PART I

Organizational Security

CHAPTER 1

Organizational Security and Compliance

ITINERARY

- ○ **Objective 1.01** Explain risk-related concepts
- ○ **Objective 1.02** Carry out appropriate risk mitigation strategies

ETA

NEWBIE	SOME EXPERIENCE	EXPERT
3 hours	2 hours	1 hour

As part of an overall company strategy, security should be officially recognized as a critical business objective just like any other important business objective. In the past, the IT department had to define security and access controls for the company network and data. In today's Internet world, corporate management adapts the legalities of the business world to computer networks by ensuring that electronic transfer of information is secure to protect both the company and their customers.

To protect their assets, employees, and customers from security risks, organizations must analyze their security practices to identify the threats to their operations and protect themselves in the most cost-efficient way. Risks to your organization must be assessed based on their probability and impact (both quantitative and qualitative), and then security measures are implemented based on this risk analysis.

To ensure security across the organization, and to assure customers that the company can be trusted, overall security policies must be implemented to include several component policies and procedures that govern how the organization uses computer networks, protects and distributes data, and offers services to customers. Each component of the security policy defines specific security best practices for a particular topic, such as a password policy. These policies and procedures include rules on company Internet use, customer data privacy, company structure, and human resources hiring and termination practices. Many companies, such as those in the financial and health care sector, must now comply with several government regulations for the protection and privacy of customer data in their industry. Organizations must be diligent in crafting their policies to adhere to these regulations, and they must employ risk mitigation techniques to avoid violating these strict standards.

For a company's security policies to be effective, they must be communicated properly to the employees to ensure companywide knowledge and compliance. Rules won't be followed if nobody knows they exist. Many companies make use of consultants to create and draft security policies and procedures, but these policies often aren't communicated to the user community and aren't used. Employees need to be aware of security issues and procedures to protect not only themselves but also the company's services and data.

This chapter describes general risk assessment and mitigation strategies, and organizational policies that should be in place to protect an organization, its networks and data, its employees, and its customers.

Objective 1.01
CompTIA Security+ Objective 2.1

Explain Risk-Related Concepts

Risk management is the act of identifying, assessing, and reducing the risk of security issues that can impact your organization's operations and assets. The following sections describe these risk-related concepts:

- **Risk Control Types** Risk control types can be separated into three logical divisions: *management, operational,* and *technical.* Each risk control type is a separate but cooperative layer in your overall risk management strategy.
- **Risk Assessment** Use risk assessments to understand your current risks, their probability and impact, and the solutions to prevent them.
- **Risk Management Options** Depending on the type of risk, you have several options based on the nature and probability of the risk, and the cost of the solution: *avoidance, transference, acceptance, mitigation,* and *deterrence.*
- **Using Organizational Policies to Reduce Risk** Your organizational security is critical for ensuring that your company's risk management plan is properly detailed, communicated, and adhered to by your employees in all its activities through the use of policies.

Risk Control Types

Risk control types can be separated into three basic functions: *management, technical,* and *operational.*

Management

Risk management is an ongoing high-level function within your organization. Risk management begins with the risk assessment and analysis to identify the risk of security breaches against company assets, assessing the probability of a risk and estimating its impact, and defining the steps to reduce the level of that risk. The solutions to these risks must be properly analyzed and budgeted to ensure that the probability and impact of the risk are properly factored into a cost-effective solution.

Technical

Technical risk control describes the actual technical measures used to prevent security risks in your organization. From physical access controls (perimeter fencing, security passes, surveillance) to environmental controls (fire suppression, temperature controls), and deep-level network and system security (firewalls, antivirus scanning, content filters, and other network security devices), these controls perform the risk mitigation and deterrence that have been defined in your organization risk analysis.

Operational

Finally, there is an overall operational risk control that must be created and implemented throughout your company. This risk control strategy is concerned with how you conduct your daily organizational business to minimize the security risk to your organization and its business activities. These include company-wide policies that must be created, distributed, and used to educate your employees on how to conduct their day-to-day activities while being vigilant about organization security. Operational risk management also includes user education and vigilant monitoring and testing to make sure your plans are being adhered to by your organization and its activities are constantly analyzed to protect against new threats.

Exam Tip

Management risk controls the high-level risk management, assessment, and mitigations plans that define your overall organization security. Technical risk controls are the technical measures deployed to prevent security risks. Operation risk controls deal with security for your day-to-day organizational business activities.

Risk Assessment

Risk assessment and mitigation deals with identifying, assessing, and reducing the risk of security breaches against company assets. By assessing the probability of a risk and estimating the amount of damage that could be caused as a result, you can take steps to reduce the level of that risk.

Suppose, for example, that your company file server contains confidential company data. The file server asset is considered extremely valuable to the company, its clients, and its competitors. A considerable amount of financial damage would be incurred by the company in the event of loss, damage, or theft of the server. The risks and threats posed to the server could be physical—such as damage caused by a natural disaster or a hardware malfunction—or nonphysical—such as viruses, network hacker attacks, and data theft if the server is easily accessible through a network. The costs associated with reducing these risks are mitigated by the potential costs of losing data on the file server.

To help reduce these risks, you can take several actions:

- Use multiple hard drives and power supplies for fault tolerance.
- Implement a good backup scheme.
- Protect the server through physical security such as door access controls.
- Install antivirus software.
- Disable unused network services and ports to prevent network attacks.

To identify the risks that pose a security threat to your company, you can perform a risk analysis on all parts of the company's resources and activities. By identifying risks and the amount of damage that could be caused by exploiting a system vulnerability, you can choose the most efficient methods for securing the system from those risks. Risk analysis and assessment can identify where too little or even too much security exists, and where the cost of security is more than the cost of the loss because of compromise. Ultimately, risk analysis and assessment is a cost/benefit analysis of your security infrastructure.

Risk analysis and assessment involves three main phases:

- **Asset identification** Identify and quantify the company's assets.
- **Risk analysis** Identify and assess the possible security vulnerabilities and threats.
- **Risk likelihood and impact** Rate your various risks according to how likely they are to occur and their impact.
- **Cost of solutions** Identify a cost-effective solution to protect assets.

Asset Identification

Company assets can include physical items such as computer and networking equipment, and nonphysical items such as valuable data. *Asset identification* involves identifying both types of assets and evaluating their worth. Asset values must be established beyond the mere capital costs—acquisition costs, maintenance, the value of the asset to the company, the value of the asset to a competitor, what clients would pay for the asset or service, the cost of replacement, and the cost if the asset were compromised should also be considered. For example, a list of a company's clients can be easily re-created from backup if the original is lost or destroyed, but if the list finds its way into the hands of a competitor, the resulting financial damage could be devastating. Ultimately, the value of the assets you're trying to protect drives the costs involved in securing that asset.

Risk Analysis

Risk analysis deals with identifying, assessing, and reducing the risk of security breaches against company assets. By assessing the probability of a risk and estimating the amount of damage that could be caused as a result, you can take steps to reduce the level of that risk. To identify the risks that pose a security threat to your company, you can perform a risk analysis on all parts of the company's resources and activities.

Quantitative risk analysis is a strict dollar-amount calculation of the exact cost of the loss or a specific company asset because of a disaster. This is a straightforward method that can be applied for simple situations. For example, if a hard drive in a RAID (redundant array of inexpensive disks) system fails, it is simply replaced with a new hard drive. There is no loss of data because the information is rebuilt from the rest of the array.

Qualitative risk analysis must take into account tangible and several other, intangible factors in determining costs. Consider a denial-of-service network attack on your company's web store server that causes four hours of downtime and corrupted data on a back-end transactional database. You are not only faced with the monetary loss from your web site being down and customers not being able to order products for many hours, but the time it takes to perform countermeasures against the attack, get your web server back into operation, recover any lost data from your database, and also take into account data that cannot be recovered. The costs in this scenario include the manpower hours in recovering from the attack, the loss of orders from the web store during the downtime, monetary loss from corrupted data that cannot be restored, and even potential loss of future business from disgruntled customers.

Exam Tip

Quantitative risk analysis is a dollar-amount calculation of the exact cost of the loss due to a disaster. Qualitative risk analysis includes intangible factors, such as loss of potential business, in determining costs.

There are additional risks often ignored in a risk analysis in regard to virtualization technology and cloud computing. Using virtualization technology, a computer can host multiple instances of an operating system environment all running from the same computer on the same hardware. The consolidation of many different types of services on the same hardware creates a security risk that if that system is hacked or fails, it will take down every virtualized server that runs on the system.

The risk of a single point of failure for cloud computing is very similar. Cloud computing aggregates services in a virtual environment where all aspects of the cloud, from the platform, to the software, to the entire infrastructure, are based on a distributed web service. If the cloud service fails, you may lose all access to your services and data until the cloud service is restored.

Travel Assistance

See Chapter 8 for more detailed information on virtualization and cloud computing.

Overall, your risk assessment must be wide in scope to use both quantitative and qualitative analysis to determine your risk factors from all aspects of your company's operations.

Risk Likelihood and Impact

As part of your risk assessment and mitigation strategy, you will need to rate your various risks according to how likely they are to occur and their impact. The risks more likely to occur and their calculated impact are ranked toward the top of the list to indicate where solution efforts should be most concentrated. For example, within a company that already practices strict physical security and access control methods, the priority of risk scenarios could be geared toward nonphysical threats, such as viruses and network hackers, because this would have a greater impact on their ability to operate.

The likelihood and impact of a risk has a strong measure on your cost analysis for budgeting funds for risk countermeasures and mitigation. A calculation used to determine this factor is *annual loss expectancy (ALE)*. You must calculate the chance of a risk occurring, sometimes called the *annual rate of occurrence (ARO),* and the potential loss of revenue based on a specific period of downtime, which is called the *single loss expectancy (SLE).* By multiplying these factors together, you arrive at the ALE. This is how much money you expect to lose on an annual basis because of the impact from an occurrence of a specific risk. Using the ALE, you can properly budget the security measures to help protect against that particular risk from occurring.

For example, if a file server is at 25 percent risk of being infected by a virus, its ARO is 0.25. During the time the file server is down and data is being recovered, none of your employees can work. For a downtime of two hours, you calculate $8000 of lost time and productivity. By multiplying these two factors (0.25 and $8000), you get an ALE value of $2000. You can use this amount to budget for additional antivirus software protection to help lower this risk and save money in your next annual budget.

Exam Tip

The Annual Loss Expectancy (ALE) is calculated by multiplying the annual rate of occurrence (ARO) and the single loss expectancy (SLE).

Solutions and Countermeasures

After you've assessed and defined risk and management procedures, you'll have collected the following information:

- **Asset identification** A list of your assets, including physical assets such as server hardware and hard disks, and nonphysical assets such as the valuable customer data stored on the hard drives.
- **Threat profiles** A list of every possible threat against your assets.
- **Risks** An evaluation of the potential risk of each threat—such as the risk of a malicious hacker being able to compromise a database server. If the server itself is compromised, but the valuable and confidential data on the database server is leaked by the hacker, the risk is far greater for this asset.
- **Impact** The potential loss in the event your assets are attacked or compromised by threats, including the asset's capital value (such as hardware cost), plus how much it will cost to replace that asset, especially lost customer data. A failed hard drive can be a relatively low cost to recoup, but if you have no backup of customer data that was stored on that hard drive, you might have lost tens of thousands of dollars' worth of data.
- **Probability** The risks more likely to occur are ranked toward the top of the list to indicate where solution efforts should be most concentrated. For example, within a company that already practices strict physical security and access control methods, the priority of risk scenarios could be geared toward nonphysical threats, such as viruses and network hackers.

Once this process is complete, a list of solutions and countermeasures to protect against each threat should be reviewed and documented. Examine your solutions with respect to what current security measures are in place and what needs to be done to make them more effective. Ensure that the functionality and effectiveness of the solution is sufficient to reduce the risk of compromise. Purchasing a fire extinguisher for the server room could seem like a fire-prevention solution, for example, but only an automatic fire detection and suppression system can fully protect a room full of servers from a large, out-of-control fire that occurs in the middle of the night. Similarly, buying a firewall to protect your servers from outside Internet traffic is a great idea for network security, but if the network administrator hasn't been trained to configure it properly, the firewall might not be effective at all.

Any solutions must be cost-effective to ensure that the benefits of the solution are in line with the actual value of the assets. For example, there's no point in spending $100,000 on a security solution to protect data that's worth only $40,000 to the company if it's lost or damaged. Ongoing maintenance also needs to be factored into the final calculations. Although a large initial cost is incurred for a tape backup solution, costs of purchasing new tapes as they're needed will be ongoing, and you'll pay for offsite storage of used tapes.

Exam Tip

The cost of the risk management solution shouldn't exceed the value of the asset if it's lost. For example, if a file server and its data are valued at $35,000 and the proposed security solution to protect it costs $150,000, then it doesn't make sense to implement the proposed solution.

Risk Management Options

When you have completed your risk analysis, and depending on your operations and budgets, you have several options for dealing with each risk:

- **Avoidance** Depending on the type of risk, you can opt to avoid the risk altogether. This option is typically used when the cost to mitigate a threat, especially if it is unlikely or has little impact, means it is not worth implementing. This can also mean you take certain steps to avoid a risk altogether, such as disabling a rarely used feature in a web application because the benefits aren't worth the great security risk it causes.
- **Transference** The organization can also transfer or "pass on" the risk to a third party, for example, an insurance company who will pay out your damages in the event a certain risk occurs, or trusting a third-party provider to store your offsite backup media.
- **Acceptance** In most cases in information security, there is a level of risk that must be accepted with any type of information system network. For example, your organization may want to sell its products directly from their web site, and the potential revenues greatly outweigh the potential network security risks involved. On the other hand, if the risk is deemed too great in comparison to the benefit, the service may not be offered, or additional mitigation techniques required.

- **Mitigation** Based on your risk analysis, there are specific risks that must be mitigated using countermeasures—for example, implementing a network firewall for network security, installing desktop and server antivirus protection, and implementing fault-tolerant systems to mitigate the impact of failed hardware.
- **Deterrence** Risk deterrence is an extension of mitigation in which more active levels of control are used to deter security threats. On the network level, this can include intrusion detection systems and threat prevention devices that proactively monitor and deter network and system attacks. This can also include honeypot devices that attract network attacks to specific "false" devices and services to ward away attacks from vital networking and service infrastructure.

False Positives and Negatives

A *false positive* is a legitimate action that is perceived as a risk or threat. A false positive is a term often used in e-mail security scanning to indicate a legitimate message that was classified as a security issue such as spam, content violation, or poor reputation check. False positives can be applied to almost any type of security scenario where security controls block what is essentially a legitimate action. For example, an intrusion detection system may send out constant alarms even though the traffic it's detecting is legitimate traffic. The administrator becomes lax in responding to alarms because he knows they are more likely than not false positives. This can allow other more serious intrusions to be ignored.

Occasional false positives are a fact of life when it comes to strict security controls, but too many can become difficult to manage and put a lot of burden on both the administrators and the end users to manage. Excessive false positives in your environment means that your security controls are too aggressive and need to be reconfigured.

Most security systems can be fine-tuned to allow future attempts from the legitimate action, as long as you can verify it is being performed by an authorized user or process in a secure way. In the example of legitimate e-mail messages being blocked, end users can create lists of trusted known senders so that future messages from the same sender can bypass certain types of scanning such as content filtering. Intrusion detection systems can have their thresholds redefined to a lower value to prevent an increase in false positives.

Security controls that are not aggressive enough can result in false negatives. A *false negative* is a security issue that has passed your security controls as legitimate. For example, an e-mail message that is spam or contains illegal content may pass through your e-mail security controls and content filters as if it were legitimate mail. An intrusion detection system may let through a denial-of-service attack because it detects the event as normal operation.

Security controls require continuous baselining and adjustments to properly set their thresholds to detect the difference between normal behavior and serious security issues. The baseline provides you with a report of what is considered normal activity, and then you set your thresholds on your security controls to detect anomalies to that normal activity. This period of recording baselines and making configuration adjustments can take several weeks to result in ideal security thresholds, but this ensures that you will have fewer issues with false positives and negatives in the future.

Exam Tip

A false positive is a legitimate action that is perceived as a risk or threat. A false negative is a security issue that has passed your security controls as a legitimate action.

Use Organizational Policies to Reduce Risk

To provide effective security, security policy and procedure creation must begin at the top of an organization with senior management. These policies and procedures must then flow throughout the company to ensure that security is useful and functional at every level of the organization. Understanding company security must begin with an understanding of the basic laws, regulations, and legal liability issues to which the company must adhere to protect the company and its assets, as well as the employees and customers.

Security policies and procedures are official company communications that are created to ensure that a standard level of security guidelines exists across the entire organization. These policies define how the employees interact with company computer systems to perform their job functions, how to protect the computer systems and their data, and how to service the company's clients properly. The upcoming sections outline policies and procedures in the following areas:

- Security policies
- Network access policies
- Human resources policies

Security Policies

The following policies concern general organizational security, including physical access, access control to data, and security through proper organizational structures and data security principles.

Physical Access Security Policy As part of your organization's overall access control policy, you must have a strong physical access policy and ensure that all employees are educated on its use.

Depending on the security level of the company, physical security may include guarded or nonguarded entrances. Even on guarded premises, the use of security access cards makes sure that only identified and authenticated employees can enter a facility. Security access cards are coded with the authorization level of the user, who will be able to access only areas of the facility that are required by his job function. For example, only network and systems administrators would be able to access a server and networks communications room with their access card.

Employees must be trained to always close automatically locking doors behind them, and not allow other, unidentified people to follow them through. Most security access cards have photographs on them to further identify users in the event they are challenged for their identity. Employees must be encouraged to report suspicious individuals within the premises who are unfamiliar and do not have proper identification.

A published organizational security policy for physical access allows your employees to have proper knowledge of security procedures and be equally active in the responsibility for physical security.

Access Control Policies The following access control policies help provide a consistent organizational structure and procedures to prevent internal fraud and corruption in your organization.

- **Least privilege** The *least privilege* principle grants users only access rights they need to perform their job functions. This requires giving users the least amount of access possible to prevent them from abusing more powerful access rights.
- **Separation of duties** A *separation of duties* ensures that one single individual isn't tasked with high-security and high-risk responsibilities. Certain critical responsibilities are separated between several users to prevent corruption.
- **Job rotation** *Job rotation* provides improved security because no employee retains the same amount of access control for a particular responsibility for a period of time. This prevents internal corruption from employees that take advantage of their long-term position and security access.
- **Mandatory vacations** *Mandatory vacation* policies require employees to use their vacations at specific times of year or use all of their vacation

days allotted for a single year. This policy helps detect security issues with employees, such as fraud or other internal hacking activities, because the anomalies might surface while the user is away.

Travel Assistance

These access control concepts and best practices are discussed in more detail in Chapter 6.

Network Security Policies

Several policies provide standard guidelines for network security within a company and encompass areas such as the Internet and internal network use, data privacy, security incident response, human resources issues, and document security.

Acceptable Use Policy An *acceptable use policy* is a set of established guidelines for the appropriate use of computer networks within an organization. The policy is a written agreement, read and signed by employees, that outlines the terms, conditions, and rules of the Internet and internal network use for the company.

An acceptable use policy helps educate employees about the kinds of tools they will use on the network and what they can expect from those tools. The policy also helps to define boundaries of behavior and, more critically, specify the consequences of violating those boundaries. The policy also specifies the actions that management and the system administrators may take to maintain and monitor the network for unacceptable use, and they include the general worst-case consequences or responses to specific policy violation situations.

Exam Tip

An acceptable use policy is a set of established guidelines for the appropriate use of computer networks within an organization.

Developing an acceptable use policy for your company's computer network is extremely important for organizational security and to limit legal liability in the event of a security issue. Acceptable use policies should cover the following issues:

- **Legality** The company's legal department needs to approve the policy before it's distributed for signing. The policy will be used as a legal document to ensure that the company isn't legally liable for any type of Internet-related incident and any other transgressions, such as cracking, vandalism, and sabotage.

- **Uniqueness to your environment** The policy should be written to cover the organization's specific network and the data it contains. Each organization has different security concerns—for example, a medical facility needs to protect data that differs significantly from that of a product sales company.
- **Completeness** Beyond rules of behavior, your policy should also include a statement concerning the company's position on Internet use.
- **Adaptability** Because the Internet is constantly evolving, your policy will need to be updated as new issues arise. You can't anticipate every situation, so the acceptable use policy should address the possibility of something happening that isn't outlined.
- **Protection for employees** If your employees follow the rules of the acceptable use policy, their exposure to questionable materials should be minimized. In addition, it can protect them from dangerous Internet behavior, such as giving out their names and e-mail addresses to crackers using social engineering techniques.

The focus of an acceptable use policy should be on the responsible use of computer networks. Such networks include the Internet—including web, e-mail, and instant messaging access—and the company intranet. Most acceptable use policies contain the following components:

- A description of the strategies and goals to be supported by Internet access in the company
- A statement explaining the availability of computer networks to employees
- A statement explaining the responsibilities of employees when they use the Internet
- A code of conduct governing behavior on the Internet
- A description of the consequences of violating the policy
- A description of what constitutes acceptable and unacceptable use of the Internet
- A description of the rights of individuals using the networks in your company, such as user privacy
- A disclaimer absolving the company from responsibility under specific circumstances
- A form for employees to sign indicating their agreement to abide by the policy

Travel Advisory

Many company web sites contain an acceptable use policy or Terms of Use statement that protects the company from any liability from users of the site.

Due Care, Due Diligence, and Due Process *Due care, due diligence,* and *due process* are terms that apply to the implementation and enforcement of companywide security policies. A company practices *due care* by taking responsibility for all activities that take place in corporate facilities. A company practices *due diligence* by implementing and maintaining these security procedures at all times to protect the company's facilities, assets, and employees. Although many companies outline plans for security policies and standards, they often never officially implement them, or the information isn't properly shared with the employees. Without training, guides, and manuals, and without employee input and feedback, no guidance comes from management regarding the policies and their use.

By practicing due care, the company shows it has taken the necessary steps to protect itself and its employees. By practicing due diligence, the company ensures that these security policies are properly maintained, communicated, and implemented. If the company doesn't follow proper due care and due diligence initiatives, it might be considered legally negligent if company security and customer data are compromised.

Due process ensures that in the event of a security issue by an employee, the employee receives an impartial and fair inquiry into the incident to ensure the employee's rights are not being violated. If, in the course of an investigation and inquiry, the employee's rights are violated, the company may face legal ramifications via lawsuits or governmental employment tribunals.

Exam Tip

Due care is taking the necessary responsibility and steps to protect the company and the employees. Due diligence ensures these security policies are properly implemented. Due process ensures an impartial and fair inquiry into violations of company policies.

Privacy Policy *Privacy policies* are agreements for protecting individually identifiable information in an online or electronic commerce environment. A company engaged in online activities or e-commerce has a responsibility to adopt and implement a policy for protecting the privacy of personally identifiable information. Organizations should also take steps to ensure online privacy when interacting with other companies, such as business partners.

The following recommendations pertain to implementing privacy policies:

- A company's privacy policy must be easy to find, read, and understand, and it must be available prior to or at the time that individually identifiable information is collected or requested.
- The policy needs to state clearly what information is being collected; the use of that information; possible third-party distribution of that information; the choices available to an individual regarding collection, use, and distribution of the collected information; a statement of the organization's commitment to data security; and what steps the organization takes to ensure data quality and access.
- The policy should disclose the consequences, if any, of an individual's refusal to provide information.
- The policy should include a clear statement of what accountability mechanism the organization uses, such as procedures for dealing with privacy breaches, including how to contact the organization and register complaints.
- Individuals must be given the opportunity to exercise choice regarding how personally identifiable information collected from them online could be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use.
- Where third-party distribution of information is collected online from the individual, unrelated to the purpose for which it was collected, the individual should be given the opportunity to opt out.
- Organizations creating, maintaining, using, or disseminating personally identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect the information from loss, misuse, or alteration.

Each company must evaluate its use of the Internet to determine the type of privacy policy it needs to protect all involved parties. The privacy policy will protect the company from legal issues, raising customers' comfort levels regarding the protection of their information. A privacy policy should include the following elements:

- **Information collection** Collect, use, and exchange only data pertinent to the exact purpose, in an open and ethical manner. The information collected for one purpose shouldn't be used for another. Notify consumers of information you have on them, as well as its proposed use, handling, and enforcement policies.
- **Direct marketing** The company can use only non–personally identifiable information for marketing purposes and must certify that the customers' personal information won't be resold to third-party marketing firms.
- **Information accuracy** Ensure the data is accurate, timely, and complete, and that it has been collected in a legal and fair manner. Allow customers the right to access, verify, and change their information in a timely, noncumbersome fashion. Inform customers of the data sources and allow them the option of removing their names from the marketing lists.
- **Information security** Apply security measures to safeguard the data on databases. Establish employee training programs and policies on the proper handling of customer data. Limit the access to a need-to-know basis on personal information and divide the information, so no one employee or unit has the whole picture. Follow all government regulations concerning data handling and privacy.

Exam Tip

> Privacy policies must be easy to find and provide information on how to opt out of any use of personal information.

Service Level Agreement Policy A *service level agreement (SLA)* is an understanding among a supplier of services and the users of those services that the service in question will be available for a certain percentage of time. For example, a web-hosting company could have an SLA with its customers that states the web servers that host the customer's web pages will be available 99.8 percent of the time. If the service level drops below this percentage, the customer might be reimbursed for business lost during the downtime.

The SLA policy describes the policies and procedures that a company performs to support the SLA agreement, including the services performed to preserve the SLA uptime and the contingency plans and communications that must be performed if the availability of the organization's services exceeds the thresholds agreed to in the SLA.

Human Resources Policies

A company's human resources (HR) department is an important link regarding company and employee security. The HR department is responsible for hiring employees, ensuring employees conform to company codes and policies during their term of employment, and maintaining company security in case of an employee termination. The following sections outline the responsibility of human resources during the three phases of the employment cycle.

Hiring Policy When hiring employees for a position within the company, the HR department is responsible for the initial employee screening. This usually takes place during the first interview: an HR representative meets with the employee to discuss the company and to get a first impression of the employee's personality, gauging whether this person would fit into the company's environment. This interview generally is nontechnical and personality-based. Further interviews are usually more skill-oriented and are conducted by the department advertising the position. The employee could possess excellent technical skills for the position, but his personality and communications skills might not be conducive to integration with the work environment.

During the interview process, HR also conducts background checks of the applicant and examines and confirms her educational and employment history. Reference checks are also performed, where HR can obtain information on the applicant from a third party to help confirm facts about the person's past. Depending on the type of company or institution, such as the government or the military, the applicant might have to go through security clearance checks or even health and drug testing.

To protect the confidentiality of company information, the applicant is usually required to sign a nondisclosure agreement, which legally prevents the applicant from disclosing sensitive company data to other companies in case of her termination. These agreements are particularly important with high-turnover positions, such as contract or temporary employment.

When an employee is hired, the company also inherits that person's personality quirks or traits. A solid hiring process can prevent future problems with new employees.

Codes of Conduct and Ethics Policy The HR department is also responsible for outlining a company's policy regarding codes of conduct and ethics. The codes are a general list of what the company expects from its employees in terms of everyday conduct—dealing with fellow employees, managers, and subordinates, including people from outside the company, such as customers and clients.

This code of conduct could include restrictions and policies concerning drug and alcohol abuse, theft and vandalism, and violence in the workplace. If an employee transgresses any of these codes of conduct and ethics, that employee could be disciplined, suspended, or even terminated, depending on the severity of the infraction.

Termination Policy The dismissal of employees can be a stressful and chaotic time, especially because terminations can happen quickly and without notice. An employee can be terminated for a variety of reasons, such as performance issues; personal and attitude problems; or legal issues such as sabotage, espionage, or theft. Or the employee could be leaving to work for another company. The HR department needs to have a specific set of procedures ready to follow in case an employee resigns or is terminated. Without a step-by-step method of termination, some areas might have been ignored during the process that compromise company security.

A termination policy should exist for each type of situation. For example, you might follow slightly different procedures for terminating an employee who's going to work for an industry-unrelated position with another company than with an employee who's going to work for a direct competitor. In the latter case, the employee might be considered a security risk if he remains on the premises for his two-week notice period, where he could transmit company secrets to the competition.

A termination policy should include the following procedures for the immediate termination of an employee:

- **Securing work area** When the termination time has been set, the employee in question should be escorted from his workstation area to the HR department. This prevents him from using his computer or other company resources once notice of termination is given. His computer should be turned off and disconnected from the network. When the employee returns to his desk to collect personal items, someone should be with him to ensure that no private company information is taken. Finally, the employee should be escorted out of the building.
- **Return of identification** As part of the termination procedure, the employee's company identification should be returned. This includes identity badges, pass cards, keys for doors, and any other security device used for access to company facilities. This prevents the person from accessing the building after being escorted from the premises.

- **Return of company equipment** All company-owned equipment must be returned immediately, such as desktops, laptops, cell phones, PDAs, organizers, or any other type of electronic equipment that could contain confidential company information.
- **Suspension of accounts** An important part of the termination procedure is the notification to the network administrators of the situation. They should be notified shortly before the termination takes place to give them time to disable any network accounts and phone access for that employee. The network password of the account should be changed, and any other network access the employee might have, such as remote access, should be disabled. The employee's file server data and e-mail should be preserved and archived to protect any work or important communications the company might need for operational or legal reasons.

Exam Tip

All user access, including physical and network access controls, needs to be disabled for an employee once they have been terminated. This prevents the employee from accessing the facility or network.

Objective 1.02
CompTIA Security+ Objective 2.2

Carry Out Appropriate Risk Mitigation Strategies

As a result of your risk analysis, many of the risks identified require security controls if you have decided to budget resources to mitigate the risk. The policies and procedures described previously help you implement security controls at the managerial, operational, and technical levels of your organization.

Security policies and procedures provide the template and framework for employees to follow and implement risk mitigation controls across your organization. To ensure these policies are being followed, however, requires continued monitoring and auditing to make sure they are in use and being adhered to.

The following sections describe additional aspects of risk mitigation that require security policies and continued monitoring to ensure the policies are being followed and do not result in additional risks for the organization. These risk mitigation strategies and policies include change management, incident response, auditing, user permission reviews, and data loss prevention.

Change Management Policy

Change management policies are official company procedures used to identify and communicate current or forthcoming changes to some aspect of the company's networks and communications services. For example, the IT department might issue a change control document to all employees to notify them of a network outage because of an upgrade to networking equipment, or that an application will be down for several hours for a software upgrade. More detailed change control communications describe longer-term outages for specific technical changes to the company's systems or network infrastructure, such as taking down part of the network for a weekend for router and switch upgrades.

Tracking, controlling, and communicating outages and changes to your network infrastructure, systems, and applications are important to keep all departments in your organization up-to-date with IT maintenance activities to prevent accidental loss of data and services. For security reasons, this activity also ensures any unplanned changes or outages are quickly detected and investigated. System and network changes without prior knowledge or approval of management and the IT department could indicate a hacker or an intruder has compromised the network.

Incident Management and Response Policy

Incident management and response should be part of a company's overall security policy. In the event of some form of security incident, be it physical intrusion, network attack, or equipment theft and vandalism, some form of procedure should be in place to deal with these events as they happen. Without any clear directives, the aftermath of a security breach can cause even more damage if employees don't know how to handle an incident properly. A clearly defined incident response policy can help contain a problem and provide quick recovery to normal operations.

The policy should cover each type of compromised security scenario and list the procedures to follow when they happen. For example, in case a server is hacked, procedures might be in place to deal with removing the server from the network, shutting down related network servers and services, and preserving evidence, such as audit trails and logs. The incident response policy should cover the following areas:

- Contact information for emergency services and other outside resources
- Methods of securing and preserving evidence of a security breach

- Scenario-based procedures of what to do with computer and network equipment depending on the security problem
- How to document the problem and the evidence properly

Travel Assistance

Incident response is described in greater detail in Chapter 2.

Perform Routine Audits

Routine audits of your security procedures and policies are an integral part of continuous security awareness. Until serious incidents occur, you will not know if your policies are being followed and adhered to, which leaves your organization and its activities at risk. Recording and collecting logs of security activity isn't helpful unless you are able to review and analyze the data, and compare it to your current policies and the level of incidents that occur.

Security and access logs should be carefully preserved and analyzed in case of a security compromise or policy violation. For example, there may be evidence of attempts at network intrusion that go completely unnoticed because of notifications and alerts in the security logs that went unnoticed or unheeded. In this case you must review your IT incident response policies and procedures to understand why these activities went unnoticed and the risk continued. By auditing and re-evaluating your policies, you can identify additional monitoring and mitigation measures that need to be put into place.

Audits of policies and procedures need to be performed at all levels of your organization, including deep level network and account management policies, physical access policies, and human resource procedures. You may find that your current policies are correctly defined but are not implemented properly or communicated efficiently to all users. Employees can become lax, and often republication and retraining for specific types of policies may be required.

User Rights and Permissions Reviews

While auditing and reviewing overall organizational policies and procedures are critical for security maintenance, you must also regularly review and audit the rights and permissions granted to your users. While at a specific moment in time, the rights and privileges you have assigned for users may be accurate and secure, over longer periods of time, employees leave the company, move to different positions and responsibilities, and may possess higher or lower security clearances than what they had previously.

Regularly auditing user security rights and permissions is extremely important in ensuring that existing security lapses in user rights policies can be resolved before a user accesses or damages data to which that user should not be allowed access. Group, geographical, and department-based policies are very important to audit because users change their locations and departments frequently. For example, a user who recently switched from the sales department to the marketing department needs her permissions reviewed to remove her from any access to shared sales department data.

User rights and permission reviews need close cooperation with human resources and department heads to be proactively notified when employees' positions and responsibilities change.

Data Loss Prevention and Regulatory Compliance

Data loss prevention (DLP) is a major growing trend for organizational security. While most security is concerned with inbound risks and threats, such as malware, network attacks, and hacker intrusions, internal data security and outbound data loss have also now become a primary security targets.

DLP is a security concept focused on preventing the loss of data and protecting its confidentiality and privacy. This includes a company's own data, and also any customer data that it stores and communicates. Data must be protected from theft, loss, and interception in storage and in transit. DLP mitigation techniques require the use of both inbound security through the use of standard network security techniques such as firewalls and antimalware appliances to prevent inbound threats, and also security for outbound traffic through the use of content filtering and encryption technology.

Travel Assistance

Data loss prevention techniques are discussed in more detail in Chapter 12.

There are now several government-directed regulations and policies regarding the protection of data for companies in specific industries. For example, companies in the medical industry must prevent confidential patient information from being compromised. Financial organizations such as banks and insurance companies must provide several layers of security for protecting financial transactions and the confidential financial information of customers such as credit card and bank account data.

The most common data protection regulations include:

- **Health Insurance Portability and Accountability Act (HIPAA)** HIPAA is a set of compliance regulations for the protection of confidential patient data in the medical, health care, and health insurance industry.
- **Sarbanes-Oxley Act (SOX)** In the financial services industry, the Sarbanes-Oxley Act defines standards for publicly held companies and accounting firms for storage, access, communications, and auditing of financial data.
- **Payment Card Industry (PCI)** This set of standards is defined for companies that process credit card financial transactions to help prevent fraud and identity theft. PCI defines several concepts that should be complied with when storing and communicating financial data.
- **EU Data Protection Directive (EUDPD)** This European Union regulation requires organizations, including multinational companies, to provide privacy protection for stored and transmitted user data.

Generally, most compliance regulations and standards include these key factors for data security:

- Proper protection of data through network security principles and technology, such as firewalls and antimalware devices
- Strong user account and password management for access control
- Use of encryption when storing and transmitting confidential data
- Extensive logging and auditing to be able to monitor and analyze reports and have audit trails for forensic evidence

CHECKPOINT

✔ **Objective 1.01: Explain risk-related concepts.** An acceptable use policy is a set of established guidelines for the appropriate use of computer networks. The company practices due care by taking responsibility for all activities that take place in corporate facilities. The company practices due diligence by implementing and maintaining these security procedures at all times to protect the company's facilities, assets, and employees. A service level agreement (SLA) is an understanding among a supplier of services and the users of those services that the service in question will be available for a certain percentage of time. A specific separation of duties ensures that one individual isn't tasked with high-security and high-risk responsibilities. Users should have only the access rights they need to perform their job functions. The employee termination process includes securing the work area, returning identification and company equipment, and suspending computer accounts.

✔ **Objective 1.02: Carry out appropriate risk mitigation strategies.** Security policies provide the template and procedures for risk mitigation, but these policies need to be implemented and adhered to. Use change management policies for communication of network changes and outages. Unplanned changes in your network could indicate security breaches. Use an incident response policy so that procedures are in place to deal with security incidents. Perform routine audits of your policies and procedures to make sure they are being adhered to. Constantly review user rights and permissions to deal with security issues deriving from changing roles and responsibilities for end users. Use DLP techniques to protect the integrity and privacy of data, and adhere to government-regulated compliance policies for data protection.

REVIEW QUESTIONS

1. After a few incidents where customer data was transmitted to a third party, your organization is required to create and adhere to a policy that describes the distribution, protection, and confidentiality of customer data. Which of the following policies do you create?

   A. Privacy
   B. Due care
   C. Acceptable use
   D. Service level agreement

2. You are performing a risk analysis for a complex web-based application. Based on your conclusions regarding the probability, impact, and mitigation cost of an attack based on DNS manipulation or poisoning against your web domain, you decide to place the responsibility of the risk on your ISP, which handles your DNS services. Which risk management option is this an example of?

   A. Acceptance
   B. Deterrence
   C. Avoidance
   D. Transference

3. As the centralized management location from which you provide Internet-based application services to several external clients, which of the following policies do you provide to your clients as an agreement for service uptime?

   A. Code of ethics
   B. Privacy
   C. SLA
   D. Due care

4. There is a suspicion that a specific employee is performing illegal activities on your company's networks. In an effort to gather evidence about his activities, which of the following principles and techniques could you employ?

   A. Password rotation
   B. Mandatory vacation
   C. Need-to-know
   D. Separation of duties

5. As part of a risk analysis of a very large and extensive back-end database, you need to calculate the probability and impact of data corruption to the data. Which of the following impact factors allows you to calculate your annualized losses due to data corruption?

   A. SLE
   B. SLA
   C. ARO
   D. ALE

6. You need to create an overall policy for your organization that describes how your users can properly make use of company communications services, such as web browsing, e-mail, and FTP services. Which of the following policies do you implement?

   A. Acceptable use policy
   B. Due care
   C. Privacy policy
   D. Service level agreement

7. After the initial configuration of an antispam e-mail filtering appliance on your network, users are complaining that too many legitimate messages are being flagged as spam in their mailboxes. Which of the following concepts is this an example of?

A. Baseline threshold
B. False negative
C. False positive
D. Legitimate positive

8. Your organization deals with sensitive health insurance information for patients that is covered by the HIPAA compliance policies. Which of the following DLP security techniques would you implement to help protect the confidentiality and privacy of your patient's health insurance data when communicating the information between health care facilities?

A. Encryption of outbound data containing health insurance information
B. A firewall to protect from inbound network attacks
C. Antivirus scanning of patient data
D. Strong physical access control of your facility

9. It has been discovered that a former member of the IT department who switched to the development team still has administrative access to many major network infrastructure devices and servers. Which of the following mitigation techniques should be implemented to help reduce the risk of this event recurring?

A. DLP
B. Incident management and response policy
C. Change management notifications
D. Regular user permission and rights reviews

10. A high-level executive has been terminated due to sharing company confidential data with competitors. Which of the following actions should be immediately performed?

A. Encrypt all outbound data sent from the user.
B. Change the password and disable all user accounts for the user.
C. Scan the user's computer for compliance violations.
D. Encrypt all data in storage that the user has access to.

REVIEW ANSWERS

1. **A** A privacy policy concerns the protection and distribution of private customer data. Any company, especially one engaged in online activities or e-commerce, has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information.

2. **D** The risk of DNS attacks occurring against your web domain is something that can only be assumed by your ISP, which takes care of your DNS services. In this part of your risk analysis, you are transferring the responsibility of the risk to your ISP to protect your web services from DNS-based attacks.

3. **C** A service level agreement (SLA) is an understanding among a supplier of services and the clients of those services that the service in question will be available for a specific percentage of time. In this case, you may guarantee your clients a 99.5 percent uptime of communications services.

4. **B** When a user is forced to take a vacation, his activities can be audited and any suspicious behavior will be more likely to be noticed and detected, because the user is not there to prevent its discovery. You may also discover that the illegal activities completely cease while the user is away, and then resume when he returns.

5. **D** ALE (annual loss expectancy) describes how much money you expect to lose on an annual basis because of the impact from an occurrence of a specific risk. ALE is calculated by multiplying the annual rate of occurrence (ARO) by the single loss expectancy (SLE).

6. **A** An acceptable use policy establishes rules for the appropriate use of computer networks within your organization. The policy describes the terms, conditions, and rules of using the Internet and its various services within the company's networks.

7. **C** A false positive is a legitimate action that is perceived as a risk or threat. A false positive is a term often used in e-mail security scanning to indicate legitimate mail that was classified as spam.

8. **A** To comply with the HIPAA regulations, you must protect the confidentiality of your patient's health insurance information. When communicating this data, you must encrypt it to ensure that it cannot be read if intercepted or stolen.

9. **D** User rights and permissions must be constantly reviewed to make sure that users have only the rights they require for their current responsibilities. When users change roles and responsibilities in the organization, you must review their permissions and modify their access accordingly.

10. **B** When a user is terminated, the first action that should be performed is to have that user's passwords changed and his user accounts disabled. This immediately prevents the user from gaining access to his accounts, data, and e-mail.