<CHN>CHAPTER FIFTEEN

<CHT>RISK MITIGATION

<COOT>Labs included in this chapter

* <COOH1>Lab 15.1 Online Research—Ethics in Information Technology
* Lab 15.2 Online Research—The Cloud
* Lab 15.3 Creating a Laptop Policy
* Lab 15.4 The Human Resources Department’s Role in Information Security
* Lab 15.5 Exploring the NIST 800-37 and NIST 800-53

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Threats, Attacks, and Vulnerabilities 15.2

Technologies and Tools 15.1, 15.3, 15.4

Architecture and Design 15.2, 15.3, 15.5

Identity and Access Management 15.2

Risk Management 15.1, 15.5

# <H1>Lab 15.1 Online Research—Ethics in Information Technology

**<H2>Objectives**

<TX1>Information is important to an organization, which can go out of business if there is significant damage to its data management capabilities. Companies are continually faced with potential damage to data as the result of human actions. External attackers try to penetrate the internal network to access or modify data, but internal users and information technology (IT) staff also can cause trouble, either accidentally or maliciously.

<TX2>Because information is the lifeblood of a company, human resources personnel and network managers must be very careful about whom they allow to work in the IT department. The ethics of IT workers in general and information security personnel in particular can be as critical as their technical skills. As you develop your technical skills, it is also important to develop an understanding of ethics as it applies to your career.

<TX2>After completing this lab, you will be able to:

* <BL>Compare the ethical standards of various IT organizations
* Analyze professional codes of ethics as they relate to your personal ethics

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Computer with Internet access

**<H2>Activity**

<FE1TX1>Estimated completion time: **60 minutes**

<TX1>In this lab, you search the Internet for information on ethics in information technology and then write a paper summarizing your findings.

1. <NL\_FIRST>Open your web browser and go to <URL>**http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct</URL>**.

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “ACM code of ethics.”

[END NOTE]

1. <NL\_MID>Review the Code of Ethics of the Association for Computing Machinery.
2. Go to <URL>**http://www.ieee.org/about/corporate/governance/p7-8.html</URL>**.

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “IEEE code of ethics.”

[END NOTE]

1. Review the Code of Ethics of the Institute of Electrical and Electronics Engineers.
2. Go to <URL>http://c.ymcdn.com/sites/www.aitp.org/resource/resmgr/forms/code\_of\_ethics.pdf</URL>.

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “AITP code of ethics.”

[END NOTE]

1. Review the Code of Ethics of the Association of Information Technology Professionals.
2. Go to <URL>https://www.isc2.org/Ethics</URL>.

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “ISC2 code of ethics.”

[END NOTE]

1. Review the Code of Ethics of the International Information Systems Security Certification Consortium (ISC)2.
2. Write a one- to two-page paper discussing the similarities and differences among the four codes of ethics that you reviewed. Discuss your impression of these codes. Are there elements that you question? Are there missing elements that should be included? Must you agree to abide by a code of ethics to be considered a professional?

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 5.1 Explain the importance of policies, plans, and procedures related to organizational security.

**<H2>Review Questions**

1. <FIB>A code of ethics \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
   1. **<**FIBA>is a means of identifying acceptable behavior
   2. has the same level of requirement as a law in many industrialized countries
   3. can be the basis of disciplinary action within an organization
   4. is used to direct members in what to believe
2. <FIB>The Code of Ethics of the Association for Computing Machinery indicates that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
   1. <FIBA>members are allowed to violate the law if there is a compelling ethical reason to do so
   2. once a member has entered in a professional contract, he or she must complete the assignment
   3. members are responsible for the effects of computing systems on society in general
   4. members must maintain confidentiality under any circumstances once they have promised to do so
3. <FIB>The Code of Ethics of the (ISC)2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
   1. <FIBA>discourages members from creating unnecessary fear or doubt in others
   2. discourages members from giving unjustified reassurance
   3. discourages members from allowing the organization’s code of ethics to overrule the member’s personal code of ethics
   4. allows members to violate the law if there is a compelling ethical reason to do so
4. <FIB>The Code of Ethics of the Institute of Electrical and Electronics Engineers \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
   1. <FIBA>requires members to avoid situations in which they may appear to have a conflict of interest, even if there is, in fact, no such conflict
   2. requires members to help their coworkers (whether they are IEEE members or not) to abide by the IEEE Code of Ethics
   3. encourages members to offer honest criticism on the technical work of others
   4. does not require members to treat others fairly, regardless of sexual preference
5. <SAESQ>Using any appropriate sources, write a one-paragraph definition of the term ethics.

# <H1>Lab 15.2 Online Research—The Cloud

**<H2>Objectives**

<TX1>“The Cloud” is one of the latest buzzwords in information technology. As with most buzzwords, there is a lot of hype associated with it, and perhaps because of this hype, many people are not sure what the term means. In essence, the cloud is simply a form of networking—that is, computers connected for the purpose of sharing resources. The cloud is a means of provisioning client systems with software resources. In a common use of the cloud, the client organization outsources most of the information technology tasks to the cloud services provider and therefore transfers many of the security risks of computing to the cloud services provider. Applications, operating systems, data storage, information security, and so forth are implemented and maintained by the cloud services provider, and the client organization is only responsible for maintaining the local area network and the client systems as well as providing an Internet connection. There are variations on this theme, but as you’ll see in this lab, one attribute is consistent: in all cloud services, the provisioning of information services is transparent to the end user.

<TX2>After completing this lab, you will be able to:

* <BL>Define cloud services
* Explain the three types of cloud services
* Identify best practices for cloud services clients

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Computer with Internet access

**<H2>Activity**

<FE1TX1>Estimated completion time: **35 minutes**

<TX1>In this lab, research cloud services.

1. <NL\_FIRST>Open your web browser and go to <URL>https://cloudsecurityalliance.org/csaguide.pdf</URL>.

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.”

[END NOTE]

1. <NL\_MID>Read the following sections of “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”:
2. <LL>Domain 1: Cloud Computing Architectural Framework
3. Domain 5: Information Lifecycle Management
4. Domain 9: Incident Response, Notification, and Remediation
5. Domain 10: Application Security
6. Domain 12: Identity and Access Management
7. Write a one- to two-page paper that does a Strength, Weakness, Opportunity, and Threats (SWOT) analysis of the cloud implementations of Information Systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.6 Explain the impact associated with types of vulnerabilities.
* 3.7 Summarize cloud and virtualization concepts.
* 4.1 Compare and contrast identity and access management concepts.

**<H2>Review Questions**

1. <FIB>Software developers at Acme Human Resources have created a program for internal use by Acme employees to track trends in the industry by merging information found on websites hosted by outside organizations and on FTP sites hosted by private industry analysts. This application runs on systems maintained by a vendor in another state that charges for these systems based on bandwidth use. The vendor’s systems are located in several states, and users of the application at Acme have no knowledge as to where or how the application is running at the time they use it. This is an example of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. <FIBA>cloud software as a service
   2. cloud platform as a service
   3. cloud infrastructure as a service
   4. none of the above
2. <MULT>According to “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” which of the following statements is correct?
   1. <MULTA>The cloud services provider should not commingle a customer’s data with data belonging to other customers in transit or when in operational storage. This requirement is not practical for data backups.
   2. The cloud services provider should be responsible for determining who should have access to data stored by customers.
   3. It is impractical in cloud services agreements to stipulate that customers shall know the geographical location of their data.
   4. In a multitenant environment, data destruction is difficult.
3. <MULT>According to “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” which of the following statements is correct?
   1. <MULTA>The customers of cloud services providers should require that they have significant involvement in security incident response.
   2. Cloud services providers should disclose their definition of security incidents to customers before any contract is signed.
   3. The appropriate response by a cloud services provider to a security incident reported from the provider’s firewall may vary depending on where the incident took place.
   4. Cloud services providers and customers should work closely together to determine who should be authorized to modify the customer’s data.
4. <MULT>According to “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” which of the following statements is correct?
   1. <MULTA>To assure the cloud services provider’s compliance with security measures, the customer should perform regular but unscheduled remote application vulnerability tests on its hosted applications.
   2. In a platform as a service environment, if the customer’s application relies on a dynamic link library (DLL) on the cloud services provider’s operating system, the customer is usually responsible for the security of the DLL.
   3. In a cloud-based computing environment, application security testing and deployment are essentially the same whether in software as a service, platform as a service, or infrastructure as a service mode.
   4. Cloud-based virtual systems that run applications should be hardened as they would be if they were in a DMZ.
5. <MULT>According to “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” which of the following statements is correct?
   1. <MULTA>If a potential software-as-a-service customer has already deployed Windows Active Directory for user identification and authentication, it could establish a trust relationship with the vendor using Active Directory Federation Services.
   2. To maintain optimal security, cloud services customers should leverage the provider’s proprietary authentication solutions.
   3. In a cloud-based computing environment, Security Assertion Markup Language is impractical as an authentication method because it was designed specifically for intra organizational security.
   4. Authentication as a service provides a secure means of enforcing access control policies in a cloud-based environment.

# <H1>Lab 15.3 Creating a Laptop Policy

**<H2>Objectives**

<TX1>Company policies define, at a high level, how an organization will fulfill its mission. Procedures specify how company policies will be implemented. For example, a policy may state that users will be authenticated by a two-factor authentication method, whereas a related procedure may detail what specific smart cards will be used, how to configure the certificate server, what types of digital certificates will be used, and so on.

<TX2>Developing policy and procedure may not be as captivating as developing software or engineering network infrastructure, but it is just as important. Without clear, complete, and appropriate policies and procedures, business would be haphazard, training of new employees would be inconsistent, and realistic goals for product and/or service quality would not likely be met. Moreover, regulatory and legal mandates would most likely be violated.

<TX2>After completing this lab, you will be able to:

* <BL>Develop a company laptop policy
* Explain how policies contribute to the achievement of an organization’s mission
* Evaluate a policy’s effectiveness and applicability and modify the policy as needed

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Computer with Internet access

**<H2>Activity**

<FE1TX1>Estimated completion time: **60–90 minutes**

<TX1>In this lab, you create a corporate policy for the management and use of laptops.

1. <NL\_FIRST>Review the following background information about the hypothetical company for which you will design a laptop policy.

* <BL>The Acme Printing and Publishing Company has corporate offices in New York City and regional offices in Scranton, Buffalo, and Baltimore. The company designs and prints internal publications for large corporations and for various U.S. government agencies. Much of the work product is considered highly classified by the company’s clients, and the Acme Information Technology and Security departments implement strong access controls.
* There are 250 employees in the corporate office and 75 employees in each regional office.
* Top-level management has decided to issue company laptops to 100 users (executives, quality control, and sales employees).
* The company laptops will be used to connect (a) to the corporate network via wired or wireless connections when in corporate locations, (b) to the Internet through an Internet service provider with which Acme has contracted, and (c) to the corporate network via VPN from remote locations.
* All laptops will run Windows 10 Enterprise Edition, Office 365, and several line-of-business applications. All network servers run Windows Server 2016.

1. <NL\_MID>You are tasked with developing a policy that governs the management and use of laptops. Consider both the company background described in Step 1 and what you have learned about information security during your security course. Take into account threats, risks, vulnerabilities, consequences (should a threat occur), and available security controls. Be sure to consider both technical (enforceable) and social (unenforceable) controls. Consider methods to assure compliance with your policy. Create an outline for the security section of the laptop policy. You should break the security section into specific areas, such as Physical Security, Access Control, and so on. For example, one of the entries under the Physical Security heading might be “All laptops will have a bar coded identification tag firmly affixed.”
2. Create the outline for your laptop policy using sources such as your course textbook and the Internet.
3. Assume that your laptop policy has been implemented and the company laptops have been issued. Your manager informs you that the following issue has been reported. A company sales employee, who was onsite at a client company’s location, connected his company laptop to the client’s network to download documents and the proprietary software program required to view them. The employee was unable to install the program and got an error message stating that he did not have the rights required to install the program and referring him to the Acme systems administrator.
4. Does your laptop policy address this issue? If not, revise your policy so that it does. If so, was the response the user received when trying to install the software consistent or inconsistent with your policy?
5. Several weeks later, your manager reported another incident. An employee used her company laptop to connect to a wireless hot spot at a coffee shop in an airport. The next day, she reported that her laptop was behaving oddly; programs were taking a long time to run, and when working on a Microsoft Word file, the document suddenly went blank and the file, which she was sure she had saved earlier, could not be found on her system. Later, from her home, she connected to the corporate network through her VPN connection. The next day, the log files of the remote access server and of the antivirus hardware/software showed that her laptop had been infected by a well-known virus and that an attempt had been made, during her VPN connection the previous day, to infect her office workstation with the same virus. The employee was clearly distraught, and there is no suspicion that this was a deliberate attack on her part.

Does your laptop policy address these issues? If not, revise your policy so that it does. If so, was the user’s experience with the use of the wireless hot spot and the infection of the laptop by a well-known virus consistent with your policy? Does your policy address the attempt by the laptop to infect the employee’s office workstation via the remote access server? If not, revise your policy so that it does. If so, was the outcome consistent with your policy?

1. Submit your laptop policy outline to your instructor.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.1 Explain use cases and purpose for frameworks, best practices, and secure configuration guide.
* 2.3 Given a scenario, troubleshoot common security issues.
* 2.4 Given a scenario, analyze and interpret output from security technologies.
* 2.5 Given a scenario, deploy mobile devices securely.
* 3.3 Given a scenario, implement secure systems design.

**<H2>Review Questions**

1. <FIB>Assume you designed the laptop policy described in this lab. Then your manager informs you that a member of the IT staff has been terminated for poor performance. Per human resources policy, the terminated employee has been immediately escorted out of the building by security personnel. His personal effects are to be collected by his manager (who is also your manager) and shipped to him. The terminated employee’s effects include a personal laptop (not issued to him by the company) that he has used to connect to the company network. Your laptop policy did not address the issue of employees connecting personal laptops to the company network, and he is not the only employee to have done so openly. No other policies prohibit this action. Your manager is concerned about confidential work-related files that may have been copied to the employee’s laptop and asks you to wipe the employee’s laptop hard drive before he ships it back to the employee. You are concerned about repercussions should you follow this instruction. The most logical thing to do next is to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. <FIBA>explain to your manager that his instruction is unethical
   2. consult the company’s legal department
   3. telephone the terminated employee and ask if it is OK to wipe the laptop hard drive
   4. ask your manager to obtain the terminated employee’s permission to wipe the drive
2. <MULT>Which of the following Windows Server 2016 features allows a corporate IT department to (a) prevent a remote access client from accessing the corporate network through a VPN connection unless the remote client meets the corporate security policies and (b) isolate and configure the remote client so that it does meet the corporate security policies?
   1. <MULTA>Routing and Remote Access Policies
   2. Network Access Protection
   3. Default Domain Policy/Computer Configuration/Windows Settings/Security Settings/User Rights Assignments/Remote Access Network Control
   4. Network Access Control
3. <FIB>A remote laptop user calls her corporate IT department complaining that she cannot install a proprietary software program needed to view a customer’s documents. The software program is located on the customer’s network, and the user, who is currently at the customer’s corporate offices, has already connected to the customer’s network and downloaded the program to her laptop. As the senior IT staff member on duty, you call the employee’s manager, who tells you that it is critical that the employee get access to the program from her laptop so that she can import the client documents into your company’s software program, which is installed on the employee’s laptop, and give the client an immediate bid on the work requested. Your company runs a Windows shop with all Windows 10 clients and all Windows Server 2016 servers. A single Active Directory domain is implemented. The most logical steps you should take are to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that are correct.)
   1. <FIBA>disable the employee’s laptop computer account in Active Directory
   2. install the customer’s program yourself
   3. log on to the employee’s laptop using Remote Desktop Protocol
   4. contact the customer’s IT department and have it install its program on the employee’s laptop
4. <MULT>Your company allows employees who use corporate laptops to connect to the Internet from public wireless hot spots. Which of the following items should your company’s laptop security policy include? (Choose all that apply.)
   1. <MULTA>File and Print Sharing are disabled on all networks except corporate-managed networks.
   2. WPA2 and WEP are to be implemented on all wireless connections.
   3. AES is required on all wireless connections to the corporate network.
   4. Split tunneling is prohibited.
5. <MULT>Which of the following authentication methods is possible to implement on a laptop computer? (Choose all that are correct.)
   1. <MULTA>Digital certificates
   2. Smart cards
   3. Fingerprint reader
   4. Photo-image pattern recognition

# <H1>Lab 15.4 The Human Resources Department’s Role in Information Security

**<H2>Objectives**

<TX1>The human resources department used to be called the personnel department. Personnel departments were concerned mostly with hiring, benefits, and payroll. As society and the courts became less tolerant of racism, sexism, discrimination, and harassment in the workplace, personnel departments became human resources departments and began to focus much more on assuring compliance with employment law.

<TX2>Human resources managers know that beyond being unethical, discrimination and harassment have cost companies a great deal in legal and settlement costs. As information security and privacy have become more subject to regulatory and legal sanctions, human resources departments have expanded their role into these areas as well.

<TX2>After completing this lab, you will be able to:

* <BL>Explain the role of a human resources department in maintaining information security

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>A computer with Internet access

**<H2>Activity**

<FE1TX1>Estimated completion time: **60–90 minutes**

<TX1>In this lab, you prepare a PowerPoint presentation on human resources and information security.

1. <NL\_FIRST>You work as an information technology policy consultant to growing companies. One of your clients is a software development company that has grown from a four-person operation to a 70-employee company in one year. The company expects to grow rapidly in terms of employees, contracts, and office locations within the next five years. Its management sees the need to formalize the organizational structure, which had, up to this point, been casually arranged. A plan is being drawn up to create a human resources department as well as a more organized IT department. You are involved in the preliminary information gathering and client education stage. After that, policies will be drafted.
2. <NL\_MID>You have been asked to prepare a one-hour presentation for management addressing the responsibilities of a human resources department as they relate to the security of information and information systems.
3. Using your favorite search engine, search on the following search strings (among others): “human resources and information security,” “human resources policy,” and “information security policy.”
4. Take notes on the information you find at various sites.
5. Create a PowerPoint presentation to accompany a one-hour talk. Create a minimum of 12 slides.
6. Submit the PowerPoint presentation to your instructor.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.1 Explain the importance of risk related concepts.
* 2.3 Given a scenario, implement appropriate risk mitigation strategies.
* 2.4 Given a scenario, implement basic forensic procedures.

**<H2>Review Questions**

1. <FIB>A human resources department typically \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
   1. <FIBA>conducts background checks of applicants for information technology positions
   2. monitors the levels of access to company resources that are assigned to different company job descriptions
   3. requires employees, contractors, and third-party users to sign agreements that address their responsibilities in handling data outside the organization’s boundaries (e.g., on mobile devices)
   4. handles customer complaints regarding privacy violations
2. <MULT>Who should receive human resources–sponsored security training? (Choose all that apply.)
   1. <MULTA>Employees
   2. Managers
   3. Contractors
   4. Executives
3. <MULT>Which of the following is a situation that a human resources department should investigate? (Choose all that apply.)
   1. <MULTA>An IT employee reports to the IT manager that a coworker has been burning copies of company-owned software for personal use.
   2. An IT employee reports to the IT manager that a coworker has been sharing his network logon credentials with his visitors.
   3. An IT employee reports to the IT manager that a coworker is planning to call in sick on the following Monday so she can visit a friend in a distant city.
   4. A manager reports that she suspects an employee of sharing confidential company information with an employee of a competitor.
4. <MULT>Which of the following is typically a responsibility of a human resources department? (Choose all that apply.)
   1. <MULTA>Assuring the return of company property from an employee who is being terminated
   2. Making a recommendation for an employee’s merit increase
   3. Maintaining documentation of employees’ agreements to abide by acceptable use policies related to the company’s digital assets
   4. Coordinating security clearance investigations for employees who require access to sensitive information
5. <TF>The level of access that an employee is granted to a corporate resource is determined by the human resources department. True or False?

# <H1>Lab 15.5 Exploring the NIST 800-37 and NIST 800-53

**<H2>Objectives**

<TX1>Developing policies and procedures for any department is a time-consuming task; doing so for an information technology department is a never-ending one. The life cycle of hardware and software is relatively short, and the complexities of interoperability between operating systems, network infrastructure devices, and services make IT policy and procedure development and maintenance an intimidating prospect. Although each organization has individual requirements, it is not necessary to reinvent the wheel when creating IT policies. The NIST 800-37 and NIST 800-53 standards provide a framework for Security controls and applying the risk management framework for federal information systems.

<TX2>After completing this lab, you will be able to:

* <BL>Explain the components of the NIST 800-37 and NIST 800-53 standards
* Explain the importance of risk frameworks as it applies to information systems

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>A computer with Internet access

**<H2>Activity**

<FE1TX1>Estimated completion time: **60–90 minutes**

<TX1>In this lab, you research the NIST 800-37 and NIST 800-53 standards and summarize your findings in a short paper.

1. <NL\_FIRST>Open your web browser and go to <URL><http://csrc.nist.gov/publications/PubsSPs.html#800-37></URL>.
2. <NL\_MID>Open another tab in your web browser and go to <URL>http://csrc.nist.gov/publications/PubsSPs.html#800-53</URL>.

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URLs no longer function, open a search engine such as Google and search for “NIST 800-37 or NIST 800-53.”

[END NOTE]

1. Read the two papers found through the links.
2. Research the NIST standards further as needed and then write a two-page paper summarizing the purpose and the provisions of the 800-37 and 800-53 standards. Answer the following questions:
3. <LL>What is the purpose of these standards and what do they provide?
4. How are they useful to the posture of risk management for a company?
5. What are the steps for following these standards?

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>3.9 Explain the importance of physical security controls.
* 5.1 Explain the importance of policies, plans, and procedures related to organizational security.
* 5.2 Summarize business impact analysis concepts.
* 5.3 Explain risk management processes and concepts.
* 5.4 Given a scenario, follow incident response procedures.

**<H2>Review Questions**

1. <MULT>The target audience for the NIST 800-37 include people associated with what part of information systems? (Choose all that apply.)
2. <MULTA>Design
3. Development
4. Implementation
5. Dissemination
6. <FIB>When referring to Tier 3 in the risk management framework in NIST 800-37, we refer to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ type of risk?
7. <FIBA>Tactical
8. Strategic
9. Physical
10. Virtual
11. <MULT>Which is the correct order for risk mitigation procedures?
12. <MULTA>Assess, Categorize, Select, Implement, Authorize, Monitor
13. Categorize, Assess, Implement, Select, Authorize, Monitor
14. Categorize, Authorize, Select, Implement, Assess, Monitor
15. Categorize, Select, Implement, Assess, Authorize, Monitor
16. <TF>Common controls, whether employed in organizational information systems or environments of operation, are authorized by senior officials. True or False?
17. <TF>The purpose of the 800-53 is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to not follow FIPS publication 200. True or False?