverse routing
   d. Last-mile protection
10. When classifying critical systems, which category matches the following description: “These functions are important and can be performed by a backup manual process but not for a long period of time?”
   a. Vital
   b. Sensitive
   c. Critical
   d. Demand driven

Suggested Readings and Resources

- **Cloud backup and storage**: [www.informationweek.com/consumer/online-backup-vs-cloud-storage/d/d-id/1107440](http://www.informationweek.com/consumer/online-backup-vs-cloud-storage/d/d-id/1107440)
Index

Numbers
3DES (Triple Data Encryption Standard), 359
4GL programming languages, 258
5GL programming languages, 258
802.11 wireless connections, security, 406
802.11 wireless standard, 299-301

A
accepting risk (risk management), 45
access control
application controls, 244
authentication
biometric systems, 338-339
by characteristic, 338-340
by knowledge, 336-337
by ownership, 338
centralized authentication, 345-346
Federation, 343-345
geofencing, 337
multi-platform authentication, 343-345
passwords, 336-337
somewhere you are systems, 340
SSO, 340-342
tokens, 338
two-factor authentication, 338 cloud computing, 218
exterior security control
bollards, 350
CCTV systems, 352, 355-356
dogs, 351
entry points, 351
fences, 349-350
gates, 350
guards, 352
HVAC, 356
lighting, 351, 354
locks, 353-354
Federation, 343-345
identification, 336
information asset protection, 370
NAC, 415
perimeter security control
bollards, 350
CCTV systems, 352, 355-356
dogs, 351
entry points, 351
fences, 349-350
gates, 350
guards, 352
HVAC, 356
lighting, 351, 354
locks, 353-354
turnstiles, 352
physical/environmental access control
bollards, 350
CCTV systems, 352, 355-356
dogs, 351
dogs, 351
entry points, 351
fences, 349-350
gates, 350
guards, 352
HVAC, 356
lighting, 351, 354
locks, 353-354
turnstiles, 352
remote access
Diameter, 346
encryption, 347
RADIUS, 345-346
risks of, 347
TACACS, 346
VPN, 347-348
security labels, bypassing, 414
SSH, 347
SSO, 340
advantages of, 341
Kerberos, 341-342
Telnet, 347
accountability
IT governance, 77
organizations, 95
vendors, quality of, 95
accounting ethics
Arthur Andersen, 30
SOX, 35, 119
accreditation, 208
ACID tests, 245, 282
active discovery stage (penetration testing), 417
acts. See laws/regulatory standards
Adleman, Len, 363
administration, 104
administrative controls (security controls)
blogs, 397
IM, 396-397
message boards, 397
social media, 397-398
websites, 397
administrative support teams (BCP), 154
adverse opinions (audit reports), 58
advisory policies, 91
AES (Advanced Encryption Standard), 362
aggregation (databases), 278
agile software development, 213
AI (Artificial Intelligence)/expert systems, BI, 258
al-Kindi and cryptanalysis, Abu, 358
ALE (Annual Loss Expectancy)
BIA criticality analysis, 148
quantitative risk analysis, 85
algorithms (encryption), 358
alpha testing, 207
alternate processing sites
cold sites, 161
hot sites, 160
mobile sites, 160
oversubscription, 163
reciprocal agreements, 162-163
subscription services, 160, 163
warm sites, 161
alternate routing, telecommunications recovery, 170
alternative processing agreements, disaster recovery, 171
alternative system development
CBD, 220
cloud computing
  access control, 218
  cloud providers, 218-219
  encryption, 219
  models of, 216
  security, 219
  services, 216
  threats to, 218-219
  training, 218
DOOS, 219
n-tier, 220-221
OOSD, 220
outsourcing, 214-215
virtualization, 221-222
WBAD, 220
analyzing risk, 44
anomaly detection IDS, 312
antivirus software, virtualization, 395
anycast addresses, 294
AP (Access Points)
  trap doors, 411
  WAP, 299, 305, 406-407
application controls
  automated application controls, 236-237
  continuous online auditing, 247-249
  data integrity controls, 245, 249
  manual application controls, 236-237
  observation, 244, 248
  separating duties, 244
  testing, 244, 248
  testing applications, 246-249
  understanding applications, 248
    documentation, 243
    flowcharts, 243-244
application layer
  OSI reference model, 287
  TCP/IP reference model, 296-297
application proxies, 307
application switches, 304
application system (EDI), 254
applications
  business application systems
    BI, 256-260
    e-commerce, 253
    EDI, 254-255
    email, 255
    flowcharts, 252
CBD, 220
copy software entries here, 186
DOOS, 219
hotspot security, 302
n-tier and application development, 220-221
OOSD, 220
smartphones/tablets security, 302
testing, 246-249
virtualization and application development, 221-222
WBAD, 220
applying for CISA certification, 8
ARM (Application Reference Model), FEAF, 112
ARO (Annual Rate of Occurrence)
  BIA criticality analysis, 147
  quantitative risk analysis, 85
ARP (Address Resolution Protocol), 294
Arthur Andersen, ethics, 30
assessing risk, 40
  audit risk, 42
  control risk, 41-42
  detection risk, 41-42
assessing risk

inherent risk, 41
material, defining, 41
qualitative analysis, 86-87
qualitative judgments, 43
quantitative analysis, 42-43, 84-87
residual risk, 42

asset identification (ERM), 82

asset management
attack methods/techniques, 399-413
prevention/detection tools/techniques, 414-418
problem/incident management, 418-429
security controls, 391-397

asset protection
access control
authentication, 336-346
exterior security control, 349-356
Federation, 343-345
identification, 336
perimeter security control, 349-356
physical/environmental access control, 349-356
remote access, 345-348
SSH, 347
SSO, 340-342
Telnet, 347
data breaches
data destruction, 378
encryption, 374-375
infrastructures, 378-379
unsecured devices, 375-378
Verizon Data Breach report, 374
hardware security controls, voice communications, 356-357

information asset protection
access control, 370
compliance laws, 370-371
data classification, 373-374
data life cycles, 363
keyloggers, 371
monitoring, 371-372
privacy controls, 372
risk-assessment, 372
security controls, 372
encryption, 357-368
voice communications, 356-357
software security controls, 356-368
assignments (employee management), rotation of, 102, 107
asymmetric encryption, 358-359, 362-368
asynchronous attacks, 411
Atbash, encryption, 357
ATM (Asynchronous Transfer Mode), 313
Atomicity (ACID tests), 245, 282
attack methods/techniques
asynchronous attacks, 411
Bluebugging, 406
Bluejacking, 406
Bluesnarfing, 406
botnets, 403-404
brute-force attacks, 413
buffer overflow attacks, 409
comparative analysis, 412
DDoS attacks, 402-403
dictionary attacks, 412
DoS attacks, 402-403
droppers, 405
dumpster diving attacks, 400
e-mail attacks, 400
hijacking attacks, 401
HOIC, 403
hping, 403
hybrid attacks, 412-413
integer overflow attacks, 412  
John the Ripper, 413  
logic bombs, 411  
LOIC, 403  
malware, 404-405  
MITM attacks, 401  
password-cracking programs, 412-413  
phishing attacks, 400  
ping of death, 402  
pretexting attacks, 400  
rainbow tables, 413  
rounding-down attacks, 412  
RUDY, 403  
salami technique, 412  
slowloris, 403  
smurfing attacks, 402  
sniffing attacks, 400  
social-engineering attacks, 399-400  
spear phishing attacks, 400  
spoofing attacks, 400  
SQL injection attacks, 408-409  
syn flooding, 403  
thunder tables, 413  
TOCTOU attacks, 411  
trap doors, 411  
Trojans, 405  
viruses, 405  
WAP-related attacks, 406  
whaling attacks, 400  
worms, 405  
wrappers, 405  
XSRF attacks, 411  
XSS attacks, 411  
zero-day attacks, 404  
attack stage (penetration testing), 417  
Attack Surface Analyzer (Microsoft), 409  
attack-detection tools, 414  
attenuation (cabling), 320  
attribute sampling, 52  
attributes (databases), 278  
audit hooks, continuous online auditing, 248  
audit monitors, EDI, 254-255  
audit planning, 236. See also audit universes  
audit risk, 42  
audit trails, employee management, 106  
audit universes  
  auditable entities, 235  
  defining, 235  
  refreshing, 235  
  risk assessment (ranking), 236  
audit-reduction tools, 415  
auditing  
  attribute sampling, 52  
  audit programs, 40  
  automated WP, 50  
  baselines, 94-96  
  business processes, 39  
  CAAT, 51-52  
  chain of custody, 49  
  challenges of, 57-59  
  closing audits, 52-53  
    communicating results, 57-58  
    negotiations/conflict management, 58-59  
  Code of Professional Ethics, 27-30  
  communicating results, 57-58  
  compliance audits, 40  
  continuous monitoring, 55-56  
  continuous online auditing, 247-249  
  corrective controls, 47  
  CSA, 54-55  
  data classification, 98
detective controls, 47
disclaimers, 58
discovery sampling, 52
documentation, 94-96
embedded audit modules, 52
ethics, 27-30
evidence handling, 49-50
fiduciary responsibility, 47
financial audits, 39
frameworks (IT governance), 80
frequency estimating sampling, 52
General Auditors, 89
guidance documents, 36
  COBIT 5, 31, 37, 41-42, 55
  FIPS, 37
  ISO, 37
  NIST, 37
hard skills, 27-28
integrated audits, 39
internal controls, 45-47
ISACA
  baselines, 31-34
  Code of Professional Ethics, 27-30
guidelines, 31-34
  procedures, 31-34
  standards, 31-34
IT governance, frameworks, 80
ITF, 52
judgmental sampling, 51
laws/regulatory standards
  compliance with, 38
  knowledge of, 35-36
life cycle of, 48-49
methodologies, 48
negotiations/conflict resolution, 58-59
nonstatistical sampling, 51
objectiveness of, 89
operational audits, 40
opinions, 52-53, 58
parallel simulations, 52
policies, 94-96
preventive controls, 47
procedures, 94-96
QA, 56-57
reconciliation audits, employee management, 106
regulatory standards
  compliance with, 38
  knowledge of, 35-36
reports, 49, 57
  opinions, 52-53, 58
  rating, 59
  writing, 53-54
right-to-audit clauses, 127
risk assessment, 40
  audit risk, 42
  control risk, 41-42
  detection risk, 41-42
  inherent risk, 41
  material, defining, 41
  qualitative analysis, 86-87
  qualitative judgments, 43
  quantitative analysis, 42-43, 84-87
  residual risk, 42
risk management
  Coca-Cola, 43
  risk acceptance, 45
  risk analysis, 44
  risk avoidance, 44
  risk monitoring, 45
  risk reduction, 44
  risks, defining, 44
  risk tolerance, 45-47
  risk transference, 45
  threats, defining, 44
skills, 27-28
soft skills, 27
standards, 94-96
statistical sampling, 51
stop-and-go sampling, 52
SURRE rule, 49
third-party audits, 126-127
variable sampling, 52
vendors, 94-96
work-related skills, 27-28
WP
automated WP, 51
leveraging WP, 54
auditors, BCP, 143
authentication
access control
biometric systems, 338-339
by characteristic, 338-340
by knowledge, 336-337
by ownership, 338
centralized authentication, 345-346
Federation, 343-345
gEOFencing, 337
multi-platform authentication, 343-345
passwords, 336-337
somewhere you are systems, 340
SSO, 340-342
tokens, 338
two-factor authentication, 338
dual-factor authentication, 93
hotspots, 302
OpenID, 344
smartphones/tablets, 302
virtualization, 395
XSRF attacks, 411
authorization
application controls, 244
authorization controls, 238, 254
automation
application controls, 236-237
control systems, SCADA, 35
data classification and, 97
sales (CRM), 259
WP, 50-51
avoiding risk (risk management), 44

B
B-to-B (Business-to-Business) transactions, 253
B-to-C (Business-to-Consumer) transactions, 253
B-to-E (Business-to-Employee) transactions, 253
B-to-G (Business-to-Government) transactions, 253
background checks, 103, 107
backups
continuous backups, 166
database backups, 395
differential backups, 166
electronic vaulting, 169
full backups, 166
grandfather-father-son rotation method, 168
hotspots, 302
incremental backups, 166
location redundancy, 168
MAID, 166
media-rotation strategies, 167-168
offsite storage, 167
onsite storage, 167
point-in-time, 169
SAN, 166-169
security, 169
simple rotation method, 167
smartphones/tablets, 302
standby database shadowing, 169
tape backups, 166
tape librarians, 167
testing, 167
Tower of Hanoi rotation method, 168
VSAN, 168
BAD (Business Application Development), 200
software development
  agile development, 213
  incremental development, 212
  prototyping, 212
  RAD, 212
  reengineering, 213
  sprints, 213
  spiral development, 212
  scrums, 213
  XP, 213
waterfall model, systems-development methodology, 200-201
development phase, 204-208
  disposal phase, 211
  implementation phase, 208-209
  initiation phase, 202-204
  operation/maintenance phase, 210
balance data (data categories), 241
banking attacks, 412
base case system evaluation (application testing), 246
baseband transmissions (cabling), 320
Basel III, 35
baselines
documentation, 92
IT governance, 93
policy development, 93
Bastille Linux, 392
bastion hosts, 306, 309
batch controls, 238-239
BCP (Business Continuity Planning), 142
  administrative support teams, 154
  auditor role, 143
BIA, 144
  criticality analysis, 147-149
  qualitative assessment, 146
  quantitative analysis, 145
communications teams, 154
coordination teams, 154
core processes, 158
corrective controls, 143
damage assessment teams, 153
detective controls, 143
development phase, 149-150
discretionary processes, 159
emergency management teams, 153
emergency operations teams, 154
emergency response teams, 153
final plan design, 151-152
finance teams, 154
impact analysis phase, 144-149
implementation phase, 151-156
incident response teams, 153
initiation phase, 143
interruptions, handling, 149-150
maintenance phase, 156
maximum acceptable outages, 158
maximum tolerable outages, 158
metrics, 157-158
monitoring phase, 156
preventive controls, 143
project management, 143
recovery strategies, 149-150
recovery test teams, 154
relocation teams, 154
responsibilities, 152-153
reviewing results, 157-158
reviewing tasks, 170
RPO, 157
RTO, 157-159
salvage teams, 153
SDO, 158
security teams, 154
supplies teams, 154
supporting processes, 158
team responsibilities, 143
testing phase, 153-154
  * paper tests, 155
  * preparedness tests, 155-156
training and awareness, 152-153
transportation teams, 154
verifying tasks, 170
WRT, 158
before-and-after image reports, 242
beta testing, 207-209
**BI (Business Intelligence), business application systems, 256**
AI/expert systems, 258
CRM, 258
data architectures, 256
data lakes, 257
data warehouses, 257
DSS, 257-258
SCM, 259
social media, 260

**BIA (Business Impact Analysis), 144**
criticality analysis
  * ALE, 148
  * ARO, 147
  * interdependencies, 149
  * SLE, 147
  * system classification, 148
qualitative assessment, 146
quantitative analysis, 145
biometric systems, authentication by, 338-339
black-box testing, 207, 409
block ciphers, 361
blogs
  * BI, 260
  * security, 397
**Blowfish encryption, 359**
**Bluetooth, 298-299**
  * Bluebugging, 406
  * Bluejacking, 406
  * Bluesnarfing, 406
  * data breaches, 377
  * Discovery mode, 405
  * hacking, 406
  * Ubertooth, 406
**Boehm, Barry, 194**
bollards, physical/environmental access control, 350
botnets, 403-404
bottom-up policy development (IT governance), 91
bottom-up testing, 206
**BPA (Business Partnership Security Agreements), 215**
brands, risk assessment (audit universes), 236
**BRI (Basic Rate Interface), ISDN, 314**
BRM (Business Reference Model), FEAF, 112
broadband transmissions (cabling), 321
broadcast addresses, 294
brute-force attacks, 413
BSC (Balanced Scorecards), performance management, 109-110
buffer overflow attacks, 409
building security, HVAC, 356
bus topologies (networks), 319
business application systems
   BI
      AI/expert systems, 258
      CRM, 258
      data architectures, 256
      data lakes, 257
      data warehouses, 257
      DSS, 257-258
      SCM, 259
      social media, 260
e-commerce, 253
EDI, 254-255
e-mail, 255
flowcharts, 252
business case analysis, project investment, 190
business ethics. See ethics
business interruptions, BCP recovery strategies, 150
business process controls
data file controls, 241-242
input controls, 237
   authorization controls, 238
   batch controls, 238-239
   hashing controls, 238
long-term business goals, 237
output controls, 242
password controls, 242
printing controls, 242
processing controls
   data integrity controls, 240-241
   edit controls, 239
short-term business goals, 237
business processes, auditing, 39
business structures, 77
BYOD (Bring-Your-Own-Device) policies, 302-303, 377-378
bypass label processing, 414

C

CA (Certificate Authorities), PKI, 366
CAAT (Computer-Assisted Audit Techniques), 51-52
cabling
   attenuation, 320
   baseband transmissions, 320
   broadband transmissions, 321
   coaxial cabling, 321-322
copper cabling, 322
   fiber-optic cabling, 321-322
   plenum-grade cabling, 321
twisted-pair cabling, 321
Caesar’s cipher, encryption, 357
capacity planning, 314
cloud providers, 318
flow analysis, 315
load balancing, 318
network analyzers
   port mirroring, 317
   Wireshark, 316
network cabling
   attenuation, 320
   baseband transmissions, 320
   broadband transmissions, 321
   coaxial cabling, 321-322
check digits (edit controls), 240
cipher text (encryption), 358, 374
CIR (Committed Information Rates), frame relay, 313
circuit switching, 313-314
circuit-level proxies, 307
CISA (Certified Information Systems Auditor) exam
applying for certification, 8
CBT, 13
CPE
  earning hours, 17-18
  policies, 16
  reporting hours earned, 16-17
credit tracking, 16-17
exam domains, 10-13
getting scores, 15
grading exams, 13
importance of certification, 4-5
intent of, 3-4
ISACA agreements, 9-10
maintaining certification, 16
mission statement, 3
passing, 9
Pearson Test Prep software, 437, 442
  customizing practice exams, 439-440
  Flash Card Mode, 439
  offline access, 438-439
  online access, 438-439
  Practice Exam Mode, 439
chains of custody, 49, 426
change documents (programs), 243
change management, 113, 418
change-control boards, 213
changeover techniques, implementation phase (NIST SDLC), 209
channels (frequencies), ISDN, 314
characteristic, authentication by, 338-340
chargeback corporate structures, 77
charters, IT steering committees, 76

CISA (Certified Information Systems Auditor) exam
applying for certification, 8
CBT, 13
CPE
  earning hours, 17-18
  policies, 16
  reporting hours earned, 16-17
credit tracking, 16-17
exam domains, 10-13
getting scores, 15
grading exams, 13
importance of certification, 4-5
intent of, 3-4
ISACA agreements, 9-10
maintaining certification, 16
mission statement, 3
passing, 9
Pearson Test Prep software, 437, 442
  customizing practice exams, 439-440
  Flash Card Mode, 439
  offline access, 438-439
  online access, 438-439
  Practice Exam Mode, 439
chains of custody, 49, 426
change documents (programs), 243
change management, 113, 418
change-control boards, 213
changeover techniques, implementation phase (NIST SDLC), 209
channels (frequencies), ISDN, 314
characteristic, authentication by, 338-340
chargeback corporate structures, 77
charters, IT steering committees, 76

copper cabling, 322
fiber-optic cabling, 321-322
plenum-grade cabling, 321
twisted-pair cabling, 321
network design, 318-319
SNMP, 315
utilization reports, 315-317
vendors, 318
Windows Performance Monitor, 315
wireless systems, 322-323
categorizing
  data, 241
  threats, 83
CBD (Component-Based Development), 220
CBT (Computer-Based Testing), CISA exams, 13
CCTV (Closed-Circuit Television) systems, physical/environmental access control, 352, 355-356
centralized authentication
  Diameter, 346
  RADIUS, 345-346
  TACACS, 346
centralized C&C (Command and Control) structures (botnets), 404
certificate servers, PKI, 366
certification, 208. See also CISA exam
chains of custody, 49, 426
change documents (programs), 243
change management, 113, 418
change-control boards, 213
changeover techniques, implementation phase (NIST SDLC), 209
channels (frequencies), ISDN, 314
characteristic, authentication by, 338-340
chargeback corporate structures, 77
charters, IT steering committees, 76

copper cabling, 322
fiber-optic cabling, 321-322
plenum-grade cabling, 321
twisted-pair cabling, 321
network design, 318-319
SNMP, 315
utilization reports, 315-317
vendors, 318
Windows Performance Monitor, 315
wireless systems, 322-323
categorizing
  data, 241
  threats, 83
CBD (Component-Based Development), 220
CBT (Computer-Based Testing), CISA exams, 13
CCTV (Closed-Circuit Television) systems, physical/environmental access control, 352, 355-356
centralized authentication
  Diameter, 346
  RADIUS, 345-346
  TACACS, 346
centralized C&C (Command and Control) structures (botnets), 404
certificate servers, PKI, 366
certification, 208. See also CISA exam
chains of custody, 49, 426
change documents (programs), 243
change management, 113, 418
change-control boards, 213
changeover techniques, implementation phase (NIST SDLC), 209
channels (frequencies), ISDN, 314
characteristic, authentication by, 338-340
chargeback corporate structures, 77
charters, IT steering committees, 76
Premium Edition, 440
Study Mode, 439
updating practice exams, 440
website, 438
popularity of, 5
question formats, 14-15
registering for exams, 7
requirements for, 6-8
retaking, 16
scheduling exams, 6
strategies for, 18-19
tips/tricks, 18-19
work experience waivers, 8
claims, integrity of, 39
Class A networks, IPv4 addressing, 293
Class B networks, IPv4 addressing, 293
Class C networks, IPv4 addressing, 294
classifying data
  information asset protection, 373-374
  PHI, 97
  PII, 97
  policy development, 96-98
clear text protocols, 378
click-wrap license agreements, 186
clients
  CRM, BI, 258
  customer service (CRM), 259
  identification as authorization control, 238
clipping levels (passwords), 379
closing phase (project management), 199
cloud computing
  access control, 218
  cloud providers
    capacity planning, 318
    contracts, 218
    security, 219
e-commerce, 253
encryption, 219
models of, 216
security, 219
services, 216
technical controls (security controls), 391
threats to, 218-219
training, 218
clustering, hardware recovery, 164
CMM (Capability Maturity Model), 116-119
CMMI (Capability Maturity Model Integration), 117-118
coaxial cabling, 321-322
COBIT 5 (Control Objectives for Information and Related Technologies 5), 31, 37, 41-42, 55, 78, 111, 273-274
CMM, 117, 118
ITIL versus, 79
Coca-Cola, risk management, 43
COCOMO II (Constructive Cost Model II) software estimation, 194
Code of Professional Ethics, 9-10, 27-30
coding
  4GL programming languages, 258
  5GL programming languages, 258
  insecure code, 378
cold sites, disaster recovery planning, 161
collision domains, 303
collision-avoidance protocols, 293
collisions, defined, 303
communication-driven DSS (Decision Support Systems), BI, 257
communications handlers (EDI), 254
communications teams (BCP), 154
community clouds, 216
comparative analysis (passwords), 412
compensating controls (employee management), 106
completeness checks (edit controls), 240
compliance (laws/regulations)
audits, 40
managing, 119-121
regulatory compliance, risk assessment (audit universes), 236
tests, 39
verifying, 38
computer forensics, 425-426
conflict resolution/negotiation, 58-59
conformity, verifying, 39
Consistency (ACID tests), 245, 282
content services switches, 304
content switches, 304
continuity planning. See BCP
continuous backups, 166
continuous monitoring, 55-56
continuous online auditing, 247-249
contractors, relationship management, 129-130
contracts
cloud provider contracts, 218
disaster recovery, 171
managing, 127-128
control frameworks, management and change management, 113
COBIT 5, 111, 117-118
COSO, 110, 115-116
CSF, 111
EA, 111-112
ISO, 111, 114-115
quality management, 114-119
control risk, 41-42
control/execution phase (project management), 199
converting/migrating data, 209
cooling (data centers), 356
COOP (Continuity of Operations) websites, 172
coordination teams (BCP), 154
copper cabling, 322
core business risk assessments (audit universes), 236
core processes, BCP, 158
corporate structures, 77
corrective controls, 47, 143
COSO (Committee of Sponsoring Organizations of the Treadway Commission), 35, 110, 115-116
costs of projects
project management, 187, 192
reviewing, 211
software (project management, planning phase), 193-194
CPE (Continuing Professional Education)
credit tracking, 16-17
earning hours, 17-18
policies, 16
reporting hours earned, 16-17
CPM (Critical Path Methodology), project management, 198
CR (Change Requests), change management, 113

crashing (critical tasks), 198
credit tracking (CPE), 16-17
credit/debit cards, PCI standards, 35-36, 119

crime (computer), prosecuting, 429

crime triangles
fraud risk factors, 419
incident response, 423

criminal hackers, 419

critical services, maintaining, 141

alternate processing sites
cold sites, 161
hot sites, 160
mobile sites, 160
oversubscription, 163
reciprocal agreements, 162-163
subscription services, 160, 163
warm sites, 161

alternative processing agreements, reviewing, 171

BCP, 142

administrative support teams, 154
auditor role, 143
BLA, 144-149
communications teams, 154
coordination teams, 154
core processes, 158
corrective controls, 143
damage assessment teams, 153
detector controls, 143
development phase, 149-150
discretionary processes, 159
emergency management teams, 153
emergency operations teams, 154
emergency response teams, 153
final plan design, 151-152

finance teams, 154
impact analysis phase, 144-149
implementation phase, 151-156
incident response teams, 153
initiation phase, 143
interruptions, 149-150
maintenance phase, 156
maximum acceptable outages, 158
maximum tolerable outages, 158
metrics, 157-158
monitoring phase, 156
preventive controls, 143
project management, 143
recovery strategies, 149-150
recovery test teams, 154
relocation teams, 154
responsibilities, 152-153
reviewing results, 157-158
reviewing tasks, 170
RPO, 157
RTO, 157-159
salvage teams, 153
SDO, 158
security teams, 154
supplies teams, 154
supporting processes, 158
team responsibilities, 143
testing phase, 153-156
training and awareness, 152-153
transportation teams, 154
verifying tasks, 170
WRT, 158

contracts, reviewing, 171
COOP websites, 172
data recovery, 165-169
disaster life cycles, 172-173
disaster recovery checklist, 172
hardware recovery
   clustering, 164
   fault tolerance, 164
MTBF, 163
MTTF, 163
MTTR, 164
RAID, 164-165
SLA, 164
incident classification, 141-142
insurance, reviewing, 171
MTD, 159
natural disasters, 140
power supplies, 171
recovery times, 161-162
redundant processing sites, 160
reviewing tasks, 170
telecommunications recovery, 169-170
verifying tasks, 170

critical tasks, planning (project management), 198
criticality analysis (BIA)
   ALE, 148
   ARO, 147
   interdependencies, 149
   SLE, 147
   system classification, 148
CRL (Certificate Revocation List), PKI, 366
CRM (Customer Relationship Management), 258, 279
cryptanalysis, 358
cryptography
   asset protection, 367-368
cryptography keys, 358
data breaches, 374-375
   ECC, 363
   PGP, 369
   quantum cryptography, 364
   SET, 368
   S/MIME, 369
   SSH, 368
CSA (Control Self-Assessments), 54-55
CSF (Cybersecurity Framework), 111
CSIRT (Computer Security Incident Response Teams), 420-422
CSMA/CD (Carrier-Sense Multiple Access/Collision Detection). See Ethernet
culture/objectives of projects (project management), 189
custody, chain of, 49
customers
   CRM, BI, 258
customer service (CRM), 259
customizing practice exams, 439-440
cut-through switches, 304

D

DAM (Database Activity Monitoring), 394. See also SIEM
damage assessment teams (BCP), 153
data access layer (BI data architectures), 256
data acquisition, SCADA, 35
data breaches
   data destruction, 378
   encryption, 374-375
   infrastructures, 378-379
   unsecured devices, 375-378
   Verizon Data Breach report, 374
data categories
   balance data, 241
   static data, 241
   system control parameters, 241
   transaction files, 241
data centers, HVAC, 356

data classification
information asset protection, 373-374
PHI, 97
PII, 97
policy development, 96
  auditing, 98
  automating classification, 97
destroying data, 97
DLP, 97
PHI, 97
PII, 97
data conversion, migrating data, 209

data destruction, 97, 378

data file controls (business process controls), 241-242

data file security, 242

data frames, 289
  Ethernet, 292-293
  MAC addresses, 293

data integrity
  ACID tests, 245
  application controls, 245, 249
databases and, 281
editing controls, 239-240
entity integrity, 245
online data integrity, 245
processing controls, 240-241
referential data integrity, 245
relational data integrity, 245

data interruptions, BCP recovery strategies, 149

data lakes (BI), 257

data life cycles, information asset protection, 369

data link layer (OSI reference model), 289

data mart layer (BI data architectures), 256

data migration and data conversion tools, 209

data mining, 256, 278

data packets, IPv4/IPv6 addresses, 294

data recovery, backups, 165
  continuous backups, 166
differential backups, 166
electronic vaulting, 169
full backups, 166
grandfather-father-son rotation method, 168
incremental backups, 166
location redundancy, 168
MAID, 166
media-rotation strategies, 167-168
offsite storage, 167
onsite storage, 167
SAN, 166-169
security, 169
simple rotation method, 167
standby database shadowing, 169
tape backups, 166
tape librarians, 167
testing, 167
Tower of Hanoi rotation method, 168
VSAN, 168
data remanence, VM, 222

data restoration, 302

data sources layer (BI data architectures), 256

data staging layer (BI data architectures), 256

data transfers, 302

data warehouses, 256-257, 279

data-driven DSS (Decision Support Systems), BI, 257
data-entry employees, 104
database tables, 241-242

databases
ACID tests, 282
administrators, 104
aggregation, 278
attributes, 278
backups, 395
CRM, 279
database-management systems, 278
  HDMS, 279
  NDMS, 279
  RDMS, 281
data integrity, 281
data mining, 278
data warehouses, 279
fields, 278
foreign keys, 278
granularity, 278
HDMS, 279
metadata, 278
NDMS, 279
RDMS, 281
relations, 278
schemas, 278
security, 408-409
  backups, 395
  DAM, 394
  database shadowing, 395
  EDR, 394
  OWASP top 10 security concerns, 393
  WAF, 393
shadowing, 169, 395
SQL injection attacks, 408-409
technical controls (security controls), 393-395
tuples, 281

DDoS (Distributed Denial of Service) attacks, 402-403
debit/credit cards, PCI standards, 35-36, 119
decentralized C&C (Command and Control) structures (botnets), 404
Defense model (ERM), Three Lines of, 87-89
Delphi technique (qualitative risk analysis), 87
DES (Data Encryption Standard), 359-361
design/development (project management), 251
destroying data, 97, 378
Detail view (Wireshark), 316
detection risk, 41-42
detection/prevention tools/techniques
  attack-detection tools, 414
  audit-reduction tools, 415
  integrity checks, 414
  log reviews, 414-415
  NAC, 415
  NetFlow, 415
  security testing, 416-418
  SIEM, 415
  trend-detection tools, 414
  variance-detection tools, 414
detective controls, 47, 143
development phase (NIST SDLC), 204
  exception handling, 207
  high/low coupling, 205
  input/output controls, 205
  reverse engineering, 205
  testing, 206
development/design (project management), 251
DevOps (Development Operations), 220
DHCP (Dynamic Host Configuration Protocol), 297
Diameter, 346
dictionary attacks, 412
DID (Direct Inward Dial), voice communication security, 357
differential backups, 166
Diffie, Dr. W, 362
digital evidence, forensics, 427
digital signatures, 365
direct changeover (changeover techniques), 209
directory services, OSI reference model, 291
disaster planning. See problem/incident management
disaster recovery, 141, 159
alternate processing sites
cold sites, 161
hot sites, 160
mobile sites, 160
oversubscription, 163
reciprocal agreements, 162-163
subscription services, 160-163
warm sites, 161
alternative processing agreements, reviewing, 171
BCP, 142
administrative support teams, 154
auditor role, 143
BLA, 144-149
communications teams, 154
coordination teams, 154
core processes, 158
corrective controls, 143
damage assessment teams, 153
detective controls, 143
development phase, 149-150
discretionary processes, 159
emergency management teams, 153
emergency operations teams, 154
emergency response teams, 153
final plan design, 151-152
finance teams, 154
impact analysis phase, 144-149
implementation phase, 151-156
incident response teams, 153
initiation phase, 143
interruptions, 149-150
maintenance phase, 156
maximum acceptable outages, 158
maximum tolerable outages, 158
metrics, 157-158
monitoring phase, 156
preventive controls, 143
project management, 143
recovery strategies, 149-150
recovery test teams, 154
relocation teams, 154
responsibilities, 152-153
reviewing results, 157-158
reviewing tasks, 170
RPO, 157
RTO, 157-159
salvage teams, 153
SDO, 158
security teams, 154
supplies teams, 154
supporting processes, 158
team responsibilities, 143
testing phase, 153-156
training and awareness, 152-153
transportation teams, 154
verifying tasks, 170
WRT, 158
contracts, reviewing, 171
COOP websites, 172
data recovery, 165-169
disaster life cycle, 172-173
disaster recovery checklist, 172
hardware recovery
  clustering, 164
  fault tolerance, 164
  MTBF, 163
  MTTF, 163
  MTTR, 164
  RAID, 164-165
  SLA, 164
incident classification, 141-142
insurance, reviewing, 171
MTD, 159
natural disasters, 140
power supplies, 171
recovery times, 161-162
redundant processing sites, 160
reviewing tasks, 170
telecommunications recovery, 169-170
verifying tasks, 170
disclaimers (audit reports), 58
Discovery mode (Bluetooth), 405
discovery sampling, 52
discovery stage (penetration testing), 417
discretionary processes, BCP, 159
disposal phase (NIST SDLC), vulnerability assessments, 211
distance-vector protocols, 295
DITKA questions, final exam preparation, 442
diverse routing, telecommunications recovery, 170
DLP (Data Loss Prevention), 97
DMCA (Digital Millennium Copyright Act), 186
DMZ (Demilitarized Zones), 306, 309
DNS (Domain Name Service), 291, 297, 312
DNSSEC (Domain Name Service Security Extensions), 297
document-driven DSS (Decision Support Systems), BI, 258
documentation
  applications, understanding, 243
  auditing, 94-96
  baselines, 92
  change-control process, 214
  employee handbooks, 100-101
  exception reports, 106, 241
  guidance documents, 36
    COBIT 5, 31, 37, 41-42, 55
    FIPS, 37
    ISO, 37
    NIST, 37
  incident response, 421, 424
  levels of control, 92
  policies, 92
  procedures, 92
  program change documents, 243
  right-to-audit clauses, 127
  SLA, 127-128
  standards, 92
  third-party documentation, 94-96
  transaction logs, 106
dogs, physical/environmental access control, 351
domain names, FQDN and DNS, 297
DoS (Denial of Service) attacks, 402-403
DOSD (Data-Oriented System Development), 219
downtime, MTD, 159
Draper, John, 357
DRM (Data Reference Model), FEAF, 112
DRM (Digital Rights Management), 283
droppers, 405
DSL (Digital Subscriber Lines), 314, 321
DSS (Decision Support Systems), BI, 257-258
DSSS (Direct-Sequence Spread Spectrum), 300
dual control, employee management, 102, 107
dual-factor authentication, 93
dual-homed gateways, 308
dumpster diving attacks, 400
duplicate checks (edit controls), 240
Durability (ACID tests), 246, 282
duties, separating (application controls), 244
dwell time, 300
dynamic forensic analysis, 427

e -

e-commerce
B-to-B transactions, 253
B-to-C transactions, 253
B-to-E transactions, 253
B-to-G transactions, 253
business application systems, 253
cloud computing, 253
transaction process, 235
EA (Enterprise Architectures), 111-112
ECC (Elliptic Curve Cryptography), 363
echo requests (ICMP), 290
edge devices
DMZ, 306, 309
firewalls
configuring, 308-310
packet filter firewalls, 307-308
proxies, 307
screened host firewalls, 309
WAF, 308
IDP, 310
IDS
anomaly detection IDS, 312
HIDS, 310
NIDS, 310
pattern-matching (signature) IDS, 311
protocol decoding IDS, 312
IPS, 310
EDI (Electronic Data Interchange)
application system, 254
audit monitors, 254-255
authorization controls, 254
business application systems, 254-255
communications handlers, 254
EDI interface, 254
EFT, 254
collision detection controls, 254
manipulation controls, 254
transmission controls, 254
eDiscovery, 302
editing controls (data integrity controls), 239-240
EDR (Endpoint Detection and Response), 394
EER (Equal Error Rates), biometric systems, 339
EFT (Electronic Funds Transfers), 254
electronic vaulting, 169
email
attacks, 400
business application systems, 255
encryption, 255
IMAP, 291, 297
OSI reference model services, 290
PEM, 255
PGP, 255
POP, 255
POP3, 291, 297
S/MIME, 255
SMTP, 255, 290
embedded audit modules, 52
emergency changes, information systems maintenance, 214
emergency incident response teams, 420-422
emergency management teams (BCP), 153
emergency operations teams (BCP), 154
emergency response teams (BCP), 153
employees
background checks, 103, 107
BYOD policies, data breaches, 377-378
database administrators, 104
data-entry employees, 104
forced vacations, 102, 107
handbooks, 100-101
hiring, 100
logic bombs, 411
managing
audit trails, 106
background checks, 103, 107
compensating controls, 106
dual control, 102, 107
exception reports, 106
forced vacations, 102, 107
handbooks, 100-101
hiring practices, 100
job rotation, 106
NDA, 102, 107
performance assessments, 101
reconciliation audits, 106
roles/responsibilities, 103-104
rotation of assignments, 102, 107
separation events (termination), 102-103
SoD, 105-107
supervisor reviews, 106
training, 101, 107
transaction logs, 106
network administrators, 104
performance assessments, 101
QA employees, 104
roles/responsibilities, 103-104
security architects, 104
separation events (termination), 102-103
SoD, 105-107
systems administrators, 104
systems analysts, 104
termination (separation events), 102-103
training, 101, 107
vacations, 102, 107
encryption. See also tokenization
3DES, 359
802.11 wireless encryption, 299
AES, 362
algorithms, 358
asymmetric encryption, 358-359, 362, 367-368
digital signatures, 365
ECC, 363
hashing, 364
PKI, 365-366
quantum cryptography, 364
RSA, 363
trap door functions, 362
Atbash, 357
block ciphers, 361
Blowfish, 359
Caesar’s cipher, 357
ciphertext, 358, 374
cloud computing, 219
cryptanalysis, 358
cryptography, 358
asset protection, 367-368
data breaches, 374-375
ECC, 363
PGP, 369
quantum cryptography, 364
SET, 368
S/MIME, 369
SSH, 368
data breaches, 374-375
DES, 359-361
digital signatures, 365
ECC, 363
encryption controls (EDI), 254
end-to-end encryption, 368
hashing, 364
key length, 358
link-state encryption, 368
man-in-the-middle attacks, 375
multiple encryption, 361
OS, 393
OSI reference model, 367-368
PEM, 255
PGP, email, 255
PKI, 365-366
plaintext, 358, 374
private key encryption
3DES, 359
AES, 362
Blowfish, 359
DES, 359-361
RC4, 360
RC5, 360
Rijndael, 360-362
SAFER, 360
public key encryption
digital signatures, 365
ECC, 363
hashing, 364
PKI, 365-366
quantum cryptography, 364
RSA, 363
trap door functions, 362
quantum cryptography, 364
RC4, 360
RC5, 360
remote access and, 347
Rijndael, 360-362
RSA, 363
S/MIME, 255
SAFER, 360
stream ciphers, 361
symmetric encryption, 358, 367-368
3DES, 359
AES, 362
Blowfish, 359
DES, 359-361
RC4, 360
RC5, 360
Rijndael, 360-362
SAFER, 360
virtualization, 395
WAP, 406-407
weak encryption, 378
end-to-end encryption, 368
Enron, ethics, 30
enterprise marketing (CRM), 259
entity integrity (data integrity controls), 245
entry points, physical/environmental access control, 351
environmental/physical access control
bollards, 350
CCTV systems, 352, 355-356
dogs, 351
entry points, 351
fences, 349-350
gates, 350
guards, 352
HVAC, 356
lighting, 351, 354
locks, 353-354
ERD (Entity Relationship Diagrams), primary keys, 203-204
ERM (Enterprise Risk Management), 80
asset identification, 82
risk assessments
qualitative analysis, 86-87
quantitative analysis, 84-87
risk management teams, 81
threat identification, 82-83
Three Lines of Defense model, 87-89
errors
correcting/controlling (application controls), 244
maintenance error reports, 242
escrow agreements (software), 185
Ethernet, 284, 292-293
ethical hacking. See penetration testing
ethics
Arthur Andersen, 30
Enron, 30
ISACA Code of Professional Ethics, 9-10, 27-30
e’TOM (Enhanced Telecom Operations Map), 273-275
EU (European Union) Privacy Shield law, 35
EUC (End-User Computing), 208
EULA (End-User Licensing Agreements), 282
events
analyzing, incident response, 422
separation events (termination), 102-103
stochastic events, 85
evidence
digital evidence, forensics, 427
handling, 49-50
exams
CISA exam
applying for certification, 8
CBT, 13
CPE, 16-18
credit tracking, 16-17
exam domains, 10-13
getting scores, 15
grading exams, 13
importance of certification, 4-5
intent of, 3-4
ISACA agreements, 9-10
maintaining certification, 16
mission statement, 3
passing, 9
Pearson Test Prep software, 437-442
popularity of, 5
question formats, 14-15
registering for exams, 7
requirements for, 6-8
retaking, 16
scheduling exams, 6
strategies for, 18-19
tips/tricks, 18-19
work experience waivers, 8
Pearson Test Prep Software, 437, 442
customizing practice exams, 439-440
Flash Card Mode, 439
offline access, 438-439
online access, 438-439
Practice Exam Mode, 439
Premium Edition, 440
Study Mode, 439
updating practice exams, 440
website, 438
practice exams
customizing, 439-440
Flash Card Mode, 439
Practice Exam Mode, 439
Study Mode, 439
updating, 440
exception handling, 207
exception reports, 106, 241
execution phase (project management), 199
existence checks (edit controls), 240
expert systems/AI (Artificial Intelligence), BI, 258
exposure factor (quantitative risk analysis), 84
exterior lighting, physical/environmental access control, 355
exterior security control
bollards, 350
CCTV systems, 352, 355-356
dogs, 351
entry points, 351
fences, 349-350
gates, 350
guards, 352
HVAC, 356
lighting, 351, 354
locks, 353-354
turnstiles, 352
external/ internal labeling, 242

F

fabric virtualization. See VSAN
facility interruptions, BCP recovery strategies, 149
FACTA (U.S. Fair and Accurate Credit Transaction ACT of 2003), 35, 120
failures, hardware recovery, 163
FAR (False Accept Rates), biometric systems, 339
fault tolerance
hardware recovery, 164
RAID, 164-165
FEAF (Federal Enterprise Architecture Framework), 112
feasibility
project investment, 191
project management, 251
Federation, 343-345
fences, physical/environmental access control, 349-350
FERPA (Family Educational Rights and Privacy Act), 370
FFIEC Handbook, 36
FHSS (Frequency-Hopping Spread Spectrum), 300
fiber-optic cabling, 321-322
fiduciary responsibility, auditing and, 47
frameworks, 509

fields (databases), 278
file sharing, OSI reference model, 290
file totals (data integrity controls), reconciliation of, 241
final acceptance testing, 206
final preparation, CISA exams
   chapter-ending review tools, 441
   DITKA questions, 442
   memory tables, 441-442
   Pearson Test Prep software, 437, 442
      customizing exams, 439
      customizing practice exams, 440
      Flash Card Mode, 439
      offline access, 438-439
      online access, 438-439
   Practice Exam Mode, 439
   Premium Edition, 440
   Study Mode, 439
   updating exams, 440
   website, 438
review questions, 442
finance teams (BCP), 154
financial attacks, 412
financial audits, 39
financial reporting, COSO, 35
FIPS (Federal Information Processing Standards), 37
firewalls
   configuring, 308-310
   packet filter firewalls, 307-308
   proxies, 307
   screened host firewalls, 309
   WAF, 308, 393
firing employees. See separation events (termination)
FISMA (Federal Information Security Management Act), 35, 120, 370
FitSM, 273-274
Flash Card Mode (practice exams), 439
flow analysis, 315
flowcharts
   applications, understanding, 243-244
   business application systems, 252
forced vacations, 102, 107
foreign keys (databases), 278
forensics
   chains of custody, 426
   computer forensics, 425-426
digital evidence, 427
   dynamic forensic analysis, 427
   network forensics, 427
problem/incident response, 425
   forensic types, 427-428
   processes/procedures, 426-427
   software forensics, 427
   static forensic analysis, 428
FPA (Function Point Analysis), software size estimation, 195-196
FQDN (Fully Qualified Domain Names), 292, 297
frame relay, 313
frames (data), 289
   Ethernet, 292-293
   MAC addresses, 293
frameworks
   ARM, 112
   BRM, 112
   DRM, 112
   FEAF, 112
   IRM, 112
IT governance, 77
   auditing, 80
   COBIT 5, 78-79
   ITIL, 78-79
   overlapping of, 79
management and control frameworks
  change management, 113
  COBIT 5, 111, 117-118
  COSO, 110, 115-116
  CSF, 111
  EA, 111-112
  ISO, 111, 114-115
  quality management, 114-119
PRM, 112
SRM, 112

service management
  COBIT, 273-274
  databases, 278-282
  DRM, 283
  eTOM, 273-275
  FitSM, 273-274
  ISO 20000, 273-274
  ITIL, 273
  OS, 275-277
  software licensing, 282-283
FRAP (Facilitated Risk Assessment Process), qualitative risk analysis, 87
fraud
  FACTA, 35, 120
  risk factors (problem/incident management), 419-420
frequencies
  bands, wireless technologies, 301
  channels, ISDN, 314
  frequency estimating sampling, 52
FRR (False Reject Rates), biometric systems, 339
FTP (File Transfer Protocol), network file sharing, 290
full backups, 166
full operation tests, BCP, 156
full-mesh networks, 320
function testing, 207
funding system services (IT governance), 77
fuzzing, 409

G
GAN (Global Area Networks), 284
Gantt charts, 197-198
gap analysis, 192, 211
gates, physical/environmental access control, 350
gateways, 305, 308
General Auditors, 89
general controls, 243
geofencing, 337
GLBA (Gramm-Leach-Bliley Act), 370
grading CISA exams, 13
grandfather-father-son backup rotation method, 168
guards, physical/environmental access control, 352
guidance documents, 36
  COBIT 5, 31, 37, 41-42, 55
  FIPS, 37
  ISO, 37
  NIST, 37

H
hacking, 419
  Bluetooth, 406
  ethical hacking. See penetration testing
Halstead Complexity Measures, FPA and software size estimation, 196
handbooks (employee), 100-101
Hanoi backup rotation method, Tower of, 168
hard skills, IS auditing, 27-28
hybrid clouds  511

hardening, VM, 395

hardware

recovery

classification, 164
fault tolerance, 164
MTBF, 163
MTTF, 163
MTTR, 164
RAID, 164-165
SLA, 164

security controls, voice communications, 356-357
unsecured devices, data breaches, 375-378

hashing, 364

hashing controls, hash totals, 238

HDMS (Hierarchical Database-Management Systems), 279

health care/insurance, HIPAA, 35, 119, 370

health information, PHI and data classification, 97

Hellman, Dr. M. E., 362

Hex view (Wireshark), 316

HIDS (Host-based Intrusion Detection Systems), 310

high/low coupling, 205

hijacking attacks, 401

HIPAA (Health Insurance Portability and Accountability Act), 35, 119, 370

hiring employees, 100

HOIC (High Orbit Ion Cannons), 403

honeyhats, 306, 422

host-to-host/transport layer (TCP/IP reference model), 295

hot sites, disaster recovery planning, 160

hot-swappable disks, RAID, 164

hotspots, 302-303

hping, 403

HR (Human Resources), employee management

audit trails, 106

background checks, 103, 107

compensating controls, 106
dual control, 102, 107

exception reports, 106

forced vacations, 102, 107

handbooks, 100-101

hiring practices, 100

job rotation, 106

NDA, 102, 107

performance assessments, 101

reconciliation audits, 106

roles/responsibilities, 103-104

rotation of assignments, 102, 107

separation events (termination), 102-103

SoD, 105-107

supervisor reviews, 106

training, 101, 107

transaction logs, 106

vacations, 102, 107

HTTP (Hypertext Transfer Protocol), OSI reference model, 292

hubs, 303-305

humidity (data centers), 356

HVAC (Heating, Ventilation and Air Conditioning) systems, physical/environmental access control, 356

hybrid attacks, 412-413

hybrid botnets, 404

hybrid clouds, 216
Biometric systems, 338-339
by characteristic, 338-340
by knowledge, 338-339
by ownership, 338
geofencing, 338
passwords, 338-339
somewhere you are systems, 340
tokens, 338
two-factor authentication, 338

Identification, 336

ICMP (Internet Control Message Protocol), echo requests, 290

IDA Pro, static forensic analysis, 428

Identification
access control, 336
client identification as authorization control, 238
dual-factor authentication, 93
hotspots, 302
smartphones/tablets, 302

Identifying
assets (ERM), 82
threats (ERM), 82-83

Identity
PII, data classification, 97
theft/fraud, FACTA, 35, 120

IDP (Intrusion Detection and Prevention), 310

IDS (Intrusion Detection Systems)
anomaly detection IDS, 312
HIDS, 310
NIDS, 310

pattern-matching (signature) IDS, 311
protocol decoding IDS, 312

Illegal software, 283

IM (Instant Messaging), security, 396-397

IMAP (Internet Message Access Protocol), 291, 297

Impact analysis. See BIA

Implementation phase
NIST SDLC
accreditation, 208
certification, 208
changeover techniques, 209

project management, 251

Incident classification (disaster recovery), 141-142

Incident response teams (BCP), 153

Incident/problem management
change management, 418
crime jurisdiction, 429
criminal hackers, 419
fraud risk factors, 419-420
hackers, 419

Incident response
defining incidents, 422
documentation, 421, 424
escalation/response procedures, 424
event analysis, 422
forensic investigation, 425-428
honeypots, 422
incident response teams, 420-422
processes/procedures, 422-424
phreakers, 419
prosecuting computer crime, 429
script kiddies, 419
terrorists, 420

Incremental backups, 166
incremental software development, 212
industry guidance documents, 36
  COBIT, 5, 31, 37, 41-42, 55
  FIPS, 37
  ISO, 37
  NIST, 37
information asset protection
  access control, 370
  compliance, 370-371
  data classification, 373-374
  data life cycles, 369
  keyloggers, 371
  monitoring, 371-372
  privacy controls, 372
  risk assessment, 372
  security controls, 372
information systems maintenance
  change-control boards, 213
  documenting, 214
  emergency changes, 214
  unauthorized changes, 214
informative policies, 92
infrastructures, data breaches, 378-379
inherent risk, 41
initiation phase
  NIST SDLC, 202
    ERD, 203-204
    RFP, 204
  project management, 193
input controls (business process controls), 237
  authorization controls, 238
  batch controls, 238-239
  hashing controls, 238
input/output controls, 205
insecure code, 378
insider fraud risk factors (problem/ incident management), 419
insurance, disaster recovery, 171
integer overflow attacks, 412
integrated audits, 39
integrated testing facilities
  application testing, 246
  continuous online auditing, 247
integrity checks, 414
integrity of claims, 39
integrity of data and databases, 281
interface testing, 206
internal controls, auditing with, 45-47
internal/external labeling, 242
Internet layer (TCP/IP reference model)
  distance-vector protocols, 295
  IP addressing, 293-294
  link-state routing protocols, 295
  routing protocols, 294-295
Internet security
  PGP, 369
  SET, 368
  S/MIME, 369
  SSH, 368
interruptions, BCP recovery strategies, 149
investment in projects (project management)
  business case analysis, 190
  feasibility studies, 191
  ROI, 191
IOCE (International Organization on Computer Evidence), forensics and digital evidence, 427
IP (Internet Protocol), 288
  ARP, 294
  IPv4
    broadcast addresses, 294
    Class A networks, 293
Class B networks, 293
Class C networks, 294
multicast addresses, 294
subnets, 293
unicast addresses, 294
IPv6, 294
VoIP, 295, 313
IP addresses, verifying, 290
IP Security (Internet Protocol Security), 348
iPods, pod slurping, 376
IPS (Intrusion Prevention Systems), 310
IRM (Infrastructure Reference Model), FEAF, 112
IRR (Internal Rate of Return), ROI, 192
IS auditing
attribute sampling, 52
audit programs, 40
automated WP, 50
baselines, 94-96
business processes, 39
CAAT, 51-52
chain of custody, 49
challenges of, 57-59
closing audits, 52-53
communicating results, 57-58
evidence handling, 49-50
fiduciary responsibility, 47
financial audits, 39
frequency estimating sampling, 52
General Auditors, 89
guidance documents, 36
COBIT 5, 31, 37, 41-42, 55
FIPS, 37
ISO, 37
NIST, 37
hard skills, 27-28
integrated audits, 39
internal controls, 45-47
ISACA
baselines, 31-34
Code of Professional Ethics, 27-30
guidelines, 31-34
procedures, 31-34
standards, 31-34
ITF, 52
judgmental sampling, 51
laws/regulatory standards
compliance with, 38
knowledge of, 35-36
life cycle of, 48-49
methodologies, 48
negotiations/conflict resolution, 58-59
nonstatistical sampling, 52
objectiveness of, 89
operational audits, 40
opinions, 52-53, 58
parallel simulations, 52
policies, 94-96  
preventive controls, 47  
procedures, 94-96  
QA, 56-57  
reconciliation audits, employee management, 106  
regulatory standards  
  compliance with, 38  
  knowledge of, 35-36  
reports, 49, 57  
  opinions, 52-53, 58  
  rating, 59  
  writing, 53-54  
right-to-audit clauses, 127  
risk assessment, 40  
  audit risk, 42  
  control risk, 41-42  
  detection risk, 41-42  
  inherent risk, 41  
  material, defining, 41  
  qualitative analysis, 86-87  
  qualitative judgments, 43  
  quantitative analysis, 42-43, 84-87  
  residual risk, 42  
risk management  
  Coca-Cola, 43  
  risk acceptance, 45  
  risk analysis, 44  
  risk avoidance, 44  
  risk monitoring, 45  
  risk reduction, 44  
  risks, defining, 44  
  risk tolerance, 45-47  
  risk transference, 45  
  threats, defining, 44  
skills, 27-28  
  soft skills, 27  
standards, 94-96  
statistical sampling, 51  
stop-and-go sampling, 52  
SURRE rule, 49  
third-party audits, 126-127  
variable sampling, 52  
vendors, 94-96  
work-related skills, 27-28  
WP  
  automated WP, 51  
  leveraging WP, 54  
ISA (Interconnection Security Agreements), 215  
ISACA (Information Systems Audit and Control Association)  
  baselines, 31-34  
CISA exams  
  applying for certification, 8  
  CBT, 13  
  CPE policies, 16  
  credit tracking, 16-17  
  earning CPE hours, 17-18  
  exam domains, 10-13  
  getting scores, 15  
  grading, 13  
  ISACA agreements, 9-10  
  maintaining certification, 16  
  question formats, 14-15  
  registration, 7  
  reporting CPE hours earned, 16-17  
  requirements for, 6-8  
  retaking, 16  
  scheduling exams, 6  
  work experience waivers, 8  
COBIT 5, 31, 37, 41-42, 55  
Code of Professional Ethics, 27-30
CPE
  earning hours, 17-18
  policies, 16
  reporting hours earned, 16-17
credit tracking, 16-17
guidelines, 31-34
ISACA website, Code of Professional Ethics, 9-10
My Certifications, 7, 15-17
procedures, 31-34
standards, 31-34
ISDN (Integrated Services Digital Network), 314
ISO (International Organization for Standardization), 37, 111
ISO 9001 certification, quality management, 114-115
ISO 20000, 273-274
Isolation (ACID tests), 245, 282
IT acquisition, software
escrow agreements, 185
licensing agreements, 185-186
IT governance
accountability, 77
auditing, 80
best practices, 77
CMM, 116-119
compliance, managing, 119-121
corporate structures, 77
defining, 71
employee management
  audit trails, 106
  background checks, 103, 107
  compensating controls, 106
  dual control, 102, 107
  exception reports, 106
  forced vacations, 102, 107
  handbooks, 100-101
  hiring practices, 100
  job rotation, 106
  NDA, 102, 107
  performance assessments, 101
  reconciliation audits, 106
  roles/responsibilities, 103-104
  rotation of assignments, 102, 107
  separation events (termination), 102-103
  SoD, 105-107
  supervisor reviews, 106
  training, 101, 107
  transaction logs, 106
ERM
  asset identification, 82
  qualitative risk analysis, 86-87
  quantitative risk analysis, 84-87
  risk management teams, 81
  threat identification, 82-83
  Three Lines of Defense model, 87-89
frameworks, 77
  COBIT 5, 78-79
  ITIL, 78-79
  overlapping of, 79
funding system services, 77
goals of, 77
IT steering committees, 75-76
ITSM, 79
management and control frameworks
  change management, 113
  COBIT 5, 111, 117-118
  COSO, 110, 115-116
  CSF, 111
  EA, 111-112
  ISO, 111, 114-115
  quality management, 114-119
maturity models, 116-119
laws/regulatory standards

outsourcing
contract management, 127-128
performance monitoring, 128
relationship management, 129-130
third-party audits, 126-127
third-party outsourcing, 125-126

performance management, 107
BSC, 109-110
KGI, 109
KPI, 109
metrics, 108-109
risk thresholds, 109
target values, 108
thresholds, 109
units, 108

policies
defining supporting policies, 77
developing, 90-99

processes
defining supporting processes, 77
optimizing, 121-125

IT suppliers, outsourcing
contract management, 127-128
performance monitoring, 128
relationship management, 129-130
third-party audits, 126-127
third-party outsourcing, 125-126

ITF (Integrated Test Facilities), 52
ITIL (IT Infrastructure Library), 78-79, 273
ITSM (IT Service Management), 79

J
JBOD (Just a Bunch of Disks), hardware recovery, 165
job rotation, employee management, 106

John the Ripper, 413
judgmental sampling, 51
jurisdictions (computer crime), 429

K
Kali Linux, 379
Kerberos, 341-342
key verification (edit controls), 240
keyloggers, information asset protection, 371
KGI (Key Goal Indicators), performance management, 109
KLOC (Kilo Lines of Code), software size estimation, 195
knowledge, authentication by, 336-337
knowledge-driven DSS (Decision Support Systems), BI, 258
known plaintext attacks, 374
KPI (Key Performance Indicators), performance management, 109

L
L2TP (Layer 2 Tunneled Protocol), 348
labeling (internal/external), 242
lagging risk indicators, 120
LAN (Local Area Networks), 284
last-mile protection, telecommunications recovery, 170
laws/regulatory standards
Basel III, 35
compliance with, 38
COSO, 35
EU Privacy Shield law, 35
FACTA, 35, 120
FFIEC Handbook, 36
FISMA, 35, 120
HIPAA, 35, 119
knowledge of, 35-36
PCI standards, 35-36, 119
SCADA, 35
SOX, 35, 119
layer 2 switches, 304
leading risk indicators, 120
least privilege (security policies), principle of, 99
licensing
    DRM, 283
    software
        EULA, 282
        illegal software, 283
        licensing agreements, 185-186
lighting, physical/environmental access control, 351, 354
limit checks
    data integrity controls, 241
    edit controls, 239
link-state encryption, 368
link-state routing protocols, 295
Linux
    Bastille Linux, 392
    Kali Linux, 379
live VM migration, 222
load balancing, capacity planning, 318
lockout thresholds, 337, 379
locks, physical/environmental access control, 353-354
logic bombs, 411
logical relationship checks (edit controls), 240
logs
    OS logs, 393
    reviewing/auditing, 414-415
    transaction logs, 106, 242
LOIC (Low Orbit Ion Cannons), 403
long-haul diversity, telecommunications recovery, 170
long-term business goals, defined, 237
losses
    ALE
        BIA criticality analysis, 148
        quantitative risk analysis, 85
defining, 83
    SLE
        BIA criticality analysis, 147
        quantitative risk analysis, 85
threats and, 83
lost/stolen smartphones/tablets, 302
LTO (Linear Tape-Open) backups, 166

MAC (Media Access Control)
    addresses, 293, 304
MAID (Massive Array of Inactive Disks), 166
maintenance error reports, 242
maintenance/operation phase (NIST SDLC)
    patch management, 210
    review process, 211
    vulnerability assessments, 210
malicious software, 379
malware, 404-405
MAN (Metropolitan Area Networks), 284
man-in-the-middle attacks, 375
managed switches, 304
management services, OSI reference model, 291
managing

assets

attack methods/techniques, 399-413
prevention/detection tools/techniques, 414-418
problem/incident management, 418-429
security controls, 391-397

change, 113
changes, 418
compliance, 119-121
contracts, 127-128
customers, CRM and BI, 258

employees

audit trails, 106
background checks, 103, 107
compensating controls, 106
dual control, 102, 107
exception reports, 106
forced vacations, 102, 107
handbooks, 100-101
hiring practices, 100
job rotation, 106
NDA, 102, 107
performance assessments, 101
reconciliation audits, 106
roles/responsibilities, 103-104
rotation of assignments, 102, 107
separation events (termination), 102-103
SoD, 105-107
supervisor reviews, 106
training, 101, 107
transaction logs, 106

management and control frameworks

change management, 113
COBIT 5, 111, 117-118
COSO, 110, 115-116

CSF, 111
EA, 111-112
ISO, 111, 114-115
quality management, 114-119

performance, 107
BSC, 109-110
KGI, 109
KPI, 109
metrics, 108-109
risk thresholds, 109
target values, 108
thresholds, 109
units, 108

problem/incident management

change management, 418
computer crime jurisdictions, 429
escalation/response procedures, 424
forensic investigation, 425-428
fraud risk factors, 419-420
incident response, 420-422
processes/procedures, 422-424
prosecuting computer crime, 429

projects

defining requirements, 251
design/development, 251
feasibility, 251
implementation phase, 251
post-implementation phase, 252
software acquisition process, 251
system change procedures, 252
systems controls, 250-251
testing, 251

quality

CMM, 116-119
COSO, 115-116
ISO, 114-115

relationships (contractors/IS suppliers/vendors), 129-130
managing

See SCM

supply chains. See SCM

manipulation controls (EDI), 254
manual application controls, 236-237
manual authorization controls, 238
manual recalculations (data integrity controls), 240
mapping (application testing), 246
master license agreements, 186
material (risk management), defining, 41
maturity models, 116-119
maximum acceptable outages, BCP, 158
maximum tolerable outages, BCP, 158

media-rotation strategies (backups)
  grandfather-father-son rotation method, 168
  simple rotation method, 167
  Tower of Hanoi rotation method, 168

memory
  buffer overflow attacks, 409
  RAM lookup tables, 304
  smartphones/tablets, 302
  virtual memory, 277

memory tables, final exam preparation, 441-442

mesh topologies (networks), 319

message boards, security, 397

messaging
  IM security, 396-397
  pretexting attacks, 400

metadata, 278

metrics (performance management), 108-109

Microsoft Attack Surface Analyzer, 409

migrations
  data migration and data conversion tools, 209
  VM migration (live), 222

MIMO (Multiple Input, Multiple Output), 301

mining data, 278

mirroring ports, 317

MITM (Man-In-The-Middle) attacks, 401

mobile sites, disaster recovery planning, 160

model-driven DSS (Decision Support Systems), BI, 257

modems, 305
MOM (Means, Opportunity, and Motive), fraud risk factors, 419
monitoring
audit monitors, EDI, 254-255
continuous monitoring, 55-56
DAM, 394
embedded audit modules, 52
information asset protection, 371-372
OSI reference model, 290
performance, 130
IT suppliers, 128
systems/capacity planning, 315-323
risk (risk management), 45
RMON, 290
third-party monitoring, 318
MOU (Memorandums of Understanding), 215
MPLS (Multiprotocol Label Switching), 313
MTBF (Mean Time Between Failures), hardware recovery, 163
MTD (Maximum Tolerable Downtime), 158-159. See also maximum acceptable outages
MTTF (Mean Time To Failure), hardware recovery, 163
MTTR (Mean Time To Repair), hardware recovery, 164
MU-MIMO (Multi-user Multiple Input, Multiple Output), 301
multi-platform authentication, Federation, 343-345
multicast addresses, 294
multiple encryption, 361
multiplexing, OFDM, 300
My Certifications (ISACA website), 7, 15-17

N
n-tier, application development, 220-221
NAC (Network Access Control), 415
NAT (Network Address Translation), 310
natural disasters, recovery planning, 140
NDA (Non-Disclosure Agreements), 102, 107
NDMS (Network Database-Management Systems), 279
negotiations/conflict resolution, 58-59
NetFlow, 415
network access layer (TCP/IP reference model), 292-293
network administrators, 104
network analyzers
port mirroring, 317
Wireshark, 316
network forensics, 427
network layer (OSI reference model), 288
network sniffers, 400
networking cards (wireless), 299
networks, 283
802.11 wireless standard, 299-301
anycast addresses, 294
ARP, 294
Bluetooth, 298-299
broadcast addresses, 294
topologies, 319
cabling
attenuation, 320
baseband transmissions, 320
broadband transmissions, 321
coaxial cabling, 321-322
copper cabling, 322
fiber-optic cabling, 321-322
plenum-grade cabling, 321
twisted-pair cabling, 321
collision domains, 303
DHCP, 297
DMZ, 306, 309
DNS, 291, 297, 312
DNSSEC, 297
directory services, 291
edge devices, 306-312
Ethernet, 292-293
firewalls
configuring, 308-310
packet filter firewalls, 307-308
proxies, 307
screened host firewalls, 309
WAF, 308
FQDN, 292
FTP, 290
full-mesh networks, 320
GAN, 284
gateways, 305, 308
hubs, 303-305
IDP, 310
IDS
anomaly detection IDS, 312
HIDS, 310
NIDS, 310
pattern-matching (signature) IDS, 311
protocol decoding IDS, 312
IMAP, 291, 297
IP, VoIP, 313
IPS, 310
ISDN, 314
LAN, 284
MAC addresses, 293
MAN, 284
mesh topologies, 319
modems, 305
monitoring, 290
multicast addresses, 294
NAT, 310
OSI reference model, 286
application layer, 287
data link layer, 289
directory services, 291
email services, 290
file sharing services, 290
HTTP, 292
IP address verification services, 290
management services, 291
monitoring services, 290
network layer, 288
physical layer, 289
presentation layer, 287
print services, 291
processing data, 289-290
protocol analysis services, 290
session layer, 288
TCP/IP model versus, 292
transport layer, 288
PAN, 284
ping, 290
POP3, 291, 297
PPTP, 293
protocols, 285-286
RAM lookup tables, 304
repeaters, 303
ring topologies, 319
RIP, 295
RMON, 290
routers, 304-305
SAN, 285
SMTP, 290
SNMP, 291
social networks, BI, 260
SSH, 291
standards, 285-286
star topologies, 319
subnet, 293, 309
switches, 304-305
TCP, 295
TCP/IP reference model
  application layer, 296-297
  DHCP, 297
  DNS, 297, 312
  DNSSEC, 297
  host-to-host/transport layer, 295
  Internet layer, 293-295
  network access layer, 292-293
  OSI model versus, 292
Telnet, 291
Token Ring protocol, 293
traceroute, 290
UDP, 295
unicast addresses, 294
VoIP, 295, 313
VPN, 293, 347-348
WAN, 284
  circuit switching, 313-314
  packet switching, 312-313
WAP, 305
wireless technologies
  802.11 wireless standard, 299-301
  Bluetooth, 298-299
  BYOD policies, 302-303
  DSSS, 300
  encryption, 299
  FHSS, 300
  frequency bands, 301
  hotspots, 302-303
MIMO, 301
MU-MIMO, 301
OFDM, 300
smartphones, 302-303
spreading codes, 300
SSID, 299
tables, 302-303
WAP, 299
WEP, 299-301
wireless networking card, 299
WPA, 299
WLAN, 322
WPAN, 284
NIDS (Network-based Intrusion Detection Systems), 310
NIST (National Institute of Standards and Technology), 37
CSF, 111
penetration testing, 417-418
SDLC, waterfall model, 200-201
  development phase, 204-208
  disposal phase, 211
  implementation phase, 208-209
  initiation phase, 202-204
  operation/maintenance phase, 210
NOC (Net Present Value), ROI, 192
nonstatistical sampling, 51

O

objectives/culture of projects (project management), 189
observation, application controls, 244, 248
OBS (Object Breakdown Structure), project management, 189
occurrence (rates of), ARO and quantitative risk analysis, 85
OFDM (Orthogonal Frequency-Division Multiplexing), 300
Office Space, 412
offsite storage (backups), 167
OLA (Operating Level Agreements), 215
one-to-many search process. See identification
one-to-one checking (data file controls), 242
one-to-one search process. See authentication
online auditing (continuous), 247-249
online data integrity (data integrity controls), 245
onsite storage (backups), 167
OOSD (Object-Oriented System Development), 220
open Wi-Fi, data breaches, 377
OpenID, SOA, 344
operation/maintenance phase (NIST SDLC), 210
patch management, 210
review process, 211
vulnerability assessments, 210
operational audits, 40
operational interruptions, BCP recovery strategies, 149
opinions (audit reports), 52, 58
optimizing processes, 121
PDCA method, 123-125
Taguchi method, 122-125
organizational forms (project management), 188-189
organizational risks, quantitative risk analysis, 85
organizations
accountability, 95
expectations of, 95
OS (Operating Systems), 275-276
encryption, 393
hardening, 392
log security, 393
password security, 393
patch security, 393
secondary storage, 277
security, 391-393
technical controls (security controls), 391-393
user account security, 393
utility software, 277
virtual memory, 277
vulnerability assessments, security, 393
OSI (Open Systems Interconnection) reference model, 286
application layer, 287
data link layer, 289
directory services, 291
encryption, 367-368
file sharing services, 290
HTTP, 292
IP address verification services, 290
IP email services, 290
management services, 291
monitoring services, 290
network layer, 288
physical layer, 289
presentation layer, 287
print services, 291
processing data, 289-290
protocol analysis services, 290
session layer, 288
TCP/IP model versus, 292
transport layer, 288
OSPF (Open Shortest Path First), 295
OSSTMM (Open Source Security Testing Methodology Manual), penetration testing, 417
outages, BCP, 158
output controls (business process controls), 242
output/input controls, 205
outsider fraud risk factors (problem/incident management), 419-420
outsourcing, 214. See also vendors
  BPA, 215
  contract management, 127-128
  ISA, 215
  MOU, 215
  OLA, 215
  performance monitoring, 128
  relationship management, 129-130
  third-party audits, 126-127
  third-party outsourcing, 125-126
  UA, 215
oversight boards (project management), 188
oversubscription, disaster recovery planning, 163
OWASP top 10 security concerns, 393
ownership, authentication by, 338

P

Pac-Man, 412
packet filtering, firewalls, 307-308
packet switching, 312-313
PAN (Personal Area Networks), 284
parallel operation
  application testing, 246
  changeover techniques, 209
parallel simulations, 52, 246
parallel testing, 207
parity checking (data file controls), 242
passive discovery stage (penetration testing), 417
passwords
  as authorization control, 238
  brute-force attacks, 413
  changing, 337
  clipping levels, 379
  comparative analysis, 412
  complexity of, 337
  cracking programs, 412-413
  dictionary attacks, 412
  dual-factor authentication, 93
  good password characteristics, 337
  hybrid attacks, 412-413
  John the Ripper, 413
  lockout thresholds, 337-379
  OS security, 393
  password controls (business process controls), 242
  rainbow tables, 413
  thunder tables, 413
  verification policies, 337
  weak passwords, 378
patches
  managing, 210
  OS patching, 393
  unpatched systems, 378
pattern-matching (signature) IDS, 311
payback analysis, 211
payback period (ROI), 192
PBX (Private Branch Exchange) systems, voice communication security, 357
PCI (Payment Card Industry) standards, 35-36, 119
PCI-DSS (Payment Card Industry Data Security Standard), 370
PDCA (Plan-Do-Check-Act) process optimization technique, 123-125
Pearson IT Certification website, 438
Pearson Test Prep software, 437, 442
  offline access, 438-439
  online access, 438-439
practice exams
  customizing, 439-440
  Flash Card Mode, 439
  Practice Exam Mode, 439
  Study Mode, 439
  updating, 440
Premium Edition, 440
website, 438
PEM (Privacy Enhanced Mail), 255
penetration testing, 416-418
performance
  assessments, employee management, 101
capacity planning
  cloud providers, 318
  flow analysis, 315
  load balancing, 318
  network analyzers, 316-317
  network cabling, 320-322
  network design, 318-319
  SNMP, 315
  utilization reports, 315-317
  vendors, 318
  Windows Performance Monitor, 315
  wireless systems, 322-323
monitoring, 128-130
  systems performance monitoring
    cloud providers, 318
    flow analysis, 315
    load balancing, 318
    network analyzers, 316-317
    network cabling, 320-322
    network design, 318-319
    SNMP, 315
    utilization reports, 315-317
    vendors, 318
    Windows Performance Monitor, 315
    wireless systems, 322-323
perimeter security control
  bollards, 350
  CCTV systems, 352, 355-356
  dogs, 351
  entry points, 351
  fences, 349-350
  gates, 350
  guards, 352
  HVAC, 356
  lighting, 351, 354
  locks, 353-354
  turnstiles, 352
personal data, classifying, 97
PERT (Program Evaluation and Review Technique), 197-198
PGP (Pretty Good Privacy), 255, 369
phased changeover (changeover techniques), 209
PHI (Protected Health Information),
  data classification, 97
phishing, 400
phreakers, 356, 419
physical layer (OSI reference model), 289
physical/environmental access control
  bollards, 350
  CCTV systems, 352, 355-356
dogs, 351
  entry points, 351
  fences, 349-350
  gates, 350
  guards, 352
HVAC, 356
  lighting, 351, 354
  locks, 353-354
  turnstiles, 352
PIA (Privacy Impact Analysis), 372
picking locks, 354
PII (Personal Identifiable Information), data classification, 97
pilot changeover (changeover techniques), 209
pilot testing, 207
pineapples (Wi-Fi), 376
ping, 290
ping of death, 402
PKI (Public Key Infrastructure), 365-366
plaintext (encryption), 358, 374
planning audits. See also audit universes
planning phase (project management)
  CPM, 198
  scheduling tasks, 197-198
  software
    costs, 193-194
    size, 195-196
timebox management, 199
planning stage (penetration testing), 417
plenum-grade cabling, 321
pod slurping, 376
point-in-time backups, 169
policy development (IT governance), 90
  advisory policies, 91
  auditing, 94-96
  baselines, 92-96
  bottom-up policy development, 91
data classification, 96-98
  defining policies, 91
documentation, 92
  informative policies, 92
  procedures, 92-96
  regulatory policies, 91
  security policies, 98-99
  standards
    auditing, 94-96
documentation, 92
  supporting policies, 77
  top-down policy development, 91
POP (Post Office Protocol), 255
POP3 (Post Office Protocol), 291, 297
ports
  common port numbers, 297
  mirroring, 317
  USB ports (uncontrolled), data breaches, 377
post-implementation phase (project management), 252
POTS (Plain Old Telephone Service), 314
power supplies, UPS, 171
PPTP (Point-to-Point Tunneling Protocol), 293, 348
practice exams
customizing, 439-440
  Flash Card Mode, 439
  Practice Exam Mode, 439
  Study Mode, 439
  updating, 440
pre-disaster planning. See problem/incident management

preparedness tests, BCP, 155-156

preparing for CISA exams
chapter-ending review tools, 441
DITKA questions, 442
memory tables, 441-442
Pearson Test Prep software, 437, 442
  customizing exams, 439
  customizing practice exams, 440
Flash Card Mode, 439
offline access, 438-439
online access, 438-439
Practice Exam Mode, 439
Premium Edition, 440
Study Mode, 439
updating exams, 440
website, 438
review questions, 442

presentation layer
  BI data architectures, 256
  OSI reference model, 287
pretexing attacks, 400

prevention/detection tools/techniques
  attack-detection tools, 414
  audit-reduction tools, 415
  integrity checks, 414
  log reviews, 414-415
  NAC, 415
  NetFlow, 415
  security testing, 416-418
  SIEM, 415
  trend-detection tools, 414
  variance-detection tools, 414

preventive controls, 47, 143

PRI (Primary Rate Interface), ISDN, 314

primary keys (ERD), 203

principle of least privilege (security policies), 99
print services, OSI reference model, 291
printing controls (business process controls), 242
privacy controls, 372
private clouds, 216
private key encryption
  3DES, 359
  AES, 362
  Blowfish, 359
  DES, 359-361
  RC4, 360
  RC5, 360
  Rijndael, 360-362
  SAFER, 360

privileges
  escalation of privileges, virtualization, 222
  principle of least privilege, security policies, 99
  security policies, 99

PRM (Performance Reference Model), FEAF, 112

problem/incident management
  change management, 418
  computer crime jurisdictions, 429
  criminal hackers, 419
  fraud risk factors, 419-420
  hackers, 419
  incident response
    defining incidents, 422
    documentation, 421, 424
    escalation/response procedures, 424
    event analysis, 422
    forensic investigation, 425-428
    honeypots, 422
incident response teams, 420-422
processes/procedures, 422-424
phreakers, 419
prosecuting computer crime, 429
script kiddies, 419
terrorists, 420
procedures
documentation, 92
IT governance, 93
policy development, 93
processes
IT governance, defining supporting processes, 77
optimization techniques, 121
PDCA method, 123-125
Taguchi method, 122-125
processing controls (business process controls)
data integrity controls, 240-241edit controls, 239
program change documents, 243
programmed application controls. See automation, application controls
programming controls (data integrity controls), 240
project management
attributes of projects, 187
closing phase, 199
constraints of, 187, 192
control/execution phase, 199
cost, 187
critical tasks, 198
culture/objectives, 189
design/development, 251
feasibility, 251
gap analysis, 192
implementation phase, 251
initiation phase, 193
investment in projects
business case analysis, 190
feasibility studies, 191
ROI, 191
objectives/culture, 189
OBS, 189
organizational forms, 188-189
oversight boards, 188
planning phase
CPM, 198
scheduling tasks, 197-198
software costs, 193-194
software size, 195-196
timebox management, 199
post-implementation phase, 252
project managers, 188
QA, 188
requirements, defining, 251
responsibilities in, 188-189
roles in, 188-189
scope, 187, 192
scope creep, 204
security requirements, 191
senior management, 188
software acquisition process, 251
sponsors, 188
stakeholders, 188
steering committees, 188
structure of, 188-189
system change procedures, 252
systems controls, 250-251
teams, 188
testing, 251
time, 187
WBS, 190
prosecuting computer crime, 429
protocol decoding IDS, 312
protocols
- analyzing, OSI reference model, 290
- network protocols, 285-286

prototyping, 212
proxies, 307
public clouds, 216
public key encryption
- digital signatures, 365
- ECC, 363
- hashing, 364
- PKI, 365-366
- quantum cryptography, 364
- RSA, 363
- trap door functions, 362

QA (Quality Assurance), 56-57
- project management, 188
- quality assurance employees, 104
qualified opinions (audit reports), 58
qualitative analysis, risk assessment, 86-87
qualitative judgments, risk assessment, 43
quality assurance, systems controls, 250-251
quality management
- CMM, 116-119
- COSO, 115-116
- ISO, 114-115
quantitative analysis, risk assessment, 42-43, 84-87
quantum cryptography, 364
questions
- CISA exams, format of, 14-15
- DITKA questions, final exam preparation, 442
- review questions, final exam preparation, 442

RA (Registration Authorities), PKI, 366
RAD (Rapid Application Development), 212
RADIUS (Remote Access Dial-In User Service), 345-346
RAID (Redundant Array of Independent Disks), 164-165
rainbow tables, 413
RAM (Random Access Memory)
- lookup tables, 304
range checks (edit controls), 239
ransomware, 395
rates of occurrence, ARO and quantitative risk analysis, 85
rating audit reports, 59
RC4 (Rivest Cipher 4) encryption, 360
RC5 (Rivest Cipher 5) encryption, 360
RDMS (Relational Database-Management Systems), 281
reasonableness checks (edit controls), 239
reasonableness verification (data integrity controls), 240
recalculations (manual), data integrity controls, 240
reciprocal agreements, disaster recovery planning, 162-163
reconciliation audits, employee management, 106
reconciliation of file totals (data integrity controls), 241
recovery planning
- alternate processing sites, 160
  - cold sites, 161
  - hot sites, 160
  - mobile sites, 160
  - oversubscription, 163
reciprocal agreements, 162-163
subscription services, 160, 163
warm sites, 161
alternative processing agreements, reviewing, 171
BCP, 142

core processes, 158
corrective controls, 143
damage assessment teams, 153
detective controls, 143
development phase, 149-150
discretionary processes, 159
damage assessment teams, 153
detective controls, 143

damage assessment teams, 153
detective controls, 143
development phase, 149-150
discretionary processes, 159
emergency management teams, 153
emergency operations teams, 154
emergency response teams, 153
final plan design, 151-152
finance teams, 154
impact analysis phase, 144-149
implementation phase, 151-156
incident response teams, 153
initiation phase, 143
interruptions, 149-150
maintenance phase, 156
maximum acceptable outages, 158
maximum tolerable outages, 158
metrics, 157-158
monitoring phase, 156
preventive controls, 143
project management, 143
recovery strategies, 149-150
recovery test teams, 154
relocation teams, 154
responsibilities, 152-153
reviewing results, 157-158
reviewing tasks, 170
RPO, 157
RTO, 157-159
salvage teams, 153
SDO, 158
security teams, 154
supplies teams, 154
supporting processes, 158
team responsibilities, 143
testing phase, 153-156
training and awareness, 152-153
transportation teams, 154
verifying tasks, 170
WRT, 158
contracts, reviewing, 171
COOP websites, 172
data recovery, 165-169
disaster life cycle, 172-173
disaster recovery checklist, 172
hardware recovery
cluster, 164
fault tolerance, 164
MTBF, 163
MTTF, 163
MTTR, 164
RAID, 164-165
SLA, 164
incident classification, 141-142
insurance, reviewing, 171
MTD, 159
natural disasters, 140
power supplies, 171
recovery times, 161-162
redundant processing sites, 160
reviewing tasks, 170
telecommunications recovery, 169-170
verifying tasks, 170
recovery test teams (BCP), 154
recovery times, disaster recovery planning, 161-162
red team activities. See penetration testing
reducing risk (risk management), 44
redundancy, telecommunications recovery, 169
redundant processing sites, 160
reengineering, 213
referential data integrity (data integrity controls), 245
registering for CISA exams, 7
regression testing, 207
regulatory compliance risk assessments (audit universes), 236
regulatory policies, 91
regulatory standards
  compliance with, 38
  knowledge of, 35-36
relational data integrity (data integrity controls), 245
relations (databases), 278
relationship management (contractors/IT suppliers/vendors), 129, 130
relocation teams (BCP), 154
remanence (data), VM, 222
remote access
  Diameter, 346
  encryption, 347
  RADIUS, 345-346
  risks of, 347
  security, 396
  TACACS, 346
  VPN, 347-348
repeaters, 303
reporting stage (penetration testing), 417
reports
  audit reports, 49, 57
  opinions, 52-53, 58
  rating, 59
  writing, 53-54
before-and-after image reports, 242
distribution on (application controls), 244
exception reports, 106, 241
financial reports, COSO, 35
maintenance error reports, 242
transaction logs, 242
residual risk, 42
restoring data, 302
retaking CISA exams, 16
reverse engineering, 205
reviewing projects, 211
review questions, final exam preparation, 442
RFP (Requests for Proposal), 204
right-to-audit clauses, 127
Rijndael encryption, 360-362
ring topologies (networks), 319
RIP (Routing Information Protocol), 295
risk analysis, 44
risk assessment, 40
  audit risk, 42
  control risk, 41-42
  detection risk, 41-42
  information asset protection, 372
  inherent risk, 41
  material, defining, 41
  qualitative analysis, 86-87
  qualitative judgments, 43
quantitative analysis, 42-43, 87
  ALE, 85
  ARO, 85
costs of losses, 85-86
exposure factor, 84
organizational risks, 85
SLE, 85
stochastic events, 85
residual risk, 42
risk management
Basel III, 35
Coca-Cola, 43
ERM, 80
  asset identification, 82
  qualitative risk analysis, 86-87
  quantitative risk analysis, 84-87
  risk management teams, 81
  threat identification, 82-83
  Three Lines of Defense model, 87-89
lagging risk indicators, 120
leading risk indicators, 120
organizational risk, quantitative risk analysis, 85
risk acceptance, 45
risk analysis, 44
risk avoidance, 44
risk monitoring, 45
risk reduction, 44
risk, defining, 44
risk tolerance, 45-47
risk transference, 45
threats, defining, 44
risk thresholds, performance management, 109
Rivest, Ron, 363
RMON (Remote Network Monitoring), 290
ROI (Return on Investment), 191, 211
rotating jobs, employee management, 106
rotation of assignments (employee management), 102, 107
rounding-down attacks, 412
routing, 304-305
  protocols, 294-295
  telecommunications recovery, 170
Royce, W.W., 200
RPO (Recovery Point Objectives), BCP, 157
RSA (Rivest, Shamir, Adleman) encryption, 363
RTO (Recovery Time Objectives), BCP, 157-159
RUDY (R U Dead Yet?), 403
run-to-run totals (data integrity controls), 240

S

S/MIME (Secure/Multipurpose Internet Mail Extensions), 255, 369
SAFER (Secure and Fast Encryption Routine), 360
salami technique, 412
sales automation (CRM), 259
salvage teams (BCP), 153
SAML (Security Assertion Markup Language), SOA, 344
SAN (Storage Area Networks), 166, 285
  SCSI, 168
  snapshots, 169
  VSAN, 168
Sarbanes-Oxley Act (SOX), 4-5, 35, 119
satisfactory audit reports, 58
SCADA (U.S. Supervisory Controls and Data Acquisition), 35
SCARF/EAM (Systems Control Audit Review File/Embedded Audit Modules), continuous online auditing, 247
scheduling
  CISA exams, 6
tasks, project management, 197-198
schemas, 278
SCM (Supply Chain Management), BI, 259
scope of projects (project management)
  project management, 187, 192
  scope creep, 204
scores (CISA exams), getting, 15
screened host firewalls, 309
screened subnets, 309
script kiddies, 419
scripting, XSS attacks, 411
scrubbing locks, 354
scrum, software development, 213
SCSI (Small Computer System Interface), SAN, 168
SDLC (Systems Development Life Cycle)
  auditor’s role in, 249
BAD
    software development, 212-213
    systems-development methodology, 200-211
software development
  agile development, 213
  incremental development, 212
  prototyping, 212
  RAD, 212
  reengineering, 213
  scrums, 213
  spiral development, 212
  sprints, 213
  XP, 213
waterfall model, systems-development methodology, 200-201
  development phase, 204-208
  disposal phase, 211
  implementation phase, 208-209
  initiation phase, 202-204
  operation/maintenance phase, 210
SDO (Service Delivery Objectives), BCP, 158
secondary storage, virtual memory, 277
security
  architects, 104
  asynchronous attacks, 411
  backups, 395
  black-box testing, 409
  blogs, 397
  Bluetooth, 406
  botnets, 403-404
  brute-force attacks, 413
  buffer over flow attacks, 409
  bypass label processing, 414
  cloud computing, 219
  DAM, 394
databases, 408-409
  backups, 395
  DAM, 394
  EDR, 394
  OWASP top 10 security concerns, 393
  shadowing, 395
  WAF, 393
DDoS attacks, 402-403
dictionary attacks, 412
DoS attacks, 402-403
droppers, 405
dumpster diving attacks, 400
EDR, 394
e-mail attacks, 400
FIPS, 37
FISMA, 35, 120
fuzzing, 409
hijacking attacks, 401
HOIC, 403
hping, 403
hybrid attacks, 412-413
IM, 396-397
integer overflow attacks, 412
labels, bypassing, 414
log reviews/audits, 414-415
logic bombs, 411
LOIC, 403
malware, 404-405
message boards, 397
MITM attacks, 401
NIST, 37
OS, 391
  encryption, 393
  hardening OS, 392
  logs, 393
  passwords, 393
  patches, 393
  user accounts, 393
  vulnerability assessments, 393
OWASP top 10 security concerns, 393
passwords
  brute-force attacks, 413
  comparative analysis, 412
  cracking programs, 412-413
dictionary attacks, 412
hybrid attacks, 412-413
John the Ripper, 413
OS security, 393
  rainbow tables, 413
  thunder tables, 413
penetration testing, 416-418
phishing attacks, 400
ping of death, 402
policies, 98-99
pretexting attacks, 400
project management, 191
ransomware, 395
rounding-down attacks, 412
RUDY, 403
salami technique, 412
security teams (BCP), 154
slowloris, 403
smurfing attacks, 402
sniffing attacks, 400
social media, 397-398
social-engineering attacks, 399-400
spear phishing attacks, 400
spoofing attacks, 400
SQL injection attacks, 394, 408-409
syn flooding, 403
testing
  penetration testing, 416-418
  vulnerability scanning, 416
TOCTOU attacks, 416
trap doors, 411
Trojans, 405
virtualization, 395-396
viruses, 405
VM, hardening, 395
vulnerability scanning, 416
WAF, 393
WAP, 406-407
websites, 397
whaling attacks, 400
wireless networks, 406
worms, 405
wrappers, 405
XSRF attacks, 411
XSS attacks, 411
zero-day attacks, 404

**security controls**

administrative controls
  - blogs, 397
  - IM, 396-397
  - message boards, 397
  - social media, 397-398
  - websites, 397

encryption
  - 3DES, 359
  - AES, 362
  - algorithms, 358
  - asymmetric encryption, 358-359, 362-366
  - Atbash, 357
  - block ciphers, 361
  - Blowfish, 359
  - Caesar’s cipher, 357
  - ciphertext, 358
  - cryptanalysis, 358
  - cryptography, 358, 363-364, 367-368, 374-375
  - data breaches, 374-375
  - DES, 359-361
  - digital signatures, 365
  - ECC, 363
  - end-to-end encryption, 368
  - hashing, 364
  - key length, 358
  - link-state encryption, 368
  - multiple encryption, 361
  - OSI reference model, 367-368
  - PKI, 365-366
  - plaintext, 358
  - private key encryption, 359-362
  - public key encryption, 362-366
  - quantum cryptography, 364
  - RC4, 360
  - RC5, 360
  - Rijndael, 360-362
  - RSA, 363
  - SAFER, 360
  - stream ciphers, 361
  - symmetric encryption, 358-362, 367-368

hardware, voice communications, 356-357

information asset protection, 372

software
  - encryption, 357-368
  - voice communications, 356-357

technical controls
  - cloud computing, 391
  - databases, 393-395
  - OS, 391-393
  - virtualization, 395-396

voice communications
  - PBX systems, 357
  - phreakers, 356
  - VoIP, 357

security teams (BCP), 154

semi-quantitative analysis (qualitative risk analysis), 87

senior management (project management), 188

separating duties (application controls), 244

separation events (termination), 102-103

sequence checks (edit controls), 239
servers
certificate servers, PKI, 366
clustering, hardware recovery, 164
virtual servers, 221, 395-396

service management frameworks
COBIT, 273-274

databases
ACID tests, 282
aggregation, 278
attributes, 278
CRM, 279
data integrity, 281
data mining, 278
data warehouses, 279
database-management systems, 278-281
fields, 278
foreign keys, 278
granularity, 278
HDMS, 279
metadata, 278
NDMS, 279
RDMS, 281
relations, 278
schemas, 278
tuples, 281

DRM, 283
eTOM, 273-275
FitSM, 273-274
ISO 20000, 273-274
ITIL, 273
OS, 275-277
software licensing
EULA, 282
illegal software, 283

services
SOA, 344-345
SPML, 344

session layer (OSI reference model), 288
SET (Secure Electronic Transaction), 368
shadowing databases (standby), 169
Shamir, Adi, 363
shared cost corporate structures, 77
sharing files, OSI reference model, 290
Shewart, Walter A., 123
Shibboleth, SOA, 344-345
Shodan, 420
short-term business goals, defined, 237
shrink-wrap license agreements, 186
SIEM (Security Information and Event Management), 394, 415. See also DAM
signatures
as authorization control, 238
digital signatures, 365
simple backup rotation method, 167
site-to-site VPN, 348
size of software (project management, planning phase), 195-196
skills (work-related) for IS auditing, 27-28
SLA (Service Level Agreements), 127-128, 164
SLE (Single Loss Expectancy)
BIA criticality analysis, 147
quantitative risk analysis, 85
SLOC (Source Lines of Code), software size estimation, 195
slowloris, 403
smartphones/tablets, 302-303, 377
SMTP (Simple Mail Transfer Protocol), 255, 290
smurfing attacks, 402
snapshots
application testing, 246
continuous online auditing, 248
SAN, 169
sniffing attacks, 400
SNMP (Simple Network Management Protocol), 291, 315
SOA (Service-Oriented Architectures)
  OpenID, 344
  SAML, 344
  Shibboleth, 344-345
  SPML, 344
  WAYF, 345
  WS Security, 344
  XML, 344
sociability testing, 207
social media
  BI, 260
  security, 397-398
social-engineering attacks, 399-400
SoD (Segregation of Duties), employee management, 105-107
soft skills, IS auditing, 27
software
  acquisition process (project management), 251
  antivirus software, virtualization, 395
  buffer overflow attacks, 409
  COCOMO II software estimation, 194
  costs of (project management, planning phase), 193-194
  data recovery, 165-169
  development tools/methods
    agile development, 213
    incremental development, 212
    prototyping, 212
    RAD, 212
    reengineering, 213
    scrums, 213
    spiral development, 212
    sprints, 213
    XP, 213
  escrow agreements, 185
  forensics, 427
  licensing, 185
    click-wrap agreements, 186
    DMCA, 186
    EULA, 282
    illegal software, 283
    master agreements, 186
    shrink-wrap agreements, 186
  malicious software, 379
  malware, 404-405
  Pearson Test Prep software, 437, 442
    customizing practice exams, 439-440
    Flash Card Mode, 439
    offline access, 438-439
    online access, 438-439
    Practice Exam Mode, 439
    Premium Edition, 440
    Study Mode, 439
    updating practice exams, 440
    website, 438
  ransomware, 395
  security controls
    encryption, 357-368
    voice communications, 356-357
  size estimation (project management, planning phase), 195-196
  utility software, 277
somewhere you are systems, authentication by, 340
SOX (Sarbanes-Oxley) Act, 4-5, 35, 119
spear phishing, 400
spiral software development, 212
SPML (Service Provisioning Markup Language), SOA, 344

sponsors
   project management, 188
   sponsor pays corporate structures, 77

spoofing attacks, 400

spreading codes, 300

sprints, software development, 213

SQL injection attacks, 394, 408-409

SRM (Security Reference Model), FEAF, 112

SSAE 16 (Statement on Standards for Attestation Engagements 16) assessments, 127

SSAE 18 (Statement on Standards for Attestation Engagements 18) assessments, 127

SSH (Secure Shell), 291, 347, 368

SSID (Service Set ID), 299

SSL (Secure Sockets Layer), 348

SSO (Single Sign-On), 340
   advantages of, 341
   Kerberos, 341-342

stakeholders (project management), 188

standards
   documentation, 92
   IT governance, 92
   networks, 285-286
   policy development, 92
   SSAE 16, 127
   SSAE 18, 127

standby database shadowing, 169

star topologies (networks), 319

stateless connections, 292

static data (data categories), 241

static forensic analysis, 428

statistical sampling, 51

steering committees (project management), 188

stochastic events, 85

stolen/lost smartphones/tablets, 302

stop-and-go sampling, 52

storage
   backups
      electronic vaulting, 169
      grandfather-father-son rotation method, 168
      location redundancy, 168
      media-rotation strategies, 167-168
      offsite storage, 167
      onsite storage, 167
      security, 169
      simple rotation method, 167
      standby database shadowing, 169
      testing, 167

      Tower of Hanoi rotation method, 168

   offsite storage, 167
   onsite storage, 167
   storage cards, smartphones/tablets, 302

store-and-forward switches, 304

stream ciphers, 361

striping, RAID, 164-165

Study Mode (practice exams), 439

subnets, 293, 309

subscription services, disaster recovery planning, 160, 163

substantive tests, 39, 45

Summary view (Wireshark), 316

Superman III, 412

superusers (privileged accounts), 99

supervisor reviews, employee management, 106

supplies teams (BCP), 154

supply chains, managing. SCM, 259
### supply interruptions, BCP recovery strategies
- BCP recovery strategies, 149

### supporting processes, BCP
- BCP, 158

### SURRE rule, evidence handling
- Evidence handling, 49

### switches
- Switches, 304-305

### symmetric encryption
- Symmetric encryption, 358, 367-368
  - 3DES, 359
  - AES, 362
  - Blowfish, 359
  - DES, 359-361
  - RC4, 360
  - RC5, 360
  - Rijndael, 360-362
  - SAFER, 360

### syn flooding
- SYN flooding, 403

### systems
- Administrators, 104
- Alternative system development
  - **CBD**, 220
  - **Cloud computing**, 216-219
  - **DOSD**, 219
  - **n-tier**, 220-221
  - **OOSD**, 220
  - **outsourcing**, 214-215
  - **virtualization**, 221-222
  - **WBAD**, 220
- Analysts, 104
- Change procedures (project management), 252
- Controls
  - Parameters (data categories), 241
  - Project management, 250-251
  - Quality assurance, 250-251
  - SDLC, auditor’s role in, 249
- Copy software entries here, 186
- Performance monitoring
  - **cloud providers**, 318
  - Flow analysis, 315
  - **load balancing**, 318
  - **network analyzers**, 316-317
  - **network cabling**, 320-322
  - **network design**, 318-322
  - **SNMP**, 315
  - **utilization reports**, 315-317
  - **vendors**, 318
  - **Windows Performance Monitor**, 315
  - **wireless systems**, 322-323
- Testing, 206

### T
- **T-carriers**, 314
- Table lookups (edit controls), 240
- Tables
  - Database tables, 241-242
  - Memory tables, final exam preparation, 441-442
  - Rainbow tables, 413
  - Thunder tables, 413
- Tablets/smartphones, 302-303
- **TACACS** (Terminal Access Control Access Control System), 346
- Tagging (application testing), 246
- Taguchi process optimization technique, 122-125
- Tape backups, 166
- Tape librarians, 167
- Target values (performance management), 108
- **TCO** (Total Cost of Ownership), ROI, 192
- **TCP** (Transmission Control Protocol), 288, 295
- TCP/IP reference model
  - Application layer, 296-297
  - **DHCP**, 297
  - **DNS**, 297, 312
DNSSEC, 297
host-to-host/transport layer, 295
Internet layer
  distance-vector protocols, 295
  IP addressing, 293-294
  link-state routing protocols, 295
  routing protocols, 294-295
network access layer, 292-293
OSI model versus, 292
teams (project management), 188
technical controls (security controls)
  cloud computing, 391
databases, 393-395
OS, 391-393
virtualization, 395-396
telecommunications recovery, 169-170
Telnet, 291, 347
tension wrenches, picking locks, 354
termination (separation events), 102-103
terrorists, incident/problem management, 420
TES (Terminal-Emulation Software), 291
testing
  ACID tests, 245
  alpha testing, 207
  application controls, 244, 248
  applications, 246-249
  backups, 167
  BCP, 153-154
    full operation tests, 156
    paper tests, 155
    preparedness tests, 155-156
  beta testing, 207-209
  black-box testing, 207, 409
  bottom-up testing, 206
  CISA tests
    applying for certification, 8
    CBT, 13
    CPE, 16-18
    credit tracking, 16-17
    exam domains, 10-13
    getting scores, 15
    grading exams, 13
    importance of certification, 4-5
    intent of, 3-4
    ISACA agreements, 9-10
    maintaining certification, 16
    mission statement, 3
    passing, 9
    Pearson Test Prep software, 437-442
    popularity of, 5
    question formats, 14-15
    registering for exams, 7
    requirements for, 6-8
    retaking, 16
    scheduling exams, 6
    strategies for, 18-19
    tips/tricks, 18-19
    work experience waivers, 8
  compliance tests, 39
  final acceptance testing, 206
  function testing, 207
  integrated testing facilities
    application testing, 246
    continuous online auditing, 247
  interface testing, 206
  ITF, 52
  parallel testing, 207
  Pearson Test Prep software, 437, 442
    customizing practice exams, 439-440
    Flash Card Mode, 439
    offline access, 438-439
online access, 438-439
Practice Exam Mode, 439
Premium Edition, 440
Study Mode, 439
upating practice exams, 440
website, 438
pilot testing, 207
practice tests
customizing, 439-440
Flash Card Mode, 439
Practice Exam Mode, 439
Study Mode, 439
upating, 440
project management, 251
regression testing, 207
security
penetration testing, 416-418
vulnerability scanning, 416
socialability testing, 207
substantive tests, 39, 45
system testing, 206
top-down testing, 206
UAT, 207-209
unit testing, 206
walk-through testing, 155
white-box testing, 207
text messaging, pretexting attacks, 400
third-party audits, 94-96, 126-127
third-party monitoring, 318
third-party outsourcing, 125-126, 214-215
third-party vendors, capacity planning, 318
threat analysis, ARO and BIA criticality analysis, 147
ThreatExpert, dynamic forensic analysis, 427
threats
categorizing, 83
defining, 44, 83
identifying (ERM), 82-83
losses and, 83
risk management, defining, 44
vulnerabilities and, 83
Three Lines of Defense model (ERM), 87-89
thresholds (performance management), 109
thumb drives, data breaches, 375
thunder tables, 413
time, project management, 187, 192
critical tasks, planning, 198
scheduling tasks, 197-198
timebox management, project management, 199
TLS (Transport Layer Security), 348
TOCTOU (Time-Of-Check, Time-Of-Use) attacks, 411
Token Ring protocol, 293
tokenization, 219. See also encryption
tokens, authentication by, 338
tolerating risk (risk management), 45-47
top-down policy development (IT governance), 91
top-down testing, 206
total document numbers (batch controls), 238
total dollar amounts (batch controls), 238
total item counts (batch controls), 238
Tower of Hanoi backup rotation method, 168
ttraceroute, 290
tracing (application testing), 246
tracking changes, 418
traffic monitoring, add capacity planning entries, 316
training
  BCP, 152-153
  cloud computing, 218
  employees, 101, 107
transaction files (data categories), 241
transaction logs, 106, 242
transaction selection (application testing), 246
transferring
  data, 302
  risk (risk management), 45
transmission controls (EDI), 254
transport layer (OSI reference model), 288
transport/host-to-host layer (TCP/IP reference model), 295
transportation teams (BCP), 154
trap door functions, public key encryption, 362
trap doors, 411
trend-detection tools, 414
Trojans, 405
tubular locks, 353
tumbler locks, 353
tunneling, 348
tuples (databases), 281
turnstiles (access control), 352
twisted-pair cabling, 321	two-factor authentication, 338

U

U.S. government laws/regulations
  FACTA, 35, 120
  FIPS, 37
  FISMA, 35, 120
  HIPAA, 35, 119
  NIST, 37
  SCADA, 35
  SOX, 35, 119
  UA (Uptime Agreements), 215
  UAT (User Acceptance Testing), 207-209
  Ubertooth, 406
  UDP (User Datagram Protocol), 288, 295
  unauthorized changes, information systems maintenance, 214
  unicast addresses, 294
  unit testing, 206
  units (performance management), 108
  unpatched systems, 378
  unqualified opinions (audit reports), 58
  unrated audit reports, 58
  unsatisfactory audit reports, 58
  unsecured devices, data breaches, 375-378
  untied websites, 397
  updating practice exams, 440
  UPS (Uninterruptible Power Supplies), 171
  USB drives, data breaches, 375
  USB Killer, 375
  USB ports (uncontrolled), data breaches, 377
  USB Rubber Ducky, 376
user location systems. See somewhere you are systems
users
  access control
    authentication, 336-345
    exterior security control, 349-356
    Federation, 343-345
    identification, 336
    perimeter security control, 349-356
physical/environmental access control, 349-356
remote access, 345-348
SSH, 347
SSO, 340-342
Telnet, 347
BYOD policies, data breaches, 377-378
CRM, BI, 258
customer service (CRM), 259
identification as authorization control, 238
logic bombs, 411
security, 393
user accounts, 393
utility software, 277
utilization reports, capacity planning, 315-317

V

vacations (forced), 102, 107
validity checks (edit controls), 239
variable sampling, 52
variance-detection tools, 414
vaulting (electronic), 169
vendors. See also outsourcing
accountability, 95
auditing, 94-96
BPA, 215
capacity planning, 318
eXpectations of, 95
ISA, 215
MOU, 215
OLA, 215
outsourcing, 214-215
quality of, 95
relationship management, 129-130
RFP, 204
UA, 215
ventilation (data centers), 356
verification
BCP tasks, 170
conformity, 39
disaster recovery tasks, 170
IP addresses, 290
key verification (edit controls), 240
passwords, 337
reasonableness verification (data integrity controls), 240
regulatory compliance, 38
virtual memory, 277
virtual servers, 221
virtualization
application development, 221-222
authentication, 395
everification, 395
fabric virtualization. See VSAN
physical controls, security, 395
remote access services, security, 396
resource access, security, 396
security, 395-396
servers, 395-396
technical controls (security controls), 395-396
VM escapes, 395
viruses, 405
VLAN (Virtual Local Area Networks), 304-305
VM (Virtual Machines), 221
data remanence, 222
escapes, 395
hardening, 395
live VM migration, 222
security, hardening, 395
voice communications
recovery, telecommunications recovery, 170
security controls
PBX systems, 357
phreakers, 356
VoIP, 357
VoIP (Voice over Internet Protocol), 295, 313, 357
VPN (Virtual Private Networks), 293, 347-348
VSAN (Virtual Storage Area Networks), 168
vulnerabilities
assessments, 210
defining, 83
OS vulnerability assessments, 393
scanning, 416
threats and, 83

W

WAF (Web Application Firewalls), 308, 393
walk-through testing, 155
WAN (Wide Area Networks), 284
circuit switching, 313-314
packet switching, 312-313
WAP (Wireless Access Points), 299, 305, 406-407
warded locks, 353
warehouses (data), 279
warm sites, disaster recovery planning, 161
WAYF (Where Are You From), SOA, 345
WBAD (Web-based Application Development), 220
WBS (Work Breakdown Structure), project management, 190
web pages, XSS attacks, 411
websites
Basel III, 35
COOP websites, 172
COSO, 35
FACTA, 35
FISMA, 35
HIPAA, 35
ISACA website
Code of Professional Ethics, 9-10
CPE policies, 16
credit tracking, 16-17
earning CPE hours, 17-18
ethics/standards/competency agreements, 9-10
getting CISA exam scores, 15
maintaining CISA certification, 16
My Certifications, 7, 15-17
registering for CISA exams, 7
reporting CPE hours earned, 16-17
laws/regulatory standards, 35
PCI standards, 35-36
Pearson IT Certification website, 438
Pearson Test Prep website, 438
SCADA, 35
security, 397
SOX, 35, 119
untied websites, 397
XSRF attacks, 411
WEP (Wired Equivalent Privacy), 299-301, 407
whaling, 400
white-box testing, 207
Wi-Fi
open Wi-Fi, data breaches, 377
pineapples, 376
Wigle, WAP security, 406
Windows Performance Monitor, 315
wireless networks, 406-407
wireless technologies
  802.11 wireless standard, 299-301
  Bluetooth, 298-299
  BYOD policies, 302-303
  DSSS, 300
  encryption, 299
  FHSS, 300
  frequency bands, 301
  hotspots, 302-303
  MIMO, 301
  MU-MIMO, 301
  OFDM, 300
  smartphones, 302-303
  spreading codes, 300
  SSID, 299
  tablets, 302-303
  WAP, 299
  WEP, 299-301
  wireless networking cards, 299
  WPA, 299
Wireshark, 316, 400
WLAN (Wireless Local Area Networks), 299-301, 322
work experience waivers, CISA certification, 8
worms, 405
WP (Work Papers), 50
  automated WP, 51
  leveraging WP, 54
WPA (Wi-Fi Protected Access), 299, 407
WPA2 (Wi-Fi Protected Access 2), 407
WPAN (Wireless Personal Area Networks), 284
wrappers, 405
wrenches (tension), picking locks, 354
writing audit reports, 53-54
WRT (Work Recovery Time), BCP, 158
WS Security (Web Services Security), SOA, 344

X
X.25, 313
X.509 standard, PKI, 366
XML (Extensible Markup Language), SOA, 344
XP (Extreme Programming) development model, 213
XSRF (Cross-Site Request Forgery) attacks, 411
XSS (Cross-Site Scripting) attacks, 411

Y-Z
Zachman, John, 112
zero-day attacks, 404