Chapter 1

Risk Management

THE FOLLOWING COMPTIA CASP+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **4.1 Given a set of requirements, apply the appropriate risk strategies**

- **Risk assessment**
  - Likelihood
  - Impact
  - Qualitative vs. quantitative
  - Exposure factor
  - Asset value
  - Total cost of ownership (TCO)
  - Return on investment (ROI)
  - Mean time to recovery (MTTR)
  - Mean time between failure (MTBF)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
  - Single loss expectancy (SLE)
  - Gap analysis
- **Risk handling techniques**
  - Transfer
  - Accept
  - Avoid
  - Mitigate
- **Risk types**
  - Inherent
  - Residual
  - Exceptions

- **Risk management life cycle**
  - Identify
  - Assess
  - Control
    - People
    - Process
    - Technology
    - Protect
    - Detect
    - Respond
    - Restore
  - Review
  - Frameworks
- **Risk tracking**
  - Risk register
  - Key performance indicators
    - Scalability
    - Reliability
    - Availability
  - Key risk indicators
- **Risk appetite vs. risk tolerance**
  - Tradeoff analysis
  - Usability vs. security requirements
- **Policies and security practices**
  - Separation of duties
  - Job rotation
  - Mandatory vacation
  - Least privilege
  - Employment and termination procedures

- Training and awareness for users
- Auditing requirements and frequency

✓ 4.4 Explain the Importance of Business Continuity and Disaster Recovery Concepts

- **Business impact analysis**
  - Recovery point objective
  - Recovery time objective
  - Recovery service level
  - Mission essential functions
- **Privacy impact assessment**
- **Disaster recovery plan (DRP)/business continuity plan (BCP)**
  - Cold site
  - Warm site
  - Hot site
  - Mobile site
- **Incident response plan**
  - Roles/responsibilities
  - After-action reports
- **Testing plans**
  - Checklist
  - Walk-through
  - Tabletop exercises
  - Full interruption test
  - Parallel test/simulation test

This chapter discusses risk. As a CASP+, you should be able to interpret business and industry influences and explain associated security risks. From a computing standpoint, risk is all around you. Everywhere you turn, there are risks; they begin the minute you first turn on a computer and grow exponentially the moment the network card becomes active.

Even in the nontechnical sense, there is risk: Who do you let in the facility? Are visitors escorted? Do you allow employees to connect personal devices such as tablet computers, smartphones, and so forth to company networks? There is even risk when deciding what approach to use for email. You may use an in-house email server or outsource email and use a cloud-based solution, such as Gmail or `Outlook.com`. Here again, you will find that there is the potential for risk in each choice. These are just the tip of the iceberg. This chapter discusses what CompTIA expects you to know for the exam related to risk.

Risk Terminology

Before discussing risk management, it is important to make sure that some basic terms are defined. All industries share basic vocabulary and semantics. IT security is no different, and within the topic of risk, there are some terms that you will see again and again. Let's begin by reviewing these terms:

Asset An *asset* is an item of value to an institution, such as data, hardware, software, or physical property. An asset is an item or collection of items that has a quantitative (numeric) or qualitative (subjective) value to a company.

Risk *Risk* is the probability or likelihood of the occurrence or realization of a threat.

Vulnerability A *vulnerability* can be described as a weakness in hardware, software, or components that may be exploited in order for a threat to destroy, damage, or compromise an asset.

Threat A *threat* is any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an IT asset or data asset. The likelihood of the threat is the probability of occurrence or the odds that the event will actually occur.

Motivation *Motivation* is the driving force behind the activity. As an example, hackers can be motivated by many different reasons. Some common reasons include prestige, money, fame, and challenge.

Risk Source The *source* of a risk can be either internal or external. Internal risk can be anything from a disgruntled employee to a failed hard drive. External risk includes natural disasters such as floods and person-made events such as strikes and protests. As an example, the risk source might be that the lock on a server cabinet is broken, whereas the threat is that someone can now steal the server hard drive.

From the standpoint of IT security, the following are some common examples of threats:

Natural Disaster *Natural disasters* are events over which we have no control, such as bad weather (hurricanes, snowstorms, tornadoes), fires, floods, earthquakes, and tsunamis, but could also include global events like pandemics.

Malicious Code *Malicious code* includes all forms of damaging programs, such as viruses, worms, Trojans, keyloggers, and so forth. This software is distinguishable in that it is developed to damage, alter, expose, or destroy a system or data. For example, viruses are executable programs that can replicate and attach to and infect other executable objects. Some viruses also perform destructive or discreet activities (payload) after replication and infection are accomplished.

Breach of Physical Security A *breach of physical security* can be instigated by a trusted insider or an untrusted outsider. Intruders, vandals, and thieves remove sensitive information, destroy data, or physically damage or remove hardware such as hard drives and mobile devices.

Hacker Attack *Hacker attacks* generally result in stolen, lost, damaged, or modified data. Loss or damage to an organization's data can be a critical threat if there are no backups or external archiving of the data as part of the organization's data recovery and business continuity plan. Also, if the compromised data is of a confidential nature, this can also be a critical threat to the organization, depending on the potential damage that can arise from this compromise.

Distributed Denial of Service A *distributed denial-of-service (DDoS)* attack on a network or web-based system is designed to bring down the network or prevent access to a particular device by flooding it with useless traffic. DDoS attacks can be launched in several ways. What was done manually with simple tools before is now automated and coordinated, on a massive scale with multiple systems.

The attack might leverage networked devices, such as the famous Mirai malware-driven botnet that used multiple systems simultaneously. Or, an attacker may also use more advanced DDoS tools such as Tribal Flood Network, Shaft, or Low Orbit Ion Cannon.

Currently, most DDoS attacks are launched via botnets. Regardless of the technique, the result is that the targeted system has a reduced or limited ability to communicate.

Cyberterrorism *Cyberterrorism* is when attackers use computers, Internet communications, and other cyber tools to penetrate and disrupt critical national infrastructures such as water, electric, and gas plants; oil and gasoline refineries; nuclear power plants; waste management plants; and so on.

This list is by no means all-inclusive.

The Risk Assessment Process

All companies have only a limited amount of funds, and those funds must be spent wisely. This means spending money in areas that need the most protection. The purpose of the *risk assessment* is to identify weaknesses and gaps in the deployment of controls and to identify more accurately what areas require the highest level of protection. It evaluates risks in terms of the likelihood and the magnitude of an impact, to determine a response strategy, and to monitor progress in reducing the threat. The risk assessment will also identify a baseline for the organization's current level of information security. This baseline will form the foundation for how the organization needs to increase or enhance its current level of security based on the criticality or exposure to risk that is identified during the risk assessment.

There are several important aspects of the risk assessment process:

- Asset identification
- Information classification
- The actual risk assessment
- Risk analysis options for risk appetite and deterrence
- Implementing controls

The following sections discuss each step of the process and provide an overview of the risk assessment process.

Asset Identification

Information and systems must have value to determine their worth. Asset identification is the process of identifying all of the organization's assets. A good inventory management system can help greatly in identifying assets. Just keep in mind that assets can be both tangible and intangible. The following assets commonly are examined:

- Tangible
  - Documentation
  - Data

  - Hardware
  - Software
- Intangible
  - Reputation (goodwill)
  - Services

Real World Scenario

Does Reputation Have a Value?

Although we typically think of assets as something tangible, an asset can also be intangible. Reputation is one good example. As businesses have grown larger and the Internet has increased the ability for news stories to move quickly around the world, companies must work harder at protecting their reputations. The experiences of global organizations such as BP and Johnson & Johnson demonstrate how protecting corporate reputations means moving beyond compliance to manage the corporate image. Should customers decide that a company has poor practices or has failed to provide effective security controls, billions of dollars could be lost.

Once all assets are identified, the individuals assessing them must ask more than just what the asset originally cost. They must also start to consider the return on investment (ROI) of any potential control that may be used. Other key considerations are as follows:

- What did the asset cost to acquire or create?
- What is the liability if the asset is compromised?
- What is the production cost if the asset is made unavailable?
- What is the value of the asset to competitors and foreign governments?
- How critical is the asset, and how would its loss affect the company?

Placing a value on an asset is never easy. Asset valuation is a difficult task, and it requires a lot of expertise and work to do it properly. In real life, the process is typically carried out by a team of professionals who have a background in such tasks and have access to specialized software and tools.

Asset identification and valuation can be made easier if an information classification program has been put in place. Information can be classified into levels of *confidentiality*,

integrity, and *availability* based on the specific organization or industry. This is known as the *CIA security triad*. We will examine this topic next.

Information Classification

Information classification strengthens the organization in many ways. Labeling information secret or strictly confidential helps employees see the value of the information and give it a higher standard of care. Information classification also specifies how employees are to handle specific information. For example, company policy might state, "All sensitive documents must be removed from the employee's desk when leaving work. We support a clean desk policy."

Two widely used information classification systems have been adopted. Each is focused on a different portion of the CIA security triad. These two approaches are as follows:

Government Classification System This system focuses on confidentiality.

Commercial Classification System This system focuses on integrity.

The governmental information classification system is divided into the categories Unclassified, Confidential, Secret, and Top Secret, as you can see in Table 1.1.

TABLE 1.1 Governmental information classification

Classification	Description
Top Secret	Its disclosure would cause grave damage to national security. This information requires the highest level of control.
Secret	Its disclosure would be expected to cause serious damage to national security and may divulge significant scientific, technological, operational, and logistical as well as many other developments.
Confidential	Its disclosure could cause damage to national security and should be safeguarded against.
Unclassified	Information is not sensitive and need not be protected unless For Official Use Only (FOUO) is appended to the classification. Unclassified information would not normally cause damage, but over time Unclassified FOUO information could be compiled to deduce information of a higher classification.

The commercial information classification system is focused not just on confidentiality but also on the integrity of information; therefore, it is categorized as public, sensitive, private, and confidential, as shown in Table 1.2.

TABLE 1.2 Commercial information classification

Classification	Description
Confidential	This is the most sensitive rating. This is the information that keeps a company competitive. Not only is this information for internal use only, but its release or alteration could seriously affect or damage a corporation.
Private	This category of restricted information is considered personal in nature and might include medical records or human resource information.
Sensitive	This information requires controls to prevent its release to unauthorized parties. Damage could result from its loss of confidentiality or its loss of integrity.
Public	This is similar to unclassified information in that its disclosure or release would cause no damage to the corporation.

Depending on the industry in which the business operates and its specific needs, one of these options will typically fit better than the others. Regardless of the classification system chosen, security professionals play a key role in categorizing information and helping to determine classification guidelines. Once an organization starts the classification process, it's forced to ask what would happen if specific information was released and how its release would damage or affect the organization.

Risk Assessment

With an organization's assets inventoried, valued, and classified, the next step can begin. This step, the actual risk assessment itself, is where potential risks and threats are identified. These activities are typically carried out by a risk assessment team, and the likelihood of the threat is determined. The team is tasked by top management with identifying threats and examining the impact of the identified threats.

This process can be based on real dollar amounts or on nondollar values. When nondollar values are used, the team typically determines the minimum required security controls based on an aggregate score. One common approach is to determine the aggregate by combining the identified vulnerabilities as they apply to confidentiality, integrity, and availability of the asset. Before we look at qualitative and quantitative risk assessment, let's briefly review some facts about the team that will be carrying out this project.

The Risk Management Team

The *risk management team* is responsible for identifying and analyzing risks. Its members should consist of managers and employees from across the company. After the purpose and membership of the team are established, the team can begin developing and implementing a risk management program.

This team should be led by someone high enough up in the corporate structure to communicate easily with senior management and obtain the funding that will be needed for the risk assessment process to be a success. A successful outcome can be measured in many different ways. A success may mean that the team is able to decrease insurance costs, reduce attacks against the company's website, or verify compliance with privacy laws.

With a team in place and funding secured, the team will next turn its attention to gathering data and identifying threats. The first people to ask about threats should always be the asset owners; they know what the business is facing and where the threats may come from. IT will help map those business threats into IT-related concerns. The following additional sources may be used:

- Actuarial tables and insurance records
- Audit reports
- Business owners and senior managers
- Facility records
- Legal counsel
- Human resources
- Government records
- Network administrators
- Operations
- Security administrators

A threat is any circumstance or event that has the potential to impact an asset negatively by means of unauthorized access, destruction, disclosure, or modification.

Quantitative and Qualitative Risk Assessment

Now that the team has been established and has started to assemble data, a decision has to be made as to what type of risk analysis will be performed. The two techniques for doing this are as follows:

Quantitative Risk Assessment This method assigns a cost (monetary value) to the elements of risk assessment and the assets and threats of a risk analysis.

Qualitative Risk Assessment This method ranks threats by nonmonetary value and is based on scenario, intuition, and experience.

Quantitative Risk Assessment

Thus far, we have discussed building a risk management team that has the support of senior management, identifying tangible and nontangible assets, and starting to identify

potential threats. The impact of these threats must be measured in some way. One approach is to assess the threat in dollar terms. The team is simply asking the question, "What would this cost?"

A threat may not result in a loss. For a loss to occur, the threat must be coupled with a vulnerability. The vulnerability could be the penetrability of a hollow-core server room door. Or, maybe it's the lack of a hardened backup facility elsewhere. It might even be the lack of video surveillance in the reception area. The resulting loss could be any of the following:

- Financial loss
- Danger or injury to staff, clients, or customers
- Breach of confidence or violation of law
- Exposure of confidential information
- Theft of equipment, hardware, or software

To start the calculation of loss, you would need to quantify all elements of the process, including the value of the asset, the impact, and the threat frequency. Here are the steps for doing this:

1. Determine the asset value (AV) for each information asset.
2. Identify threats to the asset.
3. Determine the exposure factor (EF) for each information asset in relation to each threat.
4. Calculate the single loss expectancy (SLE).
5. Calculate the annualized rate of occurrence (ARO).
6. Calculate the annualized loss expectancy (ALE).

Calculation of loss is a time-consuming process because it must be done for all assets.

The two most widely used *quantitative risk assessment* formulas are as follows:

$$SLE = AV \times EF$$

and

$$ALE = ARO \times SLE$$

The strength of a quantitative risk assessment is that it assigns dollar values. Dollar values are easy to understand. If someone says that a potential threat coupled with a vulnerability could result in a $1 million loss, this value is easy for management to work with and conceptualize. The primary disadvantage of quantitative risk assessment is that because it is dollar-based, the team must attempt to compute a dollar value for all elements. This is time-consuming, and some qualitative measures must be applied to quantitative elements. Because this is such a huge task, quantitative assessments are usually performed with the

help of automated software tools. These tools can help with trend analysis and to look for patterns over time. Trend analysis examines historical loss data to determine patterns in loss frequency or loss severity. As an example, hurricanes along the Atlantic coast are becoming more destructive. In fact, three of the top five most costly Atlantic hurricanes in U.S. history occurred in 2017.

```
en.wikipedia.org/wiki/List_of_costliest_Atlantic_hurricanes
```

Let's look at a simple example of quantitative risk assessment in action. In Exercise 1.1, you will calculate the ALE for a file server.

EXERCISE 1.1

Calculating Annualized Loss Expectancy

As a security practitioner for a medium-sized firm, you have been asked to determine the ALE for a file server. Your organization has installed a file server with data valued at $25,000. The organization uses the file server to allow remote offices to upload their daily records to be processed the following morning. Currently, this server is not fully patched and does not have an antivirus program installed. Your research indicates that there is a 95 percent chance that the new file server will become infected within one year. If such an infection were to occur, you estimate that 75 percent of the data value could be lost. Without antivirus, there's a good chance that recovering the missing files and restoring the server could require up to four hours and divert the support team from other duties. An approved vendor has offered to sell a site license for the needed software for $175.

1. **Examine the exposure factor**. This has been calculated at 75 percent. Remember that the exposure factor identifies the percentage of the asset value that will be affected by the successful execution of the threat.
2. **Determine the SLE**. The formula is as follows:

   $$SLE = AV \times EF$$

   Since we know the asset value is $25,000 and the exposure factor is 75 percent, the resulting SLE will be $18,750.
3. **Evaluate the ARO**. The ARO is a value that represents the estimated frequency with which a given threat is expected to occur. This is defined as the number of times that this event is expected to happen in one year. Your research indicates that there is a 95 percent chance that an infection will occur in one year.
4. **Calculate the ALE**. The ALE is an annual expected financial loss to an organization's IT asset because of a particular threat occurring within one year.

   $$ALE = ARO \times SLE$$

   or

   $$\$18,750 \times 0.95 = \$17,812.50$$

With an annualized loss expectancy so high, it makes sense for the company to purchase antivirus software. Without antivirus software to mitigate the risk, the ALE is a significant portion of the cost of the file server.

In the real world, risk calculations rely heavily on probability and expectancy. Software products, actuary tables, industry information, and the history of prior events can help, but some events are hard to calculate. Storms or other natural phenomena are not easy to assign to patterns. Such events can be considered stochastic. A *stochastic event* is based on random behavior because the occurrence of individual events cannot be predicted, yet measuring the distribution of all observations usually follows a predictable pattern.

Quantitative risk management faces challenges when estimating risk, so you must rely on some elements of the qualitative approach.

Qualitative Risk Assessment

The second method by which the risk assessment can be completed is by qualitative means. *Qualitative risk assessment* is scenario-based and does not attempt to assign dollar values to the components of the risk analysis. Part of this process requires the team to perform extreme scenario planning and look at worst-case scenarios. As an example, what if a hurricane hit your surfboard manufacturing facility on Galveston Island? How bad could it be? It's like playing a game of "what if?"

A qualitative assessment ranks the potential of a threat and sensitivity of assets by grade or scale such as low, medium, or high. You can see an example of this in National Institute of Standards and Technology (NIST) SP 800-53 (`nvd.nist.gov/800-53`). This document assigns the potential impact on confidentiality, integrity, and availability (CIA) using the values low, moderate, and high. You will want the support of a team of individuals to help you assess potential risks, and you should incorporate stakeholder input into impact-level decisions on the controls needed to protect the CIA of identified assets. Since a rating of low, medium, or high is subjective, each category must be defined. Examples are as follows:

Low Minor inconvenience; can be tolerated for a short period of time but will not result in financial loss

Medium Can result in damage to an organization, cost a moderate amount of money to repair, and result in negative publicity

High Will result in a loss of goodwill between the company and client or employee; may result in a large legal action or fine or cause the company to lose significant revenue or earnings

Although a qualitative assessment generally requires much less time than a quantitative one, a qualitative assessment does not provide cost values. Table 1.3 shows an example of a scored result of a qualitative review. One common approach is specified in Federal Information Processing Standard (FIPS) publication 199 (`csrc.nist.gov/publications/detail/fips/199/final`). It defines the process of determining the aggregate score by first

measuring impact on CIA and ranking risk as high, medium, or low. Because cost values are absent, this method lacks the rigor that accounting teams and management typically prefer.

TABLE 1.3 Sample qualitative aggregate score findings

Asset	Loss of confidentiality	Loss of integrity	Loss of availability
PII	High	High	Medium
Web server	Medium	Medium	Low
PR material	Low	Low	Low
HR employee records	High	High	Medium

Some examples of qualitative assessment techniques are as follows:

ISAM The *INFOSEC Assessment Methodology (ISAM)* provides nongovernment organizations with the ability to complete a qualitative assessment that ranks assets as critical, high, medium, or low and to determine the impact based on CIA.

Delphi Technique The *Delphi Technique* is a group assessment process that allows individuals to contribute anonymous opinions and is often used to forecast the likelihood and outcomes of different types of events.

Facilitated Risk Assessment Process The *Facilitated Risk Assessment Process (FRAP)* is a subjective process that obtains results by asking a series of questions. It is designed to be completed in a matter of hours, making it a quick process to perform.

Two other assessment techniques used to study failures include failure modes and effects analysis (FMEA) and failure mode, effects, and criticality analysis (FMECA). FMEA is used for the analysis of potential failures within a system. FMECA is similar, but it includes a criticality analysis.

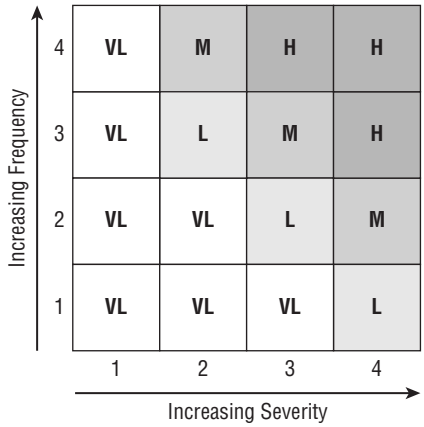
Risk Assessment Options

With the quantitative or qualitative risk assessment complete, the next step is to make a risk determination and decide which security controls should be applied.

The first step is to examine the amount of loss and the total impact that was calculated earlier. Risk ranking is one approach. An aggregate score can be used to examine the impact of the loss of confidentiality, integrity, or availability. A risk-ranking matrix looks at the

severity and frequency of each consequence. For example, severity might be ranked on a scale of 1 to 4, and frequency is ranked by the occurrence assigned to each impact, where 4 is the highest and 1 is the lowest. Figure 1.1 shows an example of a risk-ranking matrix and one method for determining a risk score.

FIGURE 1.1 Risk-ranking matrix



The outcome of this process is the ranking of priorities and data that can be used to determine how to deal with the risk. How you deal with risk will depend on the organization's *risk appetite*; that is, the total amount of risk the company is willing to accept. When speaking to individual risks, risk tolerance describes the amount of risk the organization is willing to accept. There are four possible alternatives for handling the potential risks:

Avoid To *avoid* the risk means to eliminate the risk, to withdraw from the practice, or to not become involved. This may be a viable option; there may also be an opportunity cost associated with avoiding the activity.

Accept To *accept* the risk means that it is understood and has been evaluated. Senior management has made the decision that the benefits of moving forward outweigh the risk. If those in charge have not been provided with good data on risk or have made invalid assumptions, poor choices may be made. This can give rise to disasters with global impact (BP, Fukushima, Chernobyl, Challenger, and so on).

Transfer To *transfer* the risk is to deflect it to a third party. For example, insurance is obtained. Instead of managing the risk directly, the organization incurs an ongoing continual cost from that third party.

Mitigate To *mitigate* the risk means that a control is used to reduce the risk. For example, installing a firewall is one method by which risk can be mitigated.

Just keep in mind that you can never eliminate all risk. There will always be some remaining residual risk. *Residual risk* is the risk that remains after your organization has taken proper precautions and implemented appropriate controls. There is also *inherent risk*, defined as the risk of carrying out a specific activity. As an example, an inherent risk of riding a motorcycle is that you might get hit by a car.

A particular risk may be intentionally left unmitigated or controlled in a manner that would normally be unacceptable. That risk would be an exemption to the typical risk management process. Risk exception recognizes the areas where you are not compliant in regard to laws, policies, or regulations. Resources are at risk for exposure to malicious activity and/or for penalties issued due to noncompliance. Exemptions are handled on a case-by-case basis, and as the name implies, they are strictly against the norm. An organization is expected to have prepared for such an occurrence through an exemption policy. The policy would dictate what management levels are required to approve the exemption, how it's documented, and how it will be monitored.

Finally, *risk deterrence* is having some process, policy, or system in place that discourages others from exploiting a vulnerability that, if exploited, would realize the risk. For example, what if, despite all of the mitigating controls in place, a server of top-secret military plans is accessible from the Internet? A risk deterrent is the law in place that, when enforced, would put an attacker in prison for exploiting the server.

Regardless of what you decide, you should incorporate stakeholder input into your decisions on how to deal with the identified risk. With so many risks to consider, the best place to start is with those that have a high-risk score. These items have the potential to cause great harm to the organization and should be addressed first. There are sometimes *risk exceptions*, such as when loss of life is a factor.

One easy way to remember these for the CASP+ exam is to think of AATM (avoid, accept, transfer, mitigate). Though not a cash machine, it may help you pass the exam.

Implementing Controls

Once a decision has been made on how to handle identified risk, it is time to execute risk mitigation planning, strategies, and controls. The document used to drive the process forward is the *risk assessment report*. This report contains all of the findings, information, assessments, and recommendations for the organization. The final assessment report becomes the instrument for management to make sound business decisions pertaining to what controls should be implemented.

This will require that you have designed some type of information classification system. These systems are usually based on either confidentiality or integrity. Regardless of the classification systems you use, you must classify and categorize data types into levels of CIA based on the organization/industry. As an example, the DoD might be more interested in the confidentiality of information, whereas a cloud service provider might be more interested in availability. The risk team will want to determine the minimum required security controls based on aggregate score. Without an asset valuation, it is difficult to understand a control's

return on investment (ROI) or cost-benefit analysis, pertaining to the investment in security countermeasures. Controls can be physical, technical, or operational.

Physical Controls Examples include locks, fences, CCTV, lights, gates, and guards.

Technical Controls You will want to implement technical controls based on CIA requirements and the policies of the organization. Examples of such controls include encryption, VPNs, security protocols (IPsec, SSL, TLS, and so on), VLANs, firewalls, and IDSs.

Operational Controls Examples include hiring practices, security awareness training, employment practices, termination practices, business continuity, and disaster testing and training.

Controls can also serve many purposes, such as prevention, deterrence, correction, mitigation, and so on. Once the proper control has been designed, it must be put in place. As an example, a fence is a physical control that can be used to deter or even delay an attacker. The purpose of implementing controls is to address the identified risks, threats, and vulnerabilities. To implement controls, a budget must be established. Although much of the risk assessment process has been performed by the team, now it's time for management to prioritize, create a budget, and have a tactical and strategic plan for implementing the recommendations presented in the final report. To determine what controls to put in place, you must consider the *total cost of ownership (TCO)*. The TCO can help determine the total cost of an asset or countermeasure. It includes purchase price, maintenance fees, updates, insurance, and the like. All costs are included. The risk assessment team must try to find a solution that provides the greatest risk reduction while maintaining the lowest annual cost.

These recommendations may have an impact on the entire organization and may take months, if not years, to implement fully. For the business to benefit from the technical recommendations and controls in place, it is necessary to translate technical risks into business terms. The recommendations must be structured and prioritized in the context that suits the business. This prioritization of tactical and strategic recommendations will enable the organization to make sound business decisions with the defined goals and objectives of the risk and vulnerability assessment.

Once controls are implemented, there is still more work to be done, as employees must be trained. IT security must work with management to implement ongoing security awareness and security training. Implementing organizational change requires an education and security awareness training plan for all employees or authorized users of the organization's IT systems, resources, and data. Mitigating risk requires all employees and users within the organization to abide by the security awareness training.

Policies Used to Manage Employees

A CASP+ must support the development of policies used to manage employees. Most employees want to do the right thing, are honest, and seek to excel in their jobs, but there must still be a structure of control. This control begins before an employee is onboarded (hired) and continues until their employment is offboarded (terminated).

Employee controls help protect the organization and build good security. Understand how each of the controls in the following sections is used and its primary attributes.

Pre-Employment Policies

Before an employee is hired, controls should be applied regarding how the potential employee is interviewed, what information is collected about the individual, and what is checked.

Many organizations start the pre-employment process with a background check. A *background check* is used to verify that the employee has a clean background and that any negative history is uncovered before employment. Although a background check is a good start, let's not forget education. *Education verification* is the act of verifying someone's educational background. With the rise of degree mills, it is easier than ever for individuals to fake their educational backgrounds, and the only way a company can know for sure is if the potential employee's credentials are verified.

Once employees are hired, an array of other policies will help manage their access to sensitive information and their levels of control. This is our next topic.

Employment Policies

For most new employees, a new job starts with initial training. This initial training provides employees with information on how to handle certain situations and what types of activities are and are not allowed. Employees don't know proper policies and procedures if they are not informed and trained. It is at this point that many employees will be asked to sign an acceptable use policy (AUP). The AUP defines what employees, contractors, and third parties are authorized to do on the organization's IT infrastructure and its assets. AUPs are common for access to IT resources, systems, applications, Internet, email, company phone systems (landlines), and company-issued or company-paid smartphones and other handheld devices. Employees are also given employee handbooks. Employees should sign an acknowledging receipt of all this information stating that they agree to follow the rules and regulations specified.

A nondisclosure agreement (NDA) is another important and legally enforceable document. An NDA is a contract that establishes confidentiality between two parties—the owner of the information and the recipient of that information.

AUPs typically outline what is and what is not acceptable behavior and the consequences of prohibited activities.

The handbook should detail the employee code of conduct, acceptable use of company assets, and employee responsibilities to the company. It should address the following issues:

- Security practices, policies, and procedures
- Paid holiday and vacation policy

- Work schedule and overtime policy
- Moonlighting and outside employment
- Employee evaluations
- Disaster response and emergency procedures
- Disciplinary procedures for noncompliance

Companies use a variety of controls to limit what an employee does and what level of access the employee holds. Although these practices may not be applicable for every business, they are common techniques used to limit the damage that could be caused by an unethical employee. In many ways, it's about least privilege. The *principle of least privilege* means that just because an employee is cleared to access a particular file, document, or physical location, this doesn't mean that they should be able to do so. Employees are given just enough access to allow them to conduct their normal duties, and nothing more. Common employee controls include the following:

Mandatory Vacations Uncovers misuse and gives the organization a time to audit the employee while they are not at work. The mandatory vacation is most commonly found in financial firms or applied to job roles where money is handled.

Job Rotation Rotates employees to new areas of assignment. This not only helps ensure backup if an employee is not available, but job rotation also can reduce fraud or misuse by providing the company with a means of rotating people to prevent an individual from having too much control over an area.

Dual Control Requires employees to work together to complete critical actions, thereby forcing employees who are planning anything illegal to collude with others. A common example is that of a combination or code for a safe. Two employees are required to open it successfully. Closely related to dual control is the *m* of *n* concept. This simply means that an activity, such as cryptographic recovery, is divided up among several individuals so that no one person acting alone can perform the entire key recovery process.

Separation of Duties Limits what one employee can do. For example, one employee may be able to write a check, but another must approve it.

Least Privilege Restricts the employee's access to only what is needed to do the job and nothing more. Closely related to the concept of least privilege is need to know.

IT security must support the development of HR policies that address such issues as separation of duties, job rotation, mandatory vacation, and least privilege.

Even if someone has met all of the requirements to be employed by a company and has been initially trained, this does not mean they are trained forever. Anytime a new process or technology is introduced in an organization, employees should be trained in its proper

operation. Security training also needs to be repeated on an annual basis. The short-term benefit of training and awareness for users is that it helps clarify acceptable behavior. As for the long term, training helps reinforce the danger from hackers and cybercrime. Raising the awareness of employees makes a potential attacker's job harder. Awareness training can consist of lunch schedules, learning programs, multiday events, or even degree programs. Common training methods include the following:

- Apprenticeship programs
- Classroom training
- Continuing education programs
- Degree programs
- In-house training
- On-the-job training
- Vendor training

A successful employee awareness program will tailor the message to fit the audience. Nontechnical employees will need a different message than technical employees.

End of Employment and Termination Procedures

According to the Bureau of Labor Statistics, the average person will have seven different jobs in their lifetime. For a company, this means that employees will come and go. They may leave for another job, move to another area, or even retire.

This means that our final topic in this area is termination. Human resources must have approved, effective procedures in place for the termination of employees, and HR must interface with IT security to make sure that access is terminated at the time of the employee's departure. IT security must partner with HR, legal, management, and other entities to make these systems work and to maintain compliance.

These security procedures should include processes for voluntary and involuntary separation. HR should work with security to ensure that the employee has returned all equipment that has been in their possession, such as access tokens, keys, ID cards, company credit cards, and mobile devices. If termination is involuntary, there needs to be a defined process on how to address or handle the situation properly. Issues such as employee escort, exit interviews, review of nondisclosure agreements (NDAs), and suspension of network access must all be covered in the applicable policy.

Terminating an employee's access at the proper time is critical. Department heads must report termination to HR in a timely manner, and this information must be acted on. In 2009, Fannie Mae fired a contract programmer at noon, yet did not terminate their access until midnight. In those 12 hours, it is believed the former contractor loaded a logic bomb into the company's network designed to knock out 4,000 servers. You can read more at `www.wired.com/threatlevel/2009/01/fannie`.

What procedure does your company follow when employees are terminated? Exercise 1.2 reviews a company's need to have a defined procedure to handle departure.

EXERCISE 1.2

Reviewing the Employee Termination Process

The CASP+ knows well the risks inherent in granting an unauthorized person access to sensitive areas or systems. When that person is someone who just recently lost access, there might be an added risk of malicious attack or theft of data.

1. How is the IT security department made aware of the termination? Is it a manual or automated process?
2. Is employee access terminated at the time of departure?
3. Is an exit interview performed?
4. Are exiting employees asked to return keys, laptops, smartphones, and other physical property?
5. Is the former employee reminded of any NDAs or other documents such as noncompete agreements they may have signed?
6. What are the obligations of the receiving party? What level of protection must they apply to the information they have received?
7. What time period applies to the NDA? Most NDAs don't last forever and have a time period applied, such as 1 year, 5 years, or 10 years.
8. Based on the previous questions, would you recommend changes to your company's termination procedures? Are there ways to work with HR to improve the process?

Cost-Benefit Analysis

Cost-benefit analysis is a technique used to determine whether a planned action is or is not acceptable. One common way to determine the cost-benefit analysis is to calculate the *return on investment (ROI)*. ROI is determined by dividing net profit by total assets.

For ROI to be accurately calculated, it's critical to maintain proper *asset management*. Asset management is defined in the context of maintaining control over your inventory, which must be identified, managed, and continually monitored to derive a reliable return on investment.

For projects that require some future evaluation, a payback analysis may be conducted. The payback analysis determines how much time will lapse before accrued benefits will overtake accrued and continuing costs.

Cost-benefit analysis consists of three steps: calculate costs, calculate benefits, and compare the results. A cost-benefit analysis will typically ask the following kinds of questions:

- Is the solution to the problem viable?
- Do the benefits of the plan of action outweigh the costs?
- Is the application or program beneficial to the organization?

Where the cost-benefit analysis requires quantification and proof of cost-effectiveness, analysis includes intangible benefits that can be hard to quantify. One area that is often overlooked when evaluating these items is the total cost of ownership (TCO). TCO is the purchase price of an asset plus the cost of operation. As an example, you may buy a NextGen firewall for $10,000. But that's not TCO. You must also consider the costs of environmental modifications, compatibility with other countermeasures, maintenance costs, testing costs, support contracts, and so on. If you combine all those items, you arrive at the TCO.

Continuous Monitoring

You can think of monitoring as a type of change management. Anytime a change is made to systems or the operating environment, a reassessment should be performed to see how the change affects a potential risk.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Because continuous monitoring occurs immediately or closely after events in which the key controls are used, it enables the enterprise to detect control failures quickly and find ways to make improvements quickly. NIST SP 800-37 (`csrc.nist.gov/publications/detail/sp/800-37/rev-2/final`) describes continuous monitoring as an effective, organization-wide program that should include the following:

- Configuration management
- Control processes
- Security impact analyses
- Assessment of selected security
- Security status reporting
- Active involvement of asset owners

SP 800-37 also states that the continuous monitoring should address these functions:

- Reporting progress
- Addressing vulnerabilities
- Describing how the information system owner intends to address those vulnerabilities

During the lifetime of an asset, changes will occur. People come and go, equipment changes are made, configurations change, and processes are revised. These changes will affect the organization's security posture. The result has to be assessed to determine whether these changes have altered the desired security state in a negative way.

As new assets are identified or change value and as risks are reassessed and monitored, the *risk management life cycle* is revealed. Risks are continuously reviewed, reassessed, and responded to throughout the life cycle. How exactly each life-cycle step is labeled or structured depends on the risk management framework adopted by the organization.

Throughout the risk management life cycle, the organization is entering and updating data into its *risk register*. The risk register is involved at nearly every step of the risk management process. The risk register should contain each risk as it is identified, assessed, owned by someone, responded to, and ultimately reassessed and monitored.

Enterprise Security Architecture Frameworks and Governance

Enterprise Security Architecture (ESA) frameworks describe the processes used to plan, allocate, and control information security resources. ESA frameworks are used for IT governance and include people, processes, and technologies. Here are two examples of ESA frameworks:

Enterprise Architecture (EA) Used by the federal government to ensure that business strategy and IT investments are aligned

Sherwood Applied Business Security Architecture (SABSA) Another perspective on strategy based on an architectural viewpoint

Regardless of the architecture used, the goal is to measure performance and ensure that companies are receiving the best return on their security investment. ESA frameworks typically include strategy, action plans, and provisions for monitoring as well as defined metrics such as these:

- Strategic alignment
- Effective risk management
- Value delivery

- Resource management
- Performance measurement
- Process assurance integration

The chosen ESA framework must balance technical and procedural solutions to support the long-term needs of the business and deliver substantial long-term efficiency and effectiveness. Some of the most popular risk management frameworks (RMFs) include the FISMA risk management framework, COSO Enterprise Risk Management Framework, and ISO 31000 for Risk Management.

Training and Awareness for Users

The role of training cannot be emphasized enough. Most employees want to do the right thing and genuinely want to see the organization thrive. However, it is the responsibility of the company to provide training. It is also important to remember that employees don't know proper policies and procedures unless they are informed as to what they are.

Just consider something as basic as emergency response. Without proper training, some employees may be tempted to simply stop what they are doing and run for the door; this may even be OK, but what's the approved response? Does each employee know what to do? Do employees know how to respond in the face of a cyberattack, disaster, weather emergency, or any other situation? Training helps assure that employees know how to respond to potential security risks and incidents.

Consider adopting the "prudent person rule" to ensure that training incorporates the procedures followed by other firms in the same industry, such as those used by banks, hospitals, credit card handlers, or others.

Training does offer a good return as it increases effectiveness and efficiency. When new security processes or technologies are introduced, employees should be trained in them. Training increases morale and helps employees strive to do a better job.

Real World Scenario

Building a Security Awareness Program

As a security administrator, you know all about the importance of good security practices. Now imagine that you have been asked to develop a security awareness program. With this in mind, where would you start, and what would you do to help ensure that the program is a success?

The first thing that you should do is to make a list of items that can help raise awareness of good security practices. The following list includes some of the questions you should consider asking:

1. Does the program have the support of senior management?
2. Do you have existing policies and procedures that dictate good security practices?
3. Can you get all employees involved and make sure that they hear the message at least once a year?
4. Can you get help from security representatives in each area of the company to assist in the awareness program and address security incidents?
5. Can you implement annual self-assessment surveys?

An awareness program cannot be conducted in a vacuum. It takes time to change people's practices and attitudes. Consider the current security culture before expecting radical change overnight.

Timing is of critical importance when dealing with training. Security training needs to be performed when employees are hired, including AUP training and policy sign-off, and then followed up with annual reinforcement. As a CASP+, you will need to engage the HR department. In some organizations, the training task is assigned solely to HR, which has no idea how to conduct security training and may not even recognize the importance of it.

Best Practices for Risk Assessments

If you are tasked with taking part in a risk assessment, a key concern will be to define its goals and objectives. One good place to start is the mission statement. The *mission statement* typically defines a company's primary goal.

There are many techniques to consider when conducting a risk and vulnerability assessment. These best practices or approaches vary depending on the scope of the assessment and what the team is trying to protect. To secure and protect assets properly, significant amounts of time, money, and resources are required. Only then can the proper level of security be designed and implemented properly. When preparing and conducting a risk assessment, consider the following best practices or approaches:

- Create a risk assessment policy.
- Inventory and maintain a database of IT infrastructure components and IT assets.

- Define risk assessment goals and objectives in line with the organizational business drivers.
- Identify a consistent risk assessment methodology and approach for your organization.
- Conduct an asset valuation or asset criticality valuation as per a standard definition for the organization.
- Limit the scope of the risk assessment by identifying and categorizing IT infrastructure components and assets as critical, major, and minor.
- Understand and evaluate the risks, threats, and vulnerabilities to those categorized IT infrastructure components and assets.
- Define a consistent standard or yardstick of measurement for securing the organization's critical, major, and minor IT infrastructure.
- Create a business continuity plan to help ensure that critical processes and activities can continue in case of a disaster or emergency.
- Perform the risk and vulnerability assessment as per the defined standard.

Implementing these risk assessment best practices is not easy. It requires careful analysis and decision-making unique to the organization's business drivers and priorities as an organization. Table 1.4 shows an example summary of annualized loss expectancies. The proposed "cost," or single loss expectancy, is fairly low when considering that most services can be replaced nearly free of charge by cloud providers.

TABLE 1.4 Annualized loss expectancy (ALE) of DMZ assets

Asset	Threat	SLE	ARO	ALE	Countermeasure
Web server	DoS	$300	1	$300	Redundant web servers
Email server	Open relay	$0	.01	$0	Closing relay
DNS server	Cache poisoning	$100	.25	$25	DNSSEC
Firewall	Enumeration	$500	.2	$100	Hardening
Database	SQL injection	$10,000	2	$20,000	Web application firewall and input validation

You can see that the result of the risk assessment process is to determine which items to address first. You must keep in mind that all companies have limited assets and that not every single vulnerability can be addressed. The best way to start is to determine which items

would cause the most damage or which represent the greatest threat to the organization. In most situations, this will mean that the ALE will be examined. As an example, in Table 1.4, it's noted that a SQL injection attack has an ALE of $20,000. It would be of utmost importance to start by examining this threat and assessing what would be the cost of implementing a countermeasure.

Finally, you will want to keep in mind that the risk assessment process is not a one-time event. As items change, or on a periodic basis, the risk assessment process must be repeated.

Business Continuity Planning and Disaster Recovery

In general terms, *business continuity planning (BCP)* is the formation of a plan for what to do should the business suffer an interruption. This plan is often based on the results of a *business impact analysis (BIA)*. A BIA is a formal process designed to identify mission-essential functions in an organization and facilitate the identification of the critical systems that support those functions that must be continued during an emergency.

A disaster is any event that has the potential to disrupt an organization's business. The occurrence of a disaster triggers the activation of the organization's *disaster recovery plan (DRP)*.

Organizations must conduct site risk assessments for each of their facilities and create a DRP that, combined with a BIA, identifies and prioritizes the risks posed to the facility by an internal or external disaster. These assessments are considered to be a subset of business continuity planning. Business continuity planning includes the strategy to resume a business whether it has been interrupted by a minor event or a major disaster.

Two key concepts in business continuity planning are the *recovery point objective (RPO)* and the *recovery time objective (RTO)*. To understand these terms, first imagine that a business has experienced a significant interruption to its operations. Let's say that the business's operations normally involve processing payment transactions. Established business continuity planning states that a set duration of time is allowed to pass before the amount of transaction data lost during an interruption exceeds the tolerable amount. For example, imagine an inline rolling storage of two hours of transaction data. In the event of an outage, any portion up to two hours could then be processed after full operations are restored. That set duration of time is the RPO.

The RTO is more concrete. Now recall that it takes 30 minutes to recover from the disruption. It takes 30 minutes to get all servers booted up and tap into the server that's holding the two hours' worth of backlogged data. The RTO is the amount of actual time (duration) since the beginning of the interruption that is deemed tolerable before the interruption is considered intolerable to the business

Another element of the rebuilding process that helps control costs is the *recovery service level (RSL)*. The RSL is a percentage measurement (0–100 percent) of how much computing

power is needed. This is based on a percentage of the production system that you will need during an emergency.

As stated earlier, an interruption could be anything ranging from a minor power hiccup to a total building collapse. In terms of a short power hiccup, let's use the example of a storage array failure. To recover from that failure, the storage engineer requires 12 hours on average to replace the hardware involved and rebuild the data from backups. The *mean time to recovery (MTTR)* is then 12 hours. The MTTR describes the length of time between an interruption and the recovery from that interruption.

Now let's say that the power hiccups cause subsequent disk failures, which occur on average every month. Another important business continuity concept is the *mean time between failure (MTBF)*. In this case, MTBF is around 30 or 31 days.

Let's say our data center suffered a great outage and we need to implement our disaster recovery plan. Our DR planning includes readying an offsite location to become our new data center. What kind of offsite infrastructure is prepared depends on two big factors:

- How quickly should our new infrastructure help us recover?
- Does the need for our offsite infrastructure justify its expense?

The answers to those two questions will decide which of the following sites we prepare:

Cold Site We have a place filled with our to-be infrastructure. Equipment is effectively only available to set up. At least partial setup and configuration are assumed not yet done. This *cold site* is the cheapest and will require the most time to have running. Likely initial steps involve opening boxes.

Warm Site We have a place with equipment set up and configured, ready to turn on. In fact, our *warm site* is probably running but still requires considerable effort to resume operations. Likely initial steps involve restoring backups.

Hot Site We have a place with equipment set up and running as a copy of our recently lost data center. Effort to resume operations should be minimal for a *hot site*. Likely initial steps involve assuring minimal data loss since the disaster event.

Mobile Site A *mobile site* is what it sounds like: a site that can be moved or mobilized to a new location. Picture a truck trailer filled with equipment to mirror your data center.

Reviewing the Effectiveness of Existing Security Controls

It would be nice to think that all of our defensive security controls will work as designed. This is usually not the case. Consider for a moment the Maginot Line. This physical defensive structure was designed by the French before World War II as a line of concrete fortifications, tank obstacles, artillery casements, and machine gun posts to hold back the

Germans in case of an attack. However, the Maginot Line did not work as planned. At the start of the war, the Germans simply drove around it and attacked from behind the line.

This same concept can be applied to network security controls. Although we may believe that they have a high level of effectiveness, this may or may not be true. Security controls must be tested and evaluated to ensure their effectiveness. Firewalls and edge security devices do work well at stopping external attacks, but what happens when an attacker is internal and behind these edge controls? Some of the methods used to review the effectiveness of existing security controls are as follows:

Gap Analysis A *gap analysis* involves an examination of an area or environment designed to report the difference between "where we are" and "where we want to be." The analysis of that gap provides an objective viewpoint that helps form the steps necessary to close that gap.

Audits An *information security audit* is typically a review of a company's technical, physical, and administrative controls. There are many kinds of audits with multiple objectives; the most common types with which the CASP+ will likely be involved deal with security controls. Auditors usually follow one or more of these audit standards:

- Control Objectives for Information and Related Technology (COBIT) guidelines that are developed and maintained by ISACA (formerly known as the Information Systems Audit and Control Association)
- FISMA, which specifies the minimum-security compliance standards for government systems, including the military
- Financial Accounting Standards Board (FASB)
- Generally Accepted Accounting Principles (GAAP)
- American Institute of Certified Public Accountants (AICPA)
- Statements on Accounting Standards (SAS)
- Public Company Accounting Oversight Board (PCAOB), issuer of audit standards

Vulnerability Assessments *Vulnerability assessment* tools and scanners provide information on vulnerabilities within a targeted application or system or an entire network. Vulnerabilities are often graded on a scale of high, medium, or low. Vulnerability assessment tools usually provide advice on how to fix or manage the security risks that they have discovered. Externally administered vulnerability assessment services are available and are usually implemented by means of a stand-alone hardware device or by means of an installed software agent.

Although these tools work well, they are not perfect in that they offer only a snapshot in time of what problems have been identified. There is also the issue that vulnerability assessment scanners typically don't fix problems. They identify problems and then only some of the problems. Finally, any given tool can produce false positives or false negatives or may not even identify specific problems. Examples of well-known vulnerability

assessment tools include Nikto, Nessus, Wireshark, Metasploit, Nmap, Retina, LanGuard, OpenVAS, and SAINT.

Ethical Hacking *Ethical hacking* is the process of looking at a network in the same way as an attacker would. The ethical hacker is attempting to determine what the attacker can access and obtain, what an attacker can do with that information, and whether anyone would notice what the attacker is doing. Ethical hacking requires the testing team to work with management to assess the value of its assets, what is most critical, and how much protection is in place to protect these assets.

Ethical hackers are also known for penetration testing, or they may even be described as being part of a team such as red or tiger.

Conducting Lessons Learned and After-Action Reviews

After a contract has been signed or a service level agreement (SLA) has been established, an organization should conduct one or more lessons learned or after-action reviews to determine the effectiveness of the agreement process and to identify any necessary improvements to existing policies, processes, and other organizational practices. An SLA is a written contract that specifies the levels of service that will be provided by the vendor and what the customer can do if the vendor fails to meet the SLA terms. SLAs commonly cover the issues of response time.

The purpose of a lessons learned, or after-action review, is to provide insights and recommendations for when these processes are repeated. These activities can occur throughout many different types of projects, including the software development life cycle (SDLC) and incident response. The lessons learned process should be conducted after a sufficient time has elapsed after the signing of a contract. Here are some of the items that should be reviewed during the lessons learned process:

- Policies and procedures
- Technology, configuration, or system enhancements
- Personnel resources, including response team resources
- Communication procedures
- Training
- The security measures put in place
- Whether enough information was available to complete the agreement properly

- How well the partner provided its required service
- Whether the procedures outlined in the response plan were adequate and worked as intended
- Whether significant problems were encountered during the RFP process

Any relevant lessons learned should be included in the revised agreement process for reference, and the updated documents should be communicated to all of the relevant personnel.

Creation, Collection, and Analysis of Metrics

Businesses rely on monitoring and reporting to gauge how business is going and to decide what to change, fix, or improve. Before you can monitor something, you first need to know what to monitor. Most of the time, this is obvious. If you're driving your car, you're monitoring your speed and fuel usage. But what about sales, operations, or financials? Someone first has to create what to monitor, and then they can move on to collect and analyze the data.

Metrics

When monitoring something like your car's speed or your network switch's utilization, you need a snapshot value to measure. That measured value is the metric. Your car is going 65 miles per hour, and your switch is humming along at 35 percent utilization. Both numbers are *metrics*.

Metric creation and collection are not difficult. The difficulty lies in understanding the value behind the metric. Back to the car analogy, what if a driver wanted to know the number of tire revolutions instead of the car's speed? You could argue that both would tell the driver how "fast" they're driving, relatively speaking, that is, until you understand that differences in tire size make measuring tire revolutions an unreliable metric. The same thoughtfulness has to be applied for creating and collecting IT and security metrics.

Once valid metrics are created and understood, you can also create *key performance indicators (KPIs)* and *key risk indicators (KRIs)*. KPIs and KRIs are a special kind of measurement that also includes a goal. If a metric answers the question "What are we doing?" then a KPI answers the question "How are we doing?" and a KRI then addresses the question "How careful must we be?"

Key performance indicators can help an organization better measure important metrics such as scalability, availability, and reliability. For example, KPIs related to uptime provide insight into *availability*. Similarly, KPIs related to how often a failure occurs and its impact will help provide insight on *reliability*. Lastly, when it comes to *scalability*, an important KPI may indicate the growth of infrastructure. Knowing the growth in demand for services can then help the growth KPI illustrate scalability.

Trend Data

Analyzing collected metrics doesn't have to originate from within the organization. A CASP+ must analyze and interpret trend data to anticipate cyber defense aids. Luckily, many good sources of information are available to help in this process. One example is the FBI's Internet Crime Complaint Center (IC3) (`www.ic3.gov`). Each year, reports provide an overall review of cybercrime for the preceding year.

Analyzing Security Solutions to Ensure They Meet Business Needs

The CASP+ may be responsible for analyzing security solutions to ensure that they meet business needs. The CASP+ should examine the areas of performance, maintainability, and availability and their related areas, as described here:

Performance Performance is the accomplishment of a given task measured against preset known standards of accuracy, completeness, cost, and speed.

Uptime Agreements *Uptime agreements (UAs)* are one of the most well-known types of SLAs. UAs detail the agreed-on amount of uptime. For example, they can be used for network services such as a WAN link or equipment like servers.

Time Service Factor The *time service factor (TSF)* is the percentage of help-desk or response calls answered within a given time.

Abandon Rate The *abandon rate (AR)* is the number of callers who hang up while waiting for a service representative to answer.

First Call Resolution The *first call resolution (FCR)* is the number of resolutions that are made on the first call and do not require the user to call back to the help desk to follow up or seek additional measures for resolution.

Latency *Latency* can be described as delay. Latency can be examined to determine how long it takes an application to respond or even the amount of delay in a WAN network. Different applications can support varying amounts of latency. Some programs, such as FTP, can easily handle latency, while others, such as VoIP, do not handle latency well. The CASP+ must research specific applications to determine the acceptable amount of latency.

Scalability *Scalability* is the ability of a program, application, or network to continue to function as scale, volume, or throughput is changed. The CASP+ should examine current security needs and assess future growth to ensure that any selected solutions can meet long-term needs.

Capability *Capability* is the ability to meet or achieve a specific goal.

Usability The International Organization for Standardization (ISO) defines *usability* as "the extent to which a product can be used by specified users to achieve specified goals."

Security Requirements Organizations may require security in place, but the controls put in place to maintain that security must be usable. In other words, implementing security requirements that render a business process moot is unusable. The difference between *usability* and *security requirements* is that security requirements meet the criteria of usability to viable and effective. To meet both needs, a *trade-off analysis* may be required to find out whether both requirements are satisfied. Trade-off analysis can identify problems that demand finding a balance between different factors, such as the time and cost.

Recoverability *Recoverability* is yet another important characteristic in that it defines the capability to restore systems to the exact point in time at which the failure occurred.

Maintainability Yet another important characteristic of any proposed security solution is its *maintainability*. As an example of maintainability, the U.S. space shuttle was originally designed for a projected life span of 100 launches, or 10 years of operational life. The shuttle was retired in 2011 after about 30 years of service. Our point is that although your chosen solutions may not last two or three times the original design life, it is important that they be maintainable through the expected time of use.

Availability *Availability* refers to the functional state of a system and, in the networking world, is often simplified to uptime. Some terms that you should understand are mean time between failure (MTBF) and mean time to recovery (MTTR). MTBF is the total operating time divided by the number of failures; MTTR refers to the amount of time it takes to restore a system if and when a failure occurs.

Testing Plans

What's that phrase? An ounce of prevention is worth a pound of cure? In other words, a little prevention goes a long way. *Testing plans* are the first step in prevention. A testing plan provides a planned approach to practice procedures such as those drafted for disaster recovery. The following are a variety of testing plans:

Walk-Through The team will "walk through" and analyze the steps of disaster recovery. No actual recovery infrastructure setup is done as in a parallel test. The *walk-through test* is a straightforward exercise where you manually perform the steps without causing any real disruption.

Checklist Perhaps the easiest form of testing is simply reading through the *checklist* of procedures and steps toward disaster recovery. Any glaring gaps or concerns are analyzed further.

Tabletop Exercise The goal of a *tabletop exercise* is to raise situational awareness in the context of information security. It is also designed to foster discussion of incident response in brief, practical discussion periods. For management, tabletop exercises provide a great opportunity to demonstrate scenarios that are most likely to occur for the incident response group.

Parallel Tests and Simulation Tests To simulate a disaster recovery by running through all the steps alongside the disaster recovery systems and processes, you should conduct a *parallel test*. The *simulation test* is going through all motions, but production systems are still running.

Full Interruption Test As you might suspect, a *full interruption test* is the true test of confidence in disaster recovery planning. Production systems are temporarily taken offline once disaster recovery systems are set up and ready to assume the place of the shutdown systems.

Internal and External Audits

An *internal audit* is one conducted to improve an entity's operations. Medium-sized and large-sized operations usually have an internal auditing department to monitor the operations of the organization regarding the improvement of effectiveness, control, governance processes, and risk management. The department accomplishes this by providing recommendations and suggestions on the basis of the assessment of data and business transactions. The main purpose of an internal audit is to provide an independent opinion and consultancy to senior management and those charged with governance (governing bodies). Internal audits are mostly performed by an employee of the organization; however, some organizations hire the services of an audit firm for an internal audit.

An *external audit* indicates an audit of the organization by an independent audit firm, which is not controlled by the organization that it is auditing. An external audit is performed because of statutory requirements in order to express an opinion on whether the security controls, processes, and documentation are in accordance with acceptable standards and regulatory requirements in all material aspects. For an external audit, the auditor is required not to have any prior association with the organization; that is, an external auditor must be independent in their work.

Auditing requirements and frequency can be determined by a few factors, such as corporate policy. But perhaps the most common factor is regulatory compliance. A regulation might require an organization to audit annually or semi-annually.

Using Judgment to Solve Difficult Problems

Sometimes, you have to use judgment to solve difficult problems that do not have a best solution. This is where your years of experience come in handy! Ever wonder why some car mechanics are so good at diagnosing and repairing problems? That's because they have mastered the process of using judgment and experience to work through problems. There is no one right way to work through problems, since each person must find a method that works best for them. We will show you one approach here. Try it and see if it works for you.

Define the Problem You've been told there is a problem. Obtain a specific description of the problem. What are the symptoms?

Gather the Facts Ask yourself (or another CASP+) these questions when something fails or is not working properly:

- Did it ever work?
- What changed?
- Was a new piece of hardware or software added, such as a firewall or intrusion detection system?
- When did this first happen?
- Does anyone else have the same problem?

Brainstorm You are at the point where it's easy to change the first thing to come to mind. However, the best course of action is to think about all the possibilities for why something doesn't work or why something is behaving in a certain way.

Implement This is where you make a step-by-step list of the possibilities for testing. Test each possibility to see if it corrects the problem. Be careful to change one thing at a time to avoid creating any new problems. If the step-by-step procedure fails to fix the problem, then return to the beginning of the process and start over.

Evaluate Think back to what you have done, and then document causes and solutions to the problem. Share your newfound knowledge with friends and co-workers.

Summary

A CASP+ must understand threats to the business, potential risks, and ways to mitigate risks. Risk is something that you must deal with every day on a personal and business level. Policy is one way to deal with risk. On the people side of the business, policy should dictate

what employees can and cannot do. Even when risk is identified and has been associated with a vulnerability, a potential cost must still be determined. This cost can be derived via quantitative or qualitative methods. Each offers advantages and disadvantages and helps provide the tools to determine whether a threat should be accepted, avoided, mitigated, or transferred. You will want to know basic risk formulas and how to perform calculations for items such as SLE and ALE should you be asked to do so for the exam. Finally, a CASP+ must also understand the importance of proper planning and testing of business continuity planning and disaster recovery. Without BCP and DR, a business simply waits for the next disaster.

Exam Essentials

Be able to describe specific risk assessment techniques. Two basic techniques can be used to perform risk analysis: qualitative and quantitative. Qualitative risk assessment is more subjective, not monetary-based, and uses descriptors such as critical, high, medium, and low. Quantitative risk assessment assigns and uses monetary values against known risks.

Know how to make a risk determination assessment. Risk and vulnerability assessments provide the necessary information about an organization's IT infrastructure and its assets' current level of security so that the assessor can provide recommendations for increasing or enhancing that level of security. Understand that conducting a risk assessment is difficult and prone to error. Once the risk is identified and assessed, realize that analyzing the results is often problematic in itself.

Know how and when to apply security controls. Controls may or may not be applied. All companies have only limited funds to implement controls, and the cost of the control should not exceed the value of the asset. Performing a quantitative or qualitative risk assessment can help make the case for whether a control should be applied.

Know the various ways to address risk. Threats coupled with vulnerabilities can lead to a loss. To prevent or deal with the potential risk, several approaches can be used, which include accept, avoid, mitigate, and transfer.

Know the importance of business continuity and disaster recovery concepts. Businesses cannot survive a disaster without proper planning. Business continuity and disaster recovery plans must be in place, reviewed and practiced periodically, and updated on a schedule. Be sure you understand business impact analysis (BIA), privacy impact assessments, disaster recovery planning (DRP), business continuity planning (BCP), incident response, and testing plans.

Be able to apply the appropriate risk strategies and types of risk assessments. Risk assessments are a formalized approach to risk prioritization that lets an organization conduct reviews in a structured manner. Risk assessments follow two different analysis methodologies: quantitative risk assessments that use numeric data in the analysis, resulting in

assessments that allow the very straightforward prioritization of risks, and qualitative risk assessments that use subjective data for the assessment of risks that are difficult to quantify.

Understand risk mitigation, strategy, and best practices. Risk mitigation is the process of applying controls to reduce the probability or impact of a risk. Risk management is the most common risk management strategy, and the vast majority of the work of security professionals revolves around mitigating risks through the design, implementation, and management of security controls. Many of these controls involve engineering trade-offs between functionality, performance, and security.

Review Questions

You can find the answers in Appendix.

1. Which of the following is not an advantage of quantitative risk assessments?
   - **A.** Examination of real threats
   - **B.** Fast results
   - **C.** Subjective opinions
   - **D.** Dollar values
2. Which of the following is the formula for SLE?
   - **A.** SLE = AV × EF
   - **B.** SLE = AV / EF
   - **C.** SLE = ARO × EF
   - **D.** SLE = ARO × AV
3. Which of the following is not an advantage of qualitative risk assessments?
   - **A.** Speed
   - **B.** Use of numeric dollar values
   - **C.** Based on CIA
   - **D.** Performed by a team
4. Which of the following is the formula for ALE?
   - **A.** ALE = AV × ARO
   - **B.** ALE = ARO × SLE
   - **C.** ALE = SLE / ARO
   - **D.** ALE = AV / ARO
5. Which of the following is the approach for dealing with risk that incurs an ongoing continual cost from a third party?
   - **A.** Accept
   - **B.** Avoid
   - **C.** Mitigate
   - **D.** Transfer
6. Implementation of a firewall best maps to which of the following?
   - **A.** Accept
   - **B.** Avoid
   - **C.** Mitigate
   - **D.** Transfer

7. After determining the exposure factor, which is the next step of the quantitative risk assessment process?
   - **A.** Determine the SLE.
   - **B.** Determine the ARO.
   - **C.** Determine the ALE.
   - **D.** Determine the AV.

8. When problem solving, which of the following steps or guidance involves making a step-by-step list of the possibilities for testing?
   - **A.** Implement
   - **B.** Gather the facts
   - **C.** Brainstorm
   - **D.** Evaluate

9. Which of the following most helps employees know how to respond to potential security risks and incidents?
   - **A.** Brainstorm
   - **B.** Separation of duties
   - **C.** Security awareness training
   - **D.** Mandatory vacation

10. A(n) _____ can be described as a weakness in hardware, software, or components that may be exploited in order for a threat to destroy, damage, or compromise an asset.
    - **A.** Vulnerability
    - **B.** Threat
    - **C.** Exposure
    - **D.** Risk

11. A(n) _____ is any agent, condition, or circumstance that could potentially cause harm to, loss of, or damage to an IT asset or data asset, or compromise it.
    - **A.** Vulnerability
    - **B.** Risk
    - **C.** Threat
    - **D.** Exposure

12. Which of the following is not an acceptable audit standard for an auditor to follow?
    - **A.** COBIT
    - **B.** GAAP
    - **C.** FISMA
    - **D.** OpenVAS

13. Which of the following helps describe reporting the difference between "where we are" and "where we want to be"?

A. Lessons learned report

B. After-action report

C. Audit

D. Gap analysis

14. Nikto, Nessus, Retina, LanGuard, and SAINT are useful for what kind of activity?

A. Exploitation

B. Threat assessment

C. Control auditing

D. Vulnerability scanning

15. As one of the most well-known types of SLAs, which of the following details the agreed-on amount of uptime?

A. RTO

B. UA

C. FCR

D. TSF

16. The concept that users should have only the access needed is known as which of the following?

A. Audited control

B. Defense in depth

C. Deny all

D. Least privilege

17. Which of the following types of testing is best described as manually performing the recovery steps without causing any real disruption?

A. Full interruption test

B. Checklist

C. Walk-through test

D. Simulation test

18. What type of disaster recovery site is the cheapest to maintain?

A. Mobile site

B. Cold site

C. Warm site

D. Hot site

19. Which of the following terms is described as the length of time between an interruption and the recovery from that interruption?

A. MTTR

B. RPO

C. MTBF

D. Availability

20. Which of the following describes the scenario where two employees are required to open a safe, each of them with its combination or code?

A. Dual control

B. Separation of duties

C. Job rotation

D. Least privilege