Chapter 2

Information Security Risk Assessment Basics

It is the aim of this book to provide an extensive discussion of information security risk assessment. As such, you will find detailed information, discussion, and advice on all elements of the information security risk assessment. Many of the sections of this book will provide a rather detailed discussion of a single element of information security risk assessment. However, before we get into this level of discussion, it would be useful to provide a brief overview of the information security risk assessment process.

For the purposes of this book, the information security risk assessment process is defined as follows:

> Security Risk Assessment—An objective analysis of the effectiveness of the current security controls that protect an organization's assets and a determination of the probability of losses to those assets.

There are many security risk assessment methods available and currently in use. Depending on the specific one employed, a security risk assessment may have any number of steps or phases, and each of these phases may have slightly different names. However, the overall process is largely similar in all these methods. The generic phases of a security risk assessment are shown in Figure 2.1.

2.1 Phase 1: Project Definition

As with many projects, the success of the security risk assessment project relies not only on the skill and experience of the team assigned to the security risk assessment,

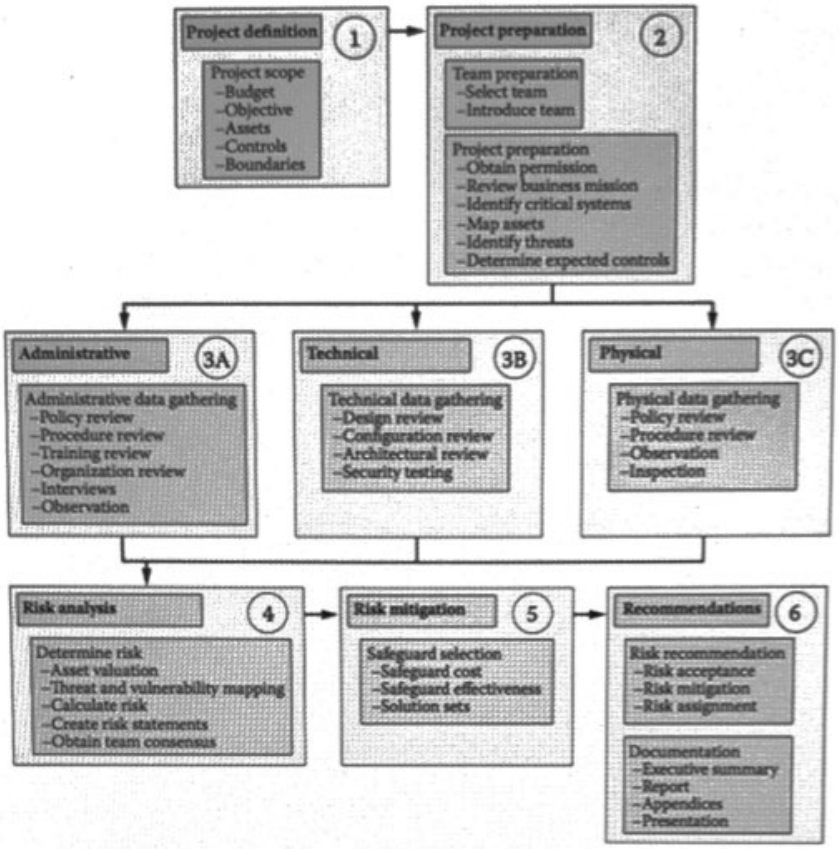

Figure 2.1 The security risk assessment process comprises the following phases: project definition, project preparation, administrative data-gathering, technical data-gathering, physical data-gathering, risk analysis, risk mitigation, and recommendations. These phases are described in more detail in the remaining chapters of this book.

but also on the effectiveness of the project management. A key component of project management is arriving at an agreement as to the scope and content of deliverables. Within the project-definition phase, the project is properly scoped and documented.

The scoping of any project includes a clear understanding of the cost and time frame of the engagement. The security risk assessment team leader needs to ensure that the project budget and time constraints are well understood. Documentation of this understanding is captured in the project plan and in the contract, if this involves a customer. A project plan not only documents the budget and time constraints, but breaks down the overall project into manageable tasks and allocates resources to those tasks.

Beyond the budget and time constraints of the project, the scoping of a security risk assessment can be more complex than the scoping of some other projects. Unique variables to the security risk assessment process include the assessment objective, the

assets and controls to be covered, and the assessment boundaries. Obtaining clarity on the security risk assessment objective is necessary to understand the customer needs. For example, a security risk assessment performed for contract compliance has a different objective than one performed for program review. The team must also seek clarity on the boundaries of the assessment through an identification of assets, systems, and other boundaries of the project. Each of these tasks is discussed in greater detail in Chapter 3.

2.2 Phase 2: Project Preparation

Based on the scope of the security risk assessment project identified in phase 1, the team leadership needs to ensure that adequate preparations are performed prior to entering the data-gathering phase. Preparation includes team preparation and project preparation.

Team preparation comprises the selection of the security risk assessment team and the introduction of the team to the organization to be assessed. Many factors go into the proper selection of the security risk assessment team, including objectivity, expertise, and experience. Introduction of the team to the customer includes formal letters of introduction as well as a request for permission and access. Each of these tasks is discussed in greater detail in Chapter 4.

2.3 Phase 3: Data Gathering

The data-gathering phase is typically performed on site and results in the collection of information concerning the effectiveness of the current administrative, physical, and technical security controls. The security risk assessment team will review the administrative controls through the collection, review, and analysis of available policies and procedures as well as observation and interviews with staff. The physical security controls will be assessed through techniques such as observation, testing, and analysis. The technical security controls will be reviewed through technical analysis, testing, and review of logs. The data-gathering phase is the most comprehensive of all of the phases and is discussed in more detail in Chapter 5. Specific advice on how to perform data-gathering for administrative, technical, and physical controls are found respectively in Chapter 6.

2.4 Phase 4: Risk Analysis

The risk-analysis phase involves a review of the data gathered and an analysis of the resulting risk to the organization. During this phase, the security risk assessment team must determine asset values, system criticality, likely threats, and the

existence of vulnerabilities based on the data gathered. Furthermore, the team must calculate the risk to the organization for each threat/vulnerability pair. The calculation and presentation of these risks can vary greatly, depending on the security risk assessment method being used.

Several elements of the risk analysis phase are considered key concepts within security risk assessments. These include assets, threats, vulnerabilities, and security risk.

2.4.1 Assets

The first element to be considered and discussed in an information security risk assessment is the assets of the organization. Assets are the items considered valuable by the organization. Later in this book, we shall discuss classes of assets, valuation of assets, and grouping of assets, but for now it is important to understand that assets are the information, resources, or other items that have value to the organization. Examples include buildings, equipments, personnel, organization reputation,[1] business documents, and many other tangible and intangible items.

Assets are an important element of a security risk assessment for several reasons. First, the enumeration of assets helps to scope the security risk assessment. Scoping of the security risk assessment will be discussed later as well, but for now, consider the following example. If an organization has commissioned a security risk assessment and has dictated that the buildings and equipment are not among the assets within the scope of the security risk assessment, then a review of the physical security controls protecting the buildings and equipment would not need to be performed. In this way, the enumeration of assets helps to scope the security risk assessment.

Second, the valuation of assets helps to determine the countermeasures employed. A countermeasure is simply a control (activity, technique, or technology) that reduces the possible loss to an organization's assets (see Table 2.1). While the selection of countermeasures can be somewhat involved, it is clear that we should not spend more on the countermeasure than the possible reduction in

Table 2.1 Asset Summary

Key Concepts	*Definition*
Asset	Resource, data, or other item of value to the organization.
Asset enumeration	A listing or grouping of assets under assessment. Asset enumeration helps to scope the information security assessment.
Asset valuation	The placement of a relative or dollar value on each asset. Asset valuation is useful in determining potential loss and countermeasure selection.

Note: Assets are those items the organization wishes to protect. The enumeration and valuing of the assets scopes and guides the security risk assessment.

the organizational loss. Later in the book, we shall discuss both asset valuation and countermeasure selection.

2.4.2 Threat Agents and Threats

The next elements to be considered and discussed in an information security risk assessment are the threats and the threat agents. A threat is an event with an undesired impact. A threat agent is the entity that may cause a threat to happen. Threats and threat agents are inextricably linked, in that it is the threat agent that causes a threat to happen. A more in-depth discussion of threats, threat classes, threat environment, and threat analysis is provided in Chapter 4 (Section 4.5). The basics of threats and threat agents are presented here as a primer on the topic. Threat agents include Mother Nature and mankind. Examples of threats include earthquakes, fires, theft, insertion of malicious code, accidental disclosure, and many others.

The main reason that threat agents and threats are important elements of the information security risk assessment is that they help to determine the scope of the vulnerabilities of the system being assessed. To begin a security risk assessment, we must understand the threats from which we plan to protect the assets. It is rather naive to believe that something undesired will never happen, and it is equally naive to believe that you can possibly anticipate or even list every possible threat. However, we can describe the threat environment of the target system. This approach helps the security risk assessment team to consider those threats that are most likely to impact the target of the security risk assessment and to ignore those that are least likely to impact the target of the security risk assessment. Those threats that are considered relevant for a specific security risk assessment are called "valid threats".

For example, an information security risk assessment being performed on an organization in Austin, Texas, would not need to consider the threat of earthquakes, snow blizzards, or perhaps even hurricanes. However, it would need to consider flooding, tornadoes, and severe thunderstorms. In this example, the threat agent is Mother Nature, and we consider some of her threats valid and others not valid for this portion of the country.

2.4.2.1 Threat Agents

Threat agents are the catalyst of the threat. A threat agent is the entity that causes a threat to happen. A list of possible threat agents is provided below for illustrative purposes:

- Nature—Any number of natural disasters could affect the support systems relied upon by your organization's information system. If the threat is a natural threat, such as storms or floods, then "nature" can be considered the threat agent.
- Employees—Organizations entrust their personnel to perform their duties accurately and consistent with the policies of the organization. A major threat to organizations is the threat that an employee could make a critical mistake in data entry, release proprietary data, or decide to defraud the organization.

- Malicious Hackers—Information systems that are networked with other systems or even the Internet expose themselves to millions of potential hackers. Even those systems that do not provide a public interface, such as the Internet, are still exposed to hackers through social engineering, modem connections, or physical attacks.
- Industrial Spies—The value of proprietary information to the competition should not be underestimated. Industrial espionage is a significant threat to most organizations and can result in loss of profits, competitive advantage, or even the business itself.
- Foreign Government Spies—Foreign spies could perform espionage for the purpose of advancing the capabilities of a foreign government or restricting our government's abilities, or this area could even include foreign-sponsored industrial espionage.

2.4.2.2 Threats

A threat is an undesired event that may result in the loss, disclosure, or damage to an organizational asset (see Table 2.2). A partial list of threats is given below:

- Errors and Omissions—Occasionally, mistakes by authorized employees, users, developers, and testers can occur during data entry or operations, or in system or application development. These errors and omissions can lead to a lack of data and system integrity, a lack of system stability, and even disclosure of sensitive information.
- Fraud and Theft—The threat to the information system could be for the purpose of fraud or theft. Information systems are targets of fraud and theft because they directly or indirectly protect assets of value. For example, financial systems directly protect the assignment of funds to accounts, whereas inventory systems indirectly

Table 2.2 Threat and Threat Agent Summary

Key Concepts	*Definition*
Threat	
Valid threat	Threats that are considered relevant for a specific security risk a assessment
Threat agent	The entity that may cause a threat to happen
Threat environment	Determining the physical, geographical, and other aspects of the organization's system helps to determine the scope and extent of applicable threats

Note: Threats and threat agents are the actions and entities the organization would like to avoid. Threats and threat agents are determined by the physical geography and mission of the organization.

protect equipment through inventory tracking. Each of these types of systems can be the target of those attempting to steal from or defraud a corporation.

- Sabotage—Those authorized by the organization to access the organization's information systems and assets must be trusted to uphold the trust placed in them. However, sometimes this trust is misplaced. Such misplaced trust leads to sabotage. Sabotage may include physical damage to facilities or equipment, destruction of processes, deletion of data, or loss of data integrity.
- Loss of Physical and Infrastructure Support—The physical and infrastructure support provides the required services for an organization's information systems, such as power, communication, and transportation. Many threats, both natural and human, endanger the ability of the support structure to supply the required services to the information system. Threats in this category include power failures, winter storms, labor strikes, and terrorist attacks.
- Espionage—Proprietary information is a highly valued asset of the organization. Proprietary information is also highly valued by the competition. The act of gathering proprietary data for the purpose of aiding another organization is referred to as "espionage." Espionage is performed by foreign governments and competitive organizations.
- Malicious Code—The connectivity of systems and the introduction of new software and data from other sources increases the threat that an organization's information system may become infected with malicious software. Malicious software could be a virus, Trojan horse, worm, logic bomb, or other software that does not perform as intended.
- Disclosure—Information systems contain vast amounts of data that are sensitive to the organization and to individuals. The concern that data about an individual could be disclosed to someone unauthorized is referred to as "privacy." The concern that data about the organization could be disclosed is referred to as "confidentiality." Both the personal privacy threat and the organizational confidentiality threat are major concerns.

2.4.3 Vulnerabilities

A vulnerability is a flaw or oversight in an existing control that may possibly allow a threat agent to exploit it to gain unauthorized access to organizational assets. In Chapters 6, 7, and 8 we shall discuss in detail how to find and describe vulnerabilities in administrative, technical and physical controls. In Chapter 9, we shall discuss how to rate these vulnerabilities. For now, it is important to understand the relationship of vulnerabilities to other elements of the information security risk assessment and the importance of the vulnerability in this effort.

Vulnerabilities are important elements of a security risk assessment because they are instrumental in determining existing and residual risk. Without vulnerabilities, there would be no risk. However, we know there is no such thing as a system without vulnerabilities, so it is the task of the security risk assessment team to assess the vulnerabilities in

the existing system and those vulnerabilities that are likely to still exist if the safeguard recommendations are implemented. When assessing vulnerabilities in the system, it is useful to categorize the vulnerabilities according to administrative, physical, and technical areas, since the departments or personnel are likely to be distributed similarly.

Administrative vulnerabilities are those vulnerabilities that exist in policies, procedures, or security activities. Examples include missing acceptable-use policies, gaps in termination procedures, or the lack of independence in security testing.[2] Physical vulnerabilities are those vulnerabilities that exist in the physical, geographical, personnel, or utility provisioning controls. Examples include holes in the fence line, location in a flight path, lack of background checks for sensitive positions, and lack of redundant power supplies. Technical vulnerabilities are those that exist in the logical controls in the organization's system. Examples include misconfigured routers, backdoors in programs, and weak passwords (see Table 2.3).

2.4.4 Security Risk

A security risk is the loss potential to an organization's asset(s) that will likely occur if a threat is able to exploit a vulnerability. In this book, we shall discuss various ways to assess (Chapter 9), reduce (Chapter 10), and report security risk (Chapter 11). Security risk (and residual security risk) is the key element of the information security risk assessment because it is the culmination of all the other assessments, calculations, and analyses. Security risk is the key measurement that

Table 2.3 Vulnerability Summary

Key Concepts	*Definition*
Vulnerability	A flaw or oversight in an existing control that may allow a threat agent to exploit it to gain unauthorized access to organizational assets
Administrative vulnerability	Gaps in policies, procedures, or security activities, e.g., missing acceptable-use policies, gaps in termination procedures, or the lack of independence in security testing
Physical vulnerability	Gaps in physical, geographical, personnel, or utility provisioning controls, e.g., holes in the fence line, location in a flight path, lack of background checks for sensitive positions, and lack of redundant power supplies
Technical vulnerability	Gaps in the logical controls in the organization's system, e.g., misconfigured routers, back doors in programs, and weak passwords

Note: Vulnerabilities are weaknesses or absences of security control. These vulnerabilities can exist in administrative, physical, or technical controls.

the organization's management really cares about; the rest of the stuff is just a way to get to the key measurement of security risk.

There are many key factors to consider when discussing security risk, but the most important factor of security risk to consider right now is the manner in which the security risk is derived and presented. There are many ways to derive and present security risk, but all of these approaches can be described as quantitative or qualitative.

The quantitative approach to deriving and presenting security risk relies on specific formulas and calculations to determine the value of the security risk. A quantitative approach to determining and even presenting security risk has the advantages of being objective and expressed in terms of dollar figures. However, such quantitative calculations can be rather complex, and accurate values for the variables in quantitative formulas may be difficult to obtain.

The qualitative approach to deriving and presenting security risk relies on subjective measures of asset valuation, threats, vulnerabilities, and ultimately the security risk. A qualitative approach to determining and presenting security risk has the advantage of being easy to understand and, in many cases, provides adequate indication of the organization's security risk. However, a security risk measurement derived from such qualitative measures is, indeed, subjective and may not be trusted by some in management positions (see Table 2.4). More detail on security risk analysis is provided in Chapter 9.

2.5 Phase 5: Risk Mitigation

Based on the risks defined in the risk analysis phase, the team must develop recommendations for safeguards to reduce the identified risks to an acceptable level. The safeguard selection process involves mapping safeguards to threat/vulnerability pairs, determining the reduction of risk, determining the cost of the safeguard, and grouping safeguards into solution sets.

Several elements of the risk mitigation phase are considered key concepts within security risk assessments. These include safeguards and residual risk.

2.5.1 Safeguards

Next we consider the security controls, or safeguards, put in place to protect the organization's assets from reasonable threats. A safeguard or countermeasure is a technique, activity, or technology employed to reduce the risk to the organization's assets. A safeguard may prevent, detect, or minimize the potential loss to an organization's assets. For this reason, safeguards are generally categorized as preventive, detective, or corrective measures. Preventive measures are controls that are designed to deter undesirable events from happening. Examples include access controls, door locks, and security awareness training. Detective measures are controls that identify conditions that indicate that an undesirable event has

Table 2.4 Security Risk Summary

Key Concepts	*Definition*	
Security risk		
Quantitative risk	A method of determining and presenting security risk that relies on specific formulas and calculations to determine the value of the security risk	
	Advantages	Disadvantages
	Objective; security risk expressed in terms of dollars	Security risk calculations are complex; accurate values are difficult to obtain
Qualitative risk	A method of determining and presenting security risk that relies on subjective measures of asset valuation, threats, vulnerabilities, and ultimately of the security risk	
	Advantages	Disadvantages
	Easy to understand; provides adequate indication of the organization's security risk	Subjective; may not be trusted by some in management positions

Note: Security risks are a measurement of the likelihood that the organization's assets are susceptible. Security risk assessment methods can be either quantitative or qualitative.

happened. Examples of detective measures include audit logs, security testing, and intrusion detection systems. Corrective measures are controls designed to correct the damage caused by undesirable events. Examples of corrective measures include security guards, termination policies, and file recovery. Note that safeguards (also referred to as controls) may be classified as being in multiple categories, such as security guards, which can be considered a preventive, detective, and corrective measure.

Safeguards are an important element in information security risk assessments for two reasons. First, all existing safeguards must be considered when determining the present vulnerability of the organization's system. If the security risk assessment team fails to consider all the safeguards in place to protect the organization's assets, then the security risk assessment results will be inaccurate and will likely err on the side of overestimating the risk. Such errors can be costly, as decisions for implementing additional security measures should be based on the results of security risk assessments.

Second, safeguards are an important element of security risk assessments because the final report should recommend safeguards to be implemented to bring the residual risk within tolerance levels of the senior management of the

Table 2.5 Safeguard Summary

Definition: A technique, activity, or technology employed to reduce the risk to the organization's assets. Safeguards protect the organization's assets from the risks of threats.	
Key concepts	
Preventive	Controls designed to deter undesirable events from happening, e.g., access controls, door locks, and security awareness training
Detective	Controls that identify conditions that indicate that an undesirable event has happened, e.g., audit logs, security testing, and intrusion detection systems
Corrective	Controls designed to correct the damage caused by undesirable events, e.g., security guards, termination policies, and file recovery

organization. Safeguard recommendations are key to the results of a security risk assessment and must be carefully considered (see Table 2.5).

2.5.2 Residual Security Risk

Residual security risk is the security risk that remains after implementation of recommended safeguards. The objective of security risk management is to accurately measure the residual security risk and keep it to a level at or below the security risk tolerance level.

Residual security risk is an important element of information security risk assessments for several reasons. First and foremost, residual risk is the security risk that the organization will inherit when safeguards are implemented. It is important that the organization's management fully understands the concept of residual security risk and is comfortable with staffing and budgeting decisions that determine the residual security risk level.

Second, the security professional and the organization's management must clearly understand that there is no such thing as 100 percent security (or 0 percent residual security risk). Even if the organization implements every one of the information security professionals' recommendations, the organization still has some residual security risk to its assets. More detail about security risk mitigation is provided in Chapter 10. Table 2.6 provides a definition of residual security risk as well as some key concepts.

2.6 Phase 6: Risk Reporting and Resolution

The final phase of a security risk assessment is the risk reporting and resolution phase. During this phase, the security risk assessment team develops a report and

Table 2.6 Residual Risk Summary

Definition: The security risk that remains after implementation of recommended safeguards. Residual risks are the leftover risks to the organization's assets after safeguards have been applied.	
Key concepts	
Static risk	The security risk that will always exist
Dynamic risk	Security risk that may be reduced through the implementation of safeguards

a presentation to the project sponsor that clearly identifies the risks found and the safeguards recommended. The final risk assessment report should provide clear information for the executive, management, and technical personnel. The executives of the assessed organization must then determine the resolution of the identified risks. The risk resolution element within this phase is considered a key concept within security risk assessments.

2.6.1 Risk Resolution

At the conclusion of a security risk assessment project, the senior management of the assessed organization must determine the resolution of each of the identified risks. In other words, the senior manager must decide to reduce the risk, accept the risk, or delegate the risk to someone else.[3]

A security risk can be reduced by implementing additional security controls or even by improving existing security controls. Suggestions for risk-reducing safeguards for each identified risk should be documented in the final report. Along with these recommendations, cost and effectiveness estimations should be included to assist in the senior manager's decision.

A security risk can be accepted if the senior manager believes that it is in the best interest of the organization to accept the risk rather than to accept the cost burdens of implementing additional safeguards. The acceptance of this risk must be performed by a senior manager of the organization, because this decision impacts the organization as a whole and not just a single department or project.

Lastly, a security risk can be transferred to another organization such as an outsourcing company or an insurance agency. The transfer of security risk is a contractual agreement that clearly spells out the risk and the burden accepted along with the conditions and limitations of such an agreement (see Table 2.7). More detail on security risk assessment reporting in provided in Chapter 11.

Table 2.7 Risk Resolution Summary

Key Concepts	*Definition*
Risk resolution	The decision by senior management of how to resolve the risk presented to them
Risk reduction	The reduction of risk to the organization to an acceptable level through the adoption of additional security controls or improvement of existing controls
Risk acceptance	The deliberate decision by senior management to accept an identified risk based on the business objectives of the organization
Risk transference	The contractual transfer of risk to another organization through outsourcing or insurance

Note: Safeguards protect the organization's assets from the risks of threats.

Exercises

1. Tasks performed within a security risk assessment have some flexibility in terms of order performed (consider Figure 2.1). Indicate the order of the tasks below by listing prerequisite tasks (tasks that must be completed prior to starting) and successors (tasks that cannot begin prior to completion of current task) for each of the tasks listed below:

Be Prepared to Justify Your Answers

Prerequisite Tasks	*Task*	*Successor Tasks*
	a. Project scope	
	b. Asset valuation	
	c. Threat identification	
	d. Policy review	
	e. Vulnerability scan	
	f. Schedule interviews	
	g. Perform interviews	
	h. Assess risk	
	i. Develop recommendations	
	j. Present report	

2. Research: How much does a security risk assessment cost?
   a. Determine the current market price for a security risk assessment.
   b. What factors are involved in the scoping of a security risk assessment?
   c. Are service organizations reluctant to give pricing information? Why or why not?
   d. Is there any confusion in terms of security risk assessments, vulnerability scans, security audits, security reviews, etc.?
3. Brainstorm: As a group or a class exercise, list the typical organizational assets. Attempt to group or categorize the assets.
   a. Consider the multiple grouping schemes and specificity of the assets. What are the pros and cons to the various schemes you created? For example, what are the pros and cons to treating all Web applications as a single asset?
   b. Are you able to find industry examples of asset classification guidance that can assist in this exercise?
4. Threat Trees: Threat trees are a way of organizing threats using tree structures.
   a. Using the threat agents and threats listed in Section 2.4.2 as a basis, create a threat tree. Start with tree "roots" (main nodes) of "natural" and "human-made" threats.
   b. What is the relationship between threat agents and threats (many–many, one–many, one–one, or many–one)?
5. In the News: Find an article on a recent computer security incident or breach.
   a. Identify as many of the following elements as possible:
      i. Threat agent/threat
      ii. Vulnerability
      iii. Assets affected
      iv. Countermeasures applied
   b. What other safeguards could you recommend?

Notes

1. Although reputation is not a tangible asset, it does have measurable economic value to the organization. On the balance sheet, this value is generally called "goodwill."
2. Administrative security controls comprise policies, procedures, and security activities. Often, the term *administrative* has a bad connotation among security engineers. Those that come from a technical background may tend to think that *administrative* means paperwork, but this is not the case. Administrative security controls include controls that require technical skills such as risk assessments, security testing, and code review.

3. Another valid management action for an identified risk is to obtain additional data. This would be especially valid in cases where a security risk assessment was performed with little rigor (e.g., survey-based) and the potential mitigation strategies are expensive. Additional data supplied by a more rigorous review (e.g., interviews, observations, and testing) can give management a more appropriate amount of information for decisions involving large expenditures.

References

Common Criteria for Information Technology Security Evaluation. Version 3.1, Revision 3 Final CCIMB-2009-07-001, July 2009.

Tipton, Harold F. and Micki Krause. *Information Security Management Handbook*, 2007.

Chapter 3

Project Definition

A security risk assessment can mean many things to many people. Within the context of this book, a security risk assessment is defined as an objective analysis of the effectiveness of the current security controls that protect an organization's assets and a determination of the probability of losses to those assets. Various regulations, guidelines, and other information sources sometimes call the security risk assessment by another name. Terms used include *security audit*, *risk assessment*, *security testing*, and so on. Other times, *security risk assessment* is used to mean something different from what is described in this book.

Realizing the confusion surrounding these terms, it is important that the security risk assessment project be well defined prior to project initiation. Definition of a security risk assessment project requires knowledge of the budget, objective, scope, and the level of rigor of analysis expected. Each of these areas is discussed in the following sections of this chapter. But first there is a quick discussion of how to ensure a successful security risk assessment.

3.1 Ensuring Project Success

Performing a security risk assessment is a project and, as such, anyone seeking to be an effective member of a security risk assessment team should understand how such a project is run successfully. Moreover, the leader of the security risk assessment team needs to be able to plan, track, and ensure the success of the security risk assessment project.

3.1.1 Success Definition

Success cannot be achieved until we define the meaning of success. For a security risk assessment project (and, for that matter, most technical projects), success is defined as achieving customer satisfaction, quality technical work, and project completion within budget.

3.1.1.1 Customer Satisfaction

The customer of a security risk assessment includes the "sponsor" of the security risk assessment and additional stakeholders within the organization being assessed. All of these stakeholders have unique points of view and distinct definitions of what they expect from a successful security risk assessment.

3.1.1.1.1 Identifying the Customer

Regardless of whether the security risk assessment is performed by internal resources or is contracted out to a security consulting firm, the primary customer of a security risk assessment is the individual responsible for commissioning it. If the security risk assessment is performed by a contracted security consulting firm, the project sponsor should be explicitly stated in the contract. If not explicitly stated, consider the project sponsor the most senior official who will be at the final briefing. For internal security risk assessments, the project sponsor is the department manager or director who commissioned the project.

Project Sponsor—The project sponsor is the person internally responsible for the success of the project. If this is a contracted effort, then the project sponsor is typically the signature authority for the project. Either way, the project sponsor will define the success of the project in terms of the quality of the technical work and project completion within time and budget constraints.

The quality of the technical work can be ensured through careful selection of project members and following the guidelines in this book. Project completion within budget can be ensured through following the guidelines in Chapter 12.

The secondary customer for the security risk assessment project includes any other stakeholder in the process. These stakeholders are numerous and play a vital role in the ultimate acceptance of the security risk assessment and, in turn, customer satisfaction. Each of these secondary customers is listed and discussed below.

- Security Officer or Security Team—The most senior security officer in the organization may be a chief security officer, with a staff, visibility, and a security budget, or it may be a systems administrator who enjoys the security aspects of setting up the network. Regardless of his position within the

corporation, the most senior security officer will be very interested in the security risk assessment project. This person can be either the biggest critic or the most ardent supporter of the security risk assessment. Typically, the senior security officer will be a supporter of the security risk assessment effort and may even be the project sponsor.

The most senior security officer will be concerned that the security risk assessment is properly scoped, accurate, and performed by professionals with the appropriate experience and credentials. Many of these concerns can be addressed through proper negotiation and development of the statement of work. The accuracy of the security risk assessment can be ensured through careful data gathering, testing, analysis, and review. The professionalism and credentials of the security risk assessment team can be addressed through the presentation of their résumé's past performance descriptions, and certifications.

Be aware that the most senior security officers will likely have their own set of security controls that they are trying to get adopted within the organization. The security risk assessment can point out the specific benefits of implementing these controls from a security risk-based approach. Therefore, the security risk assessment may be able to give the senior security officer the support needed for upcoming projects, or the security risk assessment may recommend other projects with a larger return on investment (ROI) than the ones currently planned. Be careful to ensure that you gain the necessary information from the security team, but remain objective and credible by forming your own opinions and recommendations.

- **Business Unit Managers**—Organizations divide responsibility for corporate governance among business units. These units may take on various names, such as groups, departments, or divisions. Here they are referred to simply as business units. The business unit will have a single individual in charge—sometimes referred to as the division chief, director, or even department head. Here we shall refer to them as the business unit managers. The business unit manager will be concerned with several factors, including proper understanding of the business unit, accurate security risk identification, clarity and usefulness of recommendations, and cost of implementing recommendations.
  - Understanding the Business Unit—The security risk assessment team will need to ensure that they offer the opportunity for an interview with each of the business unit managers. This interview will give the managers a chance to explain the business unit functions and to voice concerns about existing security risks. Granting the business unit manager an opportunity to explain and voice these concerns will help to ensure acceptance of the results.
  - Accurate Identification of Security Risks—The business unit managers are likely to be among the sharpest critics of security risk results that affect their business unit. This should not be surprising, as security risk results and their accompanying recommendations will affect the business unit manager's budget. The security risk assessment team should take the

necessary steps to ensure that security risk findings are accurate. These steps include the interview with the business unit manager mentioned previously, interviews with other representatives for the business unit, and the ability for each business unit manager to review draft findings of the security risk assessment.

- Clarity and Usefulness of Security Risk Recommendations—A security risk assessment that simply states that the organization is at a certain level of security risk is of little value. The most valuable component of a security risk assessment is a prioritized list of actions that may be taken to reduce the security risk. Unclear, high-level, or ambiguous recommendations such as "increase security staff" offer little guidance to those who need to act on these recommendations. Security risk recommendations need to be clear, unambiguous, and ultimately useful to the customer.
- Cost of Implementing Security Risk Recommendations—Clearly, business unit managers would rather hear that the actions recommended are cheap and easy. But that might not always be the case. The project team cannot and should not artificially reduce recommendation cost estimates for reducing security risk. Although the true cost may lead some segments of the customer population initially to be disappointed in the results, ultimately an underestimate of recommendation costs would lead to a greater disappointment. The security risk assessment team should be straightforward and as accurate as possible when stating the cost of a security risk recommendation.

■ Compliance Officer Legal Department—In many organizations, a security risk assessment is a legal requirement. Organizations with a legal requirement for obtaining a security risk assessment include health-care entities, financial institutions, and government agencies, but could include others as well. In these cases, the individual within the corporation responsible for compliance with these laws or contractual obligations would certainly be interested in the method and results of the security risk assessment.

- Security Risk Assessment Method—The organization compliance officer will be concerned that the security risk assessment will meet the legal or contractual obligations. Some customers may have strict requirements as to the security risk assessment methodology. These requirements will typically state that the security risk assessment must follow certain guidelines or methods that are spelled out explicitly in the governing law or in the contract. The security risk assessment project manager should be familiar with the governing laws affecting the customer and should ask specifically for contracts that have specific requirements for a security risk assessment.
- Security Risk Assessment Team—Although most governing law and contracts will not explicitly call for a specific security risk assessment methodology, there are some indirect requirements on the objectivity and credentials of the security risk assessment team. Several governing laws

call for an *objective review* by *security professionals*. While not stating exact requirements for these terms, the following guidelines could be applied:

- Objective Review—Objectivity requires the lack of real or perceived conflict of interest. Conflict of interest arises when the security risk assessment team has a stake in the outcome of the assessment. Namely, a conflict of interest occurs when the security risk assessment team includes members who have designed, operate, or are in charge of portions of the security program. This includes any element of the security program that is to be assessed; for example, security policies, security awareness programs, security architecture, system hardening, audit log review, physical access control, logical perimeter controls (firewalls, routers), and managed security services. Anyone representing or involved in these functions will have a vested interest in how well they are perceived. This vested interest and the interest in uncovering all flaws that present a security risk to the organization are at odds and culminate in a conflict of interest.

  To some, the exclusion of these members from the security risk assessment team may seem inappropriate or overkill. After all, these members know the systems better than anyone and can identify possible security risks with great efficiency. It is for this reason that, they argue, these members must clearly be involved in the security risk assessment process. While these are valid points, the need to ensure accurate and objective results outweigh any such benefit. These "in siders" should be interviewed, consulted, and possibly even included in many of the discussions that lead up to the findings of the security risk assessment. However, they should not be "voting" members or leaders of the security risk assessment team. In the end, those who make the final recommendations must be objective or the validity and credibility of the security risk assessment will be questionable.
- Security Professionals—The security risk assessment team needs to be composed of members who understand the concepts to be applied in a security risk assessment, needs to bring a measure of expertise to the project, and will act in a professional manner.

  An understanding of the concepts in a security risk assessment is required simply to be a productive member of the team. Without such an understanding, a team member may become lost in the process, misinterpret results, and be unable to be a productive member of the team.

  Some measure of expertise is required from each member of the team. The team will require members who can draw from experience to provide reasonable measurements of threat frequency, impact, and overall security risk. Furthermore, the team should include members with different areas of expertise so that all controls within the scope

of the assessment may be adequately covered. Depending on the scope, the security risk assessment team requires experts in the areas of administrative, physical, and technical controls, physical security, security testing, security policies and procedures, disaster recovery plans, and other areas.

Each member of the security risk assessment team will need to act in a professional manner. This includes showing the proper respect for the customer. Even more importantly, professional behavior requires the ethics necessary to ensure that information uncovered during the assessment will not be misused. Members of the security risk assessment team will uncover vulnerabilities in the customer's system. These vulnerabilities could include external exposure to sensitive company information, account names and passwords, and other vulnerabilities that could pose a severe security risk to the customer's organization if this information is not properly handled and controlled.[1]

- **Technicians, Operators, and Administrators**—These are the people in the organization who are relied upon to maintain and operate security controls. The network administrator is relied upon to apply up-to-date security patches to affected systems; the systems operator maintains user account information; the network engineers set the firewall rules that implement the security policy. All of these people within the organization have a vested interest in the perceived quality of their work. A security risk assessment that results in findings that point out gaps within their area of responsibility may be seen as unjust or unkind. Security risk assessment team members must understand that care must be taken to ensure that all findings are accurate and worded appropriately. Properly worded findings clearly indicate the problem, its potential impact, and how to fix it. Do not point fingers or attempt to place blame. Failure to recognize this population, to ensure that their concerns are addressed, and to carefully word findings could result in an unsatisfied customer. Understand that these people are not typically the direct customer, but the direct customer is influenced by them. Moreover, a security risk assessment team should always strive to be fair and accurate.

3.1.1.2 Quality of Work

The success of the security risk assessment project will be based in large part on the quality of the technical report. After all, this is the project deliverable, and it will far outlast any other tangible evidence that such a project ever occurred.

Most consumers of a security risk assessment will judge the success of the project based on what they see as a result. The result seen by most security risk assessment consumers is the final security risk assessment report. The importance of the real quality of work and the perceived quality of work reflected by this document must be well understood by the entire security risk assessment team.

Information security engineers sometimes lose sight of the objective of their activities. They sometimes give the technical activities of their project precedence and leave little time to complete a quality report for delivery to the project sponsor.

SIDEBAR 3.1 What Do We Sell?

At a previous company I have been known to ask seemingly obvious questions at staff meetings in hopes of uncovering some greater truths. One such question provided our group a useful insight into the needs of our customers and their perceived value of our services. The following question was posed at one such meeting:

"What do we sell?" I asked.

The first answer was rather expected and went down the list of services we offer, such as policy development, security risk assessments, security training, and other services.

"No, what do our customers want to buy?" I asked, hoping the slight rephrase would spark some creative thought.

This rephrased question elicited more of the same descriptions, with only slight changes to the titles we gave them.

"Let's try this another way," I said. "Our customers don't want a security policy; they don't want a security risk assessment; they don't even want security training."

"But they buy our services? Why would they buy them if they don't want them?" answered the team.

"Because our services are a means to an end," I explained. "Our customers want ..."

"Our customers buy our services because they want confidence that they are secure, or knowledgeable, or compliant," the enlightened audience interrupted.

BINGO

It is important to understand that although we, as information security professionals, may be very excited about our techniques, methods, and tools, our customers' expectations do not center on these. Their expectations center on our providing confidence that they are doing the right thing.

The takeaway from this slightly offbeat discussion is that the quality of the security risk assessment project is not solely reliant on the quality of the technical work but also heavily reliant on any element that may influence the confidence of the project sponsor. It is for this reason that correct formatting and spelling in the final deliverable—the security risk assessment report—are just as important as adequate security testing.

Inattention to the details of the final deliverable is unfortunate and short-sighted, and in the end will not accomplish the goal of either party. In the pursuit of obtaining the best configuration for your scanners, getting the most up-to-date threat estimates, and determining the precise words for acceptable-use policy statements given the organizational culture, information security engineers are apt to forget that the consumer of the information security risk assessment really does not care about such details. This is not to say that consumers do not care about quality work; of course they do. It is just that the consumer does not generally care about how the quality work gets done, just that it is quality.

For example, consider having a house built. This process involves a great many professional trades to design your house, install systems, and build to the specifications. The typical consumer of a newly constructed house judges the quality of the house on the result of inspections and a walk-through. Although it is important for the electrician to use the appropriate tools, supplies, and electrical code, the consumer only sees the exposed electrical components (e.g., switches, lights) and the inspection certificate that the system meets the electrical code. If the system did not meet the expectations of the consumer, it would not matter how great the electrician's tools or techniques were; the consumer would be dissatisfied.

Now consider the final security risk assessment report. If the final report contains the name of a previous company the consultant did work for (i.e., a "cut and paste" error), the consumer of the report is likely to lose confidence in the entire project. At this point, it does not matter how good the tools, techniques, and tests were. Many information security engineers would defend this work by saying, "That is just a typo—the results are still right." These engineers would be technically correct, but would also fail to see the importance of the delivery of a quality report.

In general, all consumers care about is that the work they have commissioned is done by professionals, and they care about the quality of the work, but they do not generally care about the details of the tools, methods, and techniques that go into the work. As consumers, we expect that professionals keep up with the latest trends and obtain the appropriate tools for the job. We do not expect to have to be experts in the activities that we outsource.

3.1.1.2.1 Quality Aspects

The consumer of a security risk assessment report includes the "sponsor" of the security risk assessment and additional stakeholders within the organization being assessed. All of these stakeholders have unique points of view and a distinct definition of what they expect from a successful security risk assessment. These were discussed in the previous section. Regardless of the stakeholder role, several quality aspects are universally expected.

General Quality Expected in Any Report—The following is a discussion of the quality aspects that are expected in any report, whether the report is technical or otherwise. These general quality aspects include grammar, format, audience, and understanding of the topic. Each of these is discussed briefly below.

Grammatically Correct—Any correspondence that ever goes to a customer is a representation of the author and the organization associated with the author. A formal project deliverable such as a report, or even a draft report, must be grammatically correct. What the author may consider a small grammatical error may or may not change the meaning of the sentence, but it will make an impression on the reader. As unfair as it may seem, that impression may have as much weight in customer satisfaction as the underlying analysis. Furthermore, grammatical errors involving the customer's name, interviewees' names, system names, and the like are likely to make an even less favorable impression.

Visually Pleasing—Without even changing the words, a report can be vastly improved during document production and the formatting process. Improvements in the formatting of the report will make the report look professional. Reports that look like they have been put together in a hurry do not convey professionalism. Moreover, it is likely that the acceptance of the conclusions of such a report will be subtly affected. When a report looks professional, it also looks more authoritative. The security risk assessment team should appoint one member of the team to produce the report. The report producer should be familiar with techniques to create a professional report. This text does not cover this topic in any detail, but you should expect the report producer to be familiar with the following elements of a professional report:

- Selection of a font
- Consistent treatment of tables, figures, bullets, etc.

- Appropriate styles for headings
- Spacing between paragraphs, graphics, and headers and footers
- Proper use of headers and footers
- Generation of a table of contents and table of figures.

Addresses Its Intended Audience—As discussed earlier in this book, the security risk assessment report is intended for several different audiences. These audiences will have differing levels of familiarity with the project and differing levels of technical expertise. For this reason, the report must be written for several different audiences.

- Executive Summary—The executive summary is written for the audience that wants to know the bottom line. An executive summary should be short and to the point. For a security risk assessment, it should answer the following question: "What are the security risks to my organization, and what should we do about them?"
- Technical Appendices—Technical details and supporting documentation to the security risk assessment report belong in an appendix or even an attached data file on flashdrive or DVD. The more technical readers of the report will want the vulnerability scan details or a list of the user accounts with short passwords. Examples of typical appendices to a security risk assessment report are as follows:
  - Vulnerability Scan—The results of a vulnerability scan run on the systems being assessed.
  - Evidence—A list of evidence used to draw conclusions. This would include interviews, test results, worksheet calculations, etc.
  - References—A list of sources of information and guidance used in the security risk assessment.
  - Solution Descriptions—Additional descriptions on proposed solutions. This could include product literature or a review of available solutions.
  - Calculations—Mathematical calculations supporting the findings.

Understanding of the Topic—It is important that the reader of the report realizes that the security risk assessment team not only knows how to perform a security risk assessment but has a grasp of the relevant background necessary for performing the work. The introduction of the report can be used to reiterate relevant background information, including a description of the organization and the need for the security risk assessment.

General Quality Expected in Technical Reports—Technical reports have their own unique requirements, and the audience reading a technical report has additional expectations. Technical reports, such as a security risk assessment, are expected to contain technical data and draw conclusions based on an assessment of the technical data. For this reason, it is important to ensure that the technical data presented in the report is accurate, the approach is presented and the conclusions are clear.

Technically Accurate—Technical reports are based on technical data. Any inaccuracies in the data could lead to incorrect conclusions. It is important that the technical members of the security risk assessment team review all technical data to ensure its accuracy. This includes removal of false positives in vulnerability scanning and ensuring that account names, system names, and IP addresses are correct.

Approach Described—The security risk assessment approach used by the team should be described in the final report. This has several benefits. First, it gives the report credibility. If the report references and follows a well-known or well-developed approach for performing security risk assessments, then the customer will be less likely to question the methods employed to determine the conclusions. Second, a description of the approach will allow the customer to follow the process and the logic of the analysis more closely, which will allow the customer to provide a better review of the draft report and a better understanding of the process.

Clearly Presented Conclusions—The conclusions of a technical report are the most important element. These are likely the items that will be implemented. It is important that these conclusions be well articulated so that the implementer of the conclusions will know what is expected. For example, it is not very useful to simply recommend that the organization develop security policies. This advice provides little insight or direction and is an indication that the security risk assessment team may not clearly understand how to write security policies. A better recommendation would be a description of the security policies that are currently missing and perhaps an outline of the basic structure for each.

Quality Expected in Security Risk Assessment Reports—A security risk assessment report is a specific type of technical report with its own unique quality requirements. A security risk assessment report is expected to provide a clear and accurate identification of the security risk to an organization's assets. Furthermore, the security risk assessment report is expected to contain adequate and relevant evidence to support its findings, clear and relevant recommendations, and clear compliance results for relevant information security regulations. For this reason, it is important to ensure that the security risk identified in the report is clear and accurate, evidence presented is accurate and relevant, recommendations are clear and relevant, and any compliance results are clearly stated.

Clear and Accurate Identification of Security Risk—The identification of security risk is the basic objective of the security risk assessment. Therefore, it is not surprising that customers would expect an identification of security risk as part of the security risk assessment report. However, it is important to convey the security risk in a meaningful way to the customer. The description of the residual security risk can be presented in a quantitative or qualitative manner, depending on the overall approach of the security risk assessment. In either case, the residual security risk

should be presented in a context that is understandable by the customer. As such, a description should accompany the residual security risk statement, for example, a range for quantitative security risk measurements or managerial description for qualitative security risk approaches.

Adequate and Relevant Evidence—The results of a security risk assessment are recommendations for changes at an organization. Prior to those changes being implemented, the organization will likely scrutinize elements of the security risk assessment report to ensure that the recommendations are well founded. A quality security risk assessment report will contain adequate and relevant evidence for its conclusions and recommendations.

Clear and Relevant Recommendations—Hopefully many of the recommendations from the security risk assessment report will be implemented. Most organizations will have set aside resources to implement the recommendations of the security risk assessment, but these recommendations cannot be implemented if they are not clear, and they are not likely to be implemented if they are not relevant to improving the organization's security risk. The security risk assessment team must ensure that all recommendations are based on relevant data and solid analysis. If it is unclear why the recommendations would improve the security posture of the organization, then the recommendations have not been clearly articulated. Also, the security risk assessment team should include cost and effort estimations for implementing each of the recommendations. Organizations typically require such estimations prior to moving forward with a project.

Clear Compliance Results—For those organizations operating within regulated industries (e.g., health care, energy, government), an analysis as to their compliance with the regulation is useful, if not a requirement of the security risk assessment project.[2] If such an analysis is performed, the security risk assessment report should contain a table that clearly indicates those areas that meet the regulations and those that do not.

3.1.1.3 Completion within Budget

The biggest success factor of any project is whether it is completed on time and within budget. The project leader of the security risk assessment team must manage the project carefully to ensure that the project is completed within the time allotted and with the resources granted. Any project not completed within time or budget constraints is in danger of being canceled or completed too late to have an impact. Moreover, a project with significant overruns is typically an indication of the project team's inexperience.

The goal of completing within budget is not limited to outside consultants performing a security risk assessment. This goal applies equally to internal security risk assessment projects. In either case, the project has been granted a limited amount of resources (e.g., time, money) and must be completed within those constraints.

Project leaders of security risk assessments must ensure that they meet this most important quality aspect of their project.

3.1.2 Setting the Budget

One of the biggest gating factors for scoping a security risk assessment is how much is in the budget for the security risk assessment. If no such line item exists in the budget, consider how much you plan on spending. Exact figures are not required here, but there is a huge difference in the scope and rigor of a $450,000 security risk assessment and a $45,000 one. The fact is, the more time that the team spends reviewing the security controls, the more rigorous the security risk assessment will be. So if you plan on spending over $250,000 on a security risk assessment, then you would expect (and demand) more rigor than if you wanted to keep the cost down to less than $50,000.

In addition to the rigor of analysis, the amount of money you plan to spend on the security risk assessment will also be affected by the size of the organization, the geographical separation of organizational elements, the complexity of the security controls, and the threat environment in which your organization operates.

Organization Size—A small organization, up to 500 employees, is likely to have many factors that simplify a security risk assessment. The organization structure is likely to be relatively simple and centrally located. This brings down the cost/effort in obtaining interviews with key personnel and gaining approval for testing and access to information. A small organization is also likely to be more centralized and to have fewer complex controls, which may reduce the effort required to assess their effectiveness. A larger organization is more likely to have a more complex organizational structure, and decentralized and complex controls.

Geographic Separation—If your organization has just one location, then the effort to gather the information required to perform the security risk assessment is significantly reduced. An organization with multiple sites and geographically separated systems and key personnel will require additional funds for travel and information gathering.

Complexity—The more complex the security controls, the more effort is required to assess their effectiveness. For example, an organization with physical access controls that include perimeter barriers, armed guards, biometrics, a closed-circuit television (CCTV) system, zoned areas, smart-card badge access, and multiple types of intrusion detection is going to require some effort to effectively review. An organization with a more simple physical security control that includes locked doors and visitor control will clearly require less effort.

Threat Environment—Certain organizations operate within a higher security risk environment than others. For example, a high-profile and controversial national lobbying organization will clearly be exposed to a greater number of

serious threats than the headquarters of a nationally franchised sandwich shop. A security risk assessment for an organization existing within a more serious threat environment will require more careful consideration of the threats. An organization existing within a less serious threat environment is likely to be affected by the standard array of threats that affect most organizations.

The other factor to consider for scoping a security risk assessment is the size of the overall information security budget. An organization should plan to spend only a portion of their overall security budget on an assessment. This sounds rather obvious, but it remains overlooked by many organizations. Consider an organization that spends nearly its entire information security budget in a given year on a widely scoped and rigorous security risk assessment and has little or no budget left to fix anything. A main benefit of a security risk assessment is to provide guidance for security risk–based spending, so that ultimately the security risk to the organization is lowered to a reasonable level. If the entire budget is spent on a security risk assessment, the organization may be unable to implement any of the recommendations. The result is that the organization is more aware of their security risks, but their assets are in the same danger as before.

A better approach is for the organization to determine a percentage or ratio of the budget that should be spent on the security risk assessment (see Figure 3.1). As with many elements of establishing and maintaining an information security program within an organization, there is no well-known or accepted ratio or percentage. Furthermore, it is not recommended that such a ratio or percentage be the only factor in determining how much to spend. However, an organization should carefully review their budget allocation if they are spending more than 25 percent of their security budget on a security risk assessment.

3.1.3 Determining the Objective

A security risk assessment can provide many possible benefits: a basis for risk-based spending, a periodic review of the security program, and a part of a system of checks

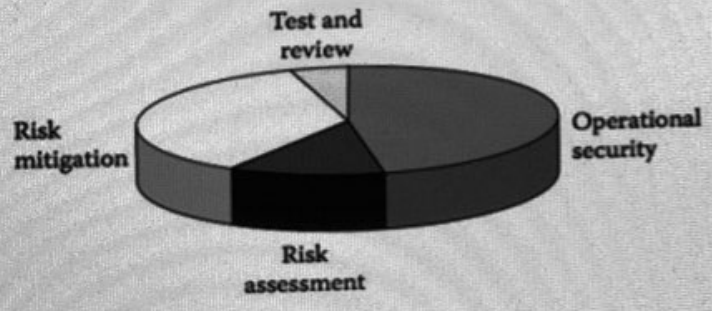

Figure 3.1 Security spending ratios. The exact spending ratios for elements within a security program will differ greatly among organizations. However, the relative spending ratios shown here are likely to be applicable to most organizations.

and balances for sensitive tasks. Understanding and documenting the objective of a specific security risk assessment helps to focus the project on meeting the needs of the organization. The core aspect of a security risk assessment remains an analysis of the effectiveness of the current security controls that protect an organization's assets. This is the objective of the security risk assessment.

> Security Risk Assessment Objective—accurate analysis of the effectiveness of current security controls that protect an organization's assets.

Most organizations simply want an objective review of their controls. This may be provided by an independent team of security professionals who understand the security risk assessment methodology, possess the proper experience and credentials, and are provided the resources to adequately perform the assessment.

3.1.4 Limiting the Scope

The scope of the security risk assessment is the boundary of the security controls and assets included in the review. The definition of what is "in" and "out" of the scope of the assessment may be rather easy in some organizations but more difficult in others. In either case, the project sponsor and the security risk assessment team should carefully and clearly define the scope of the assessment in terms of the security controls to be reviewed, the assets to be protected, and the system boundaries of the security risk assessment target.

Every security risk assessment is limited: limited by budget, limited by time, and so forth. Project members of a security risk assessment will constantly find themselves reaching the limitations of the project. After all, could we not all do more in-depth analysis, more insightful recommendations, and more accurate risk measurements given unlimited time and money? But, no matter how much time or budget or skill is possessed by the security risk analysis team, if a security risk exists outside the boundaries of the security risk assessment, it will not be documented in the security risk assessment.[3] The single biggest limitation of a security risk assessment is the definition of the system being assessed.

The boundaries of a security risk assessment are determined by the sponsor of the security risk assessment. Identifying the security risk assessment boundaries is essential for the security risk assessment team to ensure that neither underscoping nor overscoping occurs.

3.1.4.1 Underscoping

Underscoping of a security risk assessment is a dangerous practice that can happen all too often. It occurs when the security risk assessment team does not address all security concerns of the sponsor. The term *underscoping* is from the perspective of the security risk assessment team and not the project sponsor. In other words,

the security risk assessment team is not addressing the needs of the project sponsor because some of the organization's assets and relevant threats are not assessed within the security risk assessment.

Underscoping typically results in high-risk items left unaddressed and, eventually, exposure of the organization's assets. Consider the following common scenario: An officer of a financial institution recognizes that his organization is legally required to comply with the Gramm-Leach-Bliley Act (GLB Act). The GLB Act clearly requires a security risk assessment among other information security requirements. The organization hires Fly-By-Nite Security[4] to perform what they call a security risk assessment. Fly-By-Nite Security only knows how to run a vulnerability scan, but they have found that these services sell much better when they call them security risk assessments. The officer of the financial institution is unknowingly underscoping his security risk assessment by declaring (again unknowingly) administrative, physical, and most other elements of technical controls out of bounds for this assessment.

Although this example is a little extreme, similar problems can exist simply from dismissing other elements of a security risk assessment without ensuring that they are covered elsewhere. For example, it is relatively common in many organizations for physical security to be considered beyond the bounds of a security risk assessment. If the physical security controls are reviewed as a part of a separate security risk assessment, there is little to be worried about. However, if the physical security of an organization is ignored by all security risk assessments within the organization, then serious breaches in the security of multiple systems could occur. What good is writing the perfect firewall rules if a thief can walk away with the box?

3.1.4.2 Overscoping

Overscoping of a security risk assessment is dangerous as well. Overscoping occurs when the security risk assessment team assesses threats, vulnerabilities, or security risks that are outside the bounds of the security risk assessment. The term *overscoping* is from the perspective of the security risk assessment team and not the project sponsor. In other words, the security risk assessment team is assessing organizational assets and threats that are beyond the needs of the security risk assessment sponsor. If a project sponsor fails to clearly indicate the bounds of the security risk assessment, the team may perform activities that end up wasting time and money. Another danger of overscoping is that the security risk assessment team may overstep its authority to test elements of a system that are not covered under the security risk assessment. Such out-of-bounds behavior could, by itself, be a serious breach of security. Consider the following out-of-bounds activities allowed by the practice of overscoping:

Example 1: What's in a Name?—Fly-By-Nite Security is hired by the XYZ organization to test the security of its Web site. Fly-By-Nite Security obtains permission from XYZ to perform security testing, but the XYZ organization fails to properly scope the test and simply asks for a "zero-based" review. When

Fly-By-Nite Security performs its research, it finds www.xyz-org.com and www.xyz_co.com. When performing the security testing of these Web sites, Fly-By-Nite unknowingly performs security testing on both the XYZ organization (www.xyz.com) and the unrelated XYZ Manufacturing Company (www.xyz_co.com). Depending on the level of testing performed, Fly-By-Nite could end up on the wrong end of a lawsuit or criminal prosecution.

Example 2: Take Out the Trash—Fly-By-Nite Security is again hired by the XYZ organization, but this time to perform a security risk assessment at their physical location. The project manager believed that the assessment would cover only the information security systems, but the industrious Fly-By-Nite employees diligently searched the trashcans for sensitive information, checked the security of the doors to sensitive areas, and reviewed the visitor and escort procedures. The security risk assessment sponsor was disappointed that the Fly-By-Nite team spent so much time "off task," since physical security is controlled by another department altogether that had just completed an assessment the previous month. Although this behavior did not trample on another organization's assets, it still wasted time and money, and it diverted analysis from within the intended boundary of the security risk assessment.

3.1.4.3 Security Controls

An organization may have implemented a wide variety of security controls to protect its assets. These security controls can range from policies and procedures to lighting and fences to firewalls and anti-virus solutions. Rather than list these controls one after the other, it is useful to group these controls into the categories of administrative, physical, and technical. These groupings provide a common approach to define or limit the scope of the security risk assessment.

3.1.4.3.1 Administrative Security Controls

These are defined as policies, procedures, and activities that protect the organization's assets. Policies include the information security policies such as acceptable-use policy, system-monitoring policies, and security-operations policies. Procedures include emergency-response procedures, computer incident response procedures, and procedures for hardening and testing the security of servers, for example. Activities include any activity performed to ensure the protection of the organization's assets. These could include activities requiring "technical" expertise, such as audit log review or penetration testing, or "nontechnical" activities, such as exit interviews for terminated employees. Administrative controls should be within the scope of any security risk assessment. An assessment that does not include these types of controls should be referred to as security testing or a limited assessment instead, as it would not give an accurate measurement of the security risk to the organization's assets.

3.1.4.3.2 Physical Security Controls

Physical security controls are those controls that are associated with the protection of the organization's employees and facilities. These protection measures include facility perimeter controls such as fencing, lighting, gates, and access controls; surveillance such as guards and CCTV; facility protections such as seismic bracing and fireproofing; and personnel protection such as evacuation procedures and patrolled parking lots.[5]

3.1.4.3.3 Technical Security Controls

Technical security controls are those mechanisms that logically protect the organization's assets, such as routers, firewalls, anti-virus solutions, logical access controls, and intrusion detection systems. A security risk assessment should consider the capabilities of the technical security controls, their current configuration, and their arrangement within the system to provide protection of assets (i.e., system architecture).

3.1.4.4 Assets

An organization has numerous assets of value that warrant protection. Assets are defined as the resources by which the organization derives value. These can include hardware, software, systems, services, documents, capital equipment, personal property, people, goodwill, trade secrets, and many other elements of the business process. Although it is clear that many factors create value for an organization, it is not always easy to define its assets. An attempt to simplify the enumeration process includes discussing both tangible and intangible assets.

3.1.4.4.1 Tangible Assets

Tangible assets are those assets that you can "touch." These assets include hardware (or equipment), systems, networks, interconnections, telecommunications, wiring, furniture, audit records, books, documents, cash, and software. However, the number one tangible asset is always people (employees, vendors, customers, guests, visitors, and others). These assets tend to be easier to list because they are visible and perhaps even accounted for in auditing records or asset-tracking systems.

3.1.4.4.2 Intangible Assets

Intangible assets are those that you cannot "touch." These assets include employee health and safety, data, customer and employee privacy, image and reputation of the organization, goodwill, and employee morale. These assets tend to be rather difficult to list or enumerate, as they are not visible or accounted for. Nonetheless, an organization must seek to protect these intangible assets as well.

3.1.4.5 Reasonableness in Limiting the Scope

As discussed previously, not all security controls or assets may be within the scope of the security risk assessment. Although, as security professionals, we typically like to see the security risk assessment process not being hindered by a smaller scope than is warranted, there are a variety of adequate reasons for limiting the scope of a security risk assessment.

Many organizations rely on other entities to supply some of their infrastructure components. These supplied components could be physical security within a shared tenant building or an outsourced managed security service. If the security risk assessment team or the customer decides that an assessment performed by another team that covers the supplied component meets their needs, they may decide to adopt the findings of that report or to place the supplied components outside the scope of the security risk assessment.

In the following example, some of the network components and the procedures for clearing individuals are considered outside the scope of the security risk assessment. For this example, the customer determined that the clearance process for personnel with SECRET clearances was outside the scope of the evaluation for an information system on a single military base. Furthermore, the customer decided that the system boundary did not include the MILNET or the firewalls connecting the MILNET to the information system being assessed; these components were considered part of another evaluation.

Many other scope combinations and limitations are common in the industry. Common security risk assessment scopes include geographic, functional, and technology limitations. Other scope limitations have restricted the scope of the security risk assessment to tangible assets only and excluded the organization's reputation and goodwill.

3.1.5 Identifying System Boundaries

It should now be clear that the failure to properly scope a security risk assessment can have disastrous consequences. One important element of scoping a security risk assessment effort is to identify the system (or systems) being assessed. An information system is any process, or group of related processes, under a single command or management control that reside in the same general operating environment. The information system comprises the processes, communications, storage, and related resources necessary for the information system to operate.

Even though a security risk assessment may be limited to a single business unit, the information systems within that business unit may be one or many. Each information system to be assessed should be properly identified by explicitly stating its physical and logical boundaries.

3.1.5.1 Physical Boundary

Identifying the physical boundaries of an information system (or systems) to be assessed limits the scope of the security risk assessment. Such a limitation is appropriate, as security risk assessments should be limited to those resources under the control of the project sponsor. Besides, a system without boundaries cannot be assessed.

The physical boundaries of an information system properly identify those elements within the scope of the evaluation and those outside of the scope of evaluation (see Figure 3.2). Physical boundary elements include the following:

- Workstations
- Servers
- Networking equipment
- Special equipment
- Cabling
- Peripherals
- Buildings
- Individual rooms or floors within buildings

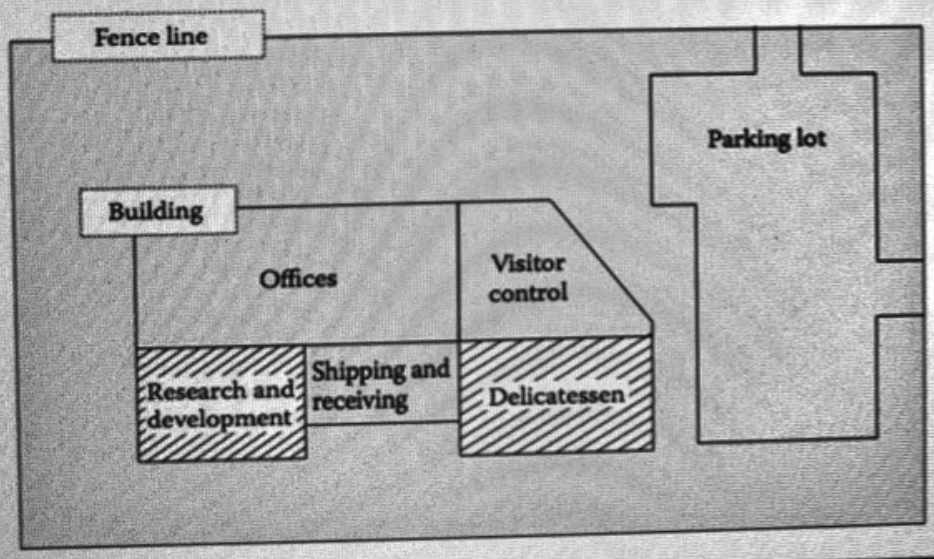

Figure 3.2 Physical system boundaries. It is important to properly identify the physical elements that are inside and outside the security risk assessment boundary. This diagram shows the physical elements inside the physical boundary by shading the covered elements.

3.1.5.2 Logical Boundaries

Identifying the logical boundaries of an information system (or systems) to be assessed also limits the scope of the security risk assessment. A limitation in scope based on logical boundaries is also appropriate, as security risk assessments should be limited to those system functions under the control of the project sponsor.

The logical boundaries of an information system properly identify the functions of the systems within the scope of the evaluation and those functions outside the scope of evaluation. The determination as to the inclusion or exclusion of system functions in the scope of the security risk assessment must be carefully considered.

By default, the logical boundaries of a security risk assessment should be inclusive of all functions within the information systems identified (see Figure 3.3). A reasoned approach for excluding certain functions should be executed. Specific reasons for the exclusion of system functions should be documented by the project sponsor or the security risk assessment team, and the identification of these functions should be included in the security risk assessment report. Specific reasons for the exclusion of system functions should accompany this discussion. The project sponsor and the security risk assessment team should refrain from excluding important system functions and should only exclude functions for good reason. Below

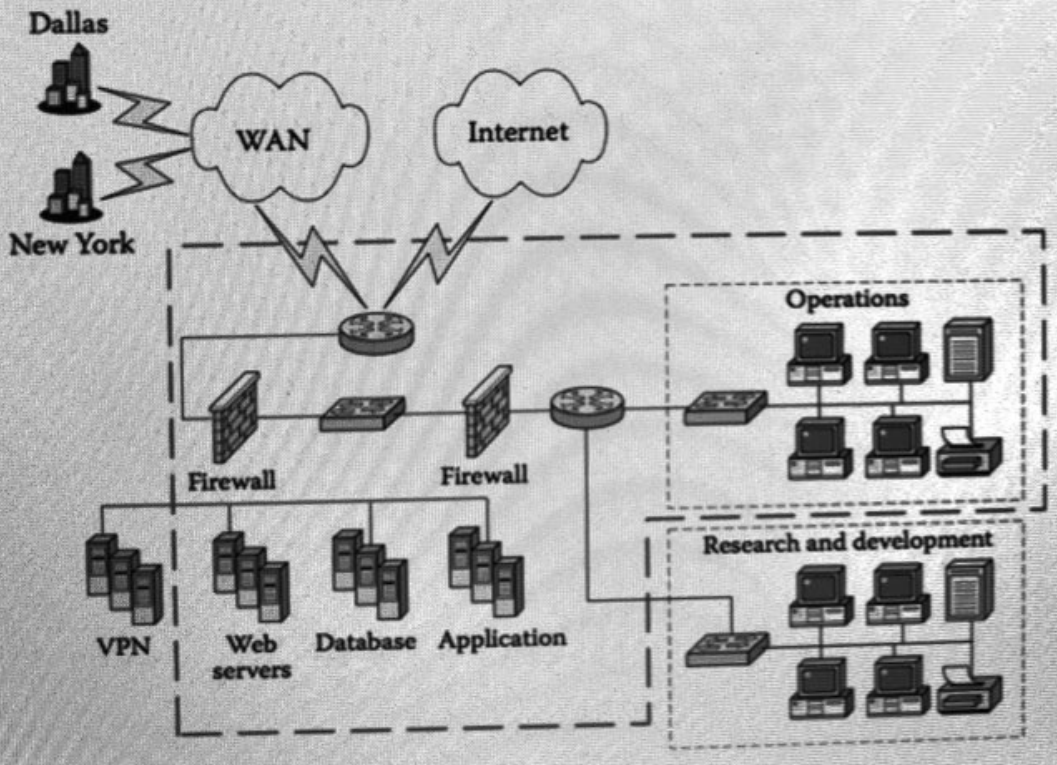

Figure 3.3 Logical system boundaries. It is important to properly identify the logical elements that are inside and outside the security risk assessment boundary. This diagram shows the logical elements inside the logical boundary by the longer dashed line surrounding the covered elements.

are some possible reasons why a system function might be excluded from a security risk assessment:

- Function Is Not Security-Relevant—Some system functions (or applications) are not relevant to a specifically targeted security risk assessment. Such nonrelevance should not be confused with nonimportance. For example, a word-processing application or a custom application for creating and submitting timecards may not be security-relevant and can be safely ignored in a security risk assessment. Most word processors operate on behalf of the user who called the program and do not operate in a privileged state. In this case, the worst the word processor can do is mangle your document, but it cannot breach the confidentiality of a document owned by another if such access is restricted. In the same manner, a custom timecard application running with user privilege would be restricted from breaching confidentiality of other files as well. However, be careful in your analysis if either of these programs is relied upon to enforce a security function, such as the integrity of the timecard file; in that case, the function of the application would be considered security-relevant.
- Function Is the Subject of Another Assessment—Even security-relevant functions may be excluded from a specific security risk assessment if they are the subject of another security risk assessment. This happens often in larger organizations in which multiple security risk assessments are performed on subsets of all of the organization's information systems. For example, if all applications rely on the services provided by an organization's Internet Data Center (IDC; e.g., power, Internet connectivity, backup, firewall, intrusion defection system), then it may be beneficial for the organization to have a security risk assessment on the IDC itself. The results of the IDC security risk assessment would then be shared with the business unit managers in charge of each of the applications. The applications may be the subject of another security risk assessment, but in this case it would not be necessary to reperform the assessment on those services provided by the IDC.[6]
- Analysis of the Function Is Beyond the Skills of the Assessment Team—This sounds like something you would typically like to avoid, but it is not as bad as it seems. It is not uncommon for security risk assessments to be scoped according to the rigor requested by the organization. Scoping of the security risk assessment can include security-relevant functions that require specific skills not within the experience of the security assessment team. For example, many security risk assessments do not include the code review or penetration testing of Web applications. It is clear that many Web applications (if not all) are security-relevant. However, the skills required to review code for common errors is not possessed by all security risk assessment teams. It may be beneficial to "carve out" that portion of the assessment and bring in the experts.[7]
- Physical or Environmental Control Makes the Function Non-Security-Relevant—Ensuring that security functions are enforced does not always

have to be satisfied by logical means. Physical or environmental controls may adequately enforce security functions and therefore obviate the need for analysis of that function. For example, protection of the confidentiality and integrity of information while in transit on the internal local area network (LAN) is certainly an important security function. However, if the internal LAN is physically protected (e.g., encased in pressurized conduit), then other logical controls to protect that information in transit are not required and therefore not relevant to the assessment.

3.1.6 Specifying the Rigor

Any team of security engineers could spend as little as a week or as much as six months assessing the ability of the organization's security controls to protect its assets. A quick assessment that lasted only a single week would be forced to review the security controls with less rigor, while a security risk assessment scheduled for six months could afford to perform a more in-depth review of the existing security controls.

An organization and the security assessment team will need to determine the appropriate rigor for the security risk assessment. While available budget could certainly limit the extent of the security risk assessment, it is not necessary to simply spend the available money. In fact, from the point of view of the security risk assessment team hired to perform the security risk assessment, this may be considered unethical. The determination of rigor should instead be based on the maturity of the security program.

One way to determine the required depth of analysis is to consider the perceived strength of the existing controls or the maturity of the organization's security program. If an organization would not be surprised if the security risk assessment resulted in the listing and description of many high-risk items, then it is not ready for the "white-glove test." A less rigorous security risk assessment on a less than mature security program will result in nearly the same recommendations. Therefore it is unwise and wasteful to spend money or perform a security risk assessment that simply increases the certainty of what was probably already known within the first several weeks of the security risk assessment. For example, if an internal vulnerability scan of a representative sample of workstations reveals that none of them is hardened, then it is unnecessary to continue to perform vulnerability scans on the remaining workstations. The conclusion that hardening policies are nonexistent or ineffective is already formed, and additional vulnerability scanning adds nothing to the analysis.

3.1.7 Sample Scope Statements

As discussed previously, the creation of a proper scope statement is an important step in defining the security risk assessment project. A proper scope statement will specify the budget, objective, target system(s), and the rigor of the assessment. Table 3.1 shows an example scope statement that provides the information

Table 3.1 Sample Scope of Work Statement

The scope of the assessment includes all the physical premises at 1313 Mockingbird Lane, the automated information systems (AISs) located on premises, the employees of ACME, all users of the AISs located on the premises, and all policies and procedures governing AIS users and ACME employees. Examination of proximate facilities and systems will only be done in reference to ACME.

The security risk assessment includes consideration of risks related to the following:

Threats

- Natural disasters, including fire, flood, earthquake, windstorm, and snow/ice storm
- Authorized personnel, including insufficient or unqualified personnel, insufficient personnel training or supervision, and malicious insider activity
- Unauthorized personnel, including hackers, script-kiddies, competitors, thieves, and vandals
- Malicious software, including viruses, worms, Trojan horses, and backdoors

Assets

- Personnel, including ACME staff and guests
- Computer systems, including databases, system software, hardware, network communications, and application software for existing and new implementations
- Data, including data in transit and storage; hard copy or soft
- Equipment, including capital equipment, laptops, and office equipment

Controls

- Existing countermeasures; safeguards already in place to address risks
- Security awareness and communication, including insufficient security awareness and communications, unclear assignment of security roles and responsibilities, and insufficient security plan documentation
- Data controls, including insufficient controls for data integrity, data retention and backup (short-term and long-term), system access, and system logging/auditing
- Maintenance controls, to include those for preventive maintenance, hardware failures, and remedial maintenance
- Physical and logical access controls

(Continued)

Table 3.1 Sample Scope of Work Statement (Continued)

- Systems architecture, including previous analyses of architecture in regard to security
- History of security and disaster incidents at the facility and the surrounding area.
- The security risk assessment analysis shall include a review of the effectiveness of security controls, including the following tasks:
  - Policy and procedure review
  - Organizational structure review
  - Social engineering
  - War dialing
  - Vulnerability scanning
  - No penetration testing
  - Application vulnerability scanning (but not application penetration testing or code review)

necessary to properly define a security risk assessment project. A statement of work for a security risk assessment should clearly define the threats, assets, controls, and tasks of the security risk assessment.

3.2 Project Description

Once the project is properly defined in terms of budget, objective, rigor, and scope, the project should be properly described in the project contract or description.

3.2.1 Project Variables

All of the variables listed above influence each other. It is not possible to perform the most widely scoped security risk assessment in the most rigorous fashion for the lowest price. The level of rigor and scope of the assessment, as well as the objective of the assessment, all influence the price and vice versa.

The customer should decide on the appropriate "values" for these project variables for their needs. Herein lies the problem. Many customers are obtaining a security risk assessment from an outside vendor because they are not experts in assessing information security, and they want an outside opinion. So, if they are not experts, how are they supposed to know the appropriate values for these project variables? The typical answer is, "Let the experts tell you."

To the customers in this situation, I have the following advice: Be careful of sole-source bids. Obtain several bids from several different companies. These bids should

explain as best as they can the level of rigor for the assessment. Note that the approach of sole-sourcing may be a responsible approach if you are working with a trusted partner.

3.2.2 Statement of Work

The statement of work (SOW) is a portion of the contract that specifies the work to be performed. This may be as simple as a single paragraph or as complex as a multiple-page document covering the expectations and the bounds of a security risk assessment. Regardless of the length or complexity of the SOW, it should document the parameters of the security risk assessment to be performed. At a minimum, these parameters should include the service description, scope of the assessment, and description of the deliverables.

3.2.2.1 Specifying the Service Description

A security risk assessment should be clearly defined in the statement of work. There should be no confusion as to whether this service is a vulnerability scan, penetration test, compliance audit, or security risk assessment. Using our definition above, the security risk assessment should be defined as

> A probability determination of asset losses based on asset valuation, threat analysis, and an objective review of the effectiveness of current security controls.

A more complete service description would include the more detailed definition of the security risk assessment. This can best be accomplished by briefly describing the elements of a security risk assessment. By adding the following sentence, the definition of a security risk assessment becomes even clearer:

> The security risk analysis shall consist of an identification of tangible and intangible assets under protection, an identification of the threats to and vulnerabilities of the current system controls, an analysis of the threat/vulnerability likelihood, the impact of the threat to the identified assets, and recommendations for security controls to mitigate the security risks.

3.2.2.2 Scope of Security Controls

The statement of work should further describe the scope of the security risk assessment by clearly stating if administrative, physical, and technical controls are included in this assessment. Physical boundaries are typically defined by building address. If various elements of the physical controls are handled by different organizations, it may be necessary to provide further refinement and identification of the physical controls to be reviewed. For example, if an organization is located within a shared facility, the building grounds, security force, and building entry

control may not be under the control of the organization seeking the assessment. Furthermore, this organization may not be able to grant sufficient access for the security risk assessment team to effectively assess the adequacy of these controls. Either the organization should obtain permission and adequate access for the security risk assessment team, or they should request the organization that does control the building's physical security controls to obtain and share an objective security risk assessment covering those elements.

Administrative boundaries are typically defined by a description of the policies and procedures covered by the assessment. The complete set of policies that impact the administrative security controls within an organization can very often be owned by various departments within the organization. For example, a complete set of security policies will likely include policies from human resources, legal, help desk, network administration, business development, and operations. Moreover, many policies and procedures may be implicit, that is, practiced but not documented. It is important to specify all policies and procedures to be considered in the assessment.

Technical boundaries are defined as the systems, communication devices, and networks that are to be assessed. These boundaries are typically defined by system and network names. Often some systems or system components are determined to be outside the boundaries of a security risk assessment by the organization. Reasons for ignoring portions of the systems can range from recent reviews having been conducted, to control by another organization, to a planned rollout of new controls. Be sure to clearly identify all technical elements as either within scope or out of scope, e.g., modems, VPN (virtual private network) pool, wireless networks. The technical boundaries of the system are best described in a well-labeled system diagram.

3.2.2.3 Specifying Deliverables

The deliverables for a security risk assessment always include the security risk assessment report. Other deliverables may be various drafts of the report, risk calculation worksheets, interview notes, etc. An SOW can go to great lengths to describe a security risk assessment report, but it simply contains four major elements. To be valuable to the customer, security risk assessment reports should clearly document the security risk assessment process, results, recommendations, and evidence.

The security risk assessment report should describe the process or methodology used in the security risk assessment. The description of the process should be no more than a few pages. The security risk assessment methodology description provides the reader with the confidence that an adequate methodology was used and gives a roadmap to understanding the results. Many security risk assessment results may seem coded. For example, the security risk assessment may conclude that there exist 8 level I risks and 14 level II risks. Without a description of how these security risk levels were determined and what they mean, the security risk assessment report is less useful.

The security risk assessment report should also have a section that clearly presents the results. This section should be understandable by the senior manager and the technical readers. The results section should include a title or short description of the security risk, an indication of its likelihood and impact, a resultant level of the security risk, and a recommendation for mitigating the security risk.

The recommendations in the security risk assessment report should be described in enough detail that those who decide to implement them understand what is requested. This is not to say that the recommendations should provide step-by-step instructions for implementing the change, just enough that it is clear. For example, instead of saying "Improve logical perimeter security," state "Perimeter security should be improved through the addition of firewalls on all external interfaces and the development of a DMZ (demilitarized zone) architecture."

Many times, the results of a security risk assessment are questioned by members of the organization who commissioned the assessment. The security risk assessment team should keep careful notes and collect evidence to defend its findings. Evidence includes documents, interviews, and the results of inspections and testing. Evidence notations need not be elaborate. A simple notation such as "interview with Bob Smith, system administrator, on March 16, 2010" should be fine.

SIDEBAR 3.2 Negotiation

Coming to an agreement of terms and documenting the agreement for a security risk assessment effort requires negotiation skills. Negotiation skills can be learned in many different forums, including business school and professional education. Describing these skills is beyond the scope of this book, but the major elements required to adequately negotiate are described here:

Understanding the Customer's Needs—Negotiation is a process of discovering the needs of others and modifying the arrangement in an attempt to meet everyone's needs. Negotiation cannot even start until the customer's needs are understood. The possible needs for a security risk assessment are numerous and should not be assumed. It is far too easy to assume that a customer simply wants a security risk assessment to identify the possible security risk to the organization's assets.

Identifying Next-Best Alternatives—An important concept in negotiations is being aware of the other party's next-best alternative. The next-best alternative for the contracting organization is typically your competition or even an in-house effort. Understanding the market and the competitive advantages of the competition is essential to the consulting firm in contract negotiations. The next-best alternative for the contractor is typically other consulting work. Having a good understanding of the consulting firm's utilization rate, current backlog, and sales pipeline is useful to the contracting organization in contract negotiations.

Finding Win–Win Solutions—If the negotiating parties are able to discuss the needs of each organization, many win–win situations can occur. Negotiating parties often assume that the other party's desires are in conflict with their own. If the negotiators are able to open up the discussion, many discoveries regarding mutual and complementary needs can be uncovered. For example, after some open discussion, many parties find that the concerns of each party are not solely focused on money. Issues such as time to start and complete the project, individuals assigned to the project, details of the report, and ability to follow up with assessor long after the report are complete typically. These issues are important to the customer organization and typically are easy for the consulting organization to arrange.

Giving a Little More than Was Negotiated—Even after a negotiated contract, the consulting organization should strive to give more than is expected. Look for opportunities to

impress the customer by taking on additional research, providing links for more information, comparing results to named competitors or industries, or other items that may be especially appreciated.

3.2.2.4 Contract Type

The direction of the negotiation depends directly on the type of contract. Contracts can be either a firm fixed price or based on time and materials. The difference between these two types of contracts is a matter of who is taking the risk.

3.2.2.4.1 Time and Materials Contract

In a time and materials contract, the risk belongs to the contracting organization. The contracting organization and the contractor come to an agreement as to an estimated number of hours required to complete the security risk assessment. If the security risk assessment comes in at the estimated amount of time, then all is fine. If the security risk assessment takes more time than expected, then the contracting organization can decide whether they would like the contractor to continue or not. If the security risk assessment takes less time than expected, then the contracting organization pays less than expected. The risk and reward (less likely) belong to the contracting organization.

Variations and other measures exist, such as a "not to exceed" limit, but the time and materials contract still places the risk on the contracting agency, because the real deliverable here is hours. If the contractor delivers hours toward the development of the security risk assessment report, then, according to the contract, the contractor should be paid even if the report is not quite finished. Time and materials contracts are well suited for tasks where it is difficult to define the task up front or if there may be considerable unknowns. It is a rare case when a security risk assessment is best suited for a time and materials contract.

3.2.2.4.2 Firm-Fixed-Price Contract

In a firm-fixed-price contract, the risk belongs to the contractor. The contractor and the contracting organization come to an agreement as to the description of the project and the price to be paid when the project is complete. If the security risk assessment is completed for the effort expected, then all is fine. If the security risk assessment takes more effort than expected, then the contractor must continue to expend effort until the project is complete to the satisfaction of the contracting organization within the definition of the contract. If the security risk assessment takes less effort than expected, then the contractor still gets paid the originally agreed price. The risk and reward belong to the contractor.

In a firm-fixed-price contract, the description of the deliverables is very important. The completion of the project is completely defined by the description of the deliverables. Because the scope and level of rigor for a security risk assessment are

so difficult to describe, most contracting organizations do not want to own the risk in the contract. Therefore, most security risk assessments are performed as a firm-fixed-price effort. Both parties would be well advised to carefully describe the deliverables in the contract. To clarify understanding here, it is recommended that both parties review a sample deliverable from a previous similar effort.

3.2.2.5 Contract Terms

First, let us assume that the security risk assessment is a firm-fixed-price contract. Negotiation is the process of determining the needs of each party and coming to an agreement that comes as close as possible to meeting the needs of both parties. In order to negotiate, you must first understand the other party's needs and their next-best alternative.

3.2.2.5.1 Determining Needs

The contracting organization wants a quality security risk assessment performed by an objective and experienced team that results in an accurate security risk assessment report with clear and effective recommendations. The contractor wants to be fairly compensated for his work. From a contractor's point of view, he is just as happy to perform a three-week-long security risk assessment as a six-month-long one.[7] As you can see, the needs of the contractor are rather simple. Given an accurate description of the security risk assessment required by the contracting organization, the contractor simply wants to be compensated for the effort required to complete the task. The definitions of the scope, rigor, and overall level of effort of the security risk assessment are all in the contracting organization's court.

The contracting organization should clearly describe the scope of the security risk assessment. The remaining factors of rigor and overall level of effort can be difficult to describe. Most requests for proposals (RFPs) that go out fail to address the level of effort or rigor expected. As stated previously, a description of the security risk assessment that mentions only the scope of the project can be interpreted in many ways. A team could spend as much as six months on a rigorous assessment and as little as a few weeks on the same project at a much higher level. The level of rigor required by the contracting agency should depend on their needs and their budget, both discussed earlier in this section.

The most direct way to describe the level of rigor is to simply state how long the contractor think it would take a team to perform the assessment. For example, "The level of rigor on the assessment should be consistent with a team of three experienced professionals spending four weeks gathering data, interpreting the results, and producing the report." Of course, not all teams will take the exact same amount of time, but at least now both the contracting organization and the contractor are all in the same ballpark. This will provide a much better understanding of needs and make negotiation much smoother.

3.2.2.5.2 Determining Next-Best Alternative

Many approaches to better negotiation discuss the benefits of understanding the next-best alternative available to the other party. Understanding the next-best alternative for both the contracting organization and the contractor can help to ensure a smooth negotiation process.

The next-best alternative to a contracting organization is the "next-best" contractor. The next-best contractor is likely very close in terms of quality and price to the preferred contractor. Contractors should be aware that there are many qualified companies waiting in line to take the job if negotiations break down. However, there are some exceptions that must be explored when determining the value of the next-best contractor:

- Familiarization—The preferred contractor may stand out above the crowd if he possesses a unique familiarization with the contracting organization's systems or the technology deployed. Familiarization is both an advantage and a disadvantage and, as such, may either increase the value of the familiar contractor or actually decrease the value. On the one hand, a familiar contractor is able to spend less time and effort in learning the organization's systems or specific technology. This ability will allow the contractor to perform a similar security risk assessment for a little less money than an otherwise equally qualified competitor. On the other hand, the familiar contractor may no longer be independent and possibly has lost the ability to be objective. A contractor who has developed the systems to be assessed or who sells the technology being used fails to be objective. If familiarity with the systems comes from actually developing them, or if familiarity with the installed technology comes from being a vendor for the technology, then the case for loss of objectivity seems rather clear. A contractor, no matter how well meaning, cannot objectively review his own work or technology upon which he relies for his financial reward. If, however, familiarity with the systems and technology comes from other experience with the client or the technology, then the contractor could successfully argue that he can remain objective. To the extent that the preferred contractor remains objective despite this familiarization, that contractor could be a much better choice than the next-best alternative.
- Expertise—Contractors possessing expertise within the organization's industry, with the specific security risk assessment requirements, or with the activities to be performed with the security risk assessment have a distinct advantage when it comes to delivering the best value to the organization.

  Industry Expertise—Many industries, such as education, health care, energy, financial, gaming, retail, telecommunications, and E-commerce, have specific concerns, terminologies, and practices that are unique to that industry. A familiarization with these aspects of the industry will allow the contractor

to more efficiently and effectively serve the contracting organization. The contractor with industry expertise will be able to comprehend system functions and connections more easily, since it will seem familiar. The contractor will also find it easier to interview key personnel and anticipate their concerns, since the contractor has experience discussing the concerns with other industry leaders. Lastly, the contractor with industry experience is likely to be able to discuss and present the findings of the security risk assessment to those within an industry with whom the contractor has worked previously, because the contractor is able to correctly use the industry terminology and avoid terminology within the information security industry that may be used in a different context within the industry.

Regulation and Requirement Experience—If the security risk assessment is being performed to meet specific requirements or regulations, a contractor who has had experience with those regulations or requirements may be able to provide security risk assessment services better than other similarly qualified individuals. Specific regulations such as HIPAA, the GLB Act, PCI DSS, Sarbanes-Oxley, 21 CFR Part 11, and others may have similar wording associated with the requirement for a security risk assessment, yet each of these regulations has its own unique set of expectations based on interpretations of the requirements, case history, and the current expertise and expectations of the auditors.[8] A contractor who has experience in the regulation will not need to spend copious amounts of time coming up to speed on the regulations and other requirements that affect the nature of the security risk assessment. Furthermore, a contractor with experience in specific regulations, such as HIPAA or the GLB Act, will already be familiar with how these requirements are being interpreted within the industry, the depth of analysis accepted by reviewers, and the scope of the requirements on the various system components and controls.

- Security Risk Assessment Activity Expertise—There are many different techniques, methods, and activities that may be performed within a security risk assessment in order to determine the overall security risks to the system. Depending upon the customer requirements, some of these aspects may be required within a specific security risk assessment. Key aspects include security risk assessment methods such as OCTAVE, FRAP, and CRAMM;[9] techniques such as interviews, physical walk-throughs, and use of checklists; and activities such as social engineering, penetration testing, code review, architectural analysis, and organizational structure review. For those security engineers who have no experience with specific security risk assessment methods, techniques, or activities, the learning curve for these is likely to be steeper than for those security engineers with previous experience with these aspects.

The next-best alternative to the contractor is not to take the job. A contractor may choose to refuse to contract with the organization requiring a security risk

assessment if there appear to be unreasonable expectations. Since most security risk assessments are performed as a firm-fixed-price contract, the contractor can end up spending a lot of hours attempting to obtain sign-off on a project with unreasonable expectations. Professional and experienced contracting organizations would sooner walk away from such a project than risk poor customer satisfaction or an unprofitable project that utilizes key resources.

3.2.2.5.3 Negotiating Project Membership

Occasionally, the contracting organization may find it necessary to specify the team that will be performing the assessment. This is typically a result of getting burned in a "bait and switch" routine. For example, consider the following scenario. A large consulting firm sends around its "big guns" to present proposals to clients. The clients become enamored by the skill, experience, and depth of knowledge possessed by the presenter. Then, when it comes time for the project to begin, the large consulting firm sends out recently indoctrinated graduates to perform the project. The "big gun" presenter only plays a review role in the project. The result is a mismanaged, low-quality project that goes over budget and underdelivers on quality.

A good way to avoid this problem is to specify the qualities, experience, or credentials of the individuals on the project. Occasionally, the contracting organization may even require that named individuals be assigned to the project. Specifying named individuals can ensure a quality project, but it may unnecessarily tie the hands of the contractor. Remember that the contractor may have several bids out at once and experiences turnover from time to time. A preferred method of ensuring quality personnel is to allow substitution of named individuals with similar credentials and experience or upon the approval of the contracting organization.

Exercises

1. Compare and contrast the various audiences for a security risk assessment. How will this affect the audience view/attitude for scoping, data gathering, and results reporting? Who is the primary audience of a security risk assessment?
2. How will the various audiences likely react to the following errors in a final security risk assessment report?
   a. Misspelling of interviewee's name
   b. False positive vulnerability in scanning data and conclusions
   c. Instance of another client's name in a footer of the report
   d. Missing document in list of documents reviewed
   e. Incorrect security risk category for a finding (based on method)
3. Describe an approach for defining the boundaries of a security risk assessment. What are the dangers of improperly scoping the security risk assessment?

4. Find a physical diagram of your school campus or organization's building(s). Choose a single business unit (or school) and define the physical boundaries. What assumptions did you make?
5. There are four reasons given in Section 3.1.5.2 for why it would be reasonable to exclude a system function from a security risk assessment. Can you think of any other reasons (legitimate or not)?
6. Consider the Statement of Work (SOW) in Table 3.1.
   a. What improvements can you define?
   b. What elements seem unnecessary?
   c. Would you like to see a required method for the security risk assessment? Why or why not?
7. Create an outline (or review one provided) for a security risk assessment report. Identify the primary audience of each section.
8. Why are most security risk assessments performed on a firm-fixed-price basis? In what situations does a time and materials contract make sense?

Notes

1. One way of ensuring the professionalism of the team members is to select members with relevant professional credentials. Among the most respected credentials relevant to performing a security risk assessment are the Certified Information System Security Professional (CISSP) and the Certified Information Security Auditor (CISA).
2. Such analysis can be a considerable effort on the part of the team, so a discussion as to inclusion of compliance review in the security risk assessment should have been settled in the negotiation phase. Compliance analysis is sometimes called *gap analysis*.
3. That is not to say that if a security risk is noticed it should not be reported; it should. In fact, some security risks are required to be reported, such as the discovery of child pornography. However, the security risk assessment report should not contain such reported security risks that are outside the boundaries of the security risk assessment.
4. Fly-By-Nite Security is a completely fictitious name used throughout this book to make examples and discussions more readable. Any resemblance of this company to a real company (by name or practice) is completely unintentional. However, if this name does resemble your company name, I would have to question your marketing intelligence.
5. The alert reader will have noticed several overlaps within physical security controls, such as fireproofing protecting both the buildings and the employees. Such overlaps are welcome, as these security control measures can reduce the security risk for more than a single threat or asset.

6. This is pretty much what is done in a statement on standards for Attestation Engagements (SSAE 16). Formerly audits are performed on service organizations that provide internal controls for systems that may affect the financial statements of other organizations, for example, an IDC that houses an application that takes orders over the Internet. The IDC may have hundreds of customers, who all have the same concerns about the security controls that protect their applications. If the IDC has a SSAE 16 audit performed once, it can share the results of the audit with all customers for their use in their own audits.
7. It could be argued that the contractor would prefer to get a larger contract and thus prefer the longer effort, but let us just assume that there is enough work out there to keep him busy.

   Of course the converse is also true: not all code review or penetration test teams possess the skills to assess the results of their activities in terms of risk to the organization. In this case it is a good idea to include the code review or penetration test skill as part of the secured risk assessment team.
8. Not all regulations have associated auditors. For example, there are no auditors directly associated with the Health Insurance Portability and Accountability Act (HIPAA). Some vendors with HIPAA training would like you to believe so, but it is not true.
9. Although there may be very good reasons for specifying or preferring specific security risk assessment activities or techniques, the contracting organizations should resist specifying a security risk assessment method unless it is absolutely necessary. Contractors familiar with a specific security risk assessment method are sometimes drawn to requiring this same method within an RFP. A more flexible RFP that allows the proposing security engineers to describe the methodology they believe is most appropriate is likely to yield far better results.

References

"Guide for Developing Security Plans for Information Technology Systems.," NIST Special Publication 800-18, December 1998. http://csrc.nist.gov/publications/nistpubs/800-18/rev1/sp800-18/rev1-final.pdf. Accessed February 7, 2011.

"Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans," SP 800-53A Rev. 1, June 2010. http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf. Accessed February 7, 2011.

"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," SP 800-37 Rev. 1, February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf. Accessed February 7, 2011.