EXAM CRAM

The Smart Way to Study™

Updated for 2009

Exam **CISSP CBK**

CISSP

Second Edition

CD Features Test Engine
Powered by MeasureUp!

Michael Gregg

CISSP Exam Cram, Second Edition

International Standard Book Number: 0-7897-3806-6

ISBN-10: 0-7897-3806-6

ISBN-13: 978-0-7897-3806-6

Library of Congress Cataloging-in-Publication Data

Gregg, Michael (Michael C.)

CISSP exam cram / Michael Gregg.

p. cm.

ISBN 978-0-7897-3806-6 (pbk. w/CD)

1. Computer networks--Security measures--Examinations--Study guides. 2. Computer security--Examinations--Study guides. 3. Telecommunications engineers--Certification. I. Title.

TK5105.59.G7325 2009

005.8076--dc22

2009002001

Printed in the United States of America

First Printing: March 2009

12 11 10 09 4 3 2 1

Trademarks

Warning and Disclaimer

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

Bulk Sales

Publisher
Paul Boger

Acquisitions Editor
Betsy Brown

Senior Development Editor
Christopher Cleveland

Managing Editor
Patrick Kanouse

Project Editor
Jennifer Gallant

Copy Editor
Mike Henry

Indexer
Tim Wright

Proofreader
Matt Purcell

Technical Editor
Shawn Merdinger

Publishing Coordinator
Vanessa Evans

Book Designer
Gary Adair

Page Layout
Louisa Adair

Graphics
Macmillan India Limited

Introduction

Welcome to *CISSP Exam Cram*! This book covers the CISSP certification exam. Whether this is your first or your fifteenth *Exam Cram*, you'll find information here and in Chapter 1 that will ensure your success as you pursue knowledge, experience, and certification. This introduction explains the ISC^2 certification programs in general and talks about how the *Exam Cram* series can help you prepare for the CISSP exam.

This book is one of the *Exam Cram* series of books and will help by getting you on you way to becoming an ISC^2 Certified Information Systems Security Professional (CISSP).

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

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

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

How to Prepare for the Exam

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

- The ISC^2 website at www.isc2.org
- The study guide available at the ISC^2 website
- The CISSP open study guide website at www.cccure.org

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

Practice Tests

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

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

This book contains questions at the end of each chapter and includes two full-length practice tests. However, if you still want more, a related *Exam Cram CISSP Practice Questions* book has more than 500 additional questions. The questions are in paper form so that you can practice in an environment similar to the real exam; they are also available electronically as a practice test CD in the back of the book. Many other companies provide CISSP certification practice tests as well.

Taking a Certification Exam

When you have prepared for the exam, you must register with ISC^2 to take the exam. The CISSP exam is given throughout the year at various locations. You can find the latest schedule at https://www.isc2.org/cgi-bin/exam_schedule.cgi?displaycategory=1182. Many people decide to travel to the exam location; others wait until it is given at a location closer to them. ISC^2 has implemented regional pricing: As an example, early registration is $499 in the United States, compared to standard registration of $599. Check the ISC^2 website at https://www.isc2.org/uploadedFiles/Downloads/exam_pricing.pdf to get specific details.

You can register for an exam done online, by mail, or by fax. The online form is available at https://www.isc2.org/certification-register-now.aspx. After you register, you will receive a confirmation notice.

Arriving at the Exam Location

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

EXAM ALERT

You'll be spending a lot of time in the exam room. The total test time is 6 hours, so eat a good breakfast and take a snack and bottle of water with you to the testing area. Policies differ—some locations might allow you to take the water and energy bar to your desk whereas others might make you place it at the back of the testing area.

In the Exam Room

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

After the Exam

Examination results are not available after the exam. You must wait up to 4–6 weeks to get your results by email or snail mail. Most individuals receive these rather quickly within 4 weeks or so. If you pass the exam, you will simply receive a passing grade—your exact score will not be provided.

Retaking a Test

If you fail the exam you must wait at least 90 days to retake a failed examination. Candidates that do not pass will receive a complete breakdown on their score. Each of the ten domains will be shown as will the candidates score. As an example, you may have received a 95% score in the telecommunications domain and only 12% in cryptography. Use this feedback to better understand what areas you were weak in and where to spend your time and effort in your studies. Additionally, invest in some practice tests if you have not already done so. There is much to be said for getting used to a testing format.

Tracking Your CISSP Status

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

When you receive notice of your passing grade, a blank endorsement form will be sent with it. The endorsement form must be completed by someone who can attest to your professional experience and who is an active CISSP in good standing. If you don't know anyone who is CISSP certified, ISC^2 allows endorsements from other professionals who are certified, licensed, or commissioned, and an officer of the corporation where you are employed. You can review complete information on the endorsement form at the ISC^2 website.

About This Book

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

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

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

NOTE

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

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

The Chapter Elements

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

- Opening hotlists
- Chapter topics

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

NOTE

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

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

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

EXAM ALERT

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

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

NOTE

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

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

TIP

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

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

How Caller ID Can Be Hacked

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

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

CAUTION

The Crossover Error Rate (CER) is the point at which Type 1 errors and Type 2 errors intersect. The lower the CER is, the more accurate the device is.

- **Exam preparation practice questions**—At the end of every chapter is a list of at least 10 exam practice questions similar to those in the actual exam. Each chapter contains a list of questions relevant to that chapter, including answers and explanations. Test your skills as you read.
- **“Need to Know More?” section**—This section at the end of each chapter describes other relevant sources of information. With respect to this chapter, the best place to look for CISSP certification information is at the ISC^2 website, www.ISC2.org.

Other Book Elements

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

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

Chapter Contents

The following list provides an overview of the chapters.

- **Chapter 1, "The CISSP Certification Exam"**—This chapter introduces exam strategies and considerations.
- **Chapter 2, "Physical Security"**—This chapter details physical security and the threats and countermeasures available for protecting an organization's resources. Physical security plays a key role in securing an organization's assets. Without effective physical security, there can be no effective security structure in place.
- **Chapter 3, "Access Control Systems and Methodology"**—This chapter covers the basics of access control. This chapter addresses the three A's: authentication, authorization, and accountability. Items such as

identification, single sign-on, centralized authentication, and the role of technical, administrative, and physical controls are discussed.

- **Chapter 4, "Cryptography"**—This chapter discusses the methods, means, and systems used to encrypt and protect data. Symmetric, asymmetric, and hashing algorithms are introduced, along with PKI and cryptographic methods of attack.
- **Chapter 5, "Security Architecture and Models"**—This chapter discusses key concepts such as computer hardware, operating system design, security models, and documentation used to verify, certify, and accredited systems and networks.
- **Chapter 6, "Telecommunications and Network Security"**—This chapter discusses telecommunication technology. Items such as the OSI model, TCP/IP, network equipment, LAN, MAN, and WAN protocols, and wireless technologies are just a few of the items discussed. This is the most expansive domain and considered one of the most critical for the CISSP candidate to master.
- **Chapter 7, "Business Continuity and Disaster Recovery Planning"**—This chapter covers all the aspects of the BCP and DRP process. Although some may discount the importance the importance of this domain, events such as 9/11 demonstrate the critically of this domain. This chapter addresses key elements of disaster recovery and business continuity. One important item is that no demonstrated recovery exists until the plan has been tested. Exam candidates must understand what is needed to prevent, minimize, and recover from disasters.
- **Chapter 8, "Legal Regulations, Compliance, and Investigations"**—This chapter covers all legal issues from a global perspective. Readers must understand issues such as privacy and the transnational flow of information. Ethics are also discussed because CISSP candidates must understand and abide by the ISC^2 code of ethics. Incident response and computer forensics are introduced in this chapter because readers must understand how to deal with the potential of computer crime.
- **Chapter 9, "Applications and Systems-Development Security"**—This chapter discusses databases, the system development life cycle and the importance of building security into applications and systems as early as possible during the development process. Project management is reviewed, as are malicious code, knowledge-based systems, and application issues.

- **Chapter 10, "Information Security and Risk Management Practices"**—This chapter discusses asset management and the protection of critical resources. Quantitative and qualitative risk assessment are two major topics of this chapter. Readers must understand how these concepts are used to assess and measure risk while reducing threats to the organization. Key concepts include the development of policies, procedures, guidelines, and assorted controls.
- **Chapter 11, "Operations Security"**—This chapter covers operation controls—that is, the types of controls that the organization can implement. Topics such as background checks, duel controls, mandatory vacations, rotation of duties, and auditing are introduced. This chapter also reviews security assessments, ethical hacking, and vulnerability scanning.
- **Chapter 12, Practice Exam I**—This is a full-length practice exam.
- **Chapter 13, Answers to Practice Exam I**—This element contains the answers and explanations for the first practice exam.
- **Chapter 14, Practice Exam II**—This is a second full-length practice exam.
- **Chapter 15, Answers to Practice Exam II**—This element contains the answers and explanations for the second practice exam.

Contacting the Author

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

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

Self-Assessment

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

CISSPs in the Real World

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

TIP

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

The Ideal CISSP Candidate

The CISSP is designed for individuals that are leading, planning, organizing, or controlling the security initiative of an organization. The ideal CISSP candidate is likely to have a 4-year college education and have at least 5–7 years experience in one or more of the 10 CISSP domains. The most applicable degree is in computer science or perhaps a related field. A degree is not a prerequisite for taking the test. However, exam candidates must have a minimum of 5 years of direct full-time security work experience in two or more of the 10 domains. One year of experience can be substituted for a four-year college degree or an approved certification such as Security +. The complete list of approved certifications can be found at https://www.isc2.org/cgi-bin/content.cgi?page=1016. Don't be lulled into thinking that this is an easy test. Some words of caution might be in order:

- The CISSP exam requires the candidate to absorb a substantial amount of material. The test is 6 hours long and consists of 225 graded questions. Unlike Microsoft exams and most other IT vendor exams, it is not a computer-generated test.

- The pass mark is set high, at 700 points. The individual questions are weighted, which means that harder questions are worth more than easier ones.

- Most of the individuals attempting the exam are familiar with one to three of the domains. This means that studying for the exam can be overwhelming because there is so much material to cover. This book can help by guiding you to the areas in which you are weak or strong.

- To be eligible for the CISSP exam, students are required to have 4 years of experience, or 3 years of experience and a college degree.

Put Yourself to the Test

In this section, you answer some simple questions. The objective is for you to understand exactly how much work and effort you must invest to pass the CISSP certification exam. The simple answer to this question is this: The experience and education you have will dictate how difficult it will be for you to pass. Be honest in your answers or you will end up wasting $500 or more on an exam you were not ready to take. From the beginning, two things should be clear:

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

Your Educational Background

- **Do you have a computer science degree?**

  You'll have a good basic knowledge needed for 3 or more of the 10 domains, assuming that you finished your degree and your schooling and have some fairly sophisticated computer skills. Subject areas such as application development, networking, and database design are a great help.

- **Did you attend some type of technical school or computer cram course?**

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

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

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

- **Do you have a photographic memory?**

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

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

Testing Your Exam Readiness

Whether you attend a training class, form a study group, or study on your own, preparing for the CISSP exam is essential. The exam will cost you about $500, depending on where you are located, so you'll want to do everything you can to make sure you pass on the first try. Reading, studying, and taking practice exams are the best ways to increase your readiness. Practice exams help in a number of ways:

- Practice exams highlight weak spots for further study.
- Practice exams give you a general perspective on the question format. Practicing the questions the way they are asked can help enormously on the actual testing day.
- Two full-length practice exams are provided with this book. Que also publishes a second book, *CISSP Practice Questions Exam*, with more than 500 practice CISSP test questions; it is an excellent supplement to this book.

After the Exam

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

- Write a book.
- Read a book. (Only one per year can be used for credit.) This will give you a couple of credits, but not enough to keep your certification current.
- Do volunteer work that is approved by ISC^2. When you are certified, you can log on to the ISC^2 website for more information. A variety of volunteer work is available, including proctoring the CISSP exam.

- Attend a training class. Just about any type of technology training class is accepted as long as it is tied to one of the domains.
- Teach a training class.
- Attend a college-level security class.

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

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

7

CHAPTER SEVEN

Business Continuity and Disaster Recovery Planning

Terms you'll need to understand:

- ✓ Disaster recovery
- ✓ Business continuity
- ✓ Hot site
- ✓ Warm site
- ✓ Cold site
- ✓ Criticality prioritization
- ✓ Maximum tolerable downtime (MTD)
- ✓ Remote journaling
- ✓ Electronic vaulting
- ✓ Qualitative assessment
- ✓ Quantitative assessment
- ✓ Database shadowing

Techniques you'll need to master:

- ✓ Development and processing of contingency plans
- ✓ Completing Business impact analyses
- ✓ Creation of backup strategies
- ✓ Integrating management responsibilities
- ✓ Steering team responsibilities
- ✓ Testing emergency plans
- ✓ Notifying employees of procedures
- ✓ Testing issues and concerns
- ✓ Determining disaster recovery strategies

Introduction

Most of this book has focused on ways in which security incidents can be prevented. The business continuity plan (BCP) and disaster recovery plan (DRP) domain address the need to prepare for, and how to respond to, the occasions when things do go wrong. For a company to be successful under duress of hardship or catastrophe, it must plan how to preserve business operations in the face of these major disruptions. A BCP identifies how a business would respond in the wake of serious damage, and evolves only as the result of a risk assessment that identifies potentials for serious damage. It is an unfortunate reality that this critical planning for disasters and disruptions is an often overlooked area of IT security. One of the best sources of information about disaster recovery is http://www.drii.org, which is the Disaster Recovery Institute International (DRII).

Notable recent events such as tsunamis in Southeast Asia, 9/11 in New York, Pennsylvania, and Washington, D.C., Hurricane Katrina in New Orleans, earthquakes in China, and Hurricane Ike in Houston, continue to highlight the need for organizations to be adequately prepared. Even after these calamitous events, DRII reports that most United States companies still spend, on average, only 3.7% of their IT budget on disaster recovery planning, whereas best practice calls for 6%.

A CISSP exam candidate must know the steps that make up the BCP process to pass the business continuity and disaster recovery domain. Some key elements of this domain include project management and planning, business impact analysis (BIA), continuity planning design and development, and BCP testing and training. The DRP is a subset of the overall BCP plan and describes the planning and restoration that a business would undertake following a disastrous event.

Although some individuals believe that the creation of a disaster recovery plan completes the process, the truth is that no demonstrated recovery exists until the plan has been tested. A DRP can be tested in multiple levels, including tabletop, full interruptions, checklists, and functional tests.

Threats to Business Operations

Disasters are something that many of us would prefer not to think about. Many might see it as an unpleasant exercise or something that is safe to ignore. Sadly, disasters and incidents are something that we all will find occasion to deal with, and they are dynamic by nature. For example, mainframes face a different set of threats than distributed systems, just as computers connected to modems face a different set of threats than do wireless connected computers. This means that planning must be dynamic and able to change with time.

Threats can be man-made, technical, or natural; however, regardless of the source, threats have the potential to cause an incident. Incidents might or might not cause disruptions to normal operations. Incidents and disruptions come in many shapes and forms. Those foolish enough not to prepare could witness the death of their business. Categories of threats that should be provided for include

- **Man-made/political**—Disgruntled employees, riots, vandalism, accidents, theft, crime, protesters, accidents, and political unrest
- **Technical**—Outages, malicious code, worms, hackers, electrical power problems, equipment outages, utility problems, and water shortages
- **Natural**—Earthquakes, storms, fires, floods, hurricanes, tornados, and tidal waves

Each of these can cause an interruption in operations. The resulting interruption of services is defined as follows:

- **Minor**—Operations are disrupted for several hours to less than a day.
- **Intermediate**—Can cause operations to be disrupted for a day or longer. The organization might need a secondary site to continue operations.
- **Major**—This type of event is a true catastrophe. This type of disaster renders the entire facility unusable. Ancillary sites will be required while the original site is reconstituted or a new facility is found or built.

Disaster Recovery and Business Continuity Management

There are many different approaches to BCP and DRP. Some companies address these processes separately, whereas others focus on a continuous process that interweaves the plans. The National Institute of Standards and Technology (NIST) (http://www.csrc.nist.gov) offers a good example of the contingency process in Special Publication 800-34: Continuity Planning Guide for Information Technology Systems (http://tinyurl.com/yb3lcw). In NIST SP 800-34, the BCP/DRP process is defined as

1. Develop the contingency planning policy statement.
2. Conduct the BIA (business impact analysis).

3. Identify preventive controls.
4. Develop recovery strategies.
5. Develop an IT contingency plan.
6. Test the plan, train employees, and hold exercises.
7. Maintain the plan.

Before we go further, let's define the terms disaster and business continuity. A *disaster* is any sudden, unplanned calamitous event that brings about great damage or loss. Entire communities have concerns following a disaster; however, businesses face special challenges because they have responsibilities to protect the lives and livelihoods of their employees, and to guard company assets on behalf of shareholders. In the business realm, a disaster can be seen as any event that prevents the continuance of critical business functions for a predetermined period of time. In other words, the estimated outage might force the declaration of a disaster.

TIP

Human safety always comes first and has priority over all other concerns.

Business continuity is the process of sustaining operation of critical systems. The goal of business continuity is to reduce or prevent outage time and optimize operations. The Business Continuity Institute (http://www.thebci.org), a professional body for business continuity management, defines business continuity management in the following terms:

> Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organization, provides a framework for building resilience, ensures an effective response, and safeguards the interests of its key stakeholders, reputation, brand, and value.

Although there are competing methodologies that can be used to complete the BCP/DRP process, this chapter will follow steps that most closely align with reference documentation recommended by ISC^2. Figure 7.1 illustrates an overview of the process, the steps for which are as follows:

1. Project initiation
2. Business impact assessment
3. Recovery strategy

4. Plan design and development
5. Implementation
6. Testing
7. Monitoring and maintenance

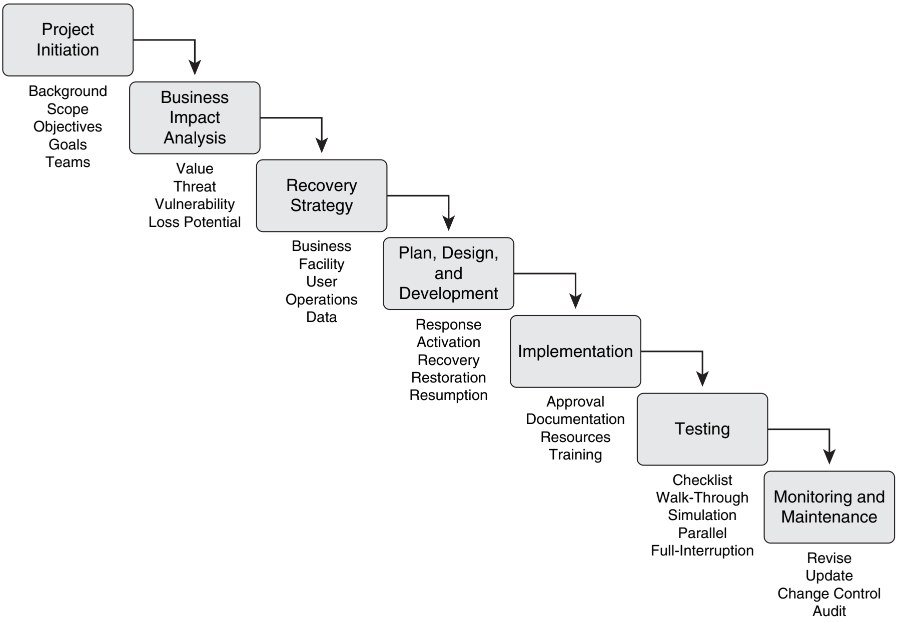


FIGURE 7.1 BCP/DRP process.

We will discuss each of these steps individually.

Project Management and Initiation

Before the BCP process can begin, it is essential to have the support of management. You might need to educate management about the need for a BCP. One way to accomplish this is to prepare and present a seminar for management that overviews the risk the organization faces, identifies basic threats, and documents the costs of potential outages. This is a good time to remind management that, ultimately, they are legally responsible. Customers, shareholders, stockholders, or anyone else could bring civil suits against senior management if they feel the company has not practiced due care. Without management support, you will not have funds to successfully complete the project, and resulting efforts will be marginally successful, if at all. Management is responsible for

- Setting the budget
- Determining the team leader
- Starting the BCP process

Management must choose a team leader. This individual must have enough creditability with senior management to influence them in regard to BCP results and recommendations. After the team leader is appointed, an action plan can be established and the team can be assembled. Members of the team should include representatives from management, legal staff, recovery team leaders, information security department, various business units, networking, and physical security. It is important to include asset owners and the individuals that would be responsible for executing the plan.

Next, determine the scope. A properly defined scope is of tremendous help in maximizing the effectiveness of the BCP plan. Be sensitive to interoffice politics, which, if out of control, can derail the planning process. Another problem to avoid is *project creep*, which occurs when more and more items that were not part of original project plan are added to the plan. This can delay completion of the project or cause it to run over budget.

The BCP benefits from adherence to traditional project plan phases. Issues such as resources (personnel, financial), time schedules, budget estimates, and any critical success factors must be managed. Schedule an initial meeting to kick off the process.

Finally, the team is ready to get to work. The team can expect a host of duties and responsibilities:

- Identifying regulatory and legal requirements that must be complied with
- Identifying all possible threats and risks
- Estimating the probability of these threats and correctly identifying their loss potential
- Performing a BIA
- Outlining the priority in which departments, systems, and processes must be up and running before any others
- Developing the procedures and steps to resume business functions following a disaster

- Assigning tasks to the employee roles, or individuals, that will complete those tasks during a crisis situation
- Documenting plans, communicating plans to employees, and performing necessary training and drills

It's important for everyone on the team to realize that the BCP is the most important corrective control the organization will have, and to use the planning period as an opportunity to shape it. The BCP is more than just corrective controls; the BCP is also about preventive and detective controls. These three elements are described here:

- **Preventive**—Including controls to identify critical assets and prevent outages
- **Detective**—Including controls to alert the organization quickly in case of outages or problems
- **Corrective**—Including controls to restore normal operations as quickly as possible

Business Impact Analysis

The next task is to create the BIA, the role of which is to measure the impact each type of disaster could have on critical business functions. The BIA is an important step in the process because it considers all threats and the implications of those threats. As an example, the city of Galveston, Texas is an island known to be prone to hurricanes. Although it might be winter in Galveston and the possibility of a hurricane is extremely low, it doesn't mean that planning can't take place to reduce the potential negative impact if and when a hurricane arrives. The steps for accomplishing this require trying to think through all possible disasters, assess the risk of those disasters, quantify the impact, determine the loss, and identify and prioritize operations that would require disaster recovery planning in the event of those disasters. The BIA is tasked with answering three vital questions:

- **What is most critical?**—The prioritization must be developed to address what processes are most critical to the organization.
- **How long of an outage can the company endure?**—The downtime estimation is performed to determine which processes must resume first, second, third, and so on, and to determine which systems must be kept up and running.

- **What resources are required?**—Resource requirements must be identified and require correlation of system assets to business processes. As an example, a generator can provide backup power, but requires fuel to operate.

NOTE

Criticality prioritization is something that companies do all the time. Consider the last time you phoned your favorite computer vendor to order new equipment. How long were you placed on hold? Most likely, your call was answered within a few minutes. Contrast that event with the last time you phoned the same company to speak to the help desk. How long was the wait? Most likely, the wait was much longer.

The development of multiple scenarios should provide a clear picture of what is needed to continue operations in the event of a disaster. The team creating the BIA will need to look at the organization from many different angles and use information from a variety of sources. Different tools can be used to help gather data. Strohl Systems BIA Professional and SunGard's Paragon software can automate portions of the data input and collection process. Although the CISSP exam will not require that you know the names of various tools, it is important to understand how the BIA process works, and it helps to know tools that are available.

Whether the BIA process is completed manually or with the assistance of tools, its completion will take some time. Anytime individuals are studying processes, techniques, and procedures they are not familiar with, a learning curve will be involved.

As you might be starting to realize, creation of a BIA is no easy task. It requires not only the knowledge of business processes but also a thorough understanding of the organization itself, including IT resources, individual business units, and the interrelationships of each. This task will require the support of senior management and the cooperation of IT personnel, business unit managers, and end users. The general steps within the BIA include

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

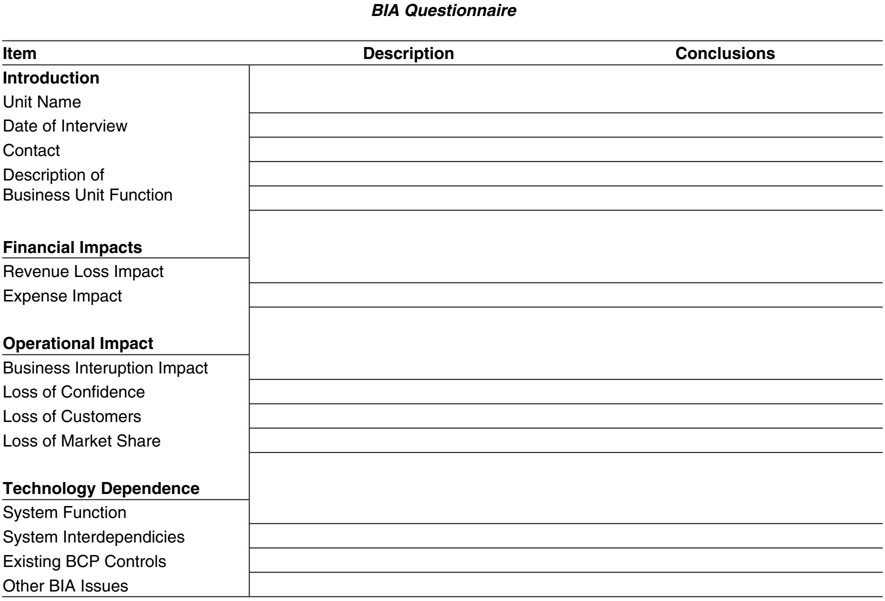
6. Define recovery alternatives and costs

NOTE

A vulnerability assessment is often included in a BIA. Although the assessment is somewhat similar to the risk-assessment process discussed in Chapter 10, "Information Security and Risk Management Practices," this assessment focuses on providing information specifically for the business continuity plan.

Assessing Potential Loss

There are different approaches to assessing potential loss. One of the most popular methods is the use of a questionnaire. This approach requires the development of a questionnaire distributed to senior management and end users. The objective of the questionnaire is to maximize the identification of real loss from the people completing business processes jeopardized by the disaster. This questionnaire might be distributed and independently completed or filled out during an interactive interview process. Figure 7.2 shows a sample questionnaire.



BIA Questionnaire

Item	Description	Conclusions
Introduction		
Unit Name		
Date of Interview		
Contact		
Description of Business Unit Function		
Financial Impacts		
Revenue Loss Impact		
Expense Impact		
Operational Impact		
Business Interuption Impact		
Loss of Confidence		
Loss of Customers		
Loss of Market Share		
Technology Dependence		
System Function		
System Interdependicies		
Existing BCP Controls		
Other BIA Issues		

FIGURE 7.2 BIA questionnaire.

The questionnaire can also be completed in a round table setting. In fact, this sort of group completion can add synergy to the process, providing the dynamics of the group allow for open communication and the required key individuals can all schedule and meet to discuss what impact specific types of disruptions would have on the organization. The importance of the inclusion of all key individuals must be emphasized because management might not be aware of critical key tasks for which they do not have direct oversight.

A questionnaire is a qualitative technique for assessing risk. Qualitative assessments are scenario-driven and do not attempt to assign dollar values to anticipated loss. A qualitative assessment ranks the seriousness of an impact using grades or classes, such as low, medium, high, or critical. This sort of grading process enables quicker progress in the identification of risks, and provides a means of classifying processes that might not easily equate to a dollar value. As an example:

- **Low**—Minor inconvenience that customers might not notice. Outages could last for up to 30 days without any real inconvenience.
- **Medium**—Loss of service would impact the organization after a few days to a week. Longer outages could affect the company's bottom line or result in the loss of customers.
- **High**—Only short term outages of a few minutes to hours could be endured. Longer outages would have a severe financial impact. Negative press might also reduce outlook for future products and services.
- **Critical**—Outage of any significance cannot be endured. Systems and controls must be in place or be developed to ensure redundancy so that no outage occurs.

The BIA can also be undertaken using a quantitative approach. This method of analysis attempts to assign a monetary value to all assets, exposures, and processes identified during the risk assessment. These values are used to calculate the material impact of a potential disaster, including both loss of income and expenses. A quantitative approach requires

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

The process of performing a quantitative assessment is covered in much more detail in Chapter 10. It is important that a quantitative study include all associated costs resulting from a disaster, such as

- Lost productivity
- Delayed or canceled orders

- Cost of repair
- The value of the damaged equipment or lost data
- The cost of rental equipment
- The cost of emergency services
- The cost to replace equipment or reload data

Both quantitative and qualitative assessment techniques require the BIA team to examine how the loss of service or data would affect the company. Each method is seeking to reduce risk and plan for contingencies, as shown in Figure 7.3.

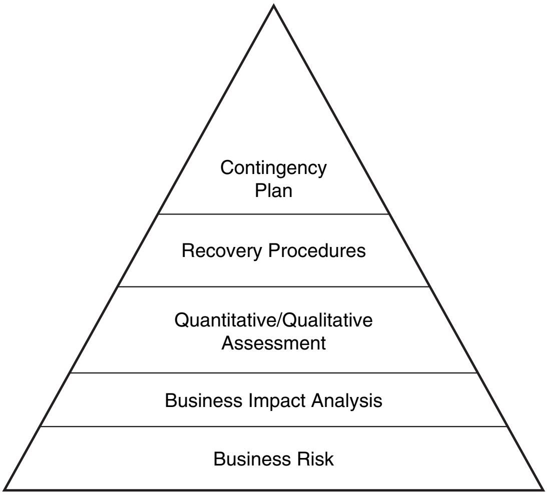


FIGURE 7.3 Risk reduction process.

The severity of an outage is generally measured by considering the *maximum tolerable downtime* (MTD) for which the organization can survive without that function or service. Will there be a loss of revenue or operational capital or will the organization be held personally liable? Although the team might be focused on what the immediate effect on an outage would be, cost can be immediate or delayed. Many organizations are under regulatory requirements. The result of an outage could be a legal penalty or fine. The organization's reputation could even be tarnished.

CAUTION

MTD is a measurement of the longest time that an organization can survive without a specific business function.

Reputation Has Its Value

Although some organizations might focus solely on dollar amounts when working through a BIA, reputation also needs to be considered. A quote from Benjamin Franklin states, “It takes many good deeds to build a good reputation, and only one bad one to lose it.” To illustrate this point, consider the following brand names and their business reputations:

- **Cisco**—An industry leader of quality networking equipment.
- **Ruth’s Chris Steak House**—An upscale eatery known for serving high-quality steaks seared at 1800° Fahrenheit.
- **Rolls-Royce**—Known for high quality automobiles.
- **Enron**—A symbol of corporate fraud and corruption.
- **Yugo**—A low quality car released in the United States in the mid 1980s.
- **ValuJet**—A once fast growing airline until a deadly crash in the Florida Everglades in 1996 played a part in the company merger and name change to AirTran.

Perhaps your vision of the companies listed is different that what was documented. The intent of the listing is to demonstrate that well-known corporate names do generate visions when people hear and read them. Companies work hard for years to gain a level of respect and positive reputation. Catastrophes don’t just happen. Most occur because of human error or as the result of a series of overlooked mistakes. Will a mistake be fatal to your organization? Reputations can be easily damaged. That is why disaster recovery is so important. The very future of your organization may rest on it.

Recovery Strategy

Recovery strategies are the predefined actions that management has approved in the event that normal operations are interrupted. To judge the best strategy to recover from a given interruption, the team must evaluate and complete:

1. Detailed documentation of all costs associated with each possible alternative
2. Quoted cost estimates for any outside services that might be needed
3. Written agreements with chosen vendors for all outside services
4. Possible resumption strategies in case there is a complete loss of the facility
5. Complete documentation of findings and conclusions as report to management of chosen recovery strategy for feedback and approval

This information is used to determine the best course of action based on the analysis of data from the BIA. With so much to consider, it is helpful to divide the organization's recovery into specific areas, functions, or categories:

- Business process recovery
- Facility and supply recovery
- User recovery
- Operations recovery
- Data and information recovery

Business Process Recovery

Business processes can be interrupted due to the loss of personnel, critical equipment, supplies, or office space; or from uprisings, such as strikes. As an example, in 2005 after Katrina, New Orleans had a huge influx of workers in the city rebuilding homes, offices, and damaged buildings. Fast food restaurants were eager to meet the demand these workers had for burgers, fries, tacos, and fried chicken. However, there was insufficient low-cost housing for the fast food industry's employees. The resulting shortage forced fast food restaurants to pay bonuses of up to $6,000 to entice potential employees to the area. It is worth noting that even if the facility is intact after a disaster, people are still required and are an important part of the business process recovery.

Workflow diagrams and documents can assist business process recovery by mapping relationships between critical functions. Let's process an order for a widget to illustrate a sample flow:

1. Is the widget in stock?
2. Which warehouse has the widget?
3. When can the widget be shipped?
4. Confirm capability to fulfill order with customer and provide total.
5. Process credit card information.
6. Verify funds were deposited in the bank.
7. Ship item to customer.
8. Restock widget for subsequent sales.

A more detailed listing would be appropriate for industrial use, but you get the idea. Building these types of flowcharts allows organizations to examine what resources are required for each step and what functions are critical for continued business operations.

Facility and Supply Recovery

Facility and supply interruptions can be caused by fire, loss of inventory, transportation problems, telecommunications, or heating, ventilating, and air conditioning (HVAC) problems. It is too late to start discussions on alternative sites when a disaster is striking your facility. Redundant services enable rapid recovery from these interruptions. Many options are available, from a dedicated offsite facility, to agreements with other organizations for shared space, to the option of building a prefab building and leaving it empty as a type of cold backup site. The following sections examine some of these options.

Subscription Services

Organizations might opt to contract their facility needs to a subscription service. The CISSP exam considers hot, warm, and cold sites to be subscription services. Data-processing facilities are expensive. The organization might decide to dedicate the funds for a hot, warm, or cold site. A *hot site* facility is ready to be brought online quickly. A hot site is fully configured and is equipped with the same system as the production network. It can be made operational within just a few hours. A hot site will need staff, data files, and procedural documentation. Hot sites are a high-cost recovery option, but can be justified when a short recovery time is required. Because hot sites are typically a subscription service, a range of associated fees exist, including monthly cost, subscription fees, testing costs, and usage or activation fees. Contracts for hot sites need to be closely examined because some charge extremely high activation fees to prevent users from utilizing the facility for anything less than a true disaster. To get an idea of the types of costs involved, http://www.drj.com reports that subscriptions for hot sites average 52 months in length and costs can be as high as $120,000 per month. Compare this to cold sites, which can also be 5 to 6 years in length and can average anywhere between $500 to $2,000 per month.

Regardless of what fees are involved, the hot site needs to be periodically tested. Theses tests should evaluate processing abilities as well as security. The physical security of the hot site should be at the same level or greater than the primary site. Finally, it is important to remember that the hot site is intended for short term usage only. As a subscriber-based service, there might be others competing for the same resource. The organization should have a plan to recover primary services quickly or move to a secondary location.

CAUTION

Hot sites should not be externally identifiable as this will increase their risk of sabotage and other potential disruptions.

For those companies lacking the funds to spend on a hot site or in situations where a short term outage is acceptable, a warm site might be acceptable. A *warm site* has data equipment and cables, and is partially configured. It could be made operational anywhere from in a few hours to a few days. The assumption with a warm site is that computer equipment and software can be procured as required due to a disaster. Although the warm site might have some computer equipment installed, it is typically of lower processing power than the primary site. The costs associated with a warm site are similar to those of a hot site but slightly lower. The warm site is a popular subscription alternative.

In situations where even longer outages are acceptable, a cold site might be the right choice. A cold site is basically an empty room with only rudimentary electrical power and computing capability. Although it might have a raised floor and some racks, it is nowhere near ready for use. It might take several weeks to a month to get the site operational. Cold sites offer the least preparedness when compared to hot and warm subscription services discussed.

TIP

Cold sites are a good choice for the recovery of noncritical services.

Redundant Sites

The CISSP exam considers redundant sites to be sites owned by the company. Although these might be either partially or totally configured, the CISSP exam does not typically expect you to know that level of detail. A *redundant site* is capable of handling all operations if another site fails. Although there is an increased cost, it offers the company fault tolerance. If the redundant sites are geographically dispersed, the possibility of more than one being damaged is reduced. For low to medium priority services, a distance of 10 to 20 miles from the primary site is considered acceptable. If the loss of services, for even a very short time, could cost the organization millions of dollars, the redundant site should be farther away. Therefore, redundant sites that are to support highly critical services should not be in the same geographical region or subject to the same types of natural disasters as the primary site.

For organizations that have multiple sites dispersed in different regions of the world, multiple processing centers might be an option. Multiple processing centers allow a branch in one area to act as backup for a branch in another area. Table 7.1 shows some sample functions and their recovery times.

TABLE 7.1 Organization Functions and Example Recovery Times

Process	Recovery Time	Recovery Strategy
Database	Minutes to hours	Database shadowing (covered in the later section, "Other Data Backup Methods")
Help desk	7 to 14 days	Warm site
Research and development	Several weeks to a month	Cold site
Purchasing	1 to 2 days	Hot site
Payroll	1 to 5 days	Multiple site

Mobile Sites

Mobile sites are another processing alternative. *Mobile sites* are usually tractor-trailer rigs that have been converted into data-processing centers. These sites contain all the necessary equipment and are mobile, permitting transport to any business location quickly. Rigs can also be chained together to provide space for data processing and provide communication capabilities. Mobile units are a good choice for areas where no recovery facilities exist and are commonly used by the military, large insurance agencies, and others.

NOTE

Mobile sites are a nonmainstream alternative to traditional recovery options. Mobile sites typically consist of fully contained tractor trailer rigs that come with all the facilities needed for a data center. Units can be quickly moved to any site necessary.

Whatever recovery method is chosen, regular testing is important to verify that the redundant site meets the organization's needs, and that the plan can handle the workload to meet minimum processing requirements.

Reciprocal Agreement

The reciprocal agreement option requires two organizations to pledge assistance to one another in case of disaster. The support requires sharing space, computer facilities, and technology resources. On paper, this appears to be a cost-effective approach, but it has its drawbacks. The parties to this agreement must place their trust in the other organization to provide aid in case of a disaster. However, a nonvictim might become hesitant to follow through when a disaster actually occurs. Also, confidentiality requires special consideration. This is because the damaged organization is placed in a vulnerable position while needing to trust the sponsoring party housing the victim's confidential information. Legal liability can also be a concern. One company agrees to help the other organization out when down and as a result it is hacked. Finally, if locations of the parties of the agreement have physical proximity, there is always the danger that disaster could strike both parties; thereby, rendering the agreement useless.

CAUTION

The biggest drawback to reciprocal agreements is that they are hard to enforce and that many times incompatibilities in company cultures, hardware, or other, are not discovered until after a disaster strikes.

User Recovery

User recovery is primarily about what employees must have to accomplish their jobs. Requirements include

- Procedures, documents, and manuals
- Communication system
- Means of mobility and transportation
- User workspace and equipment
- Alternative site facilities

At issue here is the fact that a company might be able to get employees to a backup facility after a disaster, but if there are no phones, desks, or computers, the employees' ability to work will be severely limited.

User recovery can even include food. As an example, my brother-in-law works for a large chemical company on the Texas Gulf Coast. During storms, hurricanes, or other disasters, he is required to stay at work as part of the emergency operations team. His job is to stay at the facility regardless of time; the disaster might last two days or two weeks. During a simulation test several years ago, it was discovered that someone had forgotten to order food for the facility where the employees were to remain for the duration of the drill. Luckily, the 40 or so hungry employees were not really in a disaster, and were able to order pizza and have it delivered. Had it been a real disaster, no takeout would have been available.

Operations Recovery

Operations recovery addresses interruptions caused by the loss of capability due to equipment failure. Redundancy solves this potential loss of availability, such as redundant equipment, Redundant Array of Inexpensive Disks (RAID), backup power supplies (BPS), and other redundant services.

Hardware failures are one of the most common disruptions that can occur. Preventing the disruptions is critical to operations. The best place to start planning redundancy is when equipment is purchased. At purchase time, there are two important numbers that the buyer must investigate:

- **Mean time between failure (MTBF)**—Used to calculate the expected lifetime of a device. A higher MTBF means the equipment should last longer.
- **Mean time to repair (MTTR)**—Used to estimate how long it would take to repair the equipment and get it back into production. Lower MTTR numbers mean the equipment requires less repair time and can be returned to service sooner.

A formula for calculating availability is

MTBF / (MTBF+ MTTR) = Availability

To maximize availability of critical equipment, an organization can consider obtaining a *service level agreement (SLA)*. There are all kinds of SLAs. In this situation the SLA is a contract between a company and a hardware vendor, in which the vendor promises to provide a certain level of protection and support. For a fee, the vendor agrees to repair or replace the covered equipment within the contracted time.

Fault tolerance can be used at the server or drive level. For servers, there is *clustering*, which is technology that allows you to group several servers together, where those servers are viewed logically as a single server. Users see the cluster as one unit. The advantage is that if one server in the cluster fails, the remaining active servers pick up the load and continue operation.

Fault tolerance on the drive level is achieved primarily with RAID, which provides hardware fault tolerance and/or performance improvements. This is achieved by breaking up the data and writing it to multiple disks. To applications and other devices, RAID appears as a single drive. Most RAID systems have hot-swappable disks. This means that faulty drives can be removed and replaced without restoring the entire computer system. If the RAID system uses parity and is fault tolerant, the parity data can be used to reconstruct the newly replaced drive. The technique for writing the data across multiple drives is called *striping*. Although write performance remains almost constant, read performance is drastically increased. RAID has humble beginnings that date back to the 1980s at the University of California. RAID is discussed in depth in Chapter 11, "Operations Security."

Although operations can be disrupted because of the failure of equipment, the loss of communications can also disrupt critical processes. Protecting communication with fault tolerance can be achieved through redundant WAN links, diverse routing, and alternate routing. Whatever method is chosen, the organization should verify capacity requirements and acceptable outage times. The primary methods for network protection include the following:

- **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 cheap. Most of these systems use buried facilities. These systems usually enter a facility through the basement and can sometimes share space with other mechanical equipment. Recognize that this sharing adds to the risk of potential failure. Also, many cities have aging infrastructures, which is another potential point of failure.

- **Alternate routing**—Redundant routing provides use of another transmission line if the regular line is busy or unavailable. This can include using a dialup connection in place of a dedicated connection, cell phone instead of a land line, or microwave communication in place of a fiber connection.

- **Last mile protection**—This is a good choice for recovery facilities; it provides a second local loop connection, and is even more redundantly capable if an alternative carrier is used.

- **Voice communication recovery**—Many organizations are highly dependent on voice communications. Others have started making the switch to Voice over IP (VoIP) for both voice and fax communication because of the cost savings. Some number of land lines should always be maintained to provide backup capability.

Networks are susceptible to the same types of outages as equipment. If operational recovery concerns are not addressed, these outages can be a real problem for companies that rely heavily on networks to deliver data when needed.

NOTE

Free Space Optics (FSO) is an emerging technology that can be used to obtain high bandwidth, short haul, redundant links. FSO uses LED and/or laser light to transmit data between two points and is inexpensive, easy to install, and works great on campus WANs (see http://en.wikipedia.org/wiki/Free_Space_Optics).

Data and Information Recovery

The focus here is on recovering the data. Solutions to data interruptions include backups, offsite storage, and/or remote journaling. Because data processing is essential to most organizations, the data and information recovery plan is critical. The objective of the plan is to back up critical software and data that permits quick restores with minimum loss of content. Policy should dictate when backups are performed, where the media is stored, who has access to the media, and what the reuse or rotation policy will be. Types of backup media include tape reels, tape cartridges, removable hard drives, disks, and cassettes.

Tape and optical systems still have the majority of market share for backup systems. Common types of media include

- 8mm tape
- CDR/W media (recommended for temporary storage only)
- Digital Audio Tape (DAT)
- Digital Linear Tape (DLT)
- Quarter Inch Tape (QIC)
- Write Once Read Many (WORM)

Another technology worth mentioning is MAID (Massive Array of Inactive Disk). *MAID* offers a distributed hardware storage option for the storage for 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 it provides power management and advanced disk monitoring. MAID might or might not stripe data and/or supply redundancy. The MAID system powers down inactive drives, reduces heat output, electrical consumption, and increases the drive's life expectancy.

In addition to defining the media type, the organization must determine how often backups should be performed and what type of backup should be performed. Answers will vary depending on the cost of the media, the speed of the restoration needed, and the time allocated for backups. Backup methods include

- **Full backup**—During a *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 media. If a restoration is required, only one tape or set of tapes is needed. Full backups take the most time to create, and the most space for storage media, but they also take the least time for restoration. A full backup resets the archive bit on all files.
- **Differential backup**—A *differential backup* is a partial backup performed in conjunction with a full backup. Typically, a full backup is done once a week, and a daily differential backup is done periodically thereafter to back up only those files that have changed since the last full backup. Any restoration requires the last full backup and the most recent differential backup. This method takes less time than a full backup per each backup, but increases the restoration time because both the full and differential backups will be needed. A differential backup does not reset the archive bit on files.
- **Incremental backup**—An *incremental backup* is faster yet to perform. It backs up only those files that have been modified since the previous incremental (or full) backup. Although fast to create, incremental backups require the most backup media and take the longest to recover from. A restoration requires the last full backup and all incremental backups since the last full backup. An incremental backup resets the archive bit on files.
- **Continuous backup**—Some backup applications perform *continuous backups*, and keep a database of backup information. These systems are useful when a restoration is needed because the application can provide a full restore, point-in-time restore, or restore based on a selected list of files.

EXAM ALERT

Test questions regarding different backup types can be quite tricky. Make sure you clearly know the difference before the exam.

Backup and Restoration

Backups need to be stored somewhere, and backups are needed quickly when it's time to restore. Where the backup media is stored can have a real impact on how quickly data can be restored and brought back online. The media should be stored in more than one physical location so that the possibility of loss is reduced. These remote sites should be managed by a tape librarian. It is this individual's job to maintain the site, control access, rotate media, and protect this valuable asset. Unauthorized access to the media is a huge risk because it could impact the organization's capability to provide uninterrupted service. Transportation to and from the remote site is also an important concern. Important backup and restoration considerations include

- Maintenance of secure transportation to and from the site
- Use of bonded delivery vehicles
- Appropriate handling, loading, and unloading of backup media
- Use of drivers trained on proper procedures to pick up, handle, and deliver backup media
- Legal obligations for data such as encrypted media, and separation of sensitive data sets such as credit card numbers and CVCs
- 24/7 access to the backup facility in case of an emergency

It is recommended that companies contract their offsite storage needs with a known firm that demonstrates control of their facility and is responsible for its maintenance. Physical and environmental controls at offsite storage locations should be equal to or better than the organization's own 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 agreement on response times that will be met in times of disaster. Onsite storage should maintain copies of recent backups to ensure the capability to recover critical files quickly.

Backup media should be securely maintained in an environmentally controlled facility with physical control appropriate for critical assets. The area should be fireproof, and anyone depositing or removing media should have a record of their access logged.

Software itself can be vulnerable, even when good backup policies are followed, because sometimes software vendors go out of business or no longer support needed applications. In these instances, *escrow agreements* can help.

CAUTION

Escrow agreements are one possible software-protection mechanism. Escrow agreements allow an organization to obtain access to the source code of business-critical software if the software vendor goes bankrupt or otherwise fails to perform as required.

Tape-Rotation Strategies

Although most backup media is rather robust, no backup media can last forever; it will fail over time. This means that tape rotation is another important part of backup and restoration. Additionally, backup media needs to be periodically tested. Backups will be of little use if you find out during a disaster that they have malfunctioned and no longer work.

Tape-rotation strategies can range from simple to complex.

- **Simple**—A simple tape-rotation scheme uses one tape for every day of the week and then repeats the pattern the following week. One tape can be for Monday, one for Tuesday, and so on. You add a set of new tapes each month and then archive the previous month's set. After a predetermined number of months, you put the oldest tapes back into use.
- **Grandfather-father-son (GFS)**—This scheme includes four tapes for weekly backups, one tape for monthly backups, and four tapes for daily backups (assuming you are using a five-day work week). 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 4th day; set C is used on the first non-A or non-B backup day and is used every 8th 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.

Other Data Backup Methods

Other alternatives that exist for further enhancing a company's resiliency and redundancy are listed in the following list. Some organizations use these techniques by themselves; others combine these techniques with other backup methods.

- **Database shadowing**—Databases are a high-value asset for most organizations. File-based incremental backups can read only entire database tables and are considered too slow. A database shadowing system uses two physical disks to write the data to. It creates good redundancy by duplicating the database sets to mirrored servers. Therefore, this is an excellent way to provide fault tolerance and redundancy. Shadowing mirrors changes to the database as they occur.

- **Electronic vaulting**—Electronic vaulting makes a copy of database changes to a secure backup location. This is a batch-process operation copying all current records, transactions, and/or files to the offsite location. To implement vaulting, an organization typically loads a software agent onto the systems to be backed up, and then, periodically, the vaulting service access the software agent on these systems to copy changed data.
- **Remote journaling**—Remote journaling is similar to electronic vaulting, except that information is duplicated to the remote site as it is committed on the primary system. By performing live data transfers, this mechanism allows alternative sites to be fully synchronized and fault tolerant at all times. Depending on configuration, it is possible to configure remote journaling to record only the occurrence of transactions and not the actual content of the transactions. Remote journaling can provide a very high level of redundancy.
- **Storage area network (SAN)**—An alternative to tape backup, a SAN supports disk mirroring, backup and restore, archiving, and retrieval of archived data in addition to data migration from one storage device to another. A SAN can be implemented locally or use storage at a redundant facility.

Choosing the Right Backup Method

It is not easy to choose the right backup method. To start the process, the team must consider how long of an outage the organization can endure and how current the restored information must be. These two recovery requirements are technically called

- **Recovery point objective (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)**—Specifies the maximum elapsed time required to recover an application at an alternative site. The greater the RTO, the longer the process can take to be restored and the more tolerant the organization is to interruption. Figure 7.4 illustrates the RTO can be used to determine acceptable downtime.

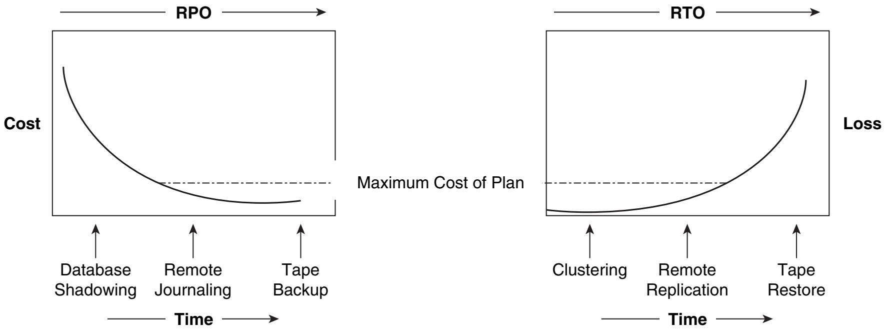


FIGURE 7.4 RPO and RTO.

What you should realize about both RPO and RTO is that the lower the time requirements are, the higher the maintenance cost will be to provide for reduced restoration capabilities. For example, most banks have a very small RPO because they cannot afford to lose any processed information.

Plan Design and Development

The BCP process is now ready for its next phase—plan design and development. In this phase, the team designs and develops a detailed plan for the recovery of critical business systems. The plan should be directed toward major catastrophes. Worst case scenarios are planned for because, by definition, the entire facility has been destroyed. If the organization can handle these types of events, less severe events such as disasters, which render the facility unusable only for a time, can be easily dealt with. The plan should be a guide for implementation. The plan should include information on both long-term and short-term goals and objectives:

1. Identify critical functions and priorities for restoration.
2. Identify support systems needed by critical functions.
3. Estimate potential outages and calculate the minimum resources needed to recover from the catastrophe.
4. Select recovery strategies and determine what vital personnel, systems, and equipment will be needed to accomplish the recovery.
5. Determine who will manage the restoration and testing process.
6. Calculate what type of funding and fiscal management is needed to accomplish these goals.

The plan should also detail how the organization will contact and mobilize employees, provide for ongoing communication between employees, interface with external groups, the media, and provide employee services. Each of these items is discussed next.

Personnel Mobilization

The process for contacting employees in case of an emergency needs to be worked out before a disaster. The process chosen depends on the nature and frequency of the emergency. *Call trees* and *outbound dialing systems* are widely used. An outbound dialing system stores the numbers to be called in an emergency. These systems can provide various services such as

- **Call rollover**—If one number gets no response, the next is called.
- **Leave a recorded message**—If an answering machine answers, a message can be left for the individual.
- **Request a call back**—Even if a message is left, the system will continue to call back until the user calls in to the predefined phone number.

A call tree is a communication system in which the person in charge of the tree calls a lead person on every branch, who in turn calls all the leaves on that branch. If call trees are used, the team will want to verify that there is a feedback mechanism built in. As an example, the last person on any branch of the tree calls and confirms that he /she got the message. This can help ensure that everyone has been contacted. Call trees can be automated with VoIP and public switched telephone networks (PSTNs) and online services. Personnel mobilization can also be triggered by emails to PDAs, BlackBerrys, and so on. Such systems require the email server to be functioning.

Interface with External Groups

Deciding how to interface with external groups is another important aspect of business continuity. Damaging rumors can easily start and it is important to have protocols in place for dealing with these incidents, accidents, and catastrophes. The organization must decide how to deal with response teams, the fire department, the police department, ambulance, and other emergency response personnel.

Someone should be identified to deal with the media. Negative public opinion can be costly. It is important to have a properly trained spokesperson to speak and represent the organization. The media spokesperson must be in the communication path to have the facts before speaking or meeting with the press. The appointed spokesperson should interface with senior management and legal counsel prior to making any public statement. Meeting with the media during a crisis is not something that should be done without preparation.

The corporate plan should include generic communiqués that address each possible incident. The spokesperson will also need to know how to handle tough questions. Liability should never be assumed; the spokesperson should simply state that an investigation has begun. Tackling these tough issues up front will allow the company to have a preapproved framework to work with should a real disaster occur.

Employee Services

Companies have an inherent responsibility to employees and to their families. This means that paychecks must continue and that employees need to be taken care of. Employees must be trained on what to do in case of emergencies and on what they can expect from the company. Insurance and other necessary services must continue.

CAUTION

The number one priority of any BCP or DRP plan is to protect the safety of employees.

During a disaster, employees must know what is expected of them and who is in charge. Someone must have the authority to allocate emergency funding as needed. As an example, after Hurricane Katrina, the U.S. Congress passed 48 C.F.R. § 13.201(b) (2005), which increased the limit on FEMA-issued credit cards to $250,000. The idea was to allow government employees to acquire needed items quickly and without delay. Although funding is important, controls must also be in place to ensure that funds are not misappropriated.

Insurance

Insurance is one option that companies can consider to remove a portion of the risk the team has uncovered during the BIA. Just as protection insurance can be purchased by individuals for a host of reasons, companies can purchase protection insurance for each of the following items:

- Outages
- Data centers
- Hacker insurance
- Software recovery

- Business interruption
- Documents, records, and important papers
- Errors and omissions
- Media transportation

Insurance is not without its drawbacks, such as high premiums, delayed claim payout, denied claims, and problems proving real financial loss. Also, most insurance policies pay for only a percentage of any actual loss and do not pay for lost income, increased operating expenses, or consequential loss.

Implementation

The BCP team is now nearing the end of the plan's development process, and is ready to submit a completed plan for implementation. The plan is the result of all information gathered during the project initiation, the BIA, and the recovery strategies phase. A final checklist for completeness ensures the plan addresses all relevant factors, such as

- Calculates what type of funding and fiscal management is needed to accomplish the stated goals
- Determines the procedures for declaring a disaster and under what circumstances this will occur
- Evaluates potential disasters and calculates the minimum resources needed to recover from the catastrophe
- Determines critical functions and priorities for restoration
- Identifies what recovery strategy and equipment will be needed to accomplish the recovery
- Identifies individuals that are responsible for each function in the plan
- Determines who will manage the restoration and testing process

The completed plan should be presented to senior management for approval. References for the plan should be cited in all related documents so that the plan is maintained and updated whenever there is a change or update to the infrastructure. When management approves the plan, it must be released and disseminated to employees. Awareness training will help make sure that everyone understands what their tasks and responsibilities are when an emergency occurs.

Awareness and Training

The goal of awareness and training is to make sure all employees know what to do in case of an emergency. If employees are untrained, they might simply stop what they're doing and run for the door anytime there's an emergency. Even worse, they might not leave when an alarm has sounded, even though the plan required they leave because of possible danger. Instructions should be written in easy to understand language that uses common terminology that everyone will understand. The organization should design and develop training programs to make sure each employee knows what to do and how to do it. Employees assigned to specific tasks should be trained to carry out needed procedures. If possible, plan for cross-training of teams so that those team members are familiar with a variety of recovery roles and responsibilities.

CAUTION

Although some companies might feel that the BCP development job is done once the plan is complete, it is important to remember that no demonstrated recovery exists until the plan has been tested.

Testing

This final phase of the process is to test and maintain the BCP. Training and awareness programs are also developed during this phase. The test of the disaster-recovery plan is critical. Without performing a test, there is no way to know whether the plan will work. Testing transforms theoretical plans into reality. Testing should be repeated at least once a year. Tests should start with easiest parts of the plan and then build to more complex items. The initial tests should focus on items that support core processing, and they should be scheduled during a time that causes minimal disruption to normal business operations. As a CISSP candidate, you should be aware of the five different types of BCP tests:

- **Checklist**—Although this is not considered a replacement for a live test, a checklist is a good first test. A checklist test is performed by sending copies of the plan to different department managers and business unit managers for review. Each recipient reviews the plan to make sure nothing was overlooked.

- **Structured walkthrough**—This test is performed by having the members of the emergency management team and business unit managers meet in a conference to discuss the plan. The plan then is "walked through" line by line. This gives all attendees a chance to see how an actual emergency would be handled and to discover discrepancies. By reviewing the plan in this way, errors and omissions might become apparent.

CAUTION

The primary advantage of the structured walkthrough is to discover discrepancies between different departments.

- **Simulation**—This is an actual simulation of a real disaster. This drill involves members of the response team acting in the same way they would if there had been an actual emergency. This test proceeds to the point of recovery or to relocation of the alternative site. The primary purpose of this test is to verify that members of the response team can perform the required duties with only the tools they would have available in a real disaster.
- **Parallel**—A parallel test is similar to a structured walkthrough but actually invokes operations at the alternative site. Operations at the new and old sites are run in parallel.
- **Full interruption**—This plan is the most detailed, time-consuming, and thorough. A full interruption test mimics a real disaster, and all steps are performed to complete backup operations. It includes all the individuals who would be involved in a real emergency; both internal and external to the organization. Although a full interruption test is the most thorough, it is also the scariest because it can create its own disaster.

EXAM ALERT

The CISSP exam will require you to know the differences of each test type. You should also note the advantages and disadvantages of each.

The final step of the BCP process is to combine all this information into the BCP plan and inter-reference it with the organization's other emergency plans. Although the organization will want to keep a copy of the plan onsite, there should be another copy offsite. If a disaster occurs, rapid access to the plan will be critical.

CAUTION

Access to the plan should be restricted so that only those with a need to know can access the entire plan.

Monitoring and Maintenance

When the testing process is complete, a few additional items still need to be considered. This is important because some might falsely believe that the plan is completed once tested. That's not true. All the hard work that has gone into developing the plan can be lost if controls are not put into place to maintain the current level of business continuity and disaster recovery. Life is not static and neither should the organization's BCP plans be. The BCP should be a living document, subject to constant change.

To ensure the plan is maintained, first build in responsibility for the plan. This can be done by

- **Job descriptions**—Individuals responsible for the plan should have this responsibility detailed in their job description. Management should work with HR to have this information added to the appropriate documents.
- **Performance reviews**—The accomplishment (or lack of accomplishment) of appropriate plan maintenance tasks should be discussed in the responsible individual's annual or biannual evaluations.
- **Audits**—The audit team should review the plan and make sure that it is current and appropriate. The audit team will also want to inspect the offsite storage facility and review its security, policies, and configuration.

Also, disaster recovery implications for monitoring, maintaining, and recovery should be made a part of any discussions for procuring new equipment, modifying current equipment, or for making changes to the infrastructure. The best method to accomplish this is to add BCP review into all change management procedures. If changes are required to the approved plans, they must also be documented and structured using change management. A centralized command and control structure eases this burden. Table 7.2 lists the individuals responsible for specific parts of the BCP process are listed in.

TABLE 7.2 BCP Process Responsibilities

Person or Department	Responsibility
Senior management	Project initiation, ultimate responsibility, overall approval, and support
Middle management or business	Identification and prioritization of critical systems unit managers
BCP committee and team members	Planning, day-to-day management, implementation, and testing of the plan
Functional business units	Plan implementation, incorporation, and testing

CAUTION

Senior management is ultimately responsible for the BCP. This includes funding, project initiation, overall approval, and support.

Disaster Life Cycle

Although the BCP deals with what is needed to keep the organization running and what functions are most critical, the DRP's purpose 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 include

- Crisis management
- Recovery
- Reconstitution
- Resumption

When disasters occur, the organization must be ready to respond. Table 7.3 shows a sample disaster recovery checklist.

TABLE 7.3 Disaster Checklist

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

EXAM ALERT

The disaster recovery manager should direct short-term recovery actions immediately following a disaster.

Individuals responsible for emergency management will need to assess damage and perform triage. Areas impacted the most will need attention first. Protection of life is a priority while working to mitigate damage. Recovery from a disaster will entail sending personnel to the recovery site. When employees and materials are at the recovery site, interim functions can resume operations. This might entail installing software and hardware. Backups might need to be loaded and systems might require configuration.

Each step might not occur in series. As an example, while the recovery process is taking place, teams will also be dispatched to the disaster site to start the cleanup, salvage, and repair process. When those processes are complete, normal operations can resume.

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.

Flat Tires Are a Fact of Life

When teaching this domain in the classroom, one of the things I always try to impress on students is that this is something that, in reality, they already really know. Consider this: While driving home from the airport, I had a flat tire. Here is what transpired step by step:

- **Crisis management**—On realizing I had a flat, I pulled safely off the freeway.
- **Recovery**—Working quickly, I jacked up the car and replaced the flat tire with the emergency spare that GM generously provides.
- **Reconstitution**—Back on the freeway, I was able to limp along with my 50-miles-per-hour-rated spare until I could reach a tire repair shop.
- **Resumption**—As expected, the technician confirmed that the tire could not be fixed. But for only $149 plus a few fees, he could get me back on the road home. With the new tire on the car and my wallet a little emptier I was, indeed, back on the road headed home.

Consider this story when you are trying to conceptualize disaster recovery and, hopefully, it will make the task a little easier.

Teams and Responsibilities

Individuals involved in disaster recovery must deal with many things; when called to action, their activities center on emergency response, assessing the damage, recovery operations, and restoration. Figure 7.5 illustrates an example of disaster recovery activities.

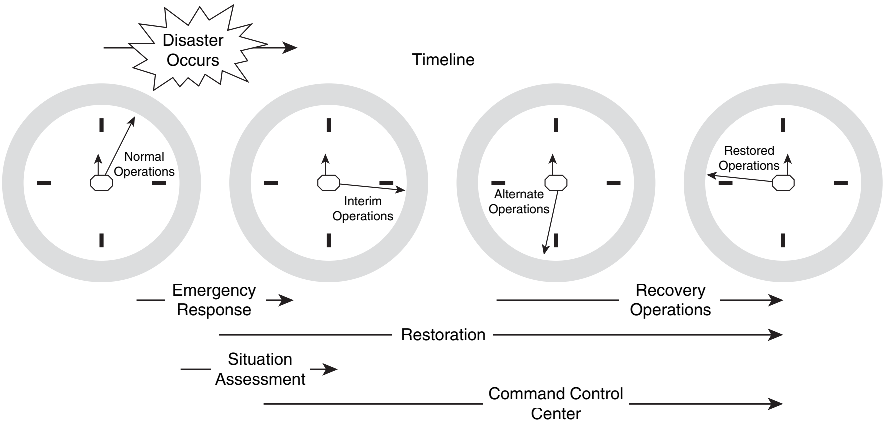


FIGURE 7.5 Disaster recovery timeline.

The salvage team is responsible for the reconstruction of damaged facilities. This includes cleanup, recovery of assets, creation of documentation for filing insurance or legal actions, and restoration of paper documents and electronic media. The recovery team has the necessary authority and responsibility to get the alternate site up and running. This site will be used as a stand-in for the original site until full operations can be restored. Although the CISSP exam will not require an in-depth understanding of all the teams and their responsibilities in a real disaster, a few additional teams and their roles are as follows:

- **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 that are financially and legally responsible. They must also handle the media and public relations.
- **Damage assessment team**—These individuals are the estimators. They must determine the damage and estimate the recovery time.
- **Communications team**—Responsible for installing communications (data, voice, phone, fax, radio, video) at the recovery site.

- **Security team**—Manages the security of the organization during the time of crisis. They must maintain order after a disaster.
- **Emergency operations team**—These individuals reside at the alternative site and manage systems operations. They are primarily operators and supervisors that are familiar with system operations.
- **Incident response team**—This team responds to incidents and acts as a central clearinghouse for information.
- **Transportation team**—This team is responsible for notifying employees that a disaster has occurred, and is also in charge of providing transportation, scheduling, and lodging for those needed at the alternative site.
- **Coordination team**—This team is tasked with managing operations at different remote sites and coordinating the recovery efforts.
- **Finance team**—Provides budget control for recovery and provides accurate accounting of costs.
- **Administrative support team**—Provides administrative support and might also handle payroll functions and accounting.
- **Supplies team**—Coordinates with key vendors to maintain needed supplies.

CAUTION

Physical security is always of great importance after a disaster. Precautions such as guards, temporary fencing, and barriers should be deployed to prevent looting and vandalism.

Exam Prep Questions

1. What is the most important aspect of disaster recovery?

❍ **A.** A complete damage assessment

❍ **B.** Control of critical assets

❍ **C.** Restoration of business functions

❍ **D.** Protection of individual life

2. Which of the following groups is responsible for project initiation?

❍ **A.** Functional business units

❍ **B.** Senior management

❍ **C.** BCP team members

❍ **D.** Middle management

3. Which team is focused on the responsibilities needed to get an alternate site up and running?

❍ **A.** Salvage team

❍ **B.** BCP management team

❍ **C.** IT management

❍ **D.** Recovery team

4. Which of the following is not considered an advantage of a mutual aid agreement?

❍ **A.** Low cost

❍ **B.** Enforcement

❍ **C.** Documentation

❍ **D.** Testing

5. Which of the following uses batch processing?

❍ **A.** Remote journaling

❍ **B.** Hierarchical storage management

❍ **C.** Electronic vaulting

❍ **D.** Static management

6. Which of the following carries the most risk?

❍ **A.** Full interruption

❍ **B.** Parallel

❍ **C.** Walkthrough

❍ **D.** Checklist

7. Which of the following is the best definition of a software escrow agreement?

❍ **A.** Provides the vendor with additional assurances that the software will be used per licensing agreements

❍ **B.** Specifies how much a vendor can charge for updates

❍ **C.** Gives the company access to the source code under certain conditions

❍ **D.** Provides the vendor access to the organization's code if there are questions of compatibility

8. Which of the following will a business impact analysis *not* provide?

❍ **A.** Determining the maximum outage time before the company is permanently crippled

❍ **B.** Detailing how training and awareness will be performed and how the plan will be updated

❍ **C.** Establishing the need for BCP

❍ **D.** Selecting recovery strategies

9. Bob had a server crash on Thursday morning. Bob performed a backup in which he used the complete backup from Sunday and several other tapes from Monday, Tuesday, and Wednesday. Which tape-backup method was used?

❍ **A.** Full restore

❍ **B.** Structured restore

❍ **C.** Differential restore

❍ **D.** Incremental restore

10. Which of the following tape-rotation schemes involves using five sets of tapes, with each set labeled A through E?

❍ **A.** Tower of Hanoi

❍ **B.** Son-father-grandfather

❍ **C.** Complex

❍ **D.** Grandfather-father-son

11. If the recovery point objective (RPO) is low, which of the following techniques would be the most appropriate solutions?

❍ **A.** Clustering

❍ **B.** Database shadowing

❍ **C.** Remote journaling

❍ **D.** Tape backup

12. You have been assigned to the BCP team responsible for backup options and offsite storage. Your company is considering the purchase of software from a small startup operation that has a proven record for unique software solutions. To mitigate the potential for loss, which of the following should you recommend?

❍ **A.** Clustering

❍ **B.** Software escrow

❍ **C.** Insurance

❍ **D.** Continuous backup

Answers to Exam Prep Questions

1. **D**. The protection of individual life is the number one priority of security management. Although answer A is important because a damage assessment needs to be made, the most important item is the protection of individual life. Answer B is incorrect because even though the control of critical assets is important, the number one consideration in disaster recovery should be the protection of life. Answer C is incorrect because, again, the protection of life should be your number one concern.

2. **B**. Although the other groups listed have responsibilities in the BCP process, senior management is responsible for project initiation, overall approval, support, and is ultimately responsible and held liable. Answer A is incorrect because the functional business units are responsible for implementation, incorporation, and testing. Answer C is incorrect because the BCP team members are responsible for planning, day-to-day management, and implementation and testing of the plan. Answer D is incorrect because middle management is responsible for the identification and prioritization of critical systems.

3. **D**. The recovery team plays a critical role in the disaster-recovery process because it is focused on the requirements to get an alternative site up and running. Answer A is incorrect because the salvage team is responsible for assessing the damage and determining what can be recovered after a disaster has occurred. Answer B is incorrect because the management team consists of the individuals in charge of the plan overall. Answer C is incorrect because IT management is responsible for day-to-day operations.

4. **B**. The parties to this agreement must place their trust in the reciprocating organization to provide aid in the event of a disaster. However, the nonvictim might be hesitant to follow through if such a disaster occurred. None of the other answers represents a disadvantage because this is a low-cost alternative, it can be documented, and some tests to verify that it would work can be performed.

5. **C**. Electronic vaulting makes a copy of data to a backup location. This is a batch process operation that functions to keep a copy of all current records, transactions, or files at an offsite location. Remote journaling is similar to electronic vaulting, except that information is processed continuously in parallel, so answer A is incorrect. Hierarchical storage management provides continuous online backup functionality, so answer B is incorrect. Static management is a distracter and is not a valid choice, so answer D is incorrect.

6. **A**. A full interruption is the test most likely to cause its own disaster. All the other answers listed are not as disruptive, so answers B, C, and D are incorrect.

7. **C**. A software escrow agreement allows an organization to obtain access to the source code of business critical software if the software vendor goes bankrupt or otherwise fails to perform as required. Answer A is incorrect because an escrow agreement does not provide the vendor with additional assurances that the software will be used per licensing agreements. Answer B is incorrect because an escrow agreement does not specify how much a vendor can charge for updates. Answer D is incorrect because an escrow agreement does not address compatibility issues; it grants access to the source code only under certain conditions.

8. **A**. A BIA is a process used to help business units understand the impact of a disruptive event. Part of that process is determining the maximum outage time before the company is permanently crippled. The other answers are part of the BCP process but are not specifically part of the BIA portion, so answers B, C, and D are incorrect.

9. **D**. Incremental backups take less time to perform but longer to restore. Answer A is incorrect because a full backup backs up everything and, therefore, takes the longest time to create. Answer B is incorrect because the term *structured* addresses how a backup is carried out, not the method used. Answer C is incorrect because a differential backup does not reset the archive bit. It takes increasingly longer each night, but would require a shorter period to restore because only two restores would be needed: the last full and the last differential.

10. **A**. This tape-rotation scheme is named after a mathematical puzzle. It involves using five sets of tapes, with 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 4th day. Set C is used on the first non-A or non-B backup day and is used every 8th day. Set D is used on the first non-A, non-B, or non-C day and is used every 16th day. Set E alternates with set D. Answer B is incorrect because Son-father-grandfather is a distracter. Answer C is incorrect because complex does not refer to a specific backup type. Answer D is incorrect because grandfather-father-son includes four tapes for weekly backups, one tape for monthly backups, and four tapes for daily backups and does not match the description described in the question.

11. **D**. The RPO is the earliest point at which recovery can occur. If the company has a low RPO, tape backup is acceptable because there is a low need to capture the most current data. If the backup occurs at midnight and the failure is at noon the next day, 12 hours of data has been lost. Answers A, B, and C are incorrect because each of these would be used when a higher RPO, or more current data, is required.

12. **B**. The core issue here is that the company is an upstart that may not be around in a few years. If this were to happen, the company must protect itself so that it has access to the code. Escrow agreements allow an organization to obtain access to the source code of business-critical software if the software vendor goes bankrupt or otherwise fails to perform as required. Answers A, C, and D are incorrect because clustering and continuous backup do nothing to provide the company access to the source code should they cease to exist. Insurance is an option, but the expense is not necessary if the organization has rights and access to the code should something occur.

Need to Know More?

Business Continuity Institute: http://thebci.org/

Testing the BCP plan:
http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bcp_05.html

Tape-backup strategies: http://www.exabyte.com/support/online/documentation/whitepapers/basicbackup.pdf

Recovery point objective: http://www.disaster-resource.com/articles/03p_068.shtml

Lessons learned in disaster recovery:
http://itmanagement.earthweb.com/secu/article.php/925011

Availability in relation to MTBF: http://www.barringer1.com/ar.htm

Electronic vaulting: http://www.disaster-resource.com/articles/electric_vault_rapid_lindeman.shtml

Free space optics: http://www.seas.harvard.edu/hbbcl/fsoc.html

Disaster recovery process: http://helpnet.vccs.edu/NOC/Mainframe/drplan.htm

Recovery strategies: http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm

Disaster recovery planning: http://www.disaster-recovery-guide.com/

Backup vaulting: http://tinyurl.com/59wbjj

Index