MICHAEL GREGG
ROB JOHNSON

Cert Guide

Learn, prepare, and practice for exam success

CISA®

Certified Information Systems Auditor®(CISA)

PEARSON IT
CERTIFICATION

Certified Information Systems Auditor® (CISA®) Cert Guide

Michael Gregg
Rob Johnson

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

Certified Information Systems Auditor® (CISA®) Cert Guide

ISBN-13: 978-0-7897-5844-6
ISBN-10: 0-7897-5844-X

Library of Congress Control Number: 2017950730

Printed in the United States of America

1 17

Trademarks

Warning and Disclaimer

Special Sales

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Acquisitions Editor
Michelle Newcomb

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Ken Johnson

Proofreader
The Wordsmithery LLC

Technical Editor
Chris Crayton

Publishing Coordinator
Vanessa Evans

Designer
Chuti Prasertsith

Compositor
Tricia Bronkella

Contents at a Glance

Table of Contents

About the Authors

Michael Gregg (CISSP, SSCP, CISA, MCSE, MCT, CTT+, 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 Dahlin, 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:

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN 9780789758446.
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 1. Go to www.PearsonTestPrep.com.

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 1. Register your book by going to PearsonITCertification.com/register and entering the ISBN **9780789758446**.

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.

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 4-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
Threats to Business Operations	1, 10
The Business Continuity Planning (BCP) Process	2–5
Recovery Strategies	6–9

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

Foundation Topics

Threats to Business Operations

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.

Key Topic

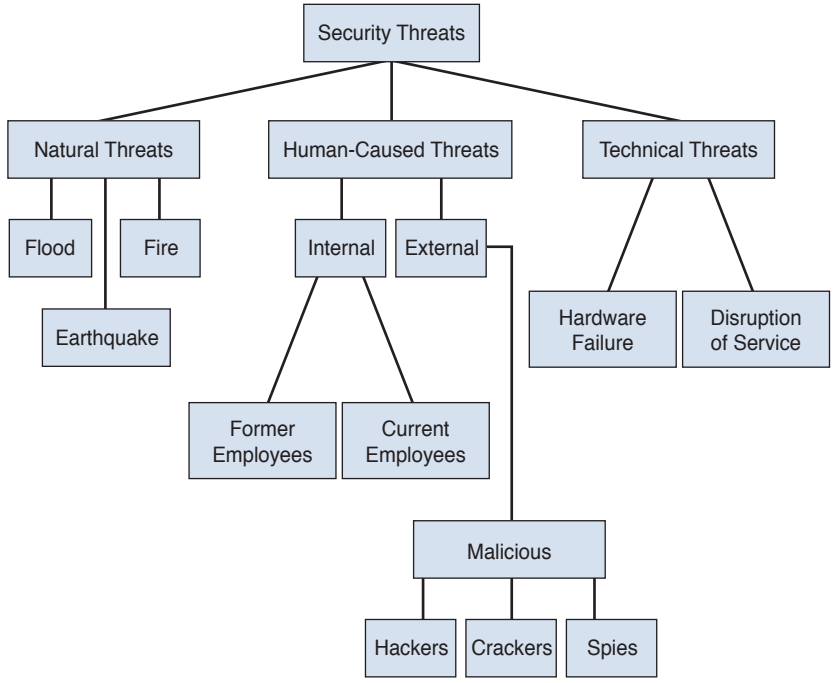

Figure 4-1 Sources of Security Threats

Answers to the "Do I Know This Already?" Quiz:

1. D; 2. B; 3. A; 4. C; 5. A; 6. A; 7. D; 8. C; 9. B; 10. C

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 4-2 Incident Classification

Level	Description
Crisis	A crisis is considered a major problem. It is of sufficient impact that it adversely affects the organization's ability to continue business functions.
Major	A major incident is of sufficient strength to negatively impact one or more departments, or it might even affect external clients.
Minor	Although these events are noticeable, they cause little or no damage.
Negligible	These detectable events cause no damage or have no longer-term effect.

NOTE Disruptive incients 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.

Key Business Process	Recovery Time Objective	Recovery Point Objective	Can This Be Performed Manually? For How Long?	Computer Systems/Applications Required to Perform This Process

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:

   Single loss expectancy = Asset value × 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:

   Annualized loss expectancy (ALE) =

   Single loss expectancy (SLE) × 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 4-3 System Classification

Classification	Description
Critical	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.
Vital	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.
Sensitive	Although these tasks are important, they can be performed manually at a reasonable cost. However, this is inconvenient and requires additional resources or staffing.
Noncritical	These services are not critical and can be interrupted. They can be restored later with little or no negative effects.

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 fist 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.

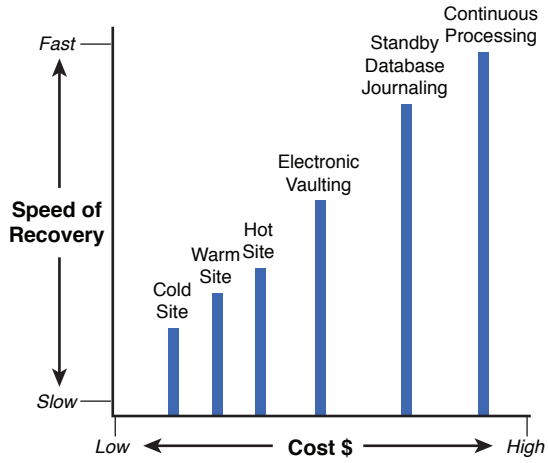

Figure 4-3 Recovery Options and Costs

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.

Key Topic

Table 4-4 BCP Process Responsibilities

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

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.

Key Topic

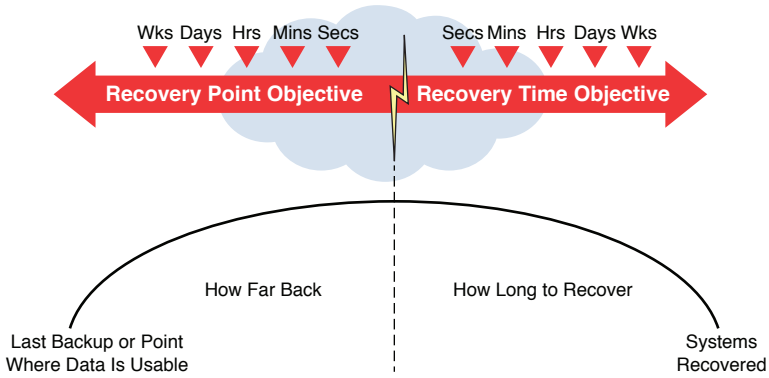

Figure 4-4 RPO and RTO

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

Item	Required Recovery Time
Critical	Minutes to hours
Urgent	24 hours
Important	72 hours
Normal	7 days
Nonessential	30 days

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.

NOTE 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 4-6 Examples of Functions and Recovery Times

Process	Recovery Time	Recovery Strategy
Database	15 minutes to 1 hour	Database shadowing at a redundant site
Applications	12–24 hours	Hot site
Help desk	24–48 hours	Hot site
Purchasing	24–48 hours	Hot site
Payroll	1–3 days	Redundant site

Process	Recovery Time	Recovery Strategy
Asset inventory	5–7 days	Warm site
Nonessential services	30 days	Cold site
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)	Hours to a few days	Mobile site

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

Key Topic

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.

- **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 offsite 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.

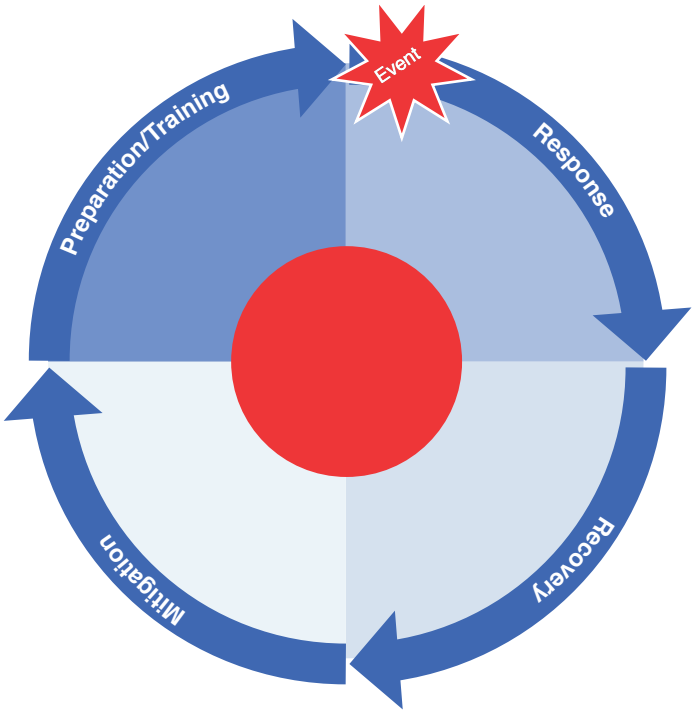

Figure 4-5 The Disaster Life Cycle

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

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

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.

Key Topic

Table 4-8 Key Topics in Chapter 4

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

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

- **The BIA process, according to NIST:** http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_bia_template.docx
- **RPO and RTO explained:** www.bluelock.com/blog/rpo-rto-pto-and-raas-disaster-recovery-explained/
- **BCP good practice guidelines:** www.drj.com/journal/fall-2013-volume-26-issue-4/the-bcis-good-practice-guidelines.html
- **Cloud backup and storage:** www.informationweek.com/consumer/online-backup-vs-cloud-storage/d/d-id/1107440
- **SLAs:** www.wired.com/insights/2011/12/service-level-agreements-in-the-cloud-who-cares/
- **Business Impact Analysis:** http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/business-impact-analysis.aspx
- **Exploring Backup Alternatives:** http://searchdatabackup.techtarget.com/feature/Modern-backup-alternatives
- **Auditing business continuity plans:** http://www.disaster-resource.com/index.php?option=com_content&view=article&id=1701:how-to-audit-business-continuity-programs

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y-Z