TT TEXTBOOK TESTBANKS

# Solutions Manual for Principles of Incident Response and Disaster Recovery 3rd Whitman

SOLUTIONS MANUAL SAMPLE PREVIEW

PUBLISHER
Cengage

COPYRIGHT
2022

RESOURCE TYPE
Solutions Manual

ISBN
9780357508329

# Solution and Answer Guide

Whitman and Mattord, *Principles of Incident Response and Disaster Recovery* 3e, 2022,
ISBN 978-0357508329; Module 1: An Overview of Information Security and Risk Management

## Table of Contents



## End of Module Exercise Solutions

### Discussion Questions and Solutions

1. Look at the section and table in this module on the 12 categories of threats. Which of the categories best fits what is going on in the situation JJ described earlier in the opening scenario of this module?

   **Solution**
   *This question could generate several different answers; the key point is not which category students choose, but how they approach the issues. For example, the situation referenced in the opening scenario could potentially fall under the Theft threat category or Sabotage or espionage, depending on the intent. The discussion of threat categories is more theoretical, whereas the situation in the scenario is a potential attack via network connectivity. See the section in the text titled "Some or all of the above" on page 12.*

2. How does the exchange between JJ and Paul earlier in this module indicate that this company has thought about contingency planning?

   **Solution**
   *There is an incident response plan that Paul thinks will cover this issue.*

### Ethical Decision Making Questions and Solutions

1. Should JJ push the issue or initiate the event review process himself?

   **Solution**
   *The plan and policy of the company should not be dependent on any one person's reaction or response. Proper responses are detailed in the plan.*

## Review Questions and Solutions

1. What is information security?

   **Solution**
   *Information security is an umbrella term for the many programs and activities that work to ensure the confidentiality, integrity, and availability of information used by organizations. This includes steps to ensure the protection of organizational information systems. Information security (InfoSec) is the protection of the confidentiality, integrity, and availability of information, whether in storage, during processing, or in transmission.*

2. How is the CNSS model of information security organized?

   **Solution**
   *The CNSS model is organized along three axes. The first represents whether the data is being stored, being processed, or in transit. The second axis represents the characteristics of confidentiality, integrity, and availability, which must be protected in each data mode. The third axis represents the controls that implement policy, technology, or education for each mode and characteristic.*

3. What three principles are used to define the C.I.A. triad? Define each in the context in which it is used in information security.

   **Solution**
   *C.I.A. represents confidentiality, integrity, and availability. Information has the characteristic of confidentiality when only the people with the rights and privileges to access it are able to do so. Information has integrity when it has not been exposed (while stored or transmitted) to corruption, damage, destruction, or other disruption of its authentic state; in other words, it is whole, complete, and uncorrupted. Finally, information has availability when authorized users—people or computer systems—are able to access it in the specified format without interference or obstruction.*

4. What is a threat in the context of information security?

   **Solution**
   *A threat is a category of objects, people, or other entities that pose a potential risk of loss to an asset.*

5. What is an asset in the context of information security?

   **Solution**
   *An asset is an organizational resource that has value and thus needs to be protected.*

6. What is an attack in the context of information security?

   **Solution**
   *An attack is an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.*

7. What is a vulnerability in the context of information security?

   **Solution**
   *A vulnerability is a weakness or fault in the mechanisms meant to protect information and information assets from attack or damage.*

8. What is a loss in the context of information security?

   **Solution**
   *A loss is a single instance of an information asset that suffers damage or destruction, unintended or unauthorized modification or disclosure, or denial of use. As a specific example, when an organization's information is stolen, it has suffered a loss.*

9. What is intellectual property? Describe at least one threat to this type of asset.

   **Solution**
   *Intellectual property (IP) consists of original ideas and inventions created, owned, and controlled by a particular person or organization. IP includes the representation of original ideas. Software piracy or copyright violations are threats to this type of asset.*

10. What is an availability disruption? Pick a utility service provider and describe what might constitute a disruption.

    **Solution**
    *An availability disruption is a reduced level of service in an element of the critical infrastructure. An example might be a utility that fails to deliver electrical power to its subscribers in a blackout.*

11. What is a hacker and what are terms used to describe their skill levels?

    **Solution**
    *A hacker is a person who accesses systems and information without authorization and often illegally. Most hackers are grouped into two general categories—the expert hacker and the novice hacker.*

12. How does a brute force password attack differ from a dictionary password attack?

    **Solution**
    *In a brute force password attack, the attacker attempts to guess a password by trying every possible combination of characters and numbers in it. In a dictionary password attack, the attacker narrows the range of possible passwords by using a list of common passwords and possibly including attempts based on the target's personal information.*

13. What is phishing, and how is spear phishing different?

    **Solution**
    *Phishing is a form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that may lead to a data loss. When a phishing attack is specifically targeted at one person or a few people, it is called spear phishing.*

14. In general terms, what is policy?

**Solution**
*A policy is a plan or course of action used by an organization to convey instructions from its senior management to those who make decisions, take actions, and perform other duties on behalf of the organization. Policies are organizational laws in that they dictate acceptable and unacceptable behavior within the context of the organization's culture.*

15. What is an enterprise information security policy, and how is it used?

**Solution**
*An enterprise information security policy (EISP), also known as a general security policy, IT security policy, or information security policy, is a policy based on and directly supportive of the mission, vision, and direction of the organization, and it sets the strategic direction, scope, and tone for all security efforts. It is an executive-level document usually drafted by, or in cooperation with, the chief information officer of the organization.*

16. Why is shaping policy considered difficult?

**Solution**
*It requires ongoing discipline by senior management to consistently maintain and apply policy.*

17. What are standards? How are they different from policy?

**Solution**
*More detailed than policy, standards state what must be done to comply with policy.*

18. What is an issue-specific security policy?

**Solution**
*An issue-specific security policy (ISSP) addresses specific areas of technology and contains a statement about the organization's position on a specific issue. It requires frequent updates.*

19. List the critical areas covered in an issue-specific security policy.

**Solution**
*The critical elements of an ISSP are a statement of policy, authorized access and usage of equipment, prohibited usage of equipment, systems management, violations of policy, policy review and modification, and limitations of liability.*

20. What is a systems-specific security policy?

**Solution**
*Systems-specific security policies (SysSPs) are detailed policies that may resemble or include standards and procedures.*

21. When is a systems-specific security policy used?

**Solution**
*SysSPs are often used when specifying the configuration or maintenance of systems.*

22. What is risk management?

**Solution**
*Risk management is the process of identifying and controlling the risks to an organization's information assets.*

23. What are the two main parts of risk management?

**Solution**
*Risk management consists of two major undertakings: risk identification and risk control.*

24. Who is expected to be engaged in risk management activities in most organizations?

**Solution**
*All management levels are engaged in risk management. Among the communities of interest, the general management of the organization must structure the IT and information security functions to lead a successful defense of the organization's information assets, which consist of information and data, hardware, software, procedures, and people.*

25. What are the basic strategies used to control risk? Define each.

**Solution**
*The five basic risk treatment strategies are:*

- *Defense—Apply safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability.*
- *Transference—Shift the risk to other areas or to outside entities.*
- *Mitigation—Reduce the impact should the vulnerability be exploited.*
- *Acceptance—Determine the potential consequences and accept the risk without control or mitigation.*
- *Termination—Remove the information asset from the environment that represents a risk to its security.*

## Real-World Exercises and Solutions

### Exercise 1-1

Go to *www.symantec.com/security-center/threat-report*, then download and review the latest Internet Security Threat Report. According to the report, what threats are currently the most dangerous? Which of these top threats represent problems for you and your use of the Internet? Which of these top threats represent problems for your school or business?

**Solution**
*This exercise will yield varying answers over time, as this is a dynamic report. The intent is to have students gain experience in maintaining situational awareness and practicing critical thinking skills. See the grading rubric provided at the end of this document for scoring guidance.*

## Exercise 1-2

Visit your school's Web site and search for any information about a computer policy or Internet security policy used at your academic institution. Compare and contrast this policy with the ones discussed in this module. Are any sections missing? If so, which ones? Does the school's policy contain sections that are not described in this module? Why do you think those sections are included?

**Solution**

*This exercise will yield varying answers based on which institution is being researched. The intent is to have students gain experience in considering policy elements from an idealistic and theoretical perspective, as in the textbook, and the ways they are used in actual practice.*

## Exercise 1-3

Go to *https://cve.mitre.org*. What type of site is this, and what information can it provide? Now, paste in the URL *https://cve.mitre.org/cve*, then click Search CVE List, and enter "Ransomware" in the search field. Click Search again. What information is provided? How would this be useful? Click on one of the named results. What additional information is provided? How could this be useful?

**Solution**

*Mitre is a cross-industry information sharing site that provides common vulnerability and exposure information for historical and emerging topics. The CVE directory provides names and descriptions of active ransomware vulnerabilities and exposures.*

## Exercise 1-4

Open a Web browser and search for the "OWASP Top Ten." Visit the site. What information is provided here? What does it mean? How could a security manager use this information?

**Solution**

*This site offers a broad consensus view of the dominant risk elements in Web application programming. The utility of the site is its ongoing improvements in software assurance and software quality improvement programs.*

## Exercise 1-5

Open a Web browser and search for "NIST Computer Security Resource Center." Link to the home page. Click the Publications link, then click on the "SP NIST Special Publications" option. Locate SP 800-100. Review the HTML version. What critical information could a security administrator or manager gain from this document? What other documents would be of value to the security manager or technician?

**Solution**

*This document provides a broad overview of the elements of an information security program and assists managers in understanding how to establish and implement an information security program.*

## Grading Rubric

| **Grading Rubric**<br>These grading criteria can be applied to open-ended discussion questions, ethical decision making questions, review questions, and real-world exercises. | | | |
|---|---|---|---|
| 3<br>Exceeds Expectations | 2<br>Meets Expectations | 1<br>Needs Improvement | 0<br>Inadequate |
| • Student demonstrates accurate understanding of the concept.<br>• Student applies the concept appropriately.<br>• Student uses sound critical analysis to develop an insightful and comprehensive response to the prompt. | • Student demonstrates accurate understanding of the concept.<br>• Student applies the concept appropriately.<br>• Student develops a complete response to the prompt. | • Student's response demonstrates a gap in understanding of the concept.<br>• Student applies the concept incorrectly.<br>• Student's response is poorly developed or incomplete. | • Student's response is missing or incomplete.<br>• Student's response demonstrates a critical gap in understanding.<br>• Student is unable to apply the concept. |

# Instructor Manual

Whitman and Mattord, Principles of Incident Response and Disaster Recovery, Third Edition, 2022, 978-0-357-508329; Module 1: An Overview of Information Security and Risk Management

## Table of Contents

## Purpose and Perspective of the Module

The purpose of this module is to provide a brief overview of the broad field of information security as well as the process of risk management.

Contingency planning is an important element of information security, but before management can plan for contingencies, it should have an overall strategic plan for information security in place, including risk management processes to guide the appropriate managerial and technical controls. This module serves as an overview of information security, with special consideration given to risk management and the role that contingency planning plays in both.

## Cengage Supplements

The following product-level supplements provide additional information that may help you in preparing your course. They are available in the instructor resources.

- PowerPoint slides
- Cognero test bank
- MindTap assets to support the textbook
- This instructor's manual

## List of Student Downloads

Students should download the following items from the Student Companion Center to complete the activities and assignments related to this module:

- Module 1 hands-on projects

## Module Objectives

The following objectives are addressed in this module:

1.1 Define and explain information security

1.2 Describe the role of information security policy in the organization

1.3 Identify and explain the basic concepts and phases of risk management

**[return to top]**

## Key Terms

In order of use:

**contingency planning** The actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster. This planning includes incident response, disaster recovery, business continuity, and crisis management efforts, as well as preparatory business impact analysis.

**security** A state of being secure and free from danger or harm. Also, the actions taken to make someone or something secure.

**information security (InfoSec)** Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

**C.I.A. triad** The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.

**confidentiality** An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

**integrity** An attribute of information that describes how data is whole, complete, and uncorrupted.

**availability** An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

**access** A subject or object's ability to use, manipulate, modify, or affect another subject or object.

**asset** The organizational resource that is being protected. An asset can be logical, such as a Web site, software information, or data. An asset can also be physical, such as a person, a computer system, hardware, or other tangible objects.

**attack** An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect.

**control, safeguard, or countermeasure** Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization.

**exploit** A technique used to compromise a system.

**exposure** A condition or state of being exposed; in information security, exposure exists when a vulnerability is known to an attacker.

**loss** In this context, a single instance of an information asset that suffers damage or destruction, unintended or unauthorized modification or disclosure, or denial of use.

**risk** The probability of an unwanted occurrence, such as an adverse event or loss.

**subjects and objects of attack** A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack: the target entity.

**threat** Any event or circumstance that has the potential to adversely affect operations and assets. The term *threat source* is commonly used interchangeably with the more generic term *threat*.

**threat agent** The specific instance or a component of a threat.

**threat event** An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.

**threat source** A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents.

**vulnerability** A potential weakness in an asset or its defensive control system(s).

**intellectual property (IP)** Original ideas and inventions created, owned, and controlled by a particular person or organization; IP includes the representation of original ideas.

**software piracy** The unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property.

**availability disruption** A reduced level of service in an element of the critical infrastructure.

**service level agreement (SLA)** A document or part of a document that specifies the expected level of service from a service provider. An SLA usually contains provisions for minimum acceptable availability and penalties or remediation procedures for downtime.

**noise** The presence of additional and disruptive signals in network communications or electrical power delivery.

**faults** Short-term interruptions in electrical power availability.

**spikes** Short-term increases in electrical power availability, also known as swells.

**surges** Long-term increases in electrical power availability.

**sags** Short-term decreases in electrical power availability.

**brownouts** Long-term decreases in the quality of electrical power availability.

**blackouts** Long-term interruptions (outages) in electrical power availability.

**trespass** Unauthorized entry into the real or virtual property of another party.

**shoulder surfing** The direct, covert observation of individual information or system use.

**hacker** A person who accesses systems and information without authorization and often illegally.

**expert hacker** A hacker who uses an extensive knowledge of the inner workings of computer hardware and software to gain unauthorized access to systems and information. Also known as elite hackers, expert hackers often create automated exploits, scripts, and tools used by other hackers.

**professional hacker** A hacker who conducts attacks for personal financial benefit or for a crime organization or foreign government. Not to be confused with a penetration tester.

**penetration tester** An information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

**novice hackers** Relatively unskilled hackers who use the work of expert hackers to perform attacks. Also known as neophytes, n00bs, or newbies. This category of hackers includes script kiddies and packet monkeys.

**script kiddies** Hackers of limited skill who use expertly written software to attack a system. Script kiddies are also known as skids, skiddies, or script bunnies.

**packet monkeys** Script kiddies who use automated exploits to engage in denial-of-service attacks.

**privilege escalation** The unauthorized modification of an authorized or unauthorized system user account to gain advanced access and control over system resources.

**brute force password attack** An attempt to guess a password by trying every possible combination of characters and numbers in it.

**dictionary password attack** A variation of the brute force password attack that attempts to narrow the range of possible passwords by using a list of common passwords and possibly including attempts based on the target's personal information.

**rainbow table** A table of hash values and their corresponding plaintext values that can be used to look up password values if an attacker is able to steal a system's encrypted password file.

**social engineering** The process of using social skills to convince people to reveal access credentials or other valuable information to an attacker.

**advance-fee fraud (AFF)** A form of social engineering, typically conducted via e-mail, in which an organization or some third party indicates that the recipient is due an exorbitant amount of money and needs only a small advance fee or personal banking information to facilitate the transfer. This may also involve prepayment for services with a payment larger than required; the overpayment is returned and then the initial payment is repudiated.

**phishing** A form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.

**spear phishing** Any highly targeted phishing attack.

**pretexting** A form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information. Pretexting is commonly performed by telephone.

**information extortion** The act of an attacker or trusted insider who steals information from a computer system and demands compensation for its return or for an agreement not to disclose the information. Also known as cyberextortion.

**ransomware** Computer software specifically designed to identify and encrypt valuable information in a victim's system in order to extort payment for the key needed to unlock the encryption.

**sextortion** A spear-phishing and blackmail attack that demands payment to preclude the distribution of hacked recordings of the target visiting pornographic Web sites.

**hacktivists** Hackers who seek to interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency. See also *cyberactivists*.

**cyberactivists** See *hacktivists*.

**cyberterrorism** The conduct of terrorist activities by online attackers.

**malware** Computer software specifically designed to perform malicious or unwanted actions.

**viruses** Types of malware that are attached to other executable programs. When activated, they replicate and propagate to multiple systems, spreading by multiple communications vectors. For example, a virus might send copies of itself to all users in the infected system's e-mail program.

**worms** Types of malware that are capable of activation and replication without being attached to an existing program.

**Trojan horses** Malware programs that hide their true nature and reveal their designed behavior only when activated.

**polymorphic threat** Malware (a virus or worm) that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures.

**back door** A malware payload that provides access to a system by bypassing normal access controls. A back door is also an intentional access control bypass left by a system designer to facilitate development.

**trap door** See *back door*.

**maintenance hook** See *back door*.

**denial-of-service (DoS) attack** An attack that attempts to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.

**distributed denial-of-service (DDoS) attack** A DoS attack in which a coordinated stream of requests is launched against a target from many locations at the same time using bots or zombies.

**zombie** See *bot*.

**bot** An abbreviation of *robot*, an automated software program that executes certain commands when it receives a specific input. See also *zombie*.

**spam** Unsolicited commercial e-mail, typically advertising transmitted in bulk.

**packet sniffers** Software programs or hardware appliances that can intercept, copy, and interpret network traffic.

**network sniffers** See *packet sniffers*.

**spoofing** A technique for gaining unauthorized access to computers using a forged or modified source IP address to give the perception that messages are coming from a trusted host.

**pharming** The redirection of legitimate user Web traffic to illegitimate Web sites with the intent to collect personal information.

**man-in-the-middle** A group of attacks whereby a person intercepts a communications stream and inserts himself in the conversation to convince each of the legitimate parties that the attacker is the other communications partner. Some man-in-the-middle attacks involve encryption functions.

**theft** The illegal taking of another's property, which can be physical, electronic, or intellectual.

**policy** In business, a statement of managerial intent designed to guide and regulate employee behavior in the organization; in IT, a computer configuration specification used to standardize system and user behavior.

**information security policies** Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets.

**standards** Detailed statements of what must be done to comply with the policy, sometimes viewed as the rules governing policy compliance. If the policy states that employees must "use strong passwords, frequently changed," the standard might specify that the password "must be at least 10 characters, with at least one number, one uppercase letter, one lowercase letter, and one special character."

**procedures** Step-by-step instructions designed to assist employees in following policies, standards, and guidelines. If the policy states to "use strong passwords, frequently changed," the procedure might advise that "in order to change your password, first click on the Windows Start button, then…."

**practices** Examples of actions that illustrate compliance with policies. If the policy states to "use strong passwords, frequently changed," the practices might advise that "according to X, most organizations require employees to change passwords at least semiannually."

**guidelines** Nonmandatory recommendations the employee may use as a reference in complying with the policy. If the policy states to "use strong passwords, frequently changed," the guidelines might advise that "we recommend you don't use family or pet names, or parts of your Social Security number, employee number, or phone number in your password."

**enterprise information security policy (EISP)** The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts. An EISP is also known as a security program policy, general security policy, IT security policy, high-level InfoSec policy, or simply an InfoSec policy.

**issue-specific security policy (ISSP)** An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as one of its processes or technologies.

**systems-specific security policies (SysSPs)** Organizational policies that often function as standards or procedures to be used when configuring or maintaining systems. SysSPs can be separated into two general groups—managerial guidance and technical specifications—but they may be written as a single unified SysSP document.

**risk management (RM)** The entire program of planning for and managing risk to information assets in the organization.

**RM framework** The overall structure of the strategic planning and design for the entirety of the organization's RM efforts.

**RM process** The identification, analysis, evaluation, and treatment of risk to information assets, as specified in the RM framework.

**risk assessment** An approach to combining risk identification, risk analysis, and risk evaluation into a single strategy.

**risk treatment** The selection of a strategy to address residual risk in an effort to bring it into alignment with the organization's risk appetite.

**residual risk** The risk to information assets that remains even after current controls have been applied.

**risk appetite** The quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.

**risk tolerance** The assessment of the amount of risk an organization is willing to accept for a particular information asset, typically synthesized into the organization's overall risk appetite.

**risk threshold** See *risk tolerance*.

**risk appetite statement** A formal document developed by the organization that specifies its overall willingness to accept risk to its information assets, based on a synthesis of individual risk tolerances.

**risk management plan** A document that contains specifications for the implementation and conduct of RM efforts.

**risk identification** The recognition, enumeration, and documentation of risks to an organization's information assets.

**information asset** Within the context of risk management, any collection, set, or database of information or any asset that collects, stores, processes, or transmits information of value to the organization. Here, the terms *data* and *information* are interchangeable.

**media** Hardware, integral operating systems, and utilities that collect, store, process, and transmit information.

**data classification scheme** A formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it.

**threat assessment** An evaluation of the threats to information assets, including a determination of their likelihood of occurrence and potential impact of an attack.

**risk analysis** A determination of the extent to which an organization's information assets are exposed to risk.

**likelihood** The probability that a specific vulnerability within an organization will be attacked by a threat.

**impact** An understanding of the potential consequences of a successful attack on an information asset by a threat.

**uncertainty** The state of having limited or imperfect knowledge of a situation, making it less likely that organizations can successfully anticipate future events or outcomes.

**risk evaluation** The process of comparing an information asset's risk rating to the numerical representation of the organization's risk appetite or risk threshold to determine if risk treatment is required.

**risk control** See *risk treatment*.

**defense risk treatment strategy** The risk treatment strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards in an effort to change the likelihood of a successful attack on an information asset. Also known as the *avoidance strategy*.

**avoidance strategy** See *defense risk treatment strategy*.

**transference risk treatment strategy** The risk treatment strategy that attempts to shift risk to other assets, other processes, or other organizations.

**mitigation risk treatment strategy** The risk treatment strategy that attempts to reduce the impact of the loss caused by an incident, disaster, or attack through effective contingency planning and preparation.

**acceptance risk treatment strategy** The risk treatment strategy that indicates the organization is willing to accept the current level of residual risk. As a result, the organization makes a conscious decision to do nothing else to protect an information asset from risk and to accept the outcome from any resulting exploitation.

**termination risk treatment strategy** The risk treatment strategy that eliminates all risk associated with an information asset by removing it from service.

**process communications** The necessary information flow within and between the governance group, RM framework team, and RM process team during the implementation of RM.

**process monitoring and review** The data collection and feedback associated with performance measures used during the conduct of the process.

**[return to top]**

# What's New in This Module

The following elements are improvements in this module from the previous edition:

- Additional material on risk management
- Revised definitions

**[return to top]**

# Module Outline

## Introduction

I. Begin the course by explaining that this text is about being prepared for the unexpected and being ready for such events as incidents and disasters. We call this contingency planning, and the sad fact is that most organizations do not incorporate it into their day-to-day business activities.

II. Discuss the effects that the September 11, 2001, attacks in New York, Pennsylvania, and Washington, D.C. had on contingency planning.

III. Introduce the term *information security*.

**Teaching Tip**: Most people have never thought seriously about dealing with a major disaster. Pose these questions to students to raise their awareness of the need for disaster planning: If you knew that your company was going to burn to the ground tonight, what would you choose to take out of the building? Do you have an evacuation "hot list"? How long would it take before you could be up and running again in a new location?

**Teaching Tip**: To learn more about information system risk management, visit ***www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204***.

## An Overview of Information Security

I. Introduce the terms *C.I.A. triad*, *confidentiality*, *integrity*, and *availability*. Use Figure 1-1 to aid the discussion.

**Teaching Tip**: There is a distinction between *data* and *information*, although not everyone agrees on the specifics. Data generally refers to raw facts, while information is data in a usable form, usually following some processing and interpretation. When talking about the value of a company's information assets, this distinction becomes more important.

**Teaching Tip**: Point out the importance of protecting information at all times and in all places. Discuss the 2005 incident in which some of Bank of America's backup tapes of credit card information were lost in transit from one facility to another.

**Teaching Tip**: To learn more about the C.I.A. triad, visit ***www.f5.com/labs/articles/education/what-is-the-cia-triad#:~:text=These%20three%20letters%20stand%20for,objectives%20for%20every%20security%20program***.

## Key Information Security Concepts

I. Introduce the terms *threat*, *asset*, *attack*, *threat agent*, *vulnerability*, *exploit*, *control*, *safeguard*, and *countermeasure*.

**Teaching Tip**: Ask students to discuss how an employee might be considered a vulnerability.

## The 12 Categories of Threats

I. Use Table 1-1 to discuss the following threats to information security:

a. Espionage or Trespass—Point out that the classic perpetrator of deliberate acts of espionage or trespass is the hacker.

**Teaching Tip**: DefCon is an annual convention of hackers that is held to share vulnerabilities and exploits.

b. Software Attacks—Introduce the terms *virus*, *worm*, *back door*, *zombie, bot*, *polymorphic threat*, *DoS attack*, and *malware*.

**Teaching Tip***:* Most students will be familiar with these terms, but may not understand the differences between them.

c. Human Error or Failure—Discuss the difference between human error and failure.

**Teaching Tip***:* Human error or failure can result in catastrophic events. The immediate cause of the Chernobyl nuclear reactor disaster was a mismanaged electrical engineering experiment conducted by engineers with no knowledge of reactor physics. For details, go to ***www.pbs.org/wgbh/pages/frontline/shows/reaction/readings/chernobyl.html***.

d. Theft—Point out that theft is often an overlapping category with software attacks, espionage or trespass, information extortion, and compromises to intellectual property.

e. Compromises to Intellectual Property—Discuss the risks involved in “bring your own device” (or BYOD) systems.

f. Sabotage or Vandalism—Introduce the term *cyberterrorism*.

g. Technical Software Failures or Errors—Introduce the term *trap door* and discuss its security implications.

h. Technical Hardware Failures or Errors—Point out that technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw.

i. Forces of Nature—Discuss why these threats are considered the most dangerous.

**Teaching Tip**: To read about lessons learned from the 2011 earthquake, tsunami, and nuclear disaster that devastated large parts of the area in and around Sendai, Japan, go to ***www.pkfindia.in/Value%20Adds/Lessons%20from%20the%20disasters%20in%20Japan.pdf***.

j. Deviations in Quality of Service by Service Providers—Note that Internet service, communication, and power irregularities can dramatically affect the availability of information and systems.

**Teaching Tip**: Ask students to discuss the impact that the total loss of telephone communications (both landlines and cell phones) would have on their school or company.

k. Technological Obsolescence—Point out that IT professionals play a large role in the identification of obsolescence.

l. Information Extortion—Note that extortion is common in credit card number theft.

m. Some or All of the Previous Categories—Explain that in today's complex attack environment, most threats do not manifest as a simple effort by only one of the previously listed categories.

**Quick Quiz 1**

1. Objects, people, or other entities that pose a potential risk of loss to an asset are called _____.

   Answer: threats

2. Name the three critical elements of the C.I.A. triad.

   Answer: confidentiality, integrity, and availability

3. A targeted solution to misuse a specific vulnerability is called a(n) _____.

   Answer: exploit

4. _____ is the protection of the confidentiality, integrity, and availability of information, whether in storage, processing, or transmission.

   Answer: Information security (InfoSec)

# The Role of Information Security Policy in Developing Contingency Plans

I. Emphasize that high-quality security programs begin and end with policy.

**Teaching Tip**: Without clearly defined and enforced policies in place, the effectiveness of a contingency plan will be seriously compromised. The organization also may be exposing itself to legal liabilities.

## Key Policy Components

I. Introduce the terms *policy*, *standards*, *procedures*, *practices*, and *guidelines*. Use Figure 1-3 to aid the discussion.

## Types of InfoSec Policies

I. To begin, note that there are three types of information security policies. Each is explained below.

II. Explain that the enterprise information security policy (EISP) guides the development, implementation, and management of the security program. It contains the requirements to be met by the information security blueprint or framework.

**Teaching Tip**: Emphasize that policy must not only define actions and expectations, but must define the consequences of failure to follow the policy. Policy without enforcement will have limited impact.

III. Discuss various approaches to creating and managing an issue-specific security policy (ISSP).

   a. Briefly discuss each common element of an ISSP:
      - Statement of policy
      - Authorized access and usage of technology
      - Prohibited usage of technology
      - Systems management
      - Violations of policy
      - Policy review and modification
      - Limitations of liability

IV. Explain that systems-specific security policies (SysSPs) can be written as a combination of two documents: managerial guidance and technical specifications.

   a. Managerial Guidance SysSP—This SysSP is created by management to guide the implementation and configuration of technology, and to address the behavior of people in the organization in ways that support the security of information.

b. Technical Specification SysSP—While a manager may work with a systems administrator to create managerial policy, the systems administrator may need to create a different type of policy to implement the managerial policy.

## Guidelines for Effective Policy Development and Implementation

I. Point out that policies are living documents that must be nurtured, given that they are constantly changing and growing. They must be properly developed, distributed, read, understood, agreed to, and uniformly applied.

**Quick Quiz 2**

1. True or False: Information security is primarily a technical problem, not a management issue.

   Answer: False. Information security is more of a management problem than a technical issue.

2. _____ are examples of actions that illustrate compliance with policies.

   a. Guidelines
   b. Practices
   c. Procedures
   d. Standards

   Answer: b. Practices

3. Which of the following is not a common type of information security policy?

   a. ISSP
   b. EISP
   c. ARSP
   d. SysSP

   Answer: c. ARSP

4. A(n) _____ is a formal statement of an organization's managerial philosophy that dictates acceptable and unacceptable behavior in an organization.

   Answer: policy

# Overview of Risk Management

I. Introduce the term *risk management (RM)*.

II. Risk management involves discovering and understanding answers to some key questions about the risk associated with an organization's information assets:

   a. Where and what is the risk (risk identification)?
   b. How severe is the current level of risk (risk analysis)?
   c. Is the current level of risk acceptable (risk evaluation)?
   d. What do I need to do to bring the risk to an acceptable level (risk treatment)?

**Teaching Tip**: Without a formal approach to risk management, a company is highly likely to be unable to mitigate the impact of a major incident.

## Knowing Yourself and Knowing Your Enemy

I. Point out that just because you have a control in place to protect an asset does not necessarily mean that the asset is protected.

II. Note that it is essential that all stakeholders conduct periodic asset inventories.

**Teaching Tip**: Point out the importance of including all departments within the company in this process, as people in different areas of activities will have unique insights into various aspects of threats and control strategies.

## Risk Management and the RM Framework

I. Introduce the terms *RM framework* and *RM process*. Use Figure 1-4 to aid the discussion.

II. Note that the RM framework consists of five key stages:

   a. Executive governance and support
   b. Framework design
   c. Framework implementation
   d. Framework monitoring and review
   e. Continuous improvement

## The RM Process

I. During the implementation phase of the RM framework, the RM plan guides the implementation of the RM process, in which risk evaluation and remediation of key assets are conducted.

II. List and briefly explain the following tasks of the RM process:

a. Establishing the *context*, which includes understanding both the organization's internal and external operating environments and other factors that could impact the RM process.

b. Identifying risk, which includes:

- Creating an inventory of information assets (see Table 1-2 in the text)
- Classifying and organizing those assets meaningfully
- Assigning a value to each information asset
- Prioritizing information assets
- Assessing threats to the cataloged assets
- Pinpointing vulnerable assets by tying specific threats to specific assets
- Using a TVA worksheet

c. Analyzing risk, which includes:

- Determining the likelihood that vulnerable systems will be attacked by specific threats
- Assessing the relative risk facing the organization's information assets so that risk management and control activities can focus on assets that require immediate attention
- Calculating the risks to which assets are exposed in their current setting
- Looking in a general way at controls that might come into play for identified vulnerabilities and ways to control the risks that the assets face
- Documenting and reporting the findings of risk identification and assessment

d. Evaluating the risk to the organization's key assets and comparing identified uncontrolled risks against its risk appetite

- Identifying individual risk tolerances for each information asset
- Combining or synthesizing individual risk tolerances into a coherent risk appetite statement

e. Treating the unacceptable risk

f. Summarizing the findings

## Risk Treatment/Risk Control

I. Explain that once the project team for information security development has identified information assets with unacceptable levels of risk, it must choose one of the following five approaches for controlling those risks:

   a. Defense—Note that there are three common methods of risk defense: defense through application of policy, defense through application of training and education programs, and defense through implementation of technology.

   b. Transference—This approach attempts to shift the risk to other assets, other processes, or other organizations.

   c. Mitigation—This approach attempts to reduce the impact of an incident or disaster through planning and preparation.

   d. Acceptance—This approach chooses to do nothing to protect the information asset. Instead, it accepts the outcome of potential exploitation.

   e. Termination—The asset is removed from the operating environment; the cost of protecting an asset sometimes outweighs its value.

**Quick Quiz 3**

1. _____ is the recognition, enumeration, and documentation of risks to an organization's information assets.

   Answer: Risk identification

2. _____ is the selection of a strategy to address residual risk in an effort to bring it into alignment with the organization's risk appetite.

   Answer: Risk treatment

3. The approach of combining risk identification, risk analysis, and risk evaluation into a single strategy is called _____.

   Answer: risk assessment

4. _____ is the risk that remains to the information asset even after the existing control has been applied.

   Answer: Residual risk

[return to top]

## Discussion Questions

You can assign these questions in several ways: in a discussion forum in your LMS, as whole-class discussions in person, or as a partner or group activity in class.

These questions are separate from the review questions and exercises in the textbook. For answers to the textbook questions, see the associated solutions for this module.

Additional class discussion options:

1. Does your company or school have a current disaster recovery plan? What are some of the activities involved in it? Do you feel confident that your company or school is prepared to survive a major disaster? Why or why not?
2. Has your company or school been the target of a network or system intrusion? What information was targeted? Was the attack successful? If so, what changes has your company or school made to ensure that this vulnerability has been controlled?

**[return to top]**

## Suggested Usage for Lab Activities

Please see the associated hands-on activities for this module.

**[return to top]**

## Additional Activities and Assignments

Please see associated solutions for the Closing Scenario at the end of the textbook module.

Additional project options include:

1. Select a major organization that was located near the area affected by Hurricane Katrina in 2005. Research their experiences and prepare a report detailing the unexpected challenges the organization encountered in returning operations to normal. Give suggestions for what might be added to the organization's contingency plan to mitigate those unexpected challenges.
2. Prepare a comparison chart for disasters caused by major forces of nature, including hurricanes, tornadoes, earthquakes, floods, and fires. List specific aspects of the incident response plan and the disaster recovery plan that would be different depending on the type of disaster.

**[return to top]**

# Additional Resources

## Cengage Video Resources

- MindTap Videos:
  - [list]

## Internet Resources

- Discussion of the causes of the Chernobyl nuclear reactor disaster: ***www.pbs.org/wgbh/pages/frontline/shows/reaction/readings/chernobyl.html***
- Cyberterrorism: ***www.huffingtonpost.com/dorian-de-wind/cyberterrorism-a-grave_b_2867430.html***
- Cyberterrorism: ***http://doras.dcu.ie/501/1/cybert_hype_reality_2007.pdf***
- More links are available in the Teaching Tips shown earlier in this document.

**[return to top]**