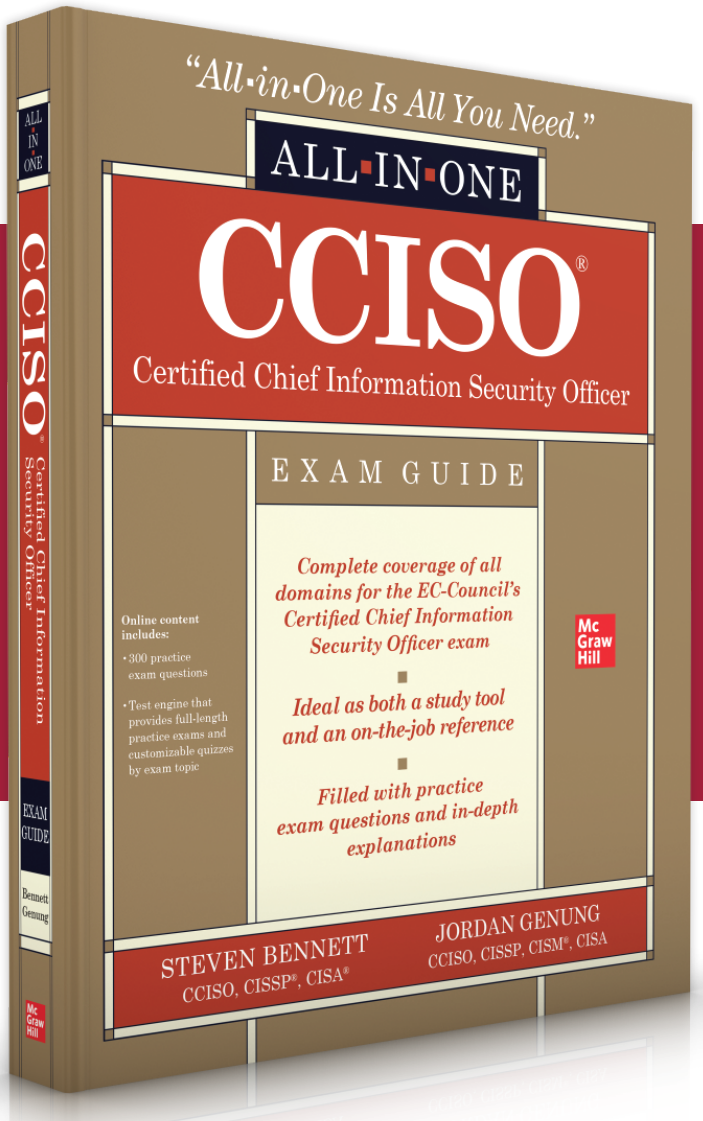
Mc Graw Hill

ALL-IN-ONE

CCISO

Certified Chief Information Security Officer

EXAM GUIDE



Sample Chapter

CHAPTER 3:
Security Program Management and Operations

LEARN MORE

BUY NOW

Because learning changes everything.®

mhprofessional.com

CHAPTER 3

Security Program Management and Operations

This chapter discusses the following topics:

- Security program management
- Security program budgets, finance, and cost control
- Security program resource management: building the security team
- Project management

The CISO carries out the job of protecting the organization's assets by implementing a well-planned and executed information security program. This chapter describes what an effective information security program looks like and how it is managed, staffed, and funded. An information security program generally has two types of activities: *subprograms*, also known as *streams of work*, which are long-term activities or ongoing activities, and *security projects*, which have a defined end state that, when achieved, signals the end of the activity. This chapter describes the management processes used to carry out both types of activities.

Security Program Management

Chapter 1 introduced the components that make up a typical security program. To review, a synopsis of the components follows (see Figure 3-1):

- **Security areas of focus** External drivers that impact the security program, such as PCI DSS, HIPAA, Sarbanes-Oxley, or FISMA, along with internal drivers, such as an IT department's IT service management policy.
- **Security streams of work** Ongoing security activities that are continuous, such as security event monitoring, incident response, vulnerability management, and so on.

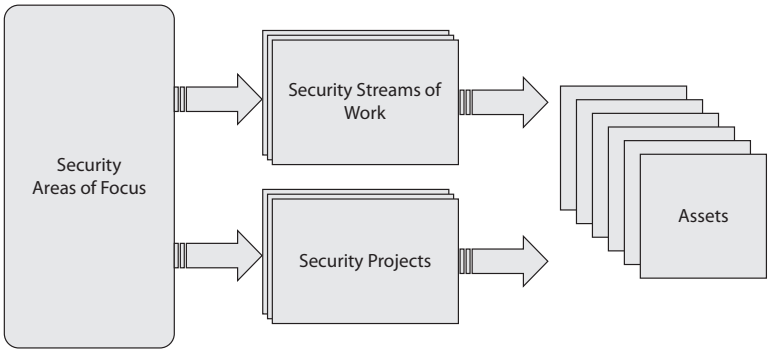


Figure 3-1 Security program components

- **Security projects** Activities initiated and implemented by the security organization that are not ongoing but instead have a defined goal or end product. Examples of security projects include choosing an identity management solution, deploying a specific GRC system (described in the adjacent sidebar), building a security awareness portal, or performing a vulnerability assessment. Projects are implemented following a project management process.
- **Assets** Resources owned by the organization. Within the context of a security program, assets are resources that require protection against threats. Assets most often consist of systems and data.

The CISO's challenge is to manage these elements in a cohesive and coordinated manner.

Security Areas of Focus

Security areas of focus are drivers that impact how the streams of work and security projects are carried out. The areas of focus impact an organization's decisions regarding which security activities are required and where they need to be applied. Areas of focus may apply to specific assets or groups of assets. For instance, PCI DSS requires specific security controls to be put into place based on where in the enterprise credit card data resides. Therefore, PCI DSS impacts the security requirements of the design, implementation, and operation of the assets in the enterprise that store, process, or transmit credit card data. PCI DSS may impact one or more streams of work and one or more security projects.

Governance, Risk Management, and Compliance

Governance, risk management, and compliance (GRC) is a term used to describe an integrated approach to these three practices and their associated activities. Some organizations implement GRC programs to enable a cohesive, holistic approach to organizational GRC, ensuring that the organization acts in accordance with its internal policies, external compliance requirements, and risk appetite through the alignment of strategy with organizational objectives. The benefit of GRC is the synchronization of information between these functions across the organization to ensure they are not siloed off from one another.

- **Governance** Ensuring that strategic goals, rules, policies, and practices align with business objectives
- **Risk management** Managing risk to acceptable levels by analyzing risk probability and impact and prioritizing control implementation
- **Compliance** Monitoring and reporting on the organization's conformity with both internal requirements (policies and procedures) and applicable external requirements (laws and regulations)

GRC is often aided by technology through the implementation of a GRC system. A *GRC system* enables an organization to accomplish GRC-related initiatives using a centralized tool. Each GRC function produces and manages a variety of information, such as asset inventory, policies, standards, procedures, audit work papers, security incident information, risk management information, compliance information, control monitoring and reporting information, and so on. This information is often maintained in distributed documents, spreadsheets, and/or systems. Key benefits of a GRC system include the ability to consolidate data into a central location, automate business processes, and compile and report on centralized GRC data.

GRC systems provide a range of features, which may include some or all of the following:

- Managing policy and procedure development, management, and review workflows
- Documenting policy exceptions
- Documenting controls and managing control monitoring workflows
- Maintaining an inventory of assets
- Managing risk assessments for assets

(Continued)

- Documenting and managing control deficiencies
- Maintaining a risk register and risk documentation
- Tracking control testing
- Managing audit documentation, plans, and engagements
- Recording and tracking of incidents
- Dashboards and reporting

When deciding whether to implement a GRC system, an organization needs to consider many factors. As with any tool, realizing value requires up-front work. With a GRC system, this up-front work may be significant, particularly for smaller security teams, if the organization fails to identify use cases or lacks a robust governance, risk management, and compliance foundation. To realize the full value of a GRC system, the organization should consider the following:

- Does the organization have a complete inventory of assets, compliance obligations, and controls?
- Are asset owners and data owners identified?
- Is there a solid foundation of policies, procedures, standards, and such?
- Have use cases for the GRC system been identified?
- Is there a thorough understanding of manual process workflows to be automated?
- Are individuals involved in the workflows identified?
- Does the organization have staff and resources to implement, manage, and maintain the GRC system?
- What kind of customization will be required?
- What kind of reporting requirements are required from the GRC system?

Although it provides many benefits, a GRC system cannot fix a poorly defined GRC program. A GRC system provides good value when used to augment a well-defined GRC program.

Areas of focus include laws, regulations, standards, or policies that the organization must comply with. The process for addressing compliance (and therefore areas of focus) is described in Chapter 1 in the "Compliance" section. The CISO is responsible for ensuring that the areas of focus are correctly integrated into the security program.

Security Streams of Work

Activities that are ongoing and do not have a beginning, middle, and end fall into the category that some CISOs call *streams of work* and others call *subprograms* of the information security program. For the purpose of this discussion, we use the term streams of work. Due to their nature, these activities go on for the life of the security program. These ongoing security activities vary from organization to organization. Here is a list of some typical security streams of work:

- Security document maintenance (security charter, policies, procedures, standards, and guidelines)
- GRC
- Risk analysis and management
- User identity management and provisioning
- Asset management
- Threat intelligence
- Security monitoring and intrusion detection
- Intrusion prevention
- Security administration
- Configuration and patch management
- Application security
- Security training and awareness
- Security testing
- Physical security
- Business continuity
- Disaster recovery

Although these activities are ongoing, they still have a life cycle process that is somewhat similar to a project management life cycle. Streams of work can be accomplished following a process model such as the Plan, Do, Study, Act (PDCA) process model, previously discussed in Chapters 1 and 2. The often-quoted William Edwards Deming, who championed the PDCA model, once said: "It is not enough to do your best; you must know what to do and then do your best." Following Deming's advice, the PDCA cycle that is commonly used in many industries works well for performing streams of work because each stream should be

- Well planned
- Performed in accordance with a plan
- Measured against criteria for success
- Continuously improved to address any shortcomings and get better over time

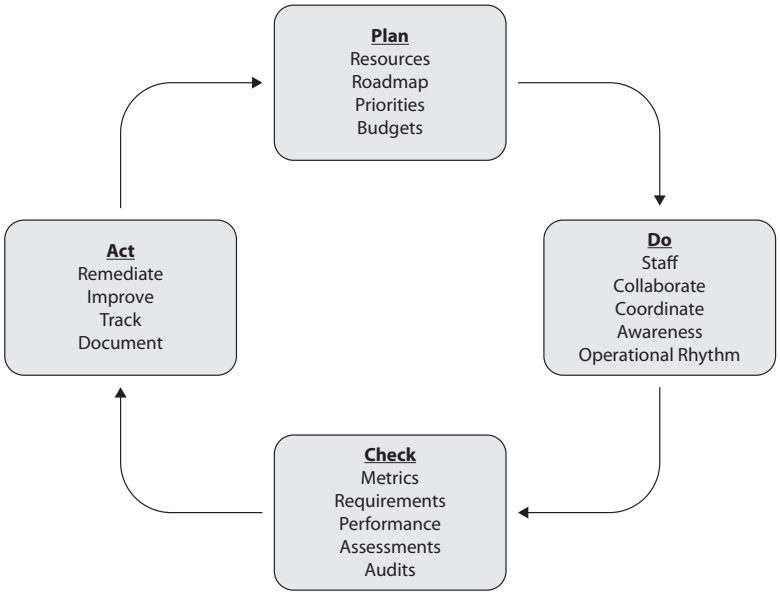


Figure 3-2 Stream of work process

Chapter 1 introduced the PDCA process as it applies to compliance management. However, the PDCA model (also called the Deming cycle or Shewhart cycle) works well for any stream of work, compliance or otherwise. Figure 3-2 illustrates how the PDCA model can be used for security streams of work, as described next.

Plan

Ongoing streams of work should be well planned, both individually and together, as a coordinated portfolio of activities. The CISO should build a roadmap for accomplishing these activities based on priorities established from performing the governance and risk analysis activities described in Chapter 1. The roadmap should be reflected in a document such as a security charter or security program plan. The roadmap reflects both short-term and long-term plans and should be updated on at least an annual basis.

Planning should reflect areas of emphasis based on the organization's business, stakeholder needs, or the results of security audits or assessments. For instance, if a vulnerability assessment indicates the organization has many unpatched systems, the organization may need to give its *patch management program* a higher priority in the short term. Plans should be updated frequently based on real needs of the organization.

Planning streams of work includes scoping the resources needed to accomplish the activities that comprise the security program. Resources may include the following:

- **Staffing** Discussed in greater detail later in this chapter in the section "Security Program Resource Management: Building the Security Team," staffing involves determining the right team to best accomplish the goals of the stream of work. Staffing planning also includes determining the organizational structure for the stream of work team and how the team structure fits within the structure of the information security department as a whole.
- **Supporting infrastructure and tools** Each stream of work has its own requirements for tools and IT infrastructure. Planning includes identifying which tools are needed and whether the organization should acquire each tool or build it in house (build versus buy). Tools also require maintenance. The needs and resources for maintaining the tools are part of the planning activity.
- **Financial resources** The money required for executing a stream of work may be expended over time. The stream of work activity may experience periods of greater spending, such as when equipment is purchased, staff is expanded, or a spike in activity occurs (for example, during an incident or compliance exercise). Budgets for spending are most often established on an annual basis.
- **"X as a Service"** Today, instead of using in-house resources or tools, many CISOs choose to outsource security functions using an "as a service" model. Such services can range from small segments of the security program such as antivirus to large segments such as complete security monitoring and intrusion detection of the enterprise. Virtually any aspect of the security program could be implemented using an as-a-service model.

The plans associated with a stream of work should include a clear definition of the objectives and goals. Without clear goals, the stream may not produce outcomes that benefit the organization. The plan should also address how the outcomes are measured and reported. Stream of work plan documents are stored in a document repository with *access controls* in place following need-to-know principles and *change control processes* in place to manage document baselines. The plans identify the assets to which the stream applies. The plans should also address the *security relationship*, including how the streams of work impact other departments, people within the organization, and external entities. The description of the security relationship should also identify the methods of communicating, coordinating, and collaborating with these stakeholders as well as the frequency of such communications.

Do

Based on the plans described in the previous section, the streams of work proceed with activities to meet the defined goals. All activities should follow the processes and procedures identified or defined in the plans. Each stream of work is staffed with a stream owner or stream manager, which may be the CISO or a designated manager or supervisor.

The security organization under the direction of the CISO should develop and refine an *operating* (or *operational*) *rhythm*, which refers to communications, usually reports and meetings, that occur on a regular basis but do not adversely impact the operational flow of the stream of work or other activity. Meetings are needed to enable team members to communicate and collaborate, resolve problems, report status, and discuss improvements. Reporting is needed to provide data and metrics to management and decision-makers. These communications must occur on a regular cadence and in a defined and repeatable manner. The security organizations that tend to perform the best are those that understand the value of an optimal operational rhythm and adjust their programs accordingly.

Stream activities should be accomplished with self-awareness. This means that everyone working on the stream should know not only what they are doing and how it fits with what everybody else is doing, but also how well the stream is performing against its goals. Streams that fail tend to be ones in which the only person that knows what is really going on is the boss. Successful streams are enabled when everyone has a stake in the outcome and knows how they can contribute to the stream's success.

The stream of work staff should document everything, including plans, procedures, guidelines, reports, and metrics. To create a living library of useful information, stream of work data should be stored in a document repository. These documents, while important to the organization, also contain information about the organization's security vulnerabilities and weaknesses. Therefore, access to stream of work documents and data should be available only to those people with a *need to know*.

Security Liaisons

To be successful, security activities, including streams of work, must be performed in close collaboration with the other groups and personnel in the organization. Therefore, the security team needs to build a *security relationship* with other organizations. Many security groups use *security liaisons*, members of the security team that conduct outreach to the rest of the organization. Security liaisons provide two-way communications, providing security *messaging, expertise, and advise* to spread the word about information security practices, including what the organization is doing to improve security, and act as the eyes and ears of the CISO to *listen to what employees think and feel about security policies, practices, and initiatives*. We all know that people are the weakest link in information security. Security liaisons can help to improve the security culture of the organization and, in turn, reduce security incidents.

Check

How does a CISO determine if the streams of work are working? They must be measured against criteria for success. Every stream of work should have a clear set of goals along with metrics to measure how well those goals are being met. Stream of work planning includes establishing how success is measured and reported. However, the PDCA check

phase involves more than just performance metrics against the primary goals of the activity. It also includes ways to assess all aspects of the activity. This may include measuring things like accuracy, usefulness, suitability, resiliency, or adaptability. The CISO should always be looking for ways to measure and understand how well each aspect of the security program is performing.

Some indicators of performance are measured daily, such as monitoring logs and detecting alerts. Other indicators are measured as part of assessments or audit actions. As explained in Chapter 2, security auditing is usually accomplished as part of a larger auditing program, but these audits can be used as a tool to assess stream of work performance. However, there may also be other measures outside of the auditing program. Many organizations use a security dashboard to show the status of stream activity, such as statistics on tickets from the security monitoring function or patched/unpatched systems from the patch management stream.

Assessments should be part of the operational rhythm, which, as previously described, is a cadence of communication reporting that includes measures of how well streams are performing.

Act

The purpose of the act phase is to maintain the quality of the security functions (streams) and to seek ways to improve them. This is accomplished by reviewing and analyzing the results and data from the check phase. The results are compared with the defined goals and objectives of each stream of work. Shortcomings and gaps are then scoped for remediation.

Some organizations formalize the remediation process using a Plan of Actions & Milestones (POA&M) or a Corrective Action Plan (CAP). These terms are from FISMA and the various guides and publications that support FISMA; however, they are also used generically to describe methods for capturing, tracking, and communicating security remediation activities. POA&Ms and CAPs are created on a system-by-system basis to track resolution of issues uncovered during security testing as part of the Risk Management Framework (RMF) process, but they can also be used to support resolution of deficiencies or needed improvements in security streams of work. The POA&M is a plan that describes the course of treatment to resolve deficiencies. It contains a CAP that describes exactly what will be done (or has been done) to resolve the deficiencies.

Part of the act phase of the PDCA cycle includes looking at the aggregation of results across the streams of work to uncover trends and determine root causes.

The activities performed during the act phase include tracking the actions undertaken to address gaps, resolve root causes, and implement improvements. If the tracking data is stored in a database, the organization will have a repository and living record of how well the streams are performing and improving over time.

Asset Security Management

Chapter 1 discussed security categorization and risk mitigation of assets. Chapter 4 describes the core competency of asset security along with other core competencies. The security management of assets is discussed in this section and illustrated in Figure 3-3.

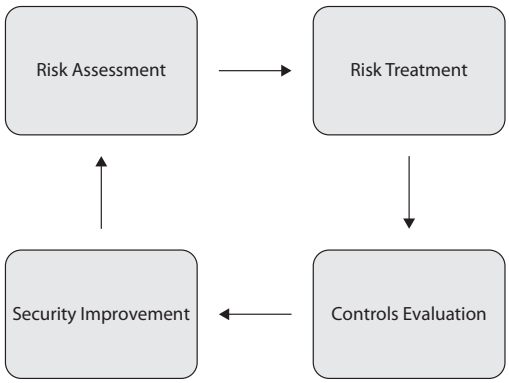


Figure 3-3 Security management of assets

Figure 3-3 is derived from ISO/IEC 27001 and shows the life cycle of how risk management is applied to a given asset. Each asset is assessed as part of the risk assessment and risk analysis process, which results in prioritization and categorization of the asset. Based on this, risk treatment is defined for the asset. The treatment is implemented, usually in the form of controls, and then evaluated. Any deficiencies or gaps uncovered during testing are then resolved. Security improvement results from monitoring the asset over time and undertaking subsequent risk analysis activities. This cycle continues for the life of the asset.

A critical aspect of an information security program is knowing what all the assets are, where they are, and what their security posture is. This situational awareness is a key function of security program management. Ideally, the security team maintains, or has access to, a single database containing this information. However, in practice, this information often is in disparate data repositories or the data is maintained by other groups such as the IT department.

Regardless of where the data is located, the security team should have access to or maintain data about each asset. Here is an example of the information that may be maintained for an asset:

- Asset name, make, model, serial number, and so on
- IP address and MAC address
- Asset type
- Name of asset owner and custodian
- Location
- Configuration information such as the security baseline, configuration settings, or standard build identification
- Licensing information and status
- Security categorization, classification, risk or impact level, or other information indicating the intended security characteristics of the asset

- Results of the most recent assessments, audit, or compliance reviews
- Current method of security monitoring of the asset
- Current operational status
- Current patch status or level
- Relationship to other systems or assets
- Security authorization status

Keeping control of the organization's assets and knowing they are properly secured is one of the biggest challenges for the CISO. Rogue devices can appear on the network either accidentally or intentionally. In addition, portable devices, including phones, tablets, and PCs, are part of the enterprise but are harder to keep track of. Many organizations use automated solutions to discover assets for the purpose of helping with asset situational awareness and to prevent unauthorized assets from connecting to the enterprise or causing disruptions.

Information assets, for the purpose of this discussion, are data. Data is quite literally the life blood of any organization and is most often the target of cyberattacks and the object of security incidents and subsequent recovery activities. Information assets, like the assets that support them (systems, hardware, and software), require management by the security team. Information asset management includes the following:

- **Information asset classification** The security team ensures that all data is classified in accordance with the organization's data classification policy and associated guidelines. Classification schemes vary based on the nature of the business environment, but every organization has at least two types (or classifications) of data:
  - Private data that requires some degree of protection
  - Public data that does not require protection
- **Data handling** The security program establishes policies, standards, and guidelines for how each classification of data should be handled while it is stored, processed, or transmitted. These rules define who, where, and how data is handled, including defining implementation methods such as encryption, access controls, labeling, and physical media.
- **Data inventory** Like supporting assets (hardware and software), information assets are tracked using inventories and associated processes to maintain an understanding of where the organization's information assets are, how they are protected, and the organization's compliance with the policies and rules that apply to the asset.

Security Projects

Security projects are activities within the security program that have a beginning and an end. Whereas streams of work are continuous, security projects have an end in mind, and when the end is achieved, the project is over. The list of active security projects for an organization is ever changing. Each year new security projects are needed as older

ones are completed. Example projects that may be part of a security program include the following:

- Acquiring and implementing a vulnerability scanning tool
- Performing a network security architecture review
- Developing a security tool
- Deploying an incident response capability
- Designing physical security controls for a datacenter
- Performing a risk assessment of a service provider
- Developing software development security standards
- Aligning security practices with an industry framework (for example, ISO/IEC 27001, NIST SP 800-53, and so on)

All of these examples result in some kind of project being created that must be properly managed to ensure success. Projects, like streams of work, require disciplined management to be successful. But the project management process differs somewhat from streams of work because projects have a defined end state and all the activities are geared toward achieving that end state. The process for project management is discussed in detail later in this chapter in "Project Management."

Security Program Budgets, Finance, and Cost Control

The extent to which the CISO is responsible for the security budget and spending varies by organization and usually aligns with the top-level organizational chart that shows who reports to whom. If the CISO reports to the CIO, the security budget is most likely part of the IT budget and the budgeting and spending process is managed through that chain. In situations where the CISO reports directly to the CEO, the CISO is usually afforded more autonomy in budgeting and spending.

When Security Functions Are Shared

In some organizations the CISO does not have responsibility for some parts of the information security budget. For instance, many security breaches are caused by unpatched systems, but in some organizations, *patch management* is not the responsibility of the CISO, instead falling within the purview of the IT group or maybe an IT service management group. Another example is *security awareness*. The CISO may be responsible for security awareness training, but the training budget may be administered by the human resources department. In situations where various security-related functions are not under the budget authority of the CISO, the CISO may be asked to provide input to the budget process for the responsible group. Such collaboration in the budget process is common.

Establishing the Budget

As discussed in the Chapter 1 section "Sizing," covering the sizing of the information security organization, some executives and CISOs like to compare their organization's security spending to the spending of similar organizations. While looking at comparative organizations can be a good data point, it should not be the primary method of determining an information security budget. The security budget should be that which is required to provide the right level of protection for the organization.

Unless the organization is a startup, in almost every case the information security budget is based on the organization's historical spending, as in, "What did we spend last year?" In fact, that isn't a bad place to start the budget process. Budgeting is all about predicting the future, and the more data the CISO has about the past, the better informed the CISO will be about what might happen down the road. This approach can be helpful especially after many years of operation, as prior learning and experience can inform the CISO as to what is working and what isn't. However, the security program is always changing, evolving, and facing new threats. As a result, there will always be changes to spending year to year. In general, what works best is a bottom-up approach built by first estimating the smallest pieces of the work, then integrating the pieces into a larger plan. The lowest-level elements should be estimated using a risk-based approach that is informed by prior experience.

Here is a list of some of the methods and factors that go into establishing the information security budget:

- **Start with a baseline** Use the prior year's data as a starting point. The CISO should consider not just the past year's spending but also the past year's budget. How did the prior year's budget compare with what actually was spent, and what can be learned from that information?
- **Build a work breakdown structure (WBS)** A WBS is a method of estimating the work required on a large effort by breaking down the work into smaller units that are easier to estimate and control. Using a WBS (which is explained in more detail in the "Project Management" section later in this chapter), the CISO can perform a bottom-up estimate of what each activity costs. The WBS aligns with the streams of work and all other activities of the security group and should align with the way the organization collects and reports costs. It wouldn't make sense to build a budget using one method but report spending using another. If the budget aligns with the way costs are reported, the CISO will be better able to manage spending and improve the budgeting process each year.
- **Look at risk assessment results** If the spending for firewall administration was X but testing indicates the firewalls are frequently misconfigured, maybe the future spending for firewall administration should be more than X. Or, as discussed in Chapter 1, if the annualized loss expectancy (ALE) of a system is $10,000, the organization likely shouldn't be spending $100,000 per year to protect it. The results of risk assessment and analysis activities can and should inform the budget process.

- **Estimate costs of addressing gaps** The CISO uses the results of assessments and audits to determine where spending should occur. Areas of noncompliance usually require spending to address them. In fact, the POA&M or CAP process should include estimating costs of the recommended actions, which in turn should be worked into the budget.
- **Address life cycle costs** Many items of hardware and software have a defined life. Modern systems and technologies can become end of life (aka end of support), become obsolete, or require upgrades. The costs of technology refresh and maintenance agreements are included in the budget.
- **Conduct value engineering** A good CISO is always considering if there is a less costly way to do something. Where efficiencies can be gained there may be a cost savings as well.
- **Determine what's new** The CISO should estimate the costs of addressing new initiatives, making improvements, incorporating new technologies, or addressing new regulations. Organizations change as well. They buy or merge with other companies, introduce new products and services, enter new markets, and so forth. All the changes each year are considered and reflected in the budget if necessary.
- **Consider what could possibly go wrong** Bad things can and will happen. The CISO should establish budgets for unexpected items such as significant security incidents, pandemics, disasters, labor strikes, or things that may pop up that can't be specifically predicted. The CISO should consider the cost and viability of purchasing security breach insurance for the organization.
- **Establish management reserves** Few organizations allow the CISO to create a budget for undefined spending, but the CISO should allow some *wiggle room* in the budget (which is sometimes referred to as a *management reserve*). It is simply an extra amount added to the estimate "just in case." Sometimes, this is done by including in budget items extra amounts that can be tapped into if needed. The best CISOs are careful not to misrepresent costs, but they don't want to leave themselves short either.
- **Do a rolling forecast** Information security program budgets are typically established annually, but many organizations create a forecast that extends beyond the next year. The CISO needs to look ahead and plan beyond the next year. It is common to create a three-year forecast that is updated on an annual basis along with the annual budget.
- **Determine what's in the budget** The budget includes all the items that the CISO is responsible for. This includes hardware, software, employees, consultants, outsourced services, vendors, managed services, and any other items within the scope of the security program for which the CISO has been designated responsibility.
- **Establish not just what to spend but when** The CISO should establish how much can be spent on each WBS element and when that spending will occur. This is usually estimated by allocating costs on a monthly basis. The finance and accounting department needs to know this information to estimate accruals and cashflow.

But the CISO needs to know this information to plan when activities will occur and track and approve spending. If a budgeted line item assumes costs that will be spread over the entire year, the budget should reflect the spending timeline. Allocating the budget by month allows the CISO to manage spending in accordance with a plan.

Capital Investment vs. Expenses

During a discussion with one CISO about *managed services*, he told us that he does not use such services, but the reason was not an obvious one. His decision was based on the financial preferences of his company. For accounting reasons, his company favors capital expenses (CAPEX) over operating expenses (OPEX), so he is encouraged to spend on infrastructure rather than pay for services. Therefore, he invests in building security capabilities in-house (considered CAPEX) instead of outsourcing the services (considered OPEX).

After estimating the budget, the CISO has to sell it to the next people up the approval chain. This process varies considerably from organization to organization, but in all cases the CISO must be able to justify the estimate. The budget should be supplemented with solid data. More importantly, the CISO must be able to speak the language of those up the chain and address their sensitivities and way of doing things. What type of data is more likely to hold water with the CEO? How has the organization *done it before*? Has the CISO thought of everything? Can *it* be done for less? The authors have seen budgets created with a great deal of effort and precision only to have them rejected or cut because the CISO couldn't convince management that all the expenditures were necessary.

CISOs use a variety of tactics to justify their budget requests. As previously mentioned, one useful tactic is to include comparisons to budgets of other organizations in the industry. Although the CISO would be ill advised to put too much emphasis on industry comparisons to *create* the budget, such comparisons can sometimes be helpful in *justifying* the budget to others. CEOs love to hear that the organization is spending less on something than the competition is spending. If industry comparisons show that is the case, the CISO can use that information to his or her advantage. Industry sources such as Gartner and Forrester and vendors such as RSA, Verizon, and IBM can be good sources of security spending data.

The two most common approaches to justifying the information security budget are to frame the discussion around risk and/or regulatory compliance:

- **Risk** The CISO has likely performed risk analysis to understand the organization's assets and their value to the business and has used this information to establish priorities and determine where and how much to spend on protecting those assets. This same information can be used to justify the spending. If the CEO or budget approver understands the relationship between the risk, impact to the business, and the cost of mitigating that risk, they are more likely to support the spending.

- **Compliance** Regulations are a common forceful driver to security spending. If the regulation says information must be protected and specifies fines for noncompliance, then the risk of those fines can justify spending.

Managing and Monitoring Spending

Once the budget is approved, it can be used as the benchmark for monitoring and controlling costs. The individual items that make up the budget, as defined in a WBS or other method, can be used to establish how costs are accounted for and tracked. For instance, if the WBS includes an element of cost for operating the security operations center (SOC), the accounting department can establish a cost account and charge numbers to be able to approve and record spending associated with the SOC. This alignment between the budget and actual spending allows the security finances to be controlled and monitored by comparing *budget versus actuals*. Comparing the actual spending to the budget on a periodic basis is key to managing security finances.

Cost accounts should be established for all items, or groups of items, in the budget. This requires close collaboration between the CISO and the finance or accounting team. Establishing the cost accounts includes defining who can approve spending and at what thresholds. Responsibility for cost accounts may lie with the CISO, or the CISO may delegate other managers to approve spending. In practice this is implemented by defining who can approve timesheets, create or approve purchase orders, or commit to contracts.

Actual spending for labor or expenses is reported to the CISO by the accounting team for each cost account. If the cost accounts align with the budget line items, as they should, the CISO can compare the planned spending as defined in the budget with the actual spending that is occurring. This shows spending underruns or overruns and allows the CISO to adjust future spending accordingly.

Security Program Resource Management: Building the Security Team

The security team is the most important resource the CISO has available to secure and protect the organization's information assets. The CISO "drives the bus" and is responsible for getting the *right* people on the bus—the *right* people are not necessarily the people with the best technical skills but rather the people that can best carry out the vision of the CISO. Therefore, the right people for the team may be those with the best mix of technical, communication, and interpersonal skills, coupled with personality traits like integrity, honesty, and humility.

Here are some of the factors that go into creating and maintaining a great security team:

- **Define the staffing strategy** Staffing the security team starts with defining a staffing strategy. The CISO should define what kind of team he or she wants and then define the path to achieving that team. Ideally, the CISO defines the goals for the team's culture, abilities, approach, methods of working, recruiting,

and retention. This provides guidance for how the team is staffed. For instance, if the CISO wants a team that is highly collaborative but hires people who are introverted and communicate poorly, achieving the collaborative team that the CISO is seeking may not be possible. Likewise, if the CISO decides that technical security knowledge is paramount, then that should be part of the staffing strategy so that the CISO obtains the strong technical staff that he or she desires.

- **Conduct a job analysis** A job analysis is a process to collect all available information about the type of work and job functions required, which enables the CISO to identify all job roles required for the team and create job descriptions for those roles. Information to be collected includes duties, responsibilities, outcomes, technologies, processes, regulatory drivers, standards, and related data. The more information collected, the easier the CISO's task is to define the roles.
- **Define job roles and create job descriptions** Job roles and descriptions are used to help recruit staff and to set clear expectations for employees. Using data collected from the job analysis, the CISO can create functional job descriptions that define each role on the team. In some organizations this activity is the responsibility of HR, and in some cases the CISO does not have the authority to define job roles and instead must use the job roles defined or enforced by HR. This may limit the CISO's ability to create and use job roles and job descriptions as a tool to hire and build the staff. Or this situation may be an opportunity for the CISO to collaborate with HR to define the team. The goal is to have a set of job descriptions that can be used as a tool to build the staff and communicate expectations to employees.
- **Use the NICE Workforce Framework** The US National Institute of Standards and Technology (NIST) has created a framework for cybersecurity job roles in which job descriptions and training requirements are available in a library for any employers to use. It is called the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181). CISOs can take advantage of these predefined *work roles* to create the organization's security job descriptions. This not only saves the CISO time but provides an additional advantage of enabling the use of work roles that have been vetted by industry and updated over time.
- **Define career paths** One tool used by many companies to attract, support, and retain employees is to define and use *career paths*. Career paths are defined sequences of job roles, training, and performance criteria that employees can follow to grow their careers while staying within the organization. In today's highly competitive recruiting landscape, employers look for ways to attract and retain employees. One thing employees want is an understanding of how they can advance their careers at a given company. Defining and documenting career paths that the organization and employees can follow helps keep employees satisfied and helps the organization to retain talent and enable employees to expand their skills and get better at their jobs.

- **Training** Like many areas in business, the security landscape is ever changing and evolving. People need training almost continuously to keep their knowledge and skills current. It is essential that the CISO has a training plan and associated budget to keep the security team properly educated. Some CISOs establish relationships with training organizations or colleges and universities to provide unique learning opportunities for their employees. We know a CISO who brings in experts throughout the year, every year, to teach security certification classes so that the entire security staff is better able to obtain important industry certifications. CISOs know that they need to invest wisely in training to enable their staff to meet the goals of the security program.
- **Handling personnel and teamwork issues** All CISOs should have a plan for handling personnel issues without disrupting operations. However, most CISOs address this by trying to prevent issues in the first place. One way to accomplish this, as mentioned earlier, is to include character and communication as part of the hiring criteria. Having the right people will go a long way in preventing issues involving relationships and teamwork. Other methods to prevent these types of issues include creating a portal to help teammates collaborate, having clearly defined roles and responsibilities, and holding regular interworking sessions to foster and facilitate better communication. If problems do occur, there should be documented procedures for bringing issues to the attention of HR, the CISO, or both and rules with disciplinary actions for causing problems that impact any aspect of the security program performance.

Is Finding Good IT Security People Really That Hard?

It is widely reported in the media and by industry groups that there is a huge shortage of people to staff IT security positions. We recently asked a CISO how he is dealing with this shortage of available talent. His reply: "What shortage?" This CISO of a multibillion-dollar company has a very large staff that has doubled in size over the past two years. He hasn't had any problem growing his staff. Why? He gets his people from within his company. Historically, most IT people did not want to do security work. But not anymore. His company's IT people are begging to work for him. His firm encourages people to move around within the company, and management encourages him to staff from within. The CISO has created a great culture within his group, resulting in people from the IT department seeking him out for roles on the security team. He chooses people based on personality rather than experience, because he knows he can provide training to give them the needed security knowledge and skills. As he put it, "You can train skills, but you can't train character."

Project Management

Project management is the lowest level in the management hierarchy (portfolio, program, and project). The goal of project management is to ensure that every project achieves the desired outcome on time and within budget. Project management includes identifying and controlling resources, measuring progress, and adjusting the plan as needed as progress is made. The CISO may directly serve as the project manager for some or all security projects, or the CISO may delegate others to serves as project managers. In either case, the CISO should be familiar with project management principles and techniques.

It is important to apply good project management practices to projects of all sizes. Some organizations focus project management efforts on large projects and tend to neglect small projects. These small projects can end up costing the organization significant time and resources if they are not properly managed. Project management may not be formalized for all projects. The extent of formalization may be governed by project size or importance; however, good project management principles should be applied to all projects. This includes, at a minimum, identifying the scope, developing criteria for measuring success, monitoring and controlling resources, and documenting these items in a plan. This section discusses some of the fundamental tenants of project management and provides a walkthrough of the project management process.

Project Management Fundamentals

Similar to the CIA triad (confidentiality, integrity, and availability) of information security, project management also has a triad, composed of the following elements:

- **Scope** Boundary of work to be performed
- **Schedule** Timeline to perform the work
- **Budget** Cost and resources required to perform the work

If one of these components changes, the other two components usually are affected. For example, changes to the scope of a project will likely affect the project budget and schedule. The manner in which these elements are applied determines the quality of the project. This interdependency is illustrated in Figure 3-4.

Ultimately, project management as a practice is focused on managing and controlling these three fundamental components to achieve the goals of the project. There is always a trade-off in project management. Decisions around cost, schedule, and scope affect the quality of the project deliverables. Successful projects are completed on time (schedule), within cost expectations (budget), and achieve the technical and business objectives (scope).

EXAM TIP CCISO candidates should be familiar with the fundamental project management terms scope, schedule, and budget and understand how these components affect the project.

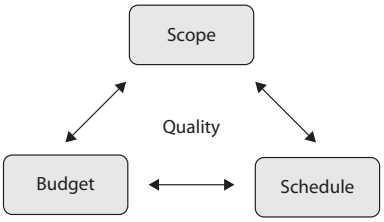


Figure 3-4 Project management fundamentals

Project Management Considerations

There is an old saying in project management and software/system development: "Good, fast, or cheap—pick two." This is a simplistic representation of the situation, but it is an important concept to illustrate. The idea is that while the goal is always to strike a balance between the three principles, sometimes two have to outweigh the other. On every project, some key decisions must be made about what principle is most important. Is the goal an end product that is of high quality (good), inexpensive to develop (cheap), or delivered quickly (fast)? There is always a trade-off to be made, as illustrated in Figure 3-5 and described here:

- Good + cheap = slow to deliver
- Cheap + fast = poor quality
- Fast + good = expensive
- Fast + good + cheap = sweet spot

The ultimate goal is usually to harmonize the three principles. It may not be possible, but it should be the goal.

Project Management Training and Certifications

There are several project management certification bodies; two well-known ones are the Project Management Institute and AXELOS. These organizations provide a range of benefits to the community, including publications, forums, conferences, networking opportunities, and best practice resources, and offer certifications and training for continuous learning.

NOTE This section does not present a comprehensive survey of project management training organizations. The organizations introduced here are simply a few of the prevalent ones in the industry, used to illustrate the range of project management training and certifications available.

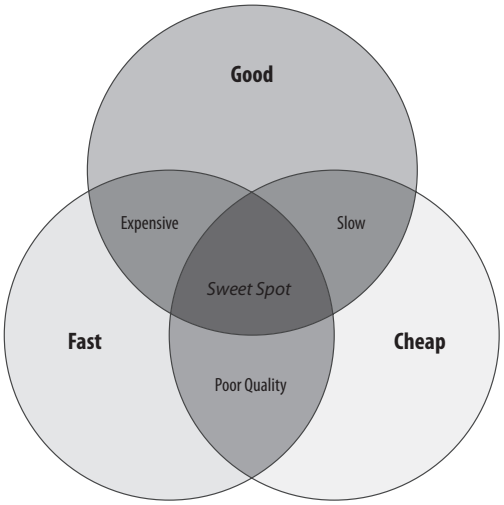


Figure 3-5
Good, fast, or cheap—pick two

Project Management Institute

The *Project Management Institute (PMI)* is a global nonprofit organization focused on project management certification and education. PMI develops standards, conducts research, produces publications, hosts conferences, and facilitates networking and collaboration for project management professionals. PMI's flagship certification is the Project Management Professional (PMP), but it also provides training and certification for the following:

- Program Management Professional (PgMP)
- Portfolio Management Professional (PfMP)
- Certified Associate in Project Management (CAPM)
- PMI Professional in Business Analysis (PMI-PBA)
- PMI Agile Certified Practitioner (PMI-ACP)
- PMI Risk Management Professional (PMI-RMP)
- PMI Scheduling Professional (PMI-SP)

AXELOS

AXELOS is a global best practice organization that provides certification and training in a variety of subject areas, including project management, IT service management, and cybersecurity. The AXELOS certification tracks include the following:

- IT Service Management (ITIL)
- Cyber Resilience (RESILIA)

- PRojects IN Controlled Environments (PRINCE2)
- PRINCE2 Agile
- AgileSHIFT
- Managing Successful Programmes (MSP)
- Management of Risk (M_o_R)
- Portfolio, Programme and Project Offices (P3O)
- Portfolio Management (MoP)
- Management of Value (MoV)

Phases of Project Management

Good project management allows a project to move in the right direction by allocating appropriate resources, providing leadership, and planning for events that may cause the project to drift astray. Projects are made up of one or more phases which collectively represent the activities and tasks involved in a project. Project management should be put in place to ensure that each phase of the project is followed. This is accomplished by choosing and following a project management model. There are many project management models from which to choose. The model outlined in this book is based on the PMI Project Management Body of Knowledge (PMBOK) process groups, outlined in Figure 3-6, which include the following:

- **Initiating** Identify the business need and define the project.
- **Planning** Develop a plan to ensure the project meets the scope, time, and cost goals.
- **Executing** Coordinate resources to execute the project plans.
- **Monitoring and Controlling** Measure project performance, monitor deviations, and take corrective actions.
- **Closing** Formal acceptance and organized closing of the project.

While these phases are discussed sequentially, in practice they may be implemented sequentially, iteratively, or concurrently. In the model depicted in Figure 3-6, the monitoring and controlling process occurs throughout the project. In practice, the monitoring and controlling process occurs during the executing phase and to some degree

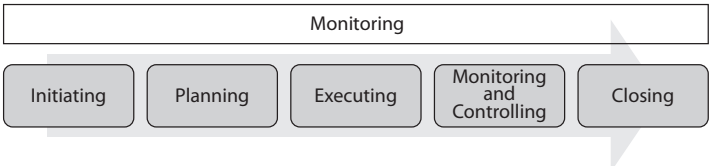


Figure 3-6 Phases of project management

in the initiating, planning, and closing phases. In addition, the initiating and planning phases may happen simultaneously in some organizations. The project management process groups can be tailored and customized to fit the organization's needs. In this section we examine project management by breaking down each of these processes and discussing the components of each.

NOTE Although the project management model discussed in this section is based on the PMI PMBOK process groups, this section is not intended to align completely with the way PMBOK approaches project management. This section is written based on the authors' experience observing how project management is applied in practice.

Initiating

Before a project can begin, up-front work must be completed in the initiating phase. First, a business need or problem must be identified, and a potential solution discussed. Depending on the feasibility of the solution, this may warrant the creation of a project. The key initiatives that take place in the initiating phase include the following:

- Collect requirements
- Define the project scope
- Identify and interview stakeholders
- Define assumptions and constraints
- Establish the general project budget and timeline
- Develop the project scope document

Collect Requirements

Every project must have a set of *requirements*, a collection of capabilities or items that are required in the final deliverable to meet the project objectives. The requirements provide the foundation for defining the project scope. The work required in collecting the requirements can vary. In some cases, the requirements are provided by the customer or defined prior to the beginning of the project. Other times the requirements are developed as part of the project. The requirements that are provided may vary in detail, and additional information gathering sessions may be required to create clear and complete requirements.

Define the Project Scope

As part of project initiating, it is important to put some kind of boundary on the work to be done. The *scope* of a project defines the boundary of the project. It is the work that is required to fulfill the customer requirements. The scope should outline what is and is not included in the project. The scope includes the project goals, requirements, stakeholders, schedule, and budget. A well-defined, documented, and monitored scope is an

important factor in a project's success. A poorly defined project scope can result in one or more of the following:

- **Scope creep** Uncontrolled growth in a project's scope due to the addition of requirements, desires, or targets
- **Cost overrun** Unexpected costs incurred during the course of a project that are in excess of budgeted amounts
- **Schedule overrun** Unexpected schedule delays incurred during the course of a project

Scope is defined in a *project scope document* or *scope statement*, which describes project deliverables and outcomes.

Identify and Interview Stakeholders

As part of project initiating, stakeholders should be identified and interviewed and their needs should be assessed. *Stakeholders* are people with a *vested interest or stake* in the project. This includes both internal and external stakeholders.

- **Internal stakeholders** Individuals within the organization such as team members, business area managers, senior executives, and so on
- **External stakeholders** Individuals external to the organization such as customers, vendors, users, contractors, suppliers, or investors

The stakeholders are identified and their details documented, including, at a minimum, their names, roles, contact information, and areas of interest. For example, some stakeholders may be performing the work, others may be affected by the work, and others may be the recipients, such as a customer, business owner, or investor. Stakeholder identification is typically accomplished through interviews, lessons learned, brainstorming sessions, or utilizing checklists. Stakeholders are sometimes classified based on their influence, interest, and power. Stakeholders with a high degree of influence and interest who can directly affect project output are sometimes referred to as *key stakeholders*.

The stakeholders are interviewed and assessed to determine their needs, expectations, and definition of success for the project. This information is documented to ensure their requirements are clearly understood.

Define Assumptions and Constraints

In the initiating phase, the possible assumptions and known constraints should be captured and documented. These form the basis for project planning.

- **Assumptions** Beliefs or expectations in planning based on knowledge or experience that may not be certain, true, or real (for example, assume that resource *X* will be available for the duration of the project).

- **Constraints** Limitations or restrictions to the project's schedule, resources, quality, budget, scope, or risk that may impact the project during executing (for example, resource *X* can be tested only during the weekends). Constraints can be business oriented or technically oriented.

Assumptions and constraints are documented at a high level during the initiating phase and should be tracked during the project life cycle. Assumptions are beliefs that may turn out to be false, and constraints are restrictions or barriers to project execution. Both can add to project risk and effect project requirements, which is why it is critical to document, analyze, and monitor them throughout the project.

Establish the General Project Budget and Timeline

The initiating phase includes discussing and estimating the initial budget for the project. The budget may not be very detailed in the initiating phase; however, it is important to have an estimate of what the general budget for the project will be. The project timeline also needs to be discussed and estimated to predict when the results generally need to be delivered.

Develop the Project Scope Document

All the components described in the initiating phase should be captured and the information integrated into a project scope document. The *project scope document* captures all scope data and high-level decisions regarding the project and typically contains the following, at a minimum:

- Scope definitions
- Stakeholder inputs
- Assumptions and constraints
- Budget and time frame
- Initial schedule and resources

The project scope document may also be referred to as the *scope statement*. The purpose of the project scope document is to document the boundary of the project. This is used to ensure that there are not deviations in the project that lead to scope creep and that there are well-defined project objectives so that success is tangible.

Planning

The planning phase encompasses the following components:

- Determine the SDLC methodology
- Develop measurable goals
- Develop the work breakdown structure
- Develop the project schedule

- Assign project resources and budget
- Assess project risk
- Document the project plan

Determine the SDLC Methodology

An important step in the planning phase is to decide which methodology and techniques to use to manage the project. This decision may be governed by the organization's project management standards and preferred methodologies or it may be left up to the discretion of the project manager. This determination includes consideration of whether to follow a systems development life cycle.

As previously introduced, the project management model outlined in this chapter includes initiating, planning (the topic of this section), executing, monitoring and controlling, and closing processes. Within this model, if the project involves developing or managing a system, product, or service, the project manager may choose to incorporate a *systems development life cycle (SDLC)* to establish a methodology to follow during (typically) the planning and executing phases. The systems development lifecycles discussed in this section include the *waterfall* methodology, *incremental*, and *agile*.

NOTE Not all projects use an SDLC within the project processes. For example, if a CISO is managing a project to map the company's security controls to NIST SP 800-53, the CISO may follow the project processes (initiating, planning, executing, monitoring and controlling, and closing) but most likely would not use an SDLC, because no system, product, or service is being developed. However, if the project includes developing and implementing new controls, such as security tools, systems, or applications, the CISO might choose to incorporate an SDLC within the project processes.

Traditional/Phased/Waterfall The phased life cycle is characterized by linear-sequential distinct steps, each of which must be completed before the subsequent step is started. This method is also commonly referred to as the *traditional* or *waterfall* approach. In this model, the project scope, schedule, and budget are determined in the beginning (planning phase) of the project. The scope is fixed going into the project, and changes to schedule and budget are carefully managed throughout. The key factor is that all the activities for each phase must be performed, documented, and completed before beginning the subsequent phase. This concept is illustrated in Figure 3-7. This model places a heavy emphasis on up-front planning and administration.

This model is useful for projects with controlled, predictive development and requirements that are clear and well documented in advance. The downside of this method is that it is an inflexible process, as it assumes the requirements can be defined in the beginning and will not change during the project. This may be beneficial for some projects, but it is detrimental for projects that have many variables that affect the project scope or projects for which the requirements are uncertain or incomplete. This method can result in the accrual of significant cost increases if changes are required later in the project.

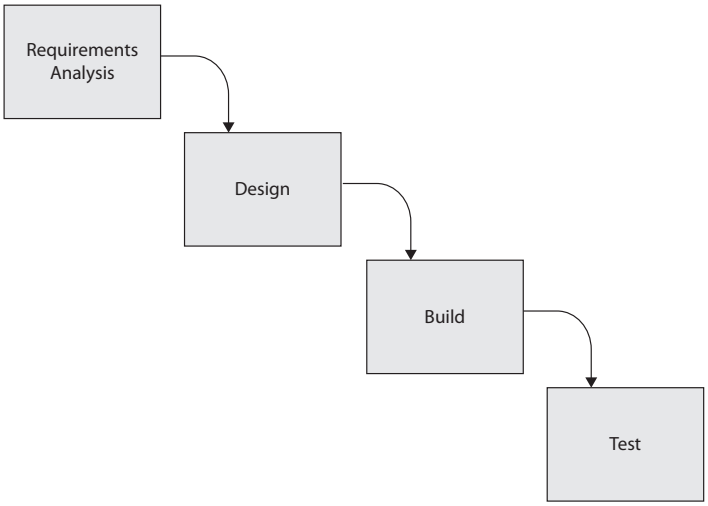


Figure 3-7 Waterfall life cycle methodology

Incremental In an *incremental* life cycle model, multiple development life cycles are carried out. Each of the life cycles has a predetermined timeframe and produces a complete increment of a capability. Each capability is then integrated with that of the previous phase to produce the whole product. This concept is illustrated in Figure 3-8.

Agile *Agile* is an overarching term for several development methodologies that utilize iterative and incremental development processes and encourage team-based collaboration. Instead of detailed requirements up front followed by rigid development,

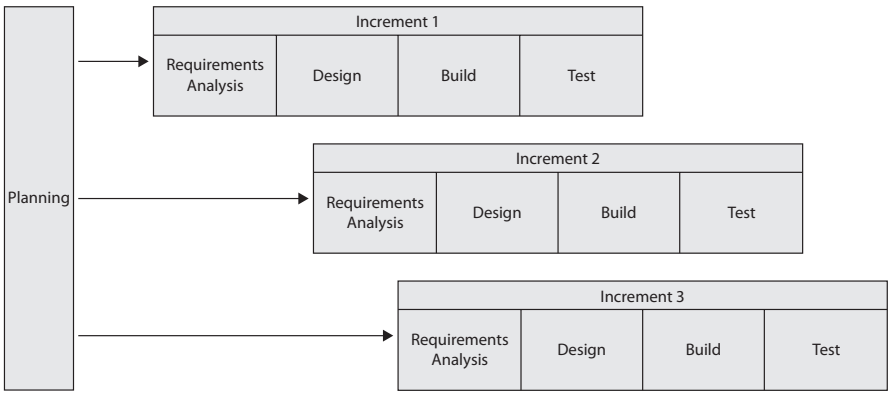


Figure 3-8 Incremental build model

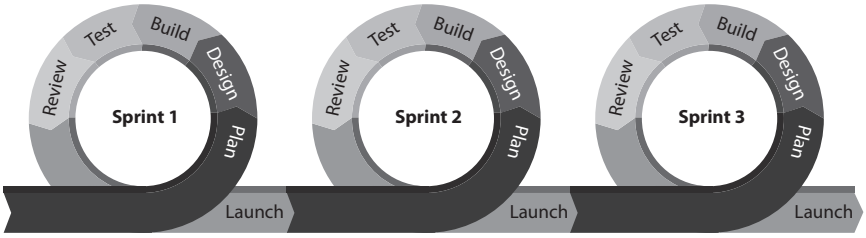


Figure 3-9 Agile methodology

the agile methodology incorporates iterative models along the way to enable speed and flexibility. In the agile methodology, the product development work is broken out into scheduled iterations known as *sprints*. This process is illustrated in Figure 3-9. The length of each sprint varies, but sprints tend to be two to four weeks long. The scope is defined before the start of an iteration.

EXAM TIP CCISO candidates should be familiar with the various development life cycle methodologies.

Develop Measurable Goals

A critical part of the planning phase is the development of measurable goals. These are used to develop metrics used in the monitoring and controlling phase throughout the project to measure success, identify deviations that require corrective action, and determine when the project is complete. A project can't be deemed a success if no one knows what success looks like. One of the methodologies for setting and measuring goals is S.M.A.R.T., introduced in Chapter 2.

Develop the Work Breakdown Structure

One of the first activities of project planning is breaking down the larger project into smaller, more manageable, bite-size chunks or efforts. These are defined as part of the previously introduced *work breakdown structure (WBS)*, which is a hierarchical decomposition of the work to be performed by the project team to accomplish and deliver against the project goals. The WBS is a project management tool used to break down the project into organized individual work elements (tasks, subtasks, and deliverables). Figure 3-10 illustrates a representation of a graphical WBS; however, a WBS can be something as simple as a task list.

The idea is that every element or task in the WBS is broken down and assigned its own budget, resources, scope, and schedule. This is one way to organize everything. The trick to creating a good WBS is including the right level of detail. If the WBS has too much detail, the project manager will have great control and a well-thought-out plan but

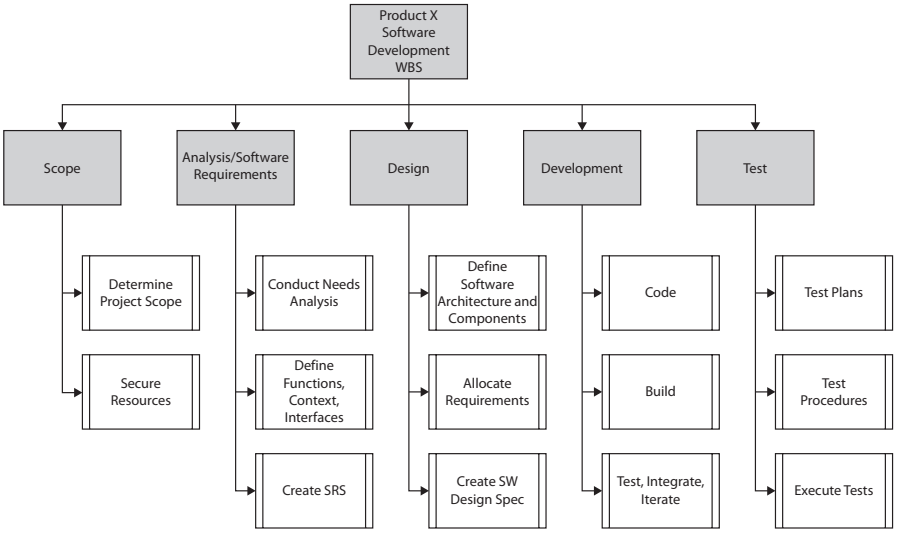


Figure 3-10 Work breakdown structure example

may get bogged down in management overhead and overload. If the WBS isn't detailed enough, the project manager will have less control and a fuzzier plan, which can lead to scope creep, budget overruns, and schedule delays.

Work breakdown structures can be *function oriented* or *task oriented*. For example, a function-oriented WBS would define tasks based on each of the project phases, such as:

- Analyze, Design, Build, Test
- Plan, Do, Check, Act
- Initiate, Plan, Execute, Monitor, Close

A task-oriented WBS would be organized by task, configuration items, or items that need to be built, such as:

- Select Scanning Tool, Implement Tool, Perform Scans, Adjust Profiles and Policies
- Asset Inventory, Hardware, Software, Network, Data
- User Interface, Communication Stack, Database, Middleware

Both function-oriented and task-oriented WBSs can be useful. The decision of which type to use ultimately comes down to the style or preference of the project manager and what makes sense for the project and the organization.

Develop the Project Schedule

Once the WBS has been developed, budgets and schedules are assigned to each element in the WBS. In developing the project schedule, it is important to factor in the following:

- **Resources and duration** What resources are involved in each particular element? What duration is expected?
- **Dependencies** What are the dependencies? What does each particular item/element require?

When going through this part of the planning phase, the project manager begins to see more clearly which activities are on the critical path. The *critical path* is the series of events or activities that, if changed, would change the overall end date of the project. If any one of the activities in the critical path is delayed, the end date of the overall project delivery is impacted. A project manager must always keep an eye on the items on the critical path.

One method for documenting and visualizing project dependencies is to use a *Gantt chart*, a type of chart that illustrates the project schedule and shows the dependencies of tasks. It provides a great way to visualize all the outputs of tasks that must be fed as input into other tasks. It shows which tasks must be completed for other tasks to commence. This helps the project manager to identify project dependencies and conceptualize and visualize items on the critical path. Microsoft Project is a popular project planning tool that uses Gantt charts to help plan and show project schedules. Figure 3-11 illustrates a high-level example of a Gantt chart in Microsoft Project.

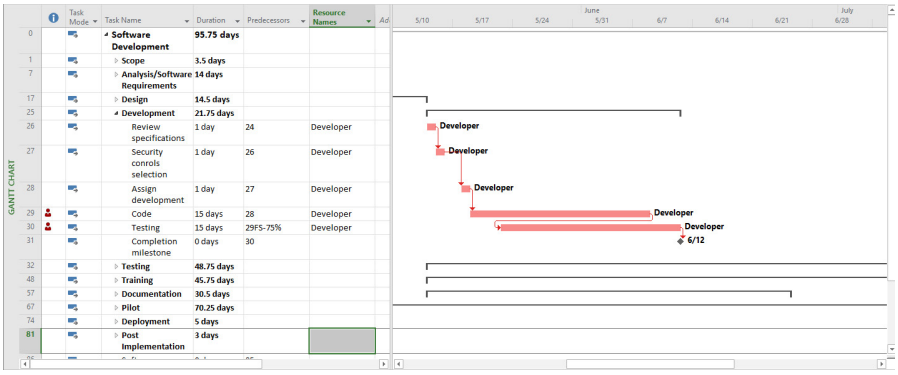


Figure 3-11 Gantt chart example (with critical path) in Microsoft Project

Assign Project Resources and Budget

Once the WBS and project schedule have been created, the resources and budget for each project element are assigned. This part of the planning phase is typically where decisions are made regarding whether to use in-house resources or external resources and whether to build, buy, or rent. The following are some of the considerations:

- **Internal resources**
  - Select and assign resources to each WBS element
  - Tailor the WBS to the resources that are available
  - May require new hires or new training of staff
  - May require acquisition of hardware and software
- **External resources**
  - Conduct competitive selection process if time/resources allow
  - Establish contracts and statements of work (SOWs)
  - Define deliverables, milestones, and obligations
  - Establish service-level agreements (SLAs)

Responsibility Matrix

A *responsibility matrix* can be used to demarcate responsibilities for each activity or task involved in meeting project deliverables. The responsibility matrix is often known as a *RACI chart*, with the acronym representing the following:

- **Responsible** Individuals responsible for completing specific project tasks or activities
- **Accountable** Typically implies management of an activity or task
- **Consulted** Individuals whose opinions are consulted regarding specific activities or tasks, typically subject matter experts (SMEs)
- **Informed** Individuals informed on progression of specific tasks or activities

Figure 3-12 shows an example of a high-level RACI chart.

Assess Project Risk

Every project has some degree of risk. In the context of project management, the risks are project risks rather than information security risks. *Project risks* are things that may occur during the project that may adversely impact the project's success. Project risks should be considered during the planning phase and managed throughout the project. An initial *project risk assessment* should be performed to understand and predict potential

Deliverable or Task	Roles			
	Project Sponsor	CISO	Project Manager	Project Team
Phase 1				
Deliverable/Task 1	CI	A	R	
Deliverable/Task 2	I	A	R	R
Phase 2				
Deliverable/Task 1	A	R	R	I
Deliverable/Task 2	I		RA	

Figure 3-12 RACI chart representation

project risks. The perceived project risks should be identified, analyzed, and ranked in a risk ranking. There are three general types of risk to consider:

- **Technical** Risk of not meeting requirements for technical reasons
- **Schedule** Risk of missing project deadlines due to internal or external factors, such as a vendor not delivering on time
- **Budget** Risk of cost overruns due to poor budget estimation or scope creep

The initial project risk assessment is followed by a determination of which actions should be taken to reduce or mitigate the risks to the project.

Document the Project Plan

The last step in the planning phase is to document the project plan. The project plan serves as a roadmap of activities to be distributed to and followed by the project team and communicated to the stakeholders. The project plan should address, at a minimum, the following components:

- Scope management plan
- Schedule management plan

- Resource management plan
- Cost management plan
- Quality management plan
- Change management plan
- Configuration management plan
- Communication plan
- Risk management plan
- System security plan

Organizations may use something as simple as a Word document or Excel spreadsheet for the project plan, or may implement a more elaborate project planning tool such as an application with a back-end database that provides a web portal to manage tasks and store documents. The choice depends on the needs and sophistication level of the organization and the complexity of the project. The plan can be documented and managed in many ways. The key is that it should be documented.

Depending on the organization and its project management practices, the project plan developed in the planning phase and the project scope document developed in the initiating phase may be the same document. In any case, some type of plan must be developed and followed throughout the life cycle of the project. Sticking to the plan is important to prevent scope creep. If the scope continually expands in an uncontrolled manner, the project might never meet its goals, might run out of funds, or might run over schedule.

Executing

Once the planning has been completed, it is time to follow the plan in the project executing phase. This phase is where the deliverables are created and produced based on the scope of the project described in the statement of work. This phase includes the following activities:

- Follow the plan, execute project tasks, and manage project budget
- Implement changes and track project progress
- Communicate and report on progress to stakeholders and other vested parties
- Report status within the team and to management
- Hold staff and vendors accountable

It is important to remember to adjust the plan as needed. No project goes completely according to plan. Project management is really all about planning and making strategic adjustments when needed.

Monitoring and Controlling

The monitoring and controlling phase of the life cycle is focused on monitoring and controlling key project variables. Although this phase is being discussed sequentially after the executing phase, in practice this phase occurs throughout the life cycle of the project. Monitoring and controlling consists of the following activities:

- Monitor and manage scope creep
- Monitor and manage project budget
- Monitor, track, and report on key performance indicators (KPIs)
- Process change requests
- Track project variations
- Track and report on project metrics and performance
- Monitor and manage costs, scheduling, resource utilization, budget, and risk

This section discusses some of the key aspects of monitoring and controlling that must occur throughout the project life cycle, including configuration management, change management, and quality management.

Configuration and Change Management

It is important to incorporate configuration management and change management on every project. *Configuration management* consists of processes and tools to manage the requirements, specifications, and standard configurations of the product or deliverable. *Change management* consists of processes and tools for identifying, tracking, monitoring, and controlling changes to the project plan and baseline.

The *configuration management plan* defines the process for making changes to the configuration of the deliverable. It documents configurable items that require formal change control and describes the process for controlling those changes. The *change management plan* documents the process for managing changes to the project and describes how to perform monitoring and controlling of changes.

The processes used for configuration and change management are documented in their respective plans and incorporated into the project plan in the planning phase of the project life cycle. Configuration and change management processes are then monitored and controlled throughout the life of the project.

Quality Management

Project *quality management* is the practice of ensuring that all project activities meet a defined level of excellence. It involves defining quality standards and putting processes in place to ensure the standards are applied correctly on the project. A *quality management system (QMS)* is a collection of processes and activities intended to ensure desired levels of quality are met. The QMS incorporates quality assurance and quality control practices,

Figure 3-13 Quality management concepts

as illustrated in Figure 3-13. These terms are sometimes used interchangeably in discussions of quality management, but there are some key differences:

- **Quality assurance (QA)** Focused on proactive *prevention* of project defects by creating a system to measure and control quality throughout the *process*
- **Quality control (QC)** Focused on *detection* of defects in the *deliverable* based on quality assurance criteria

Decisions regarding how quality management will be handled during the project are documented in the quality management plan in the planning phase, incorporated into the project plan, and monitored and controlled throughout the project life cycle. This section discusses two common methodologies for quality management, Six Sigma and the ISO 9000 family of standards.

Six Sigma Six Sigma is a process improvement methodology focused on improving process quality by using statistical methods of measuring operational efficiency and reducing variation, defects, and waste. It was originally developed by Motorola with the goal of identifying and removing defects in the manufacturing process. The maturity of a process is described by a sigma rating, which indicates the percentage of defects that the process contains. Six Sigma projects use the DMAIC and DMADV project methodologies, which are based on Deming's Plan, Do, Check, Act (PDCA) cycle. DMAIC stands for "define, measure, analyze, improve, control" and DMADV stands for "define, measure, analyze, design, verify." Although the Six Sigma methodology was originally intended for manufacturing, it has evolved and is used by many industries and business functions. Some organizations use Six Sigma to improve security assurance by measuring the success factors of different security controls and processes.

ISO 9000 Chapters 1 and 2 discussed the ISO/IEC 27000 family of standards, which focuses on implementing an information security management system (ISMS). The ISO 9000 family of standards is focused on various aspects of quality management and implementing a QMS. The publications provide guidance and tools to help organizations meet customer requirements for deliverables while ensuring quality is managed and improved. The key publications in the ISO 9000 family are outlined here:

- **ISO 9000** Quality management systems – Fundamentals and vocabulary
- **ISO 9001** Quality management systems – Requirements
- **ISO 9004** Quality management – Quality of an organization – Guidance to achieve sustained success
- **ISO 19011** Guidelines for auditing management systems

In addition, there are industry-specific standards based on ISO 9001, which include the following (with abbreviated titles indicating their application):

- **ISO 13485** Medical devices
- **ISO/TS 54001** Electoral organizations at all levels of government
- **ISO 18091** Local government
- **ISO/TS 22163** Rail organizations
- **ISO/TS 29001** Petroleum, petrochemical, and natural gas industries
- **ISO/IEC/IEEE 90003** Software engineering

Closing

The last phase of the project is *project closing*. The closing phase includes the following activities:

- Review of project scope document to ensure requirements are met
- Ensure signoff of deliverables by stakeholders
- Close out contracts, process and pay invoices, and shut down project expenditures
- Update final project costs accounting
- Securely dispose of project materials, as some records may contain sensitive information
- Archive project records that must be maintained for future reference
- Conduct lessons learned, including any feedback from stakeholders
- Release and reassign resources

A proper closing phase allows for a final review and acceptance of the project, closeout of contracts and financial activities, and release of resources. While this particular project may be complete, there is most likely another project around the corner that may require some of the resources that have been tied up.

EXAM TIP CCISO candidates should be familiar with the general phases of project management and corresponding project activities.

Project Management Oversight

The CISO typically is not responsible for actively managing every security project. The CISO is involved in project oversight but may enlist another resource such as a security project manager, deputy CISO, or other staff as the project manager. When reviewing security projects, the CISO should consider questions such as the following:

- Are projects following the organization's project management practices?
- Are the processes based on industry standards and best practices?
- Is the project plan being followed?
- Is the critical path well defined?
- Do team members and the project manager have a thorough understanding of activities in the critical path?
- How often are projects on time and on budget?
- Does the project have a defined communication plan?
- Are business objectives being achieved in a cost-effective manner?
- Is the project maintaining compliance with industry regulations and local laws?

Chapter Review

The CISO is responsible for managing the information security program of the organization. The key aspects of a security program include security areas of focus (internal and external drivers that impact how the streams of work and security projects are carried out, such as PCI DSS, HIPAA, and internal policies and requirements); security streams of work (subprograms such as the vulnerability management program, incident response program, and risk management program), often managed using the PDCA approach; security project management; asset and data security management; and security program budget and resource management. Managing these elements in a cohesive and coordinated manner is not simple and requires a thoughtful approach.

Project management is a critical skill for the CISO to master. Although the CISO typically is not the project manager for every security project, the CISO must oversee and be accountable for the projects being undertaken within the information security program. The triad for project management includes scope, schedule, and budget. If one of these components changes, the other two components usually are affected. Projects follow a project management model, which typically includes initiating, planning, executing, monitoring and controlling, and closing processes.

Quick Review

- Security program management is focused on overseeing and managing security areas of focus, security streams of work, security projects, asset and data security, and security program budget and resources.
- Security areas of focus are internal and external organizational drivers that impact how the streams of work and security projects are carried out, such as PCI DSS, HIPAA, and internal policies and requirements.
- Security streams of work (aka subprograms) of the information security program are activities that are ongoing and do not have a beginning, middle, and end, such as identity and access management, vulnerability management, and incident management.
- The triad for project management includes scope, schedule, and budget.
- The traditional project management model is made up of the following processes: initiating, planning, executing, monitoring and controlling, and closing.
- The scope of a project defines the boundary of the project. It is the work that is required to fulfill the customer requirements.
- Scope creep is uncontrolled growth in a project's scope due to the addition of requirements, desires, or targets.
- The systems development life cycle (SDLC) refers to the phases within the project that are associated with the development of a system, software, service, or product. The SDLC typically occurs within the planning and executing processes of the project management model.
- SDLC models include waterfall, iterative, incremental, and agile.
- A work breakdown structure (WBS) is a hierarchical decomposition of the work to be performed by the project team to accomplish and deliver against the project goals. It is a project management tool used to break down the project into organized individual work elements (tasks, subtasks, and deliverables).
- The critical path of a project is the series of events or activities that, if changed, would change the overall end date of the project.
- A Gantt chart illustrates a project schedule and shows the dependencies of tasks.
- A responsibility assignment matrix or RACI chart can be used to demarcate responsibilities for each activity or task involved in meeting project deliverables. RACI is an acronym for responsible, accountable, consulted, and informed.

- Configuration management focuses on the requirements, specifications, and standard configurations of the product or deliverable.
- Change management focuses on identifying, tracking, monitoring, and controlling changes to the project plan and baseline.
- Six Sigma is a process improvement methodology focused on improving process quality by using statistical methods of measuring operational efficiency and reducing variation, defects, and waste.
- The ISO 9000 family of standards is focused on various aspects of quality management and implementing quality management systems (QMSs).

Questions

1. Which of the following activities is an example of a subprogram or stream of work?
   - **A.** Conduct network monitoring
   - **B.** Deploy an intrusion detection system
   - **C.** Build an identity management system
   - **D.** Conduct a penetration test
2. When creating an information security budget, which of the following is the least important factor to consider?
   - **A.** What your boss's perception is about security
   - **B.** Ensuring the budget grows each year so the security department can continue to grow
   - **C.** The costs of labor to staff all the streams of work
   - **D.** How much the organization spent on security last year
3. Which of the following is not a good approach to use to build a strong security team?
   - **A.** Provide career paths for employees
   - **B.** Select people based on character, not just technical skills
   - **C.** Limit employee training so that employees do not increase their skills and decide to leave the company
   - **D.** Provide an environment that encourages communication and collaboration
4. What is essential to determining how well a security subprogram is performing?
   - **A.** Use the "two-person rule" whenever possible
   - **B.** Establish criteria for success and measure the activity against it
   - **C.** Bring in outside experts to review the activity
   - **D.** Interview the subprogram staff

5. Which of the following statements regarding project management is the most accurate?
   - **A.** Project management is only important for small projects.
   - **B.** Project management is important for large projects, while program management is important for ongoing projects.
   - **C.** Project management is only important for large projects.
   - **D.** Project management is important for projects of all sizes.
6. Which of the following terms describes the uncontrolled growth of a project's requirements?
   - **A.** Stakeholder input
   - **B.** Scope creep
   - **C.** Definitions creep
   - **D.** Organic growth
7. Which of the following best describes the critical path in project management?
   - **A.** Activities that, if changed, will change the end date of the project
   - **B.** Activities that will change the end date of the project
   - **C.** Activities that are critical to the project
   - **D.** Activities that are not critical to the project
8. A CISO reviewing current security projects determines that the security project manager for a network redesign did not use the approved WBS. What is this an example of?
   - **A.** Scope creep
   - **B.** Waterfall method
   - **C.** Alternate WBS
   - **D.** Not following the plan
9. Which of the following activities should occur during project closeout?
   - **A.** Conduct lessons learned
   - **B.** Outline the scope
   - **C.** Requirements gathering
   - **D.** Continue billing to the project
10. Which of the following is the main difference between a program and a project?
    - **A.** There is no difference.
    - **B.** A program consists of projects, and a project consists of activities.
    - **C.** Unlike a program, a project has no end.
    - **D.** A program may consist of many projects, while a project consists of only one project.

Answers

1. **A.** An information security program includes streams of work (aka subprograms) that continue throughout the life of the organization. Conducting network monitoring is an ongoing activity that continues for the life of the organization and security program. Building systems and deploying systems are most often projects rather than ongoing subprograms or streams of work. Penetration tests have a defined end to the activity.
2. **B.** It is a good idea to start the information security budget process by looking at what was spent the previous year, include all labor costs, and present the budget to management in terms they can understand. The desire to expand the security staff should not be a factor in defining the security budget.
3. **C.** The organization should not limit employee training for fear that employees may leave the company. That is always a risk, but if the employees aren't properly trained, the organization won't be able to build a strong team. Providing career paths, choosing people based on character, and encouraging communication are all good things to do.
4. **B.** Although interviewing the subprogram staff is always a good idea, the most essential way to determine how well a security subprogram is performing is to establish criteria for success and measure against that criteria.
5. **D.** Although a project may seem trivial, project management is critical for projects of all sizes, not only larger projects.
6. **B.** Scope creep describes the uncontrolled growth of a project's scope.
7. **A.** The critical path of a project is the series of events or activities that, if changed, would change the end date of the project. If any of the activities in the critical path is delayed, the end date of the overall project delivery is impacted.
8. **D.** The security project manager not using the approved work breakdown structure (WBS) is an example of an employee not following the approved plan. Scope creep is when the scope increases during the project, and waterfall is a type of software development methodology. Alternate WBS is an incorrect option intended as a distractor.
9. **A.** The lessons learned component of project closeout is often overlooked. This is a critical activity to learn from past mistakes and improve future projects.
10. **D.** A program may consist of multiple projects, while a project is self-contained.