National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-35

Guide to Information Technology Security Services

Recommendations of the National Institute of Standards and Technology

Tim Grance
Joan Hash
Marc Stevens
Kristofor O'Neal
Nadya Bartol

Special Publication 800-35

Guide to Information Technology Security Services

The National Institute of Standards and Technology

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2003

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Acknowledgements

The authors, Tim Grance and Joan Hash of the National Institute of Standards and Technology (NIST), and Marc Stevens, Kristofor O'Neal, and Nadya Bartol, of Booz Allen Hamilton (BAH), wish to thank their colleagues who reviewed the many drafts of this document and contributed to its technical content. We also gratefully acknowledge and appreciate the many comments we received from readers of the public and private sectors, whose valuable insights improved the quality and usefulness of this document. The authors would like to specifically acknowledge some key organizations whose extensive feedback substantially contributed to the development of the document. These organizations include: Environmental Protection Agency, Department of Treasury, Tennessee Valley Authority, and Electronic Data Systems. The authors would also like to acknowledge Ron Ross, Gary Stoneburner, Curtis Barker, Ron Tencati, Marianne Swanson, and Bill Burr of NIST, Alexis Feringa, Don Ottinger, Skip Hirsh, and Robert Young, BAH, and Shirley Radack for their extensive review and comment and keen and insightful assistance throughout the development of the document.

Executive Summary

Organizations frequently must evaluate and select a variety of information technology (IT) security services in order to maintain and improve their overall IT security program and enterprise architecture. IT security services, which range from security policy development to intrusion detection support, may be offered by an IT group internal to an organization, or by a growing group of vendors. Organizations can benefit when choices among services and service providers stimulate competition and bring innovation to the marketplace. However, it is difficult and challenging to determine service provider capabilities, measure service reliability and navigate the many complexities involved in security service agreements. Individuals who are responsible for selecting, implementing, and managing IT security services for an organization must carefully evaluate their options before selecting resources that will be entrusted to meet their particular IT security program requirements.

The factors to be considered when selecting, implementing, and managing IT security services include: the type of service arrangement; service provider qualifications, operational requirements and capabilities, experience, and viability; trustworthiness of service provider employees; and the service provider's capability to deliver adequate protection for the organization systems, applications, and information. These considerations will apply (to varying degrees) to every service depending on the size, type, complexity, cost, and criticality of the services being considered and the specific needs of the organization implementing or contracting for the services.

The *Guide to Information Technology Security Services, Special Publication 800-35*, provides assistance with the selection, implementation, and management of IT security services by guiding organizations through the various phases of the IT security services life cycle. This life cycle provides a framework that enables the IT security decision makers to organize their IT security efforts—from initiation to closeout. The systematic management of the IT security services process is critically important. Failure to consider the many issues involved and to manage the organizational risks can seriously impact the organization. IT security decision makers must think about the costs involved and the underlying security requirements, as well as the potential impact of their decisions on the organizational mission, operations, strategic functions, personnel, and service provider arrangements.

The six phases of the IT security life cycle are:

- **Phase 1: Initiation**—the organization determines if it should investigate whether implementing an IT security service might improve the effectiveness of the organization's IT security program.
- **Phase 2: Assessment**—the organization determines the security posture of the current environment using metrics and identifies the requirements and viable solutions.
- **Phase 3: Solution**—decision makers evaluate potential solutions, develop the business case and specify the attributes of an acceptable service arrangement solution from the set of available options.
- **Phase 4: Implementation**—the organization selects and engages the service provider, develops a service arrangement, and implements the solution.
- **Phase 5: Operations**—the organization ensures operational success by consistently monitoring service provider and organizational security performance against identified requirements, periodically evaluating changes in risks and threats to the organization and ensuring the organizational security solution is adjusted as necessary to maintain an acceptable security posture.
- **Phase 6: Closeout**—the organization ensures a smooth transition as the service ends or is discontinued.

This guide describes a life cycle that provides a context to assist organizations with managing the myriad issues surrounding IT security services. However, the guide does not prescribe or recommend any specific IT security service, IT security service arrangement, IT security service agreement, or IT security service provider. Each organization must perform its own analysis of its needs and assess, select, implement, and oversee the IT security service to best address its needs.

The Guide should be used in conjunction with other NIST Special Publications (SP) that focus on procurement of IT systems, including NIST SP *800-64, Security Considerations in the Information System Development Life Cycle*, and *NIST SP 800-36: Guide to Selecting Information Technology Security Products*. NIST SP 800-55, *Security Metrics Guide for Information Technology Systems* will help organizations understand the importance of using metrics and developing a metrics program.

Other NIST special publications may be helpful in providing information on specific services and technologies. These include:

- SP 800-30: Risk Management Guide for Information Technology Systems
- SP 800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure
- SP 800-33: Underlying Technical Models for Information Technology Security
- SP 800-34: Contingency Planning for Information Technology Systems
- SP 800-41: An Introduction to Firewalls and Firewall Policy
- SP 800-42: Guideline on Network Security Testing
- SP 800-48: Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
- SP 800-50: Building an Information Technology Security Awareness and Training Program
- SP 800-53: Recommended Security Controls for Federal Information Systems

NIST recommends that organizations planning to acquire IT security services should:

- Develop careful, objective business cases. The need for an IT security service should be supported by the business needs of the organization. A business case containing an analysis of the proposed solution, cost estimate, benefits analysis, project risk analysis, and an evaluation of other considered alternatives should provide sufficient documentation to describe and support these needs.
- Develop strong, specific service agreements that define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instances of non-compliance.
- Use metrics throughout the IT security life cycle. Metrics will provide the objective data to evaluate the baseline level of service in the assessment phase and assess service provider performance in the operations phase. Wherever possible, metrics should be selected to indicate progress toward the achievement or maintenance of a security condition that meets an underlying organizational need.
- Develop processes and procedures that can effectively track the myriad service agreements and the metrics that will be applied throughout the lifecycle of the many different and disparate IT security services within an organization

- Ensure that an appropriate transition (bedding in) period is in place between an existing service provider or capability and the new service provider
- Maintain the technical expertise necessary to understand and manage the security service being provided and to protect the data critical to an organization's mission
- Pay careful attention to six issue areas: strategy/mission, budget/funding, technology/architecture, organization, personnel, and policy/process.

THIS PAGE INTENTIONALLY LEFT BLANK.

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

1.2 Purpose

Organizations frequently must evaluate, select, and employ a variety of IT security services in order to maintain and improve their overall IT security programs. IT security services (e.g., security policy development, intrusion detection support, etc.) may be offered by an IT group internal to an organization, or by a growing group of vendors. Individuals who are responsible for selecting, implementing, and managing IT security services for an organization must carefully review the necessary processes and procedures, weigh a host of available options, and select resources that can be entrusted to optimally meet IT security program requirements.

Factors to be considered when selecting, implementing, and managing IT security services include: the type of service arrangement; service provider qualifications, requirements, experience, and viability; trustworthiness of service provider employees; and protection for organization systems, applications, and data. These considerations may apply (in varying degrees) depending on the size, type, complexity, cost, and criticality of the services being considered.

The purpose of this guide is to provide assistance with selecting, implementing, and managing IT security services by guiding the organization through the various phases of the IT security services life cycle. The IT security services life cycle provides a framework that enables the IT security decision makers to organize their IT security efforts—from initiation to closeout. The systematic management of the IT security services process is critically important. Failure to consider and manage the many complex issues involved can seriously impact the organization. IT security decision makers must think about the costs and security requirements, as well as organizational mission and strategic functions, personnel and service provider arrangements.

This guide discusses each phase of the IT security services life cycle to provide a starting point for evaluating and selecting sound security practices. The discussion is directed toward a wide variety of organizations with diverse IT security requirements. The guide discusses general topics such as the

importance of developing agreements that define the service levels for the service providers; however, this guide does not prescribe the service or service level that best fits the organization's needs. The specific needs of each organization should always be considered when applying the processes and concepts that are presented in this guide. Finally, in this publication, NIST provides information and advice for decision makers and other relevant parties on the security and policy issues for obtaining IT security services.

1.3 Limitations

Section 5 of this document discusses a sampling of possible IT security services but does not represent an exhaustive list. In addition to clearly identified IT security services, organizations may also wish to acquire a service, which contains a significant security component such as systems administration. These types of services are not addressed in this guide; however, the information that is included in this guide can be extended and adapted to cover other related services.

This guide does not advocate a position for or against the development of external arrangements (such as outsourcing) for IT security services. The reader should refer to OMB Circular A-76, *Performance of Commercial Activities*, to establish the foundation for the decision whether activities should be performed under contract with a commercial activity or performed in-house using Government facilities and personnel.

1.4 Intended Audience

This guide is meant for organizations that provide IT security services regardless of whether the service is provided from within the organization or procured from an outside provider. The goal is to help IT security decision makers and managers implement and manage the most appropriate IT security services, service levels, and service arrangements to best meet the organization's mission and needs.

1.5 Document Organization

The remainder of this document is organized as follows:

Chapter 2 discusses the roles and responsibilities of the various people involved with the selecting, implementing, and managing of the IT security services life cycle.

Chapter 3 provides an introduction to IT security services, including an overview of the security services life cycle and of selected IT security services. This chapter discusses the framework of a security services life cycle, an overview of issues to address throughout the life cycle, an overview of the various service arrangements that IT security decision makers could consider, and a look at tools that will be useful to the IT security decision maker in the security services life cycle.

Chapter 4 provides a more in-depth discussion of the issues related to obtaining IT security services. In the context of the security services life cycle, this chapter discusses how the security service begins, what is captured in assessing the current environment and the needs for any new service, what a service agreement should include, and how a service agreement should end or be discontinued.

Chapter 5 provides a more detailed look at a few specific IT security services, serving as an example of the application of the previous information.

In addition to these chapters, three appendixes are attached:

Appendix A provides a list of references.

Appendix B provides a list of acronyms.

Appendix C provides a sample outline for an IT security service provider service agreement.

Appendix D presents sample language for use in an organization's service agreement. This language, after appropriate tailoring for specific needs of the organization, may be used to assist in the writing of service agreements, contractual documents such as a statement of work (SOW) or memorandums of agreement/understanding (MOA/MOU).

Appendix E is a list of frequently asked questions.

THIS PAGE INTENTIONALLY LEFT BLANK.

2. Roles and Responsibilities

The list of participants for selecting, implementing, and managing a given service will depend on the type and scope of the service, the service arrangement, and type/size of organization. A large federal agency that is seeking to partner with an external organization for many of its IT security functions will have different requirements and therefore a more extensive list of participants than a small business seeking a limited-scope IT security training program for its employees. The following roles are generic to many different services. The actual list of participants may be less than or greater than the list provided below. For instance, if an internal group within an organization provides the security service, the contracting officer and Contracting Officer's Technical Representative (COTR) may not have a role.

2.1 Chief Information Officer

The CIO is responsible for the organization's IT planning, budgeting, investment, performance and acquisition. As such, the CIO oversees senior organization personnel in obtaining efficient and effective IT security services.

2.2 Contracting Officer

The Contracting Officer has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

2.3 Contracting Officer's Technical Representative

The Contracting Officer's Technical Representative (COTR) is a qualified employee appointed by the Contracting Officer to act as its technical representative in managing the technical aspects of a particular contract.

2.4 IT Investment Board (or equivalent)

The IT Investment Board, or its equivalent, is responsible for managing the capital planning and investment control process defined by the Clinger-Cohen Act of 1996 (Section 5).

2.5 IT Security Program Manager

The IT Security Program Manager is responsible for developing or applying enterprise standards for IT security. This individual plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize IT security risks to the organization. IT security program managers coordinate and perform system risk analyses, analyze risk mitigation alternatives, and build the business case for the acquisition of appropriate security solutions that help ensure mission accomplishment in the face of real-world threats. They also support senior management in ensuring that security management activities are conducted as required to meet the organization's needs.

2.6 IT System Security Officer

The IT System Security Officer is responsible for ensuring the security of an information system throughout its life cycle.

2.7 Program Manager (Owner Of Data)/Acquisition Initiator

This Program Manager represents programmatic interests during the IT security services life cycle. Program Managers play an essential role in security because they have been involved in strategic planning initiatives of the IT security service and are intimately aware of functional service requirements.

2.8 Privacy Officer

The Privacy Officer ensures that the service and service arrangement meet existing privacy policies regarding protection, dissemination (information sharing and exchange) and information disclosure.

2.9 Other Participants

The list of roles in a service acquisition can grow with the complexity involved in acquiring and managing IT systems. It is vital that all members of the acquisition team work together to ensure that a successful acquisition is achieved. Since the system certifier and accreditor will be making critical decisions near the end of the procurement process, it is helpful to include them earlier in the acquisition so that critical issues can be addressed early. System users may assist in the acquisition by helping the program manager to determine the need, refine the requirements, and inspect and accept the delivered system. Participants may also include personnel who represent information technology, configuration management, design/engineering, and facilities groups.

3. IT Security Services

This chapter provides an overview of IT security services, service arrangements, service issues, and service management tools. These overviews serve as an introduction to the IT security services life cycle discussed in Chapter 4. This life cycle is independent of an organization's decision to use internal resources or an external service provider to perform the service. Ultimately, the organization remains responsible for and affected by any security breach regardless of who performs the security service.

3.1 Overview of IT Security Services

Security services fall into one of three categories (Table 3-1).

Table 3-1. IT Security Categories

Management Services	Techniques and concerns normally addressed by management in the organization's computer security program. They focus on managing the computer security program and the risk within the organization.
Operational Services	Services focused on controls implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and rely on management activities and technical controls.
Technical Services	Technical services focused on security controls a computer system executes. These services are dependent on the proper function of the system for effectiveness.

The security services life cycle applies to any security service regardless of the category into which it falls and could even apply to an entire IT security category. As managers determine which IT security services need to be implemented, assessed, or discontinued, they should consider the impact on other IT security services.

Chapter 5 discusses in greater detail the types of IT security services. NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Computer Security Handbook*, also provides a comprehensive overview of and introduction to computer security and security controls and services.

3.2 Overview of IT Security Service Arrangements

Selecting the most appropriate services, service mix, and service level is a complex decision, as is deciding who should provide the needed service. Much of the complexity of this decision stems from the wide range of arrangements from which an organization may choose, though organizational, personnel and other issues discussed in section 3.4 also make the decision less straightforward and increases the complexity.

An operational example—an organization retains the program oversight of a firewall within the organization, but brings in an external group to handle the day-to-day monitoring of the audit logs.

The security arrangement may look different, depending on a person's role. In this example, the firewall manager may view the arrangement as an external one because an outside group performs the audit review service. The organization's top-level business manager may view this as an internal arrangement because the firewall service is implemented internally. The organization's IT security officer may view this as somewhere in the middle of the continuum, a hybrid, seeing both the internal firewall service and its external audit review component.

A broad range of possible service arrangements exists. An organization may select its internal employees and teams to provide the service required, or it may choose to fully export the service to an external service provider. This external service provider could be any organization because this term does not intend to refer to only an external commercial service provider. For example, an organization may choose to employ an external group from a subsidiary organization, a business unit, or a commercial service provider.

3.3 Overview Of IT Security Services Management Tools

Because of the potential harm that can result from poor security, IT security managers and decision makers need to use effective management tools to increase the likelihood of success. Two important tools are metrics and service agreements.

Overview of Metrics

Metrics are a management tool that facilitates decision-making and accountability through practical and relevant data collection, data analysis, and performance data reporting. The importance of a metrics program is discussed in NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*. A full and complete discussion of computer security metrics is beyond the scope of this document; however, IT security service managers should understand what metrics are and when they should be used.

For example, a metric for a management service, such as a training and awareness program, might be the percentage of new employees who receive IT security training within their first 30 days on the job. Gathering this data repeatedly, over time, will allow managers to assess how well the current training service provider performs its task today, to set targets for the service provider in the future, and then to assess how well it met the desired target. The metrics process is discussed in the next chapter.

Overview of Service Agreements

A service agreement serves as the agreement between the service provider and the organization requesting the service. As service arrangements become more complex and employ commercial service providers, the formality of the agreement should increase. A fully externalized service arrangement with a commercial entity, for example, will require a formal contract so that managers can hold service providers accountable for their actions. A fully internal service arrangement may require a less formal agreement, perhaps an agreed-on reporting process or an MOA. Regardless of the arrangement, all parties should be aware of their roles and responsibilities. Section 4.4.1 discusses the importance of service agreements.

3.4 Overview of IT Security Services Issues

Implementing a security service and service arrangement can be complex. Each security service has its own costs and risks associated with it, as does each service arrangement. Making a decision based on one issue can have major implications for the organization in other areas. The decision makers will have to balance near-term cost/value with potential long-term risks associated with new vulnerabilities, attrition, potential loss of employee productivity/morale and internal functional skills, and other impacts. The degree of completeness of the list of factors and issues considered will vary by organization; however, the factors and issues can be grouped into six categories as identified in Table 3-2.

Table 3-2: IT Security Service Issue Categories

Strategic/ Mission	When thinking about the implications of any decision, decision makers must ask themselves what is best for the organization from a strategic point of view and what best helps the organization meet its mission. Applied appropriately, security services should result in enhanced mission effectiveness, not reduced mission capability.
Budgetary/ Funding	When considering cost, the focus should be on value and full life-cycle costs. (see Section 4.2.1.2)
Technical/ Architectural	IT services, even if a management service, has technical implications. Throughout the life cycle, IT security managers must consider impacts to technical issues and the organization's enterprise architecture.
Organizational	These issues are related to the intangible elements of an organization, such as damage to an organizations image and reputation, change in focus on core competencies, and resiliency of the organization. In many cases, long accepted internal controls and business practices that have developed over time due to natural business unit divisions or regulatory requirements may have to be reconsidered when an IT security service provider is engaged.
Personnel	These issues are related to the organization's contractors and employees. Managers must remain aware of the impact of their decision on their employees. Depending on the service arrangement implemented, major ramifications could exist for current employees; understanding these potential implications is an essential element of making a good trade-off between internal and external services. Dealing with them early will ensure the employees remain an important resource for the organization.
Policy/Process	Effective security starts with strong policy, and implications to policies and process must be considered to ensure that good decisions are being made and that appropriate transitions and implementations occur.

These issues, tools, and arrangements will be discussed repeatedly in this guide because of their importance to providing IT security services.

3.5 General Considerations for IT Security Services

Listed below are some general questions that decision makers should answer to identify the service provider that best meets the organization's needs. These questions have been grouped into the various issue categories described in Section 3.4.

These questions are intended as a guide and each organization will need to decide which questions are relevant to its specific needs. The questions are not an exhaustive list and organizations may need to develop additional questions. In some instances, the organization and not the service provider may best answer the question.

Table 3-3: Questions for Service Providers[1]

Strategic/ Mission	1. What is "the service provider" mission? 2. Does "the service provider" understand the organization's mission? 3. How does "the service provider's" mission and service offering align and enhance the organization's ability to meet "the organization's" mission? 4. Describe "the service providers" business, specifying number of staff, customers, locations, and business revenues. Is "the service provider" planning any major strategic/mission changes or anticipating any budget/financial viability issues during the period of performance? 5. Is the "service" inherently governmental?
Budgetary/ Funding	1. At what cost will "the service provider" provide the service? 2. How much would the service cost at a higher service level? At a lower service level? 3. How will "the service provider" protect against cost overruns? 4. What remedies would "the service provider" offer for cost overruns?
Technical/ Architectural	1. How will "the service provider" perform the IT security service? 2. Who will provide, i.e., own, the hardware/software needed? 3. At what level will "the service provider" provide the service (e.g., % availability, metrics reports, maintenance, hardware/software refreshment, etc.)? 4. How will "the service provider" ensure this service level? 5. What remedies would "the service provider" consider appropriate (i.e. service credits) for failure to meet the service targets? 6. What are the "service provider's" requirements for early termination and extension? 7. How are scale-up/down issues handled? 8. Has "the service provider" provided this type of service at this level for this type of organization before? Can "the service provider" provide references for those past performance qualifications? 9. What is the IT security environment of "the service provider"? 10. How would the "service provider" handle emergency situations?
Organizational	1. What is "the service provider's" work environment and is it compatible with the organization? 2. How well will "the service provider" adapt to the organization's environment? 3. What is "the service provider's" reputation (in the marketplace and for meeting cost and service targets)? How does "the service provider" compare to its competitors?
Personnel	1. Will "the service provider's" staff be on-site, off-site, or a mix? 2. Will "the service provider's" staff have/be able to obtain the appropriate personnel and facility clearances? 3. What staff will "the service provider" assign to this task? What are their skills? Do the "service provider's" staff meet the organization's citizenship requirements? 4. How will "the service provider" ensure the staff stays current in the technology/service field?
Policy/Process	1. Does "the service provider" foresee changes to the organization's policies and/or processes? 2. How does "the service provider's" security policies (e.g. contingency planning) differ from that of the organization? If the organization's policy meets a higher standard, will "the service provider's" have trouble meeting this higher standard? If lower, will "the service provider" abide by the stricter policies of the organization? 3. How does "the service provider" address the comingling of its data with that of another organization? Are processes in place to ensure that an organization's data is protected?

[1] The organization is the unit that acquires and ultimately receives the security service from the service provider.

3.6 Organizational Conflict of Interest

An organizational conflict of interest (OCI) may exist when a party to an agreement has a past, present or future interest related to the work performed (or to be performed), which may diminish its capacity to provide impartial, technically sound, objective service or results in an unfair competitive advantage. Of course, it is best to avoid organizational conflicts before they arise. The Federal Acquisition Regulation (FAR) (subpart 9.5) describes two underlying principles why avoiding an OCI is important:

- Preventing the existence of conflicting roles that might bias a [service provider's] judgment
- Preventing unfair competitive advantage

According to the FAR, an unfair competitive advantage exists where a [service provider] possesses proprietary information that was obtained from a Government official without proper authorization or source selection information that is relevant to the contract but is not available to all competitors, and such information would assist that [service provider] in obtaining the contract.

Although the FAR applies to Federal contracts, any organization should be aware that an OCI could occur in any phase of the IT security services lifecycle and may provide an unfair competitive advantage.

- There are several methods that an organization can take to avoid, neutralize, or minimize the effect of an OCI. They can include: modify or eliminate the offending parts of the agreement, statement of work, contract, etc.
- Prohibit bidding on a subsequent procurement in which the service provider plays a key role in development of the requirement
- Prohibit using proprietary or privileged information which the service provider has access to
- Segment the work within the service provider to prevent involvement in performance of the work or being in a position to influence the work
- Require the service provider to avoid conduct that may result in an OCI-such as when called on to inspect its own work. The service provider must disclose its relationship and disqualify itself from performing the work
- Make privileged documents available to all parties. (neutralizing the OCI)

If an organization determines that the OCI exists but cannot be avoided and the organization wishes to proceed, the head of the organization may determine to proceed and waive the OCI.

Identifying the existence of OCIs, mitigating effect of the OCI to an acceptable level, and/or waiving the OCI is important when managing the IT security service life cycle but it can involve complex legal and regulatory issues and should not be considered without the close counsel of an organization's legal department.

4. IT Security Services Life Cycle

The IT security services life cycle provides IT security decision makers and managers with a six-phase process by which they can select, implement, and manage IT security services. This chapter details the various life-cycle phases and the issues and decisions within each phase. As Figure 4-1 illustrates, the security services life cycle has both a linear and iterative component. It proceeds linearly from initiation to implementation to closeout, but the assessment, solution, and operations phases must continually occur for an IT security service to succeed.

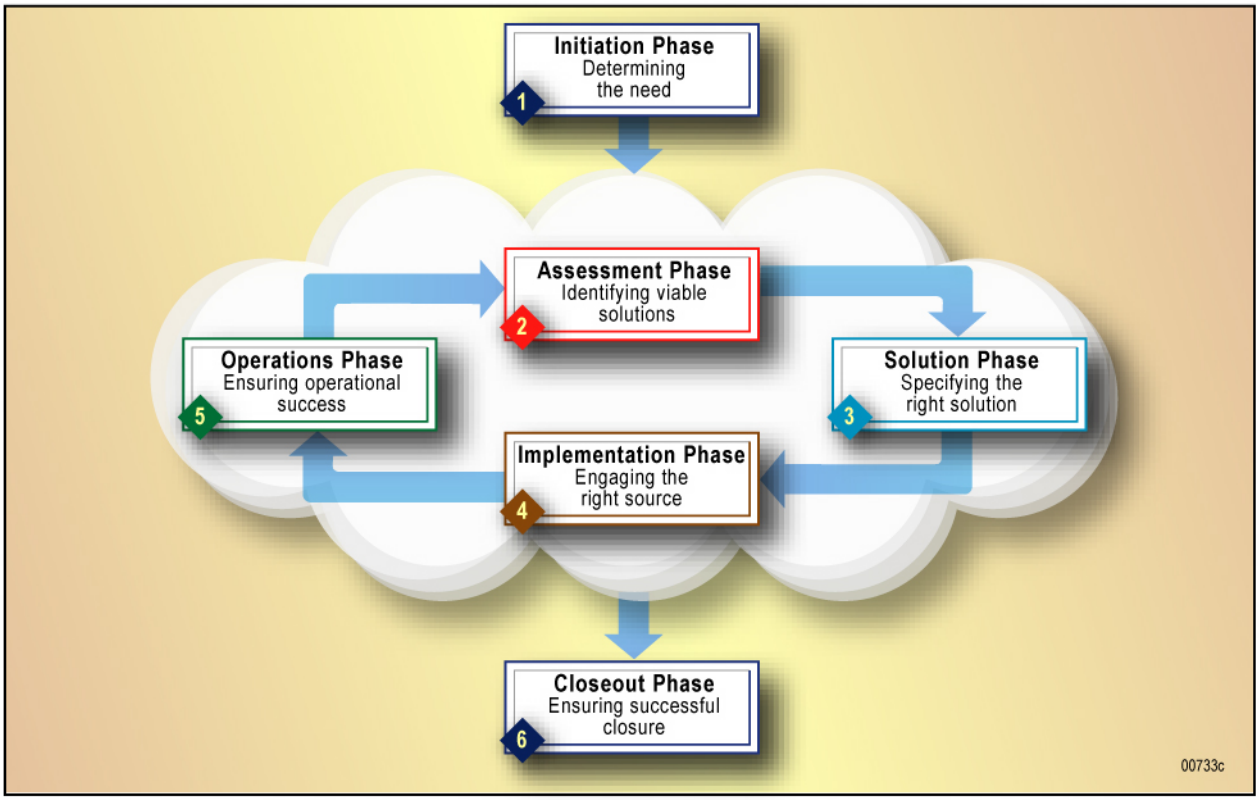

Figure 4-1. IT Security Services Life Cycle

The six phases are described as follows:

- **Phase 1: Initiation**—the need to initiate the services life cycle is recognized. Section 4.1 discusses potential triggers for this phase.
- **Phase 2: Assessment**—before decision makers can implement a service and select a service provider, an accurate portrait of the current environment must be developed. Section 4.2 discusses Phase 2 and the importance of creating and gathering appropriate metrics.
- **Phase 3: Solution**—decision makers choose the appropriate solution from the viable options identified during the assessment phase. Section 4.3 discusses the business cases and implementation plans.
- **Phase 4: Implementation**—the service and service provider are implemented during the implementation phase. Section 4.4 guides decision makers through service agreement development and service implementation.

- **Phase 5: Operations—**the service is operational, the service provider is fully installed, and constant assessment of the service level and performance is made. Section 4.5 discusses the importance of metrics in monitoring service level and performance.
- **Phase 6: Closeout—**the environment changes, the need for the service diminishes, or performance deficiencies are noted necessitating a replacement or termination of the IT security service. Section 4.6 discusses the closeout and retirement of a service and/or service provider using the exit strategies developed in Phase 3.

4.1 Phase 1: Initiation

Figure 4-2 illustrates Phase 1, Initiation, of the IT security services life cycle. This phase has a single step: an event sufficient to warrant assessing the current environment and identifying viable service solutions. The specific trigger that will meet this definition will vary by organization. The trigger will fall into one of the six issue areas listed in Section 3.4: strategy/mission, budgetary/funding, technical/architectural, organizational, personnel, and policy/process. Table 4-1 shows sample trigger events from each issue area.

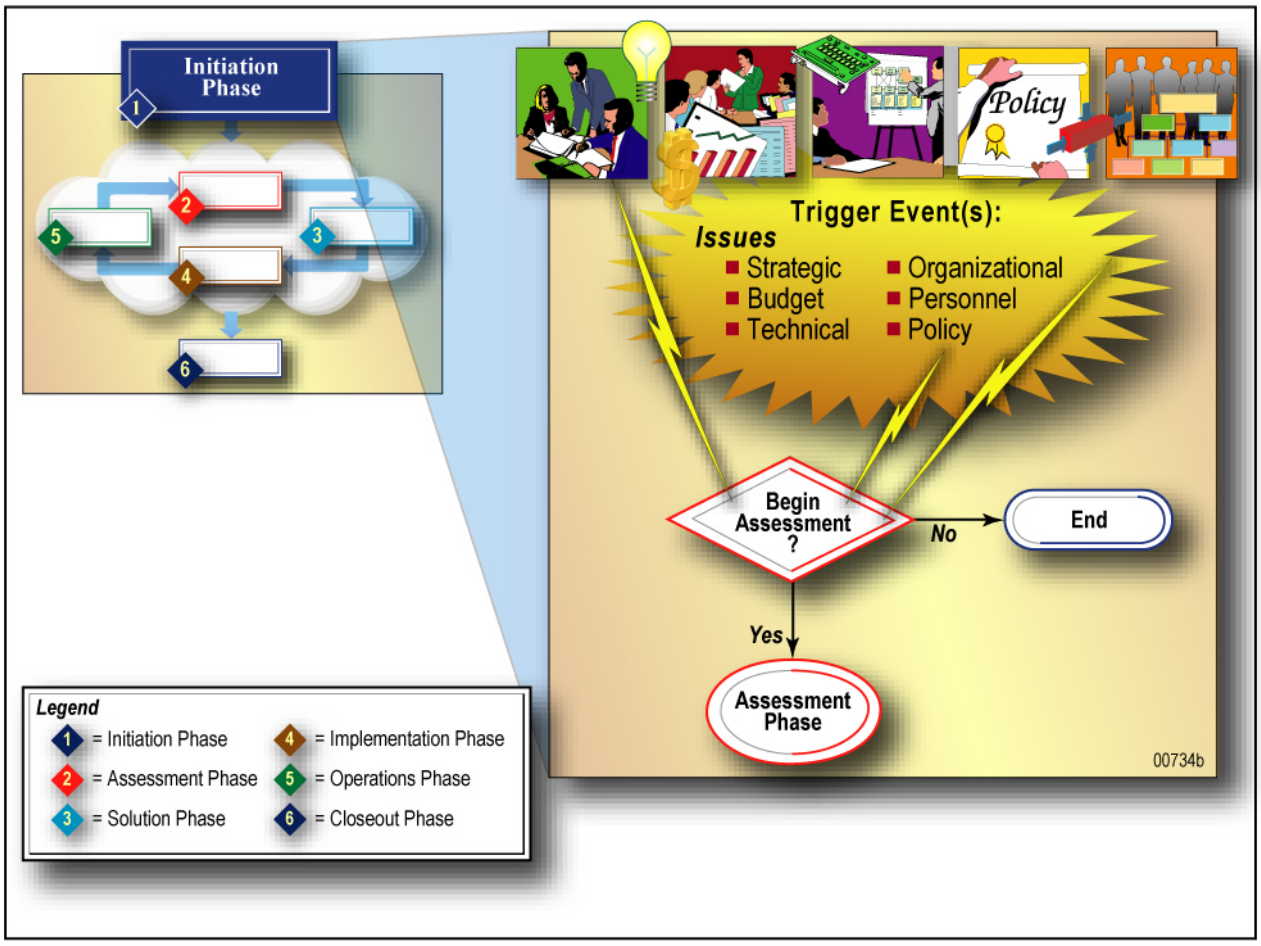

Figure 4-2. Initiation Phase

Business, IT, and IT security managers initiate the service life cycle. The decision to obtain a security service should be to obtain the most appropriate security services at the most appropriate level in the most

appropriate service arrangement so as to support the business function. The next phase of the life cycle, Assessment, is where it is determined whether the most appropriate service is one performed internally or externally.

As one IT security services life cycle is initiated, it is likely another life cycle will be ending. To ensure a smooth transition, managers should be aware of possible interactions and effects between the service that is ending and the one that is beginning.

TABLE 4-1. IT SECURITY ISSUES AND SAMPLE LIFE CYCLE TRIGGERS

Strategic/Mission	• Change in business model • Investigating new service arrangements to better focus on the organization's mission and business function
Budgetary/Funding	• Increased IT security budget, allowing greater security services • Decreased IT security budget warrants an investigation into ways to cut costs.
Technical/ Architectural	• New technology needs implemented • Upgrades to new technology
Organizational	• Current organizational environment and employee mix (if already using external service providers) not working well • Organization changing service arrangement approach
Personnel	• Several functional experts leave the organization, creating a shortage of technical expertise in a security service area
Policy/Process	• Current policies or processes not meeting organization's security needs

4.2 Phase 2: Assessment

Phase 2, Assessment, shown in Figure 4-3, follows the Initiation Phase. The steps in this phase include baselining the existing environment, analyzing opportunities and barriers, and identifying options and risks. To establish a baseline understanding of the existing environment, the decision makers will need to use metrics and the principle of total cost of ownership (TCO) to ensure the most accurate data will be used for decision-making purposes. This data will also set performance targets and cost estimates for service agreements in later phases.

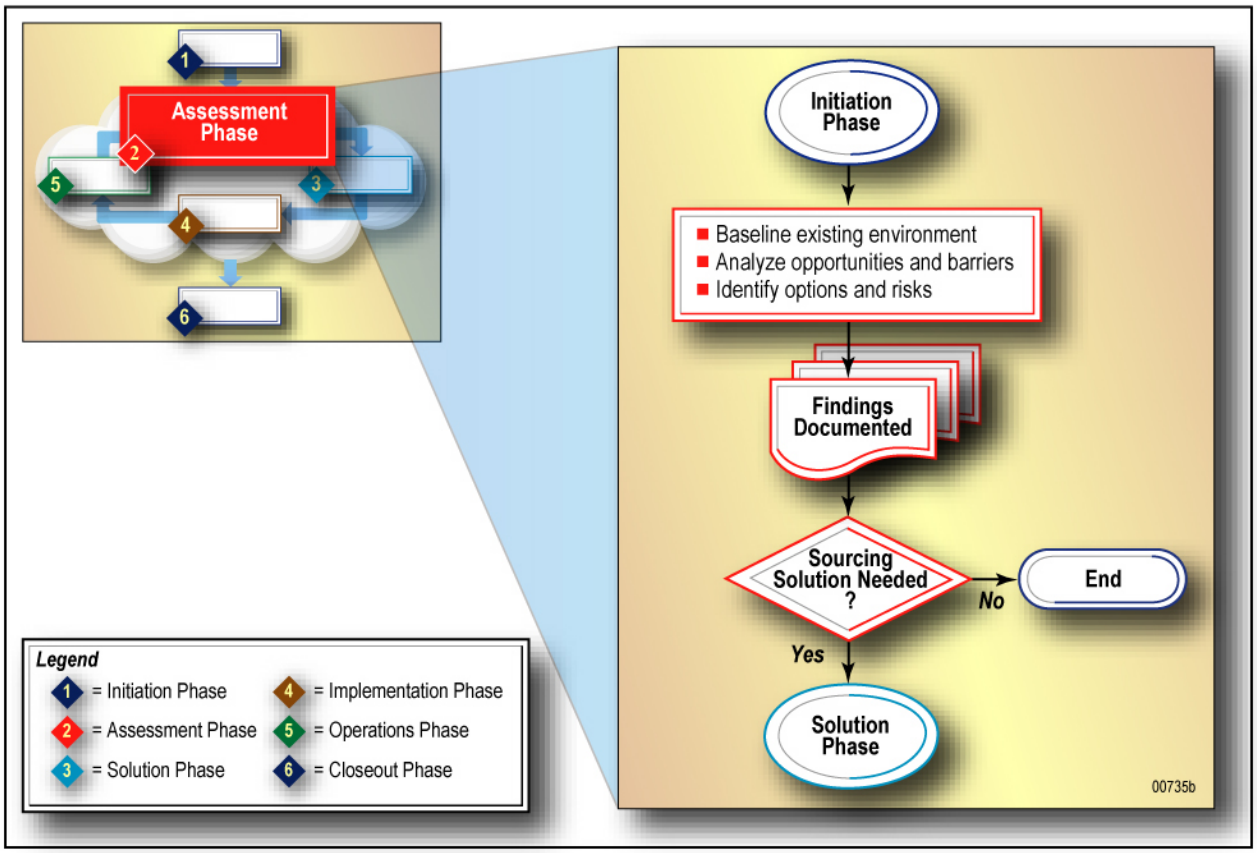

Figure 4-3. Assessment Phase

Bearing in mind the metrics and full cost of a service, the decision makers begin to consider opportunities and barriers. The IT security service issues mentioned in Section 3.4 provide a framework for analyzing opportunities and barriers, as well as external factors, such as the marketplace and the customers. Finally, the existing environment and the opportunities and barriers will provide managers with options and risks. From these options, managers will choose a solution in Phase 3.

4.2.1 Baseline Existing Environment

Once managers have initiated the IT security services life cycle, they must establish a baseline understanding of the current environment. This baseline will demonstrate to managers how well the current arrangement meets the security requirement and at what cost. Managers will need these two measurements to compare the benefits of various service arrangements or the proposals of various service providers.

The scope of this effort will depend on the nature of the security control or the specific mix of controls. All related areas of the control or the mix of controls should be included; for example, if an organization is evaluating its firewall services, it should evaluate its firewall policies and other policies, the effectiveness of the firewall architecture, and other issues specific to the study.

Data for constructing the baselines should be collected in an objective, impartial, and comprehensive manner. Stakeholders in the current environment will often be required to provide data or assist with

gathering data by which the service levels and sourcing solutions will be selected. As current stakeholders, they have an interest in the status quo, and their data-gathering techniques or reporting methods may reflect this intentionally or unintentionally. Formal tools such as metrics and TCO will help minimize any inadvertent biases in the data collection efforts. Additionally, a review of existing past metrics and data will be helpful in removing any bias when baselining the current environment.

4.2.1.1 Metrics Creation, Gathering, and Analysis

Metrics provide decision makers with objective, quantifiable data. The importance of metrics starts in this phase and continues throughout the life cycle.

Metrics creation starts with defining the "what" to measure: the metrics should map to the organization's overall functional and security goals and relate to the desired outcomes that the service will provide. Metrics for any service should include data related to the following:

- **Implementation Level**—implementation-level metrics quantify the degree of completion of required and agreed-on activities and within agreed-on timeframes.
- **Service Level**—these metrics quantify the timeliness of service delivery (i.e., average time to restore operations or number of hours to reconfigure a firewall).
- **Effectiveness**—effectiveness metrics are outcome factors that describe how well the services were delivered and their efficacy (i.e., customer service ratings, security intrusion and blockage levels, and the number of systems affected by computer viruses).
- **Business Impact**—business impact metrics quantify the effect on business parameters such as financial and operational resources (i.e., dollars lost from virus attacks, work time lost from server outages).

Additional considerations for the development of metrics include:

- Consider only those metrics that are practical to collect
- Base metrics only on obtainable and quantifiable events
- Consider all IT security service aspects from technical functionality to problem resolution procedures to appropriateness of personnel
- Base metrics on business operation objectives
- Provide sufficient insight into assessing the level of IT security services provided/offered and allow for a relevant comparison between service options
- Gather metrics to assess the causes, not only results
- Gather metrics to track trends.

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, provides more detail about the characteristics of useful metrics, as well as the importance of having a mature (or maturing) metrics program. The importance of a repeatable, consistent metrics approach to IT security will become apparent in the IT security services life cycle as the organization sets targets, writes service agreements, and monitors service provider performance in Phases 3, 4 and 5, respectively.

4.2.1.2 Total Cost of Ownership

In conjunction with a metrics program, the IT security services decision makers need to identify the full cost of the service. Metrics may be a part of this effort because they can help determine the dollar cost of various actions (e.g., cost of downtime, costs of a virus attack). The principle of full cost is often referred to as TCO. TCO includes not only implementation and operational costs but also related costs (e.g., overhead, salaries, benefits, technology upgrades, and software support, and maintenance). This information will allow decision makers to compare the costs of other service arrangements with the existing environment during the business case development in the solution phase. When the full cost is identified, the decision makers will be able to accurately relate the value of one service option over another.

4.2.2 Analyze Opportunities and Barriers

Once the organization understands the current environment from a performance and cost perspective, it can begin to analyze opportunities and barriers. Analyzing opportunities and barriers allows the organization to identify functions and areas that can change, those that cannot, and reasons for each. IT security stakeholders should participate in the process and approve analysis results. Properly performed, an analysis should include the following:

Strategic/Mission	• Identify how critical the service/function is to the business.
Budgetary/Funding	• Articulate a rational, executable fiscal program, in accordance with all applicable regulations and legislation to secure approval and funding by budget authorities
Technical/Architectural	• Determine and understand the importance of maintaining an organization's technical competencies
Organizational	• Determine which service arrangements would be appropriate for the organization's work environment and values. • Allow management to incorporate intangible benefits to all stakeholders (e.g., improved employee morale, organizational image) into the business case that will be developed.
Personnel	• Allow all stakeholders to develop and translate overarching performance goals and specific needs into specific service level requirements, such as Request for Proposal (RFP)/SOW/Service Level Agreement (SLA) requirements.
Policy/Process	• Begin to address integration/transition efforts for the desired future service arrangement strategy.

4.2.3 Identify Options and Risks

In this last step of the assessment phase, decision makers should begin to identify options and risks. The baseline showed the current environment, and the opportunities and barriers step began to describe the desired target. In this step, the "how-to" becomes clearer.

The "how-to" step will determine the service arrangement. As discussed in Chapter 3, organizations may fulfill a security service requirement using various security service arrangements—from using only internal teams and staff to fully outsourcing for the security service. At this life-cycle phase, many organizations will still need to consider many options and various service arrangements. For each of these, the organization needs to identify the benefits and risks.

Finally, the evidence may suggest the current arrangement and service level are effective and/or appropriate. It is most important to focus on business function, customers, and effective security. The choices made should best support these three focus points. Improving business and IT processes will likely be more effective and less risky than changing the service arrangement; organizations should not seek to change the current environment unless the assessment identifies improvement areas that can be met only by implementing a change in service, service arrangement, or service provider.

4.3 Phase 3: Solution

Figure 4-4 illustrates Phase 3, Solution, of the IT security services life cycle.

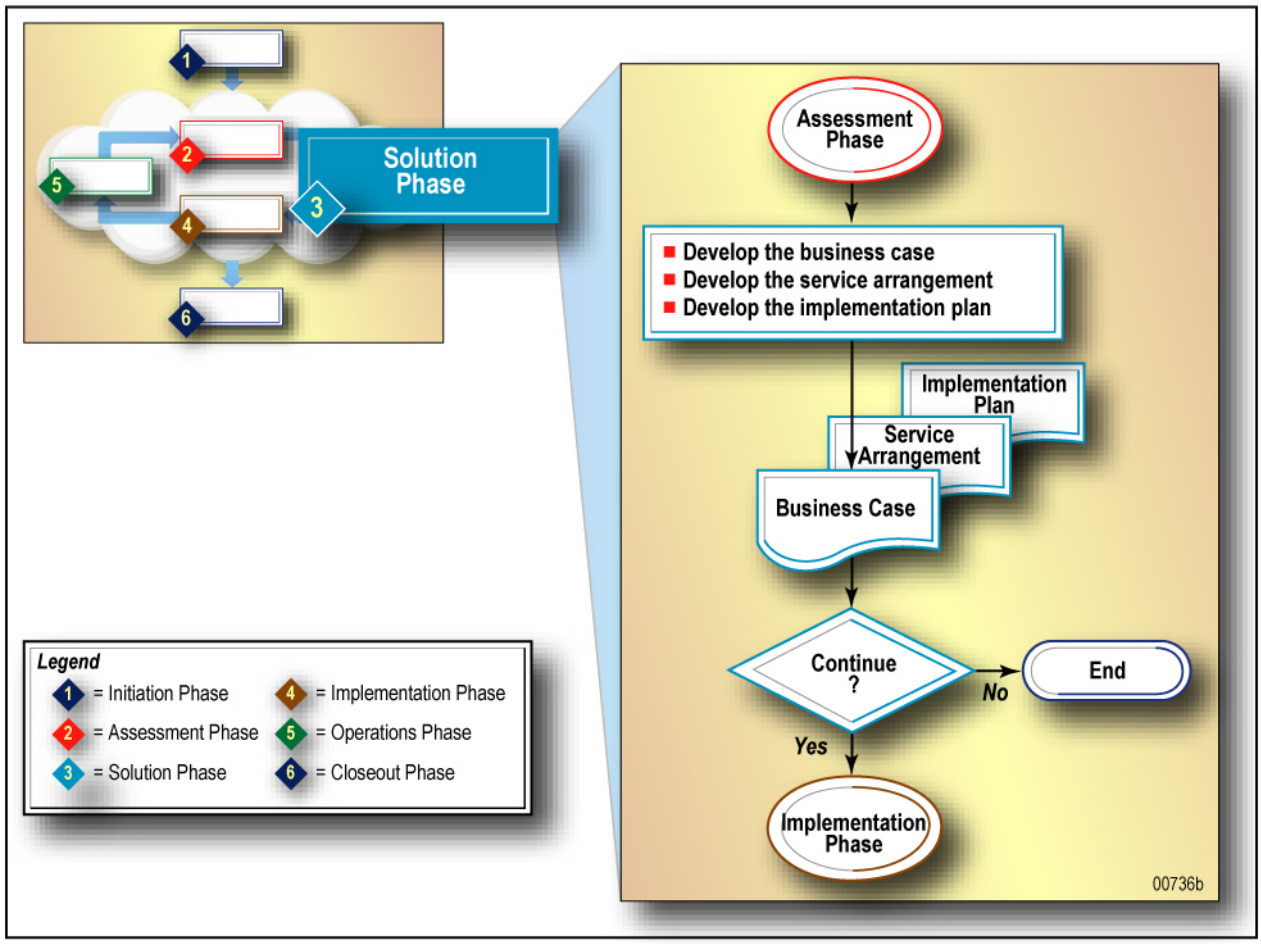

Figure 4-4. Solution Phase

Choosing a service arrangement and service level solution is only one part of this phase. Before specifying the solution, decision makers will need to develop a detailed business case for each possibility to be considered.

The business case will provide managers with the cost, benefit, and organizational risk perspective of each alternative. Comparing the costs, benefits and organizational risks will allow managers to identify a preferred solution. The implementation plan will provide managers with the means for identifying the service provider and implementing the service.

4.3.1 Develop the Business Case

During the assessment phase, the decision makers identified the current environment. To identify the preferred desired future state in this solution phase, a business case needs to be developed. The business case should provide the information necessary to identify the best solution among the alternatives. Each organization will likely have a unique methodology for developing a business case, however there are five components common to most business cases:

- **Alternative Analysis**[2]—the organization should look at all of the available options. The organization will finalize the options deemed viable enough to develop formal cost estimates, benefits analysis, and organizational risk analysis.
- **Cost Estimate**—the organization needs to develop TCO estimates for each alternative. Estimates of each alternative and the current environment must be consistent, have similar cost elements, and be based on the same assumptions.
- **Benefits Analysis**—the organization needs to formally identify the benefits of each alternative. These should be quantitative (i.e., cost savings, cost avoidance etc.), whenever possible. For example, if the organization estimates a new service implementation will lower security incident rates by 50% and each incident costs x dollars (based on metrics gathered during the assessment phase), the organization can identify the likely cost avoidance. It will also be important to look at qualitative benefits such as impact to mission, customers, etc.
- **Project Risk Analysis**—along with the benefits of each alternative, project risks must be identified. OMB has identified eight standard risk categories[3]: organizational and change management risk, business risk, data/information risk, technology risk, strategic risk, security risk, privacy risk, project resources risk. These risks might include cost overruns, schedule slippage, vendor uncertainties, privacy concerns, etc. The analysis of risks should evaluate all alternatives against the same risk factors and determine the probability of occurrence and the impact if it occurred. Then, the organization should determine the risk-adjusted cost of each alternative.
- **Evaluation of Alternatives**—finally, the organization should rank each alternative based on cost, benefit and risk. From this analysis, the organization should be able to identify the preferred alternative.

4.3.2 Develop the Service Arrangement

Developing the service arrangement could be a relatively short step as the hard work of data collection, analysis, and comparison of options has already been completed. Although the business case may not make the decision-making easy or obvious, it should provide the necessary data for decision makers to weigh, consider, and select the service arrangement that best suits the organization's needs. There will likely be some discussion and disagreement among the decision makers, but ultimately the selection must be a consensus. A service arrangement can succeed only if all business and IT security managers sufficiently buy-in to the implementing solution.

---

2 This step is most likely completed during the assessment phase.

3 OMB Circular A-11, Exhibit 300

4.3.3 Develop the Implementation Plan

At this time, the parties should determine the budget and scope of the service arrangement and begin to develop the implementation plan. The implementation plan provides a roadmap for the organization on moving from the current environment to the desired future environment. The implementation plan should address the following:

- **Project Management Roles and Responsibilities—**the implementation plan should identify the roles and responsibilities of individuals with project management roles and responsibilities for both the implementation and operations phases.
- **Budget and Scope—**IT security managers should identify the budgets and scope of the service arrangement. This effort will be important for identifying, soliciting, and assessing service providers in the next phase.
- **Implementation Process—**the program managers should begin to articulate their vision for implementing the IT security service. For example, if the program managers want to start with a test group or pilot program and/or establish a transition period for the service, the process for accomplishing this effort should be detailed here.
- **Risk Mitigation Plans—**IT security program managers should specify their plans for mitigating each risk identified throughout the assessment and solution phases.
- **Exit Strategies—**exit strategies will need to be developed to ensure the organization exits a service arrangement without disrupting other operations within the organization. The exit strategy should provide action plans for normal, planned exits, such as service agreement expiration; unexpected terminations, such as service provider bankruptcy; and potentially tension-filled exits, such as poor service provider performance.
- **Transition Management—**transition management plans should document the organization's efforts to manage the transition from the current to the desired future environment. Managers should develop plans for addressing displaced employees, handling resistance to change, shifting the organizational focus, and communicating clearly with employees about the changes. In both the transition from one service arrangement to another, there will be transition costs, perhaps significant costs. These costs should be figured into the life-cycle costs and alternatives analysis. These costs should be considered when transition plans are developed.

4.4 Phase 4: Implementation

Selecting the service arrangement and service provider may actually be the easy part of the IT security life cycle. Creating metrics and gathering data may require considerable work, especially if a metrics program is not already in place. Although the multitude of service arrangements may seem overwhelming, the objective data and methodical analysis will likely make clear the best path. Implementing those decisions requires preparation and care. Managers should develop explicit service agreements and ensure careful execution of the implementation plan. Careful planning and execution will increase the chance of success, but as the service moves to the operations phase, the leadership should manage expectations. No service arrangement will fix a problem overnight and no service provider can be expected to debut perfectly. Figure 4-5 illustrates Phase 4, Implementation, of the IT security services life cycle.

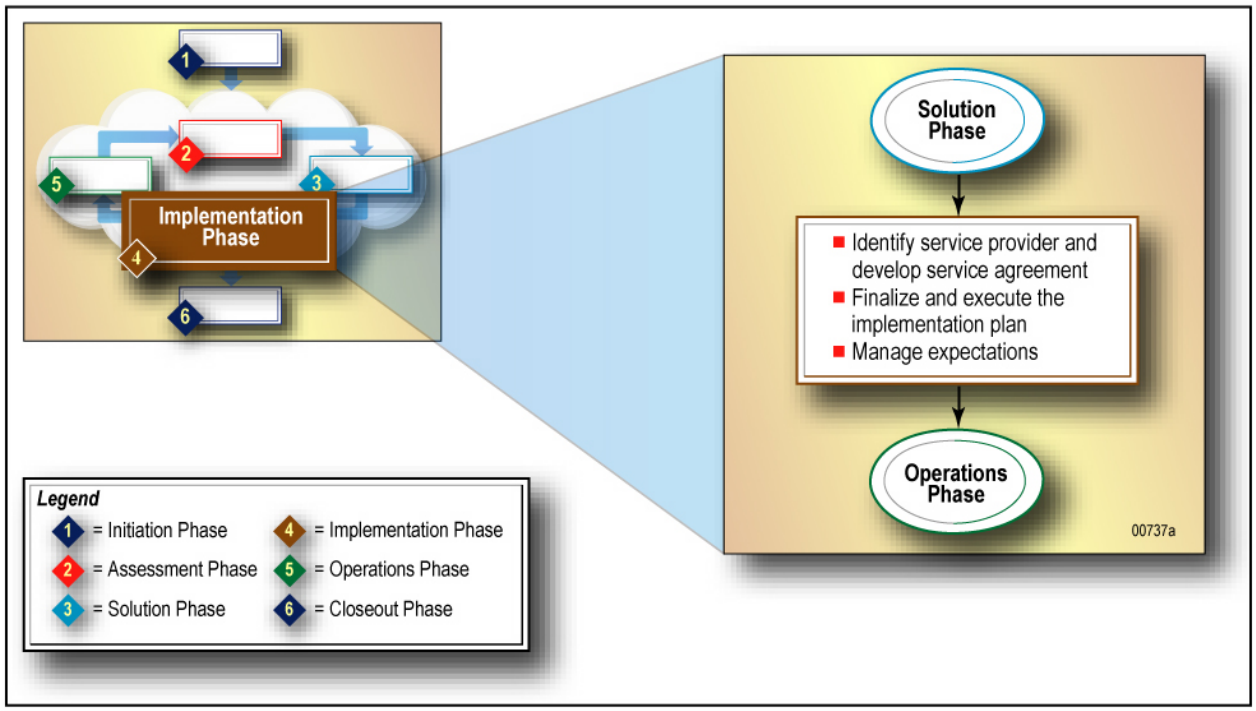

Figure 4-5. Implementation Phase

4.4.1 Identify Service Provider and Develop Service Agreement

During the solution phase, the security decision makers select the service arrangement. In this phase, they need to identify the service provider. How they do this will vary by organization, service arrangement, and type of service agreement. Internal service arrangements may already have the service provider identified. For hybrid and external service arrangements, organizations may wish to identify several potential service providers and elicit proposals. Large government organizations may release an RFP and accept formal proposals for external service arrangements. Regardless of what specific agreement methods an organization chooses to use, some basic steps apply to most situations:

Performance-based acquisition has emerged as a preferred method for engaging external service provider for many arrangements. Performance-based acquisition provides greater flexibility to service providers in suggesting an appropriate solution. Rather than requiring that a service provider to answer an RFP that specifies job positions, employee requirements, and methodologies, the organization asks the service provider to provide a cost-efficient method. The metrics identified in early phases, for example, could be turned into a statement of objectives to which the competing service providers answer with their own SOW and the cost of meeting the objectives. This is in contrast to more traditional acquisition methods where the organization would write a SOW, and the service provider would respond by indicating how much it would cost to perform that work. By placing more responsibility on the service provider, the organization is able to assess a much broader and deeper set of solutions, increasing the likelihood of finding a suitable service provider.

- **Establish Service Provider Service Level Targets—**having identified and captured the relevant data in the baseline phase, and developed the direction of the desired future environment, the IT security managers should determine the performance targets they want the service provider to meet. These service levels will be further negotiated with the service provider and formally documented in the service agreement.

- **Elicit Service Provider Proposals—**the organization may identify potential service providers in numerous ways. If the service area has few providers or exists in a new market, the organization may solicit all of the service providers in the field for quotes and their service offering. The organization may also announce an RFP and direct interested parties to provide cost proposals. Regardless of the method, the organization should try to consider as many service providers as possible to encourage competition. The organization may want to ask service providers to answer some of the questions from section 3.5 of this guide.

- **Assess the Proposals and Service Providers—**the organization should evaluate the proposals, cost quotes, and/or management plans of the various service providers, and consider each provider carefully. Although the cost of the proposal may well be a leading factor, managers need to balance cost with value, reputation of the service provider, past performance of the service provider, and ability of the service provider to support the mission of the acquiring organization. The organization also needs to ensure that the methodologies, service levels, and costs are in-line with its expectations and that they are feasible. A proposal that far exceeds the competitors in cost and service level, for example, may warrant further investigation and skepticism.

- **Select Service Provider—**once the service providers are evaluated, the decision makers should select the service provider that most closely aligns with their needs, goals, and targets.

- **Develop the Service Agreement—**Further negotiation of price and service level may be necessary; however, once these are set, a service agreement should be developed. Depending on the service arrangement, this process may be more or less formal. Internal service arrangements, for example, may consist of an agreed-on process or reporting requirement or a MOA. External service arrangements should be documented with formal contracts. Regardless of the type of document used as a service agreement, the content of the agreement should be the same for both internal and external service providers.

Agreements, regardless of type, should specify the following:

- Explicit definitions of both the organization's roles and responsibilities and the service provider's roles and responsibilities (including level of clearance or background investigation needed for staff)

- Description of the service environment, including locations, facility security requirements, and policies, procedures, and standards; and, agreements and licenses

- Defined service levels and service level costs. The service level section of the service agreement may stipulate various service levels for different types of customers or price levels and it may stipulate different service levels for various periods of performance, e.g., year 1 may demand a higher service level than year 2 of the contract.

- Defined process regarding how the managers will assess the service provider's compliance with the service level and due date targets, rules, and other terms of the agreement

- Specific remedies (e.g., financial, legal) for noncompliance or harm caused by the service provider

- Period of performance and/or deliverable due dates

- Service provider's interface to organization's management
- Organization's responsibilities with respect to making information and resources available to service provider
- Procedures and protections for commingling organization and service provider data
- Explicit rules for handling sensitive data.

Too often, service arrangements fail because one or more of these were not considered. Organizations should clearly state what they need, and service providers should clearly understand what is expected of them.

4.4.2 Finalize and Execute the Implementation Plan

Now that the service provider and service levels have been finalized, the organization can complete the implementation plan and begin to execute the plan. Some details may have changed during the service agreement negotiation, and managers should be aware of how the plan should be changed.

4.4.3 Manage Expectations

As the new service, service arrangement, and/or service provider is implemented, all parties should manage expectations. There may be some conflict as each party adapts to the new security and organizational environment and learns to operate within it. Lines of communication lines should be kept open to ensure close monitoring and cooperation between the managers and service providers.

A few important guidelines are:

- Address problems openly, whether the conflict is internal to the organization or between internal groups and external service providers.
- Allow the service provider to perform its job while still ensuring accountability.
- Maintain the security services life cycle.

4.5 Phase 5: Operations

The operations phase begins once the service provider and service have been fully implemented. During this phase, the organization, its security, and the security service provider are monitored to ensure the service arrangement best meets the firm's needs. This assessment will continue until a trigger occurs to initiate closeout of this life cycle and start of a new life cycle. Open communications should be continued, so that the organization and the service provider can address the problems that arise.

Throughout the operations phase, the organization's project managers should ensure that the service provider meets its stated service levels and complies with internal security procedures and policies. Often, for example, organizations do not ensure external service providers handle sensitive (whether personal, private, or mission sensitive) material as internal service providers do; if internal service providers needed personnel clearances, it is very likely the external service provider would also need a personnel clearance. Figure 4-6 illustrates Phase 5, Operations, of the IT security services life cycle.

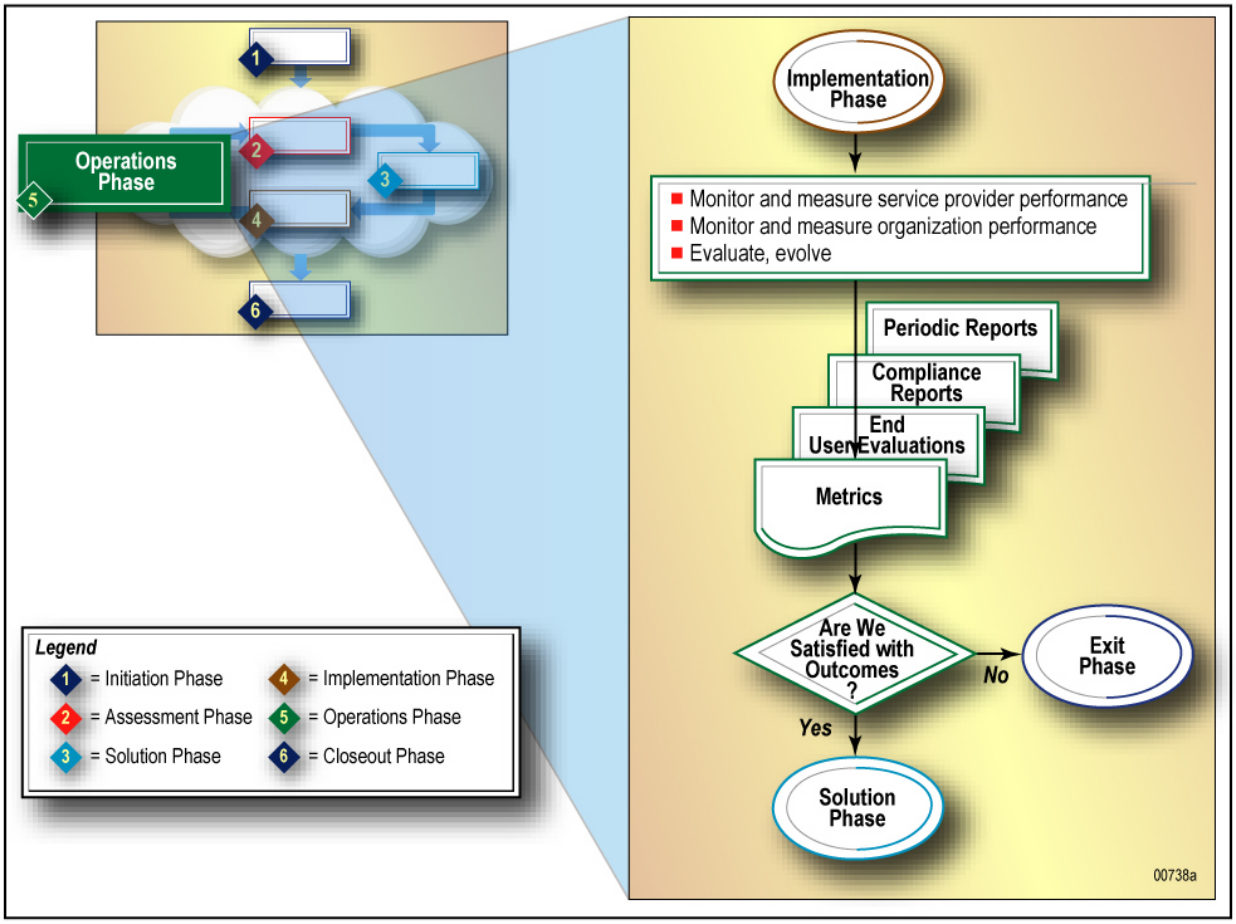

Figure 4-6. Operations Phase

4.5.1 Monitor Service Provider Performance

The operational phase is similar to the assessment phase. The data collected during the assessment phase should be used to capture the performance level of this new service provider. During the operations phase, the desired future arrangement becomes the current arrangement.

The targets set forth in the service agreement should be compared with the metrics gathered. Although metrics will provide service-level targets, the organization may also want to use end user evaluations or customer satisfaction level surveys to evaluate performance. The IT security managers will have to work with other operational managers (such as customer service managers) to ensure that the service provider is meeting service targets. The IT security managers also need to ensure service providers are complying with IT security policy and processes, as well as applicable laws and regulations. IT security managers must ensure during the operations phase that the service provider does not compromise private, confidential, personal, or mission-sensitive data. Compliance reports will help with this effort. The service agreement should have included clauses that specify penalties and/or remedies for noncompliance and management should employ these when the service provider does not perform as the contract dictates.

4.5.2 Monitor and Measure Organization Performance

While the service provider should meet the targets set forth in the service agreements, the IT security managers must look beyond the service and service provider to the entire IT security function and

organization. The IT security function should have a mix of several IT services at various levels (management, operational, and technical) and a service arrangement has technical, policy, cultural, personnel, and other impacts. Therefore, managers should ensure that the service arrangement has not negatively affected other areas while performing the service.

4.5.3 Evaluate and Evolve

The service will evolve as it matures. The monitoring and measures of the service provider and organization will allow IT security stakeholders to evaluate the organization's performance and seek ways to improve, even when meeting the targets. The world of IT security services is ever changing and security arrangements and agreements also need to change.

4.6 Phase 6: Closeout

As mentioned during the initiation phase, life cycles may overlap. As one IT security service, service arrangement, or agreement ends, another may begin. Depending on the reason for ending a service, a difficult management situation could exist. Exiting service providers may not always have the best interests of the organization in mind and may not make it easy for those replacing them. Therefore, IT security managers need to be sure to select the appropriate exit strategy and implement it well.

Figure 4-7 illustrates Phase 6, Closeout, of the IT security services life cycle.

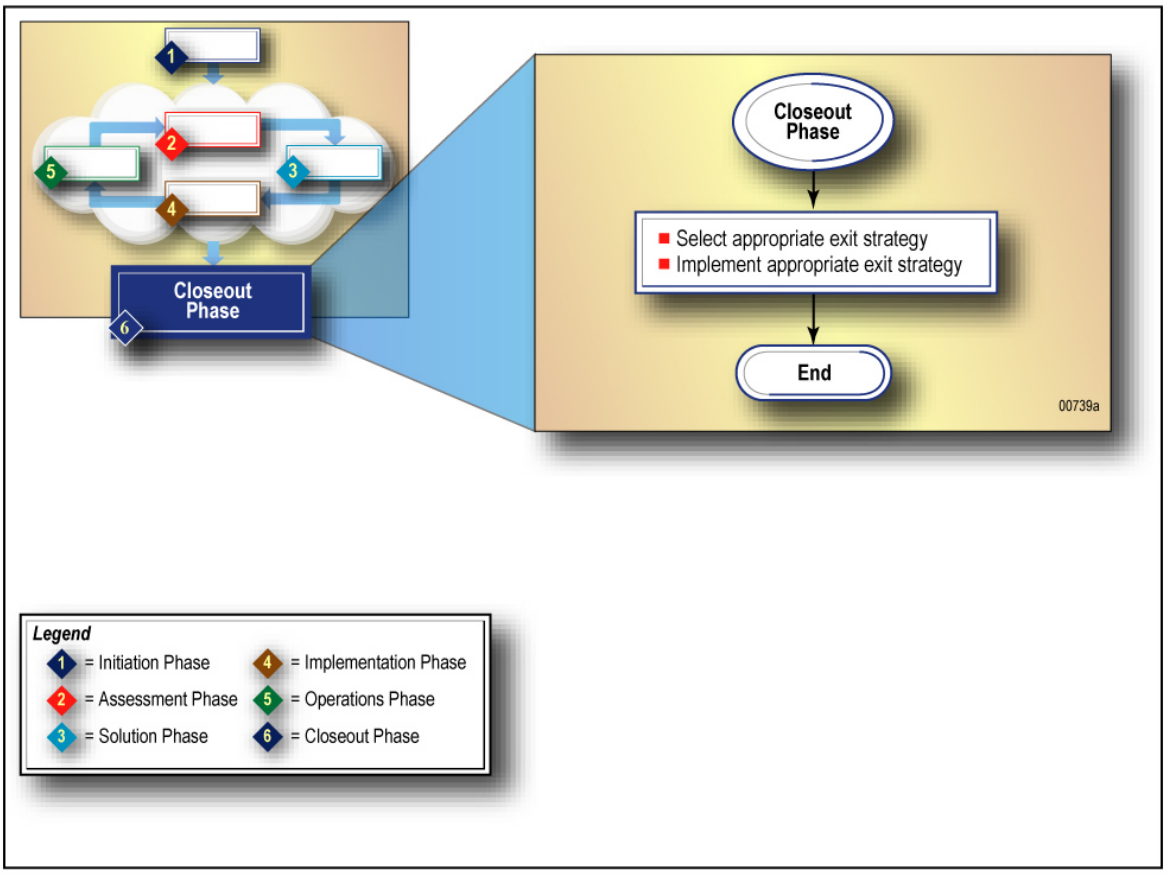

Figure 4-7. Closeout Phase

4.6.1 Select Appropriate Exit Strategy

As mentioned during the development of the exit strategy, an organization should have several exit strategies prepared and ready for implementation (section 4.3.3). Often, an organization will be able to plan in advance for the exit: the service provider and the organization have an agreed-on contract that expires in 6 months, for example. However, this will not always be the case. The service arrangement may not succeed as managers hoped, the service provider may not meet the targets, a new technology may debut, or the service provider may even have suddenly filed for bankruptcy. Managers need to be aware of these various scenarios and be ready to implement an exit strategy swiftly.

4.6.2 Implement Appropriate Exit Strategy

Once the circumstances become such that the service, service arrangement, or service provider need to be retired and the appropriate exit strategy is selected, the project managers need to implement the appropriate exit strategy. The exit strategy will best assure a careful ending and provide lessons-learned for desired future IT security service implementations.

5. Types of Services

An effective IT security program should encompass multiple layers of protection. An organization should evaluate the value and criticality of its information systems and determine the security controls that are appropriate to the level of risk. A security program, whether at the organizational or individual system level, should include an appropriate mixture of security controls: management, operational, and technical.[4] Reliance on technical resources alone will be insufficient without complementary management or operational controls.

This section presents examples of management, operational, and technical services that are discussed in this document. Table 5-1 lists these IT security services that will be discussed. Each security service is defined and the nature of the service provision explained. Then, issues and considerations unique to specific security services are provided.

Table 5-1. Security Services by Category

SECURITY SERVICE	CATEGORY
Security Program	Management
Security Policy	Management
Risk Management	Management
Security Architecture	Management
Certification and Accreditation	Management
Security Evaluation of IT Products	Management
Contingency Planning	Operational
Incident Handling	Operational
Testing	Operational
Training	Operational
Firewalls	Technical
Intrusion Detection	Technical
Public Key Infrastructure	Technical

An exhaustive list of every security service available is not provided. Security service providers may package elements of many of these services into a unique service offering with a unique name. Advances in technology will create new security services. In many cases, the issues and considerations provided for the services presented in this guide may be used or modified for other security services.

[4] Management, operational, and technical controls are discussed in detail in NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, and NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems* and in SP 800-53, *Recommended Security Controls for Federal Information Systems.*

5.1 Management Security Services

5.1.1 IT Security Program Development

An IT security program is a set of security controls, which can be grouped under the terms management, operational, and technical. Federal law and regulations, such as the *Federal Information Security Management Act* (FISMA) of 2002, OMB Circular A-130, *Security of Federal Automated Information Resources*, and other government-wide policies, standards, and procedures issued by the OMB, NIST, and other agencies establish the policies, standards, and procedures for federal organizations.

Because policy is typically written at a broad level, organizations must also develop standards, guidelines, and procedures that provide employees with a clear approach to implementing policy. Standards and guidelines specify technologies and methodologies that will be used to secure systems; procedures are detailed steps to be followed to accomplish particular security-related tasks. Standards, guidelines, and procedures may be distributed throughout an organization via handbooks, regulations, or manuals. Together, these documents will ensure that employees are aware of their role in IT security and comply with the IT security program.

IT Security Program Services

Service providers can assist organization decision makers in developing and maintaining an organization-wide security program, helping to ensure effective implementation of the program, evaluate the performance of major organization components, and provide appropriate security training of organization employees with significant security responsibilities. The service providers can also perform independent evaluations and audits of an organization IT security program.

A comprehensive IT security program service can consist of many elements that will depend on the specific needs of the organization and the relative maturity of its IT security program. The elements of an IT security program service may include the following:

- Assess the risk to operations and assets under the organization's control
- Determine the level of security appropriate to protect the organization's operations and assets
- Develop and maintain a current security plan for each system supporting the operations and assets under organizational control
- Develop security incident handling procedures
- Develop processes for sharing information regarding common vulnerabilities, including a description of procedures for external reporting
- Develop a set of effective security controls and techniques
- Develop capital planning and investment control processes that ensure appropriate integration of security controls into IT investments
- Develop a set of IT security metrics that enable an organization to effectively assess the adequacy of in-place security controls, policies, and procedures and to adequately justify security control investments

- Analyze the extent of integration of an organization's IT Security Program with its Critical Infrastructure Protection or CIP responsibilities.

5.1.2 IT Security Policy

In the context of this guide, IT security policy is defined as the "documentation of IT security decisions." IT Security Policy is fully discussed in NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook. NIST SP 800-12 categorizes IT Security Policy into three basic types:

- **Program Policy**—high-level policy used to create an organization's IT security program, define its' scope within the organization, assign implementation responsibilities, establish strategic direction, and assign resources for implementation.
- **Issue-Specific Policies**—address specific issues of concern to the organization, such as contingency planning, the use of a particular methodology for systems risk management, and implementation of new regulations or law. These policies are likely to require more frequent revision as changes in technology and related factors take place.
- **System-Specific Policies**—address individual systems, such as establishing an access control list or in training users as to what system actions are permitted. These policies may vary from system to system within the same organization. In addition, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's electronic mail (e-mail) policy or fax security policy.

IT Security Policy Services

Service providers can assist organizations in analyzing existing and developing new security policies, standards, guidelines, and procedures. The authority for approving policy is inherently a core function of an organization and therefore final approval of policies should be performed by the organization. Given this constraint, organizations should limit service providers, either internal or external, to assistance and support. A comprehensive IT security policy service can consist of many elements that will depend on the specific needs of the organization and the relative maturity of its IT security program.

IT security policy elements may include the following:

- High-level analysis of an organization's operational environment
- Emerging Technologies
- Governance processes[5]
- Procedures
- Determination of compliance to applicable guidance and regulations
- Gap analysis for the organization or program that assesses the differences between the current policy and the desired future policy
- Development of a unified set of security program policies and detailed issue- and system-specific policies

[5] Governance is about how strategy and policy decisions are made, distributed, and enforced. Governance represents the top-level of management; it defines the operating envelope for the agency or program, which is carried out by the various managers of the IT security program. Governance is composed of people (i.e., roles), organizational structures, processes, and decision support tools, many of which should be defined in policy (not necessarily the IT Security Policy).

- Development of short-, medium-, and long-term implementation plans identifying tasks, resources, priority, and ownership
- Development of IT security metrics.

5.1.3 Risk Management

Risk management is comprehensively discussed in NIST SP 800-30, Risk Management Guide for Information Technology Systems. NIST SP 800-30 notes that the primary goal of risk management is to "balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting IT systems and data."

Risk Management Services

Service providers offer various combinations of service packages for supporting risk management activities. The service provider may develop risk management guidance for supporting an organization's risk management program. The service provider may manage the risk management program as a whole but the organization should always retain the responsibility for the program. The service provider may also perform a risk assessment and/or develop a risk mitigation plan. If the organization already has a mature and operational risk management program, the service provider may audit the program for effectiveness.

5.1.4 IT Security Architecture

Security architecture refers to the strategic planning and development of an IT infrastructure that supports the mission and the security objectives. It is a process that is developed during the security design phase after a security requirements analysis has been conducted to support it.

IT Security Architecture Services

If the organization asks a service provider to design a new security architecture, the service provider must have access to the technology and security baseline of the organization's current architecture. The service provider can conduct baselining if it has not already been done by the organization. Baselining services include identifying its business needs, functional requirements, security requirements, and risk assessments, as well as the security controls in place. A service provider can identify security controls and identify and assess technologies that will enforce the organization's security policies. A service provider can develop a methodology for selecting the security solutions that best serve the organization's needs and design a technical architecture. Finally, the service provider should document the security architecture.

5.1.5 Certification and Accreditation

Accreditation is the formal declaration by an authorizing official that a system is approved to operate at an acceptable level of risk and in a particular environment using a prescribed set of technical, managerial, and operational safeguards to an acceptable level of risk. Accreditation is usually supported by a technical security evaluation, a risk assessment, a contingency plan, and signed rules of behavior. Certification is the technical security evaluation of an IT system made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

NIST SP 800-37 (draft), *Federal Guidelines for the Security Certification and Accreditation of Information Technology Systems* establishes standard processes, activities and general tasks, and management approaches designed to certify and accredit an information system.

Certification and Accreditation Services

The complexity and rigor of specific certification activities will vary depending on the system criticality, information sensitivity, system exposure, and level of concern. C&A service providers can manage or conduct a complete certification or prepare and assess individual documents in the final certification package that is ultimately presented to the accreditor for approval.

C&A service activities can include any of the following:

- Developing a security test and evaluation (ST&E) plan and test procedures
- Conducting an ST&E
- Analyzing and reporting test results
- Developing and/or conducting a vulnerability assessment
- Developing a final vulnerability assessment report
- Technical support to the certifier or accreditor.

5.1.6 IT Security Product Evaluation

Two prominent security testing and evaluation programs are now in place to assess the security features and assurances of commercial off-the-shelf (COTS) products: National Information Assurance Partnership[6] (NIAP) Common Criteria[7] (CC) Evaluation and Validation Scheme (CCEVS) and NIST Cryptographic Module Validation Program[8] (CMVP). In both programs, a government body validates the results of the testing and evaluation processes conducted by private sector laboratories to ensure that the security standards are being applied correctly and consistently. When products cannot be found on existing validated product lists, it may be possible that other parties have evaluated a particular product. In many cases, it is not cost effective to conduct comprehensive security evaluations for the one-time use of an IT security product unless that product will be used extensively throughout an organization and therefore, products on the validated product list should be considered as an alternative. Additional information regarding security assurance can be obtained from NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*.

IT Security Product Evaluation Services

The NIAP CCEVS employs a network of private sector, accredited testing laboratories to independently evaluate commercial security products in a variety of key technology areas against a set of security requirements and specifications from the international standard, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408, *Common Criteria for IT Security Evaluation*. The CMVP, also using independent, accredited, private-sector laboratories, focuses on security conformance testing of cryptographic modules against FIPS 140-2, *Security Requirements for Cryptographic Modules*, and related federal cryptographic algorithm standards.

[6] See http://niap.nist.gov
[7] Additional product evaluation services could include development and evaluation of Common Criteria protection profiles.
[8] See http://csrc.nist.gov

5.2 Operational Security Services

5.2.1 Contingency Planning

The modern networked computing environment brings significant challenges to the development of contingency plans. Networked computing has changed the scope and focus of what has traditionally been a local issue. Contingency planning is designed to reduce the consequences of any loss of data or infrastructure. Contingency planning enables organization personnel to restore critical IT functions and connectivity rapidly, effectively, and safely. The contingency plan defines the procedures, resources, tasking, and information required for performing recovery actions in response to a broad range of events. A well-executed and tested contingency plan also gives confidence that critical resources will be available when needed and facilitates an organization's continuity of operations in an emergency situation. The plan is a living document that must be updated regularly to reflect changes to the system's configuration and operations. Additional information on contingency planning is provided in NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*. This guide discusses various contingency plans that will help sustain and recover critical IT services following an emergency.

The contingency plan should address, at a minimum, the following five main components: supporting information, notification/ activation, recovery, reconstitution, and supporting appendixes.

- **Supporting Information**—provides an introduction and concept of operations for the plan
- **Notification / Activation**—items such as notification procedures, damage assessment, and plan activation
- **Recovery**—items such as a sequence of recovery activities, and recovery procedures
- **Reconstitution**—items such as the sequence of recovery activities, testing of systems, and termination of operations
- **Plan Appendixes**—items such contact information, equipment lists, service agreements, and any other related contingency plans.

Contingency Planning Services

Service providers offer their services for various phases of the contingency planning life cycle. In considering whether to contract out contingency planning services, the organization could conduct a cost-benefit analysis for each breakdown of the service offering (e.g., develop, update and test, and execute the contingency plan).

- **Develop—**service providers can develop the organization's contingency plan. This service requires gathering information from many functional areas. The vendor's first step should be to perform a business impact assessment (BIA) to determine the system's internal and external dependencies, allowable outage times, and recovery priorities. The BIA provides a basis for developing the specific recovery strategy and procedures that comprise the heart of the contingency plan.
- **Update and Test—**updating the plan as needed is critical to its success because the contingency plan is a living document. It is very common to retain the same service provider that developed the plan to update and test it. Updates to the plan should be made when changes in personnel, procedures, assets, or other resources are incorporated into the system.

  Service providers may also ensure that the plan is tested before circumstances require its use. The test may be a walk-through or a simulated drill, or a full operational exercise that encompasses all

aspects of the plan. Results of the testing exercise would be documented in the contingency plan and discussed with management. The results will determine the effectiveness of the contingency procedures and present any flaws. Staff must be trained in their contingency-related duties so that when an unexpected event interrupts operations, recovery will be easier and people will know what to expect.

- **Execute—**the responsibility for the execution phase of contingency planning lies with the organization, but service providers may support certain aspects of the execution phase. For example, an organization may outsource data recovery because service providers can provide hot or mobile sites for system and data recovery. They may provide periodic training to organization personnel on the plan and their roles in the plan.

5.2.2 Incident Handling

An IT security incident is an adverse event in a computer system or network caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms. An incident-handling capability can provide the ability to react quickly and efficiently to disruptions in normal processing. Effective incident handling can be achieved by developing and instituting effective processes and procedures for the six phases of incident response: preparation, identification, containment, eradication, recovery, and follow-up. The incident handling process should be consistent and compatible with any forensic services that the organization may require to ensure that critical evidence is handled properly.

Incident-Handling Services

Incident-handling capability should be available 24 hours per day, 7 days a week. A service provider may be able to provide one or a combination of the services listed below.

Incident-handling services may include the following:

- Developing the incident handling program
- Developing and maintaining system configuration profiles
- Providing forensics capabilities
- Testing and updating incident handling procedures
- Managing and executing the incident handling procedures

Incident-handling procedural services may include the following:

- Isolation of affected systems and platforms
- Triage
- Report assessment (interpret log files, prioritize, and analyze)
- Identification/Verification (determine nature and scope of incident)
- Categorization (determine sensitivity of compromised information, system, and incident)
- Internal and external coordination (notify and coordinate with appropriate internal and external parties on a need-to-know basis)
- Resolution

- Technical assistance (provide detailed analysis of event, such as how it occurred and what failed to work properly)
- Eradication (eliminate incident causes and effects)
- Recovery (return systems to normal operations)
- Preventative support
- Operations, maintenance, and monitoring of IDS (incident response tied directly to IDS)
- Training
- Post-incident consulting
- Third-party analysis, validation of eradication and recovery, corrective and mitigation actions, and reporting.

5.2.3 Testing

Testing the security posture of information systems and networks is a critical component of securing a system. A complete and exhaustive discussion of testing is beyond the scope of this document.[9] Testing is the only way to validate that the security measures and procedures are working as intended. Testing can also assist in identifying previously unknown weaknesses or vulnerabilities. All test activities, whether manual or automatic, require human involvement and thus could be provided as a service.

The results of testing can be used in the following ways:

- As a reference point for any corrective action
- As a benchmarking tool to enable the organization to track its progress
- To assess implementation of system security requirements
- For cost-benefit analysis
- As an input into the larger life-cycle activities, such as risk assessments, functional requirements analysis, C&A, and performance improvement efforts.

Categories of testing can include the following:

- Network mapping
- Vulnerability scanning
- Penetration testing
- ST&E
- Password cracking
- Log review
- Integrity checkers
- Virus detection
- War dialing.

[9] Readers should refer to the NIST Special Publication 800-42, *Guideline on Network Security Testing,* for more information about each category and type of security testing.

Testing Services

Because of its highly specialized and technical nature, testing is one security activity that is frequently considered for external service providers. However, because it is a highly invasive measure, it is important that service providers be capable and trusted by the organization. Testing can be conducted as a separate activity or as part of the risk management program, under risk assessment. The service provider will need clear and unambiguous direction from management (a written "rules of engagement"), a set of Internet Protocol (IP) addresses, and clearly defined scope for testing as well as input on what is required for planning and assessment, requirements analysis, test execution, and analysis results and documentation.

5.2.4 Training

Training is one of the most critical components in maintaining the security posture of operational systems. Securing any organization's IT systems cannot be achieved without skilled, knowledgeable, and trained personnel at all levels. Security training and education must be considered an ongoing effort that is an integral part of conducting business. With constantly evolving technology, education—especially in the security arena—must keep pace with the perpetual changes and advances. Managers must understand the current status of their security programs and controls to make informed judgments and investments to appropriately mitigate risks to an acceptable level. All users of IT systems must be aware of their responsibilities for protecting information and IT resources.

The IT Security Learning Continuum from NIST SP 800-16, *Information Technology Security Training Requirements*, and shown in Figure 5-1, represents instructional guidance for IT security awareness, training, and education programs. The model is created from requirements of several federal regulations, including OMB Circular A-130.

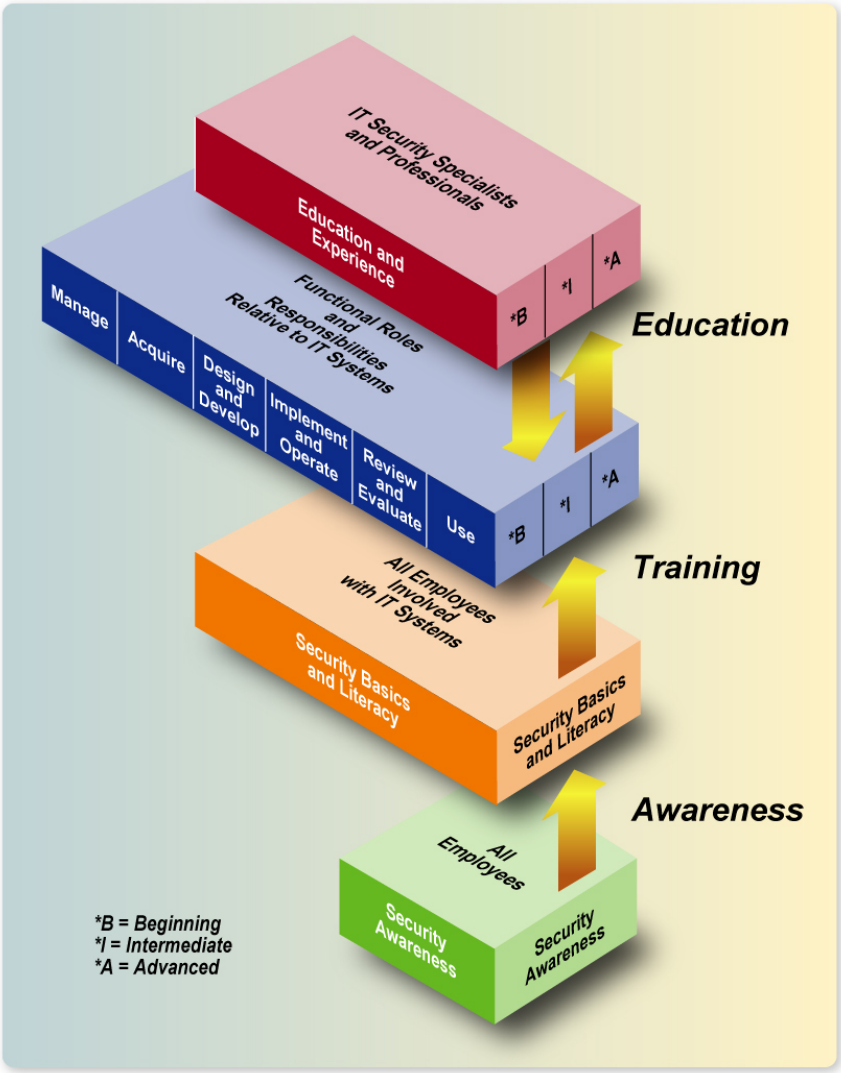

Figure 5-1. Information Technology Security Learning Continuum

The model illustrates a three-dimensional array that integrates the following:

- **Three types of training**—awareness, training, and education,
- **Six functional security roles**—manage, acquire, design and develop, implement and operate, review and evaluate and use
- **Three levels of training**—beginning, intermediate, and advanced.

The NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, provides detailed guidance on designing, developing, implementing, and maintaining an awareness and training program within an organization's IT security program. This guide builds upon NIST SP 800-16 by describing four steps in designing and implementing an IT security training and awareness program.

- Designing an Awareness and Training Program
- Developing Awareness and Training Material
- Program Implementation
- Post-Implementation

Training Services

IT security training service providers may offer a wide range of services to support the "total" security awareness and training program. They can design, develop, implement, and maintain a program for the organization, but also assist with specific elements of the organization training and awareness program. The service provider can provide the following services:

- Program level support
- Course level support
- Training support services.

5.3 Technical Security Services

5.3.1 Firewalls

A firewall is a device that has a network protection application installed to safeguard the network from intentional or unintentional intrusion. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The term “firewall” is derived from the process in which, by segmenting a network into different physical subnetworks, the firewalls limit damage that could spread from one subnet to another, acting in the same manner as fire doors or firewalls in automobiles.

Firewall Services

Service providers can perform any or all of the following firewall functions:

- Design a firewall solution that incorporates single and/or multiple firewalls
- Install and integrate a firewall(s) into new and existing networks
- Monitor firewall services to ensure availability and integration with other technical controls, such as incident response or intrusion detection systems (IDS)
- Manage the organization’s firewalls, including periodically upgrading them.

The organization can select specific service providers with a trusted family of products that belongs to them or general service providers who specialize in offering a wide variety of security services while using products and components from outside vendors.

5.3.2 Intrusion Detection

Intrusion is any set of actions that attempts to compromise the integrity, confidentiality, or availability of a resource. Intrusion detection is a passive security activity that sits on the network or on selected hosts. Devices that are part of the IDS are used to detect intrusion and provide information to a central

management console. This information is reviewed by security staff to determine if a valid security breach has taken place. An IDS performs a variety of functions:

- Monitor user and system activity
- Audit system configuration and vulnerabilities
- Assess integrity of critical system and data files
- Recognize activity patterns reflecting known attacks
- Perform statistical analyses for abnormal activity patterns
- Provide operating system audit trail management, with recognition of user activity reflecting policy violations
- Provide customized reports.

This ongoing monitoring and assessment is a necessary part of an overall security architecture. IDSs generally improve the integrity of other parts of the information security infrastructure by identifying specific indications of a possible attack and causing a reexamination of defenses. They can often trace user activity from the point of entry into the network to point of exit. IDSs can recognize specific types of attacks and alert appropriate staff (if configured to do so).

Intrusion Detection Services

To be effective, intrusion detection requires a robust knowledge base of attack signatures against which the IDS can tally its findings. Threats and vulnerabilities are not static in nature and are continuously changing and evolving. The attack signatures database should be updated frequently for the IDS to be able to detect the most recent threats. Service providers may have greater leverage to accomplish this at less cost because several customers can share the overhead of maintaining the database for a single IDS product. IDSs require a high level of expertise to operate and manage. If the nature of the intrusion is such that the IDS or the service provider is incapable of resolving the matter or the contract does not require the service provider to resolve the problem, the service provider can contact the organization, which in turn escalates the case for resolution.

5.3.3 Public Key Infrastructure

Modern security architectures protect and distribute information that is needed in a widely distributed environment, where the users, resources, and stakeholders may all be in different places at different times.[10] PKI is an approach (consisting of products, services, facilities, policies, procedures, agreements, and people) that addresses these security needs and makes use of the scalable and distributed characteristics of PKI. PKI allows organizations to conduct business electronically with the confidence that:

- The person or process identified as sending the transaction is actually the originator (nonrepudiation)
- The person or process receiving the transaction is the intended recipient (identification and authentication)
- Data integrity has not been compromised (integrity).

[10] This section on PKI is drawn extensively from NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI* and NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication.*

In addition to the three services mentioned above, a PKI can also provide two additional services: key recovery and privilege/authorization.

- **Key Recovery**—organizations must be able to recover data that the employee has encrypted, which can only be done by recovering the encryption key when the key is unavailable.[11]
- **Privilege/Authorization**—certificates can be used to vouch for a user's identity and also specify privileges the user has been granted.

Functional elements of a public key infrastructure include certification authorities (CA), registration authorities (RA), repositories, and archives. The nature of PKI is that it is a very technical security control. Several detailed NIST publications exist that further describe PKI:

- NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI*
- NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*

PKI Services

Designing, developing, deploying, and maintaining a PKI is a complex technical challenge that is compounded by a number of factors:[12]

- Interoperability
- Scalability
- High costs (deploying a PKI and enabling software applications)
- Complex policy development
- Training challenges for a technology that can be complex and difficult to understand.

PKI services can be packaged in numerous ways. The entire PKI process can be performed by a service provider, a security provider can manage the PKI in house, or PKI elements may be performed by a provider (hybrid). The following list provides examples of PKI elements[13] that could be performed by a service provider:

[11] Reasons for key recovery are varied and may include an employee forgetting a password to unlock an encrypted file, the death of an employee who has encrypted some information, or someone attempting to hide criminal activity from law enforcement officials.

[12] GAO Report 01-277, "Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology," February 2001.

[13] http://hydra.gsa.gov/aces/order.pdf, 5 September 2001.

Table 5-2. PKI Service Element Examples

Certificate Validation	Validity checking of certificates with the service provider that issued the certificate whenever the application requires authentication of those attempting access
Certificate Issuance	Issuance of certificates to applicants if identity proofing has been successfully completed by the service provider, or provided by the organization
Supplemental PKI Services	PKI-related programming, systems integration, and telecommunications interface support
Technology Updates	Incorporation of new algorithms, formats, technologies, mechanisms, and media
Ad Hoc Data Collection, Analysis, and Dissemination	Ad hoc data collection, analysis, and/or dissemination services related to PKI services
Hardware Tokens	Hardware tokens to generate key pairs and storage of the private key.

THIS PAGE INTENTIONALLY LEFT BLANK.

Appendix A—REFERENCES

NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Computer Security Handbook*, February 7, 1996.

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.

NIST SP 800-31, *Intrusion Detection Systems*, November 2001.

NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.

NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003.

NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, draft.

NIST SP 800-42, *Guideline on Network Security Testing*, October 2003.

NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, draft

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003.

NIST Publication, *Introduction to Public Key Introduction to Public Key Technology and the Federal Technology and the Federal PKI*, February 26, 2001.

NIST Interagency Report (NISTIR) 4749, *Sample Statements of Work for Federal Computer Security Services: For Use In House or Contracting Out*, June 26, 1992.

FIPS 140-2, *Security Requirements for Cryptographic Modules*, June 2001.

Federal Information Security Management Act of 2002, 44 U.S.C. Chapter 35, Subchapter III. 2002.

Federal Financial Institutions Examination Council (FFIEC), *Guidance on the Risk Management of Outsourced Technology Services*, SR Letter 00–17, November 2000.

Gartner Research, *The Price of Information Security* Gartner Group, June 1, 2001.

General Service Administration, Information System Security Managers and Information System Security Officers Training, September 2000.

Lessons Learned from the Federal Computer Incident Response Capability (FEDCIRC) Pilot: http://csrc.nist.gov/topics/incidentNIST/sanspaper.htm, August 1998.

MIS Training Institute, *Auditing your Information Security Program*, Class Notes (Personnel Security), September 2003.

OMB Circular A-11, *Planning, Budgeting, and Acquisition of Capital Assets*, June 2002.

OMB Circular A-76, *Performance of Commercial Activities*, May 2003.

OMB Circular A-130, *Management of Information Resources*, November 2000.

Web Sites

http://csrc.nist.gov

http://niap.nist.gov

http://www.cert.org/security-improvement/modules/omss/index.html

THIS PAGE INTENTIONALLY LEFT BLANK.

Appendix B—ACRONYM LIST

BIA	Business Impact Assessment
C&A	Certification and Accreditation
CA	Certification Authority
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
COTR	Contracting Officer's Technical Representative
e-mail	Electronic Mail
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
IDS	Intrusion Detection System
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PKI	Public Key Infrastructure
PUB	Publication
RA	Registration Authority
RFP	Request for Proposal
SDLC	System Development Life Cycle

SLA	Service Level Agreement
SOW	Statement of Work
ST&E	Security Test and Evaluation
TCO	Total Cost of Ownership
U.S.C.	United States Code

Appendix C—SERVICE AGREEMENT OUTLINE

A service agreement can take many different forms depending upon the type and scope of the service, the service arrangement, and type of organization. The sample service agreement outline provided in this appendix is intended solely as a guide; the specific format, clauses, and terms will be unique to each organization. IT security managers should develop their service agreements only after negotiations with the service provider and, most importantly, in consultation with their organization's legal and contractual experts.

1. Introduction–introduces the purpose, participants, and service.

    1.1. Purpose
    1.2. Participants
    1.3. General Service Description

2. Service Environment–describes the environment in which the organization will perform the service, from physical location, to hardware/software being used, to the policy and procedures the service provider will need to follow.

    2.1. Equipment
    2.2. Facilities
    2.3. Entities and Locations
    2.4. Policies, Procedures and Standards
    2.5. Agreements and Licenses

3. Roles and Responsibilities–describes the roles and responsibilities of all major participants. The service provider responsibilities need to articulate not just the service tasks, but also the documentation of their services, reporting their actions, and support functions (e.g., if the new service will likely initiate trouble calls, the service agreement should articulate who and how these calls will be handled).

    3.1. Service Provider Responsibilities
        3.1.1. Service Tasks
        3.1.2. Documentation
        3.1.3. Service Support
        3.1.4. Reporting Requirements

    3.2. Client Organization Responsibilities

4. Service Level–identifies the metric, the service level, and methodology for assessing the service level. For further guidance on developing metrics, NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, provides guidance on developing and gathering metrics, as well as sample IT security metrics. Organizations may choose to articulate the service level in a range: from unacceptable to minimum to interim to target, or they may choose to set varying service levels for various user groups or schedule times. If so, each service level will need to be articulated.

    4.1. Objectives
    4.2. Metric(s)
    4.3. Service Level
    4.4. Service Level Assessment

5. Terms and Adjustments–provides the costs and period of performance of the service levels and roles and responsibilities articulated in the previous sections as well as providing processes for resolving service agreement disputes, remedying non-compliance, and amending the agreement to account for changing requirements.

    5.1. Costs
    5.2. Period of Performance
    5.3. Dispute Resolution
    5.4. Remedies for Non-Compliance
    5.5. Maintenance of Agreements

Appendix D—SAMPLE ACQUISITION LANGUAGE

D.1 Introduction

This Appendix presents language[14] that is appropriate for inclusion into information technology (IT) security service Statements of Work (SOW) or other forms of service provider agreements and covers some of the services presented in this document. Although the language is not a substitute for good IT security management, organization staff and government service providers can use this appendix as a basis for a common understanding of each described activity. The sample language can foster easier access to more consistent, high-quality IT security services. The descriptions apply to contracting for services or obtaining them from within the organization. It is worth reiterating that close consultation and guidance with your acquisition officials and legal counsel is always prudent as they are the experts in what is often a complicated and arcane area of expertise.

D.2 Sample Acquisition Language

The language presented here is a sample and is not intended as "boiler plate." Each organization should analyze its specific needs and determine its functional, resource, schedule requirements, and constraints. The language may be used, with appropriate tailoring, by various organizational levels (e.g., department, agency, bureau, region, branch, and field office). Additional acquisition language can be found in NIST Special Publication (SP) 800-64, *Security Considerations in the Information System Development Life Cycle*.

The document uses the greater-than lesser-than symbols <> to indicate information the organization will complete. To help fill this area with appropriate information, a generic term or explanation is used (e.g., organization name). Instructions to those tailoring or refining the language are presented as notes, indicated as [NOTE].

Those tailoring the language in this appendix may find other NIST publications valuable. Those performing these tasks can also benefit from other NIST Special Publications.

Many but not all of the services discussed in this guide are presented in this appendix. In many cases, the language provided in this appendix can be tailored to fit other security services. The deliverables mentioned within the language are samples and need to be tailored to meet an organization's specific needs.

In addition to acquisition language for services discussed in this guide, acquisition language is provided for services to evaluate IT security products and general IT security services contract management.

[14] This section is drawn from NISTIR 4749, *Sample Statements of Work for Federal Computer Security Services: For use In House or Contracting Out*, December 1991. The language in Appendix C was first developed as SOW language. It should be modified if it will be used in internal MOAs.

D.3 Management Security Services

D.3.1 Develop an IT Security Program

D.3.1.1 Review Current IT Security Status

The Contractor shall, with the assistance of the <IT security officer, Chief Information Officer (CIO), Program Manager or other designated person> and the Federal Information Technology Security Assessment Framework as a guide, determine the current IT security program status. The Contractor shall determine what IT security program elements and documents exist. For those that exist, the Contractor shall review them. The Contractor shall note what elements or documents exist. The review shall examine documentation from the following:

- Application systems certifications, reviews, and risk analyses
- IT installation reviews
- Technical software evaluation
- Contingency and disaster recovery plans and tests
- Personnel security
- IT security awareness and training
- Security management and coordination.

The Contractor shall conduct an estimated <N> trips to field installations to assess the <organization name> IT security program.

The Contractor shall also review the following:

- Existing policy and procedures
- Applicable federal regulations
- Organization mission statements
- Organization information management resources policy statements
- IT security goals, policies, procedures, and standards
- IT security and privacy plans
- Other associated documents.

The Contractor shall prepare a report documenting the findings of this task, including elements or documents that do not exist. The Contractor shall deliver the Current IT security Status Report to the Contracting Officer's Technical Representative (COTR).

D.3.1.2 Develop Framework for the IT Security Program

The Contractor shall develop the framework for the IT security program. This framework shall include a draft IT security policy statement. The framework shall identify the major program elements, to include at a minimum:

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorize Processing (Certification and Accreditation)
- System Security Plan
- Personnel Security
- Physical and Environmental Protection
- Contingency Planning
- Hardware and System Software Maintenance
- Production, Input/Output Controls
- Data Integrity
- Documentation
- Security Awareness, Training and Education
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails.

The report shall identify the resources available and/or required, including staff, budget, and equipment.

The Contractor shall <prepare/revise> a draft <organization name> IT security goals and policies statement(s). The goals shall reflect federal regulations and the organization mission. The policies shall reflect the IT security goals.

The Contractor shall deliver an IT security Program Structure Report and Policy Statement to the COTR.

D.3.1.3 Review Management Procedures and Controls—Program Assessment

The Contractor shall examine the management procedures that support security. This includes a study of the organization's governance structure, the authorities and responsibilities, and the separation of functions. The Contractor shall also provide a list of management controls to be reviewed in each area (general, physical, data, and system and application software). This list shall, at a minimum, include the following:

- Written policies and operating procedures
- Error and discrepancy reporting procedures
- Organization and reporting hierarchy, including proper separation of duties
- Development and implementation of security awareness and training
- The Contractor shall deliver the Management Procedures and Controls Report to the COTR.

D.3.1.4 Prepare Program Assessment Report

The Contractor shall develop a program assessment report, which summarizes overall security program compliance with appropriate federal, state, local law and policy as well as internal policy and procedures. The report shall detail major security weaknesses requiring correction and potential savings. It shall provide a summary of each area by area reviewed, findings, impact of weaknesses in security (if any), and recommendations of actions that could be taken by management (if any). The report shall also identify those areas requiring more detailed study. The Contractor shall deliver the Program Assessment Report to the COTR.

D.3.2 Development and Review of IT Security Policies

D.3.2.1 Develop IT Security Program Details and Strategies

The Contractor shall develop a set of IT security program topics and/or strategies, including the following:

- Security policy and plans
- Risk management
- Security controls
- Rules of behavior
- Life-cycle management
- Certification and accreditation
- Personnel, physical, and environmental security
- Computer support and operations
- Contingency planning
- Training
- Incident response
- Access control
- Audit trails
- Log files

Each strategy shall include the following:

- Draft position descriptions, including authorities and responsibilities
- Staffing justifications
- Resource requirements projections
- Budget projections
- Milestones and schedules.

For each strategy, the Contractor shall develop draft policies, procedures, and standards or identify existing ones. The Contractor also shall prepare documents for each strategy incorporating the above elements.

D.3.2.2 Develop a Personnel Security Strategy

The Contractor shall develop a personnel security strategy that shall address policies, procedures, and mechanisms. The Contractor shall coordinate with the <organization name> human resources office and the information security office. This is done to ensure the developed strategy is consistent with <organization name> policies and procedures on position sensitivity classification, personnel security screening, and information confidentiality. The Contractor shall ensure the strategy applies to all employees and Contractor personnel whose duties involve accessing the computer system, system design, development or maintenance, or handling of sensitive information in hardcopy or computerized form. The Contractor shall deliver the personnel security strategy to the COTR.

D.3.2.3 Develop a System Security Strategy

The Contractor shall develop a system security strategy that shall address the controls required as a result of the nature of the information processed. A key consideration is the risk and size of loss or harm that could result from improper operation or deliberate manipulation of the system.

The security and control objectives shall be included in the strategy.

The Contractor shall also develop guidance for the preparation of IT security and privacy plans prepared in accordance with applicable federal laws, regulations, and OMB implementing instructions. The Contractor shall deliver a systems security strategy to the COTR.

D.3.2.4 Develop an IT Physical Security Strategy

The Contractor shall develop an IT physical security strategy that shall include conducting a risk assessment and ensuring contingency planning of <organization name> IT systems. This strategy shall address <organization name>'s unique environment, network, and information sensitivity needs. Included in the strategy shall be an identification of critical systems and applications. The strategy shall also cover risk assessment methodologies and techniques and backup strategies.

The Contractor shall deliver an IT physical security strategy to the COTR.

D.3.2.5 Review Physical Procedures and Controls

The Contractor shall review the physical security procedures and controls of personnel, facility, and IT assets. The Contractor shall develop a list of physical security procedures and controls in place. This list shall include authorizations for access to each area and, at a minimum include:

- Physical access controls and their effectiveness
- Locks and entry procedures
- Air conditioning, uninterruptible power supply, and fire suppression and pumping equipment for adequacy and proper maintenance
- Protection against hardware and software theft and other human and machine-related threats
- Procedures for offsite storage of data and software
- Procedures for reacting to natural disasters and other nature-based threats to the facility, such as flood, fire, earthquake, hurricane, or tornado
- Personal computer use and software copyright license policy.

The Contractor shall deliver the Physical Security Procedures and Controls Report to the COTR.

D.3.2.6 Review IT Security

The Contractor shall examine sensitive and critical IT systems and data files. The Contractor shall develop a list for review of data security techniques and methods, which shall include the following:

- Access control, integrity controls, and backup procedures
- Sensitive data procedures and implementation
- Existing privacy policies and protections
- Information access (authorization and implementation)
- Developmental systems and how systems are moved into production
- Written user responsibilities for management of information and systems.

The Contractor shall deliver the Data Security Techniques and Methods Report to the COTR.

D.3.2.7 Review Personnel Security

The contractor shall develop a report, which evaluates compliance with federal and <organization name> personnel security policies and procedures covering such elements as position sensitivity classification, personnel security screening, information confidentiality, and security training and awareness. The report shall address whether the policies and procedures cover personnel in all positions with access to sensitive data. The contractor shall deliver the Personnel Security Report to the COTR..

D.3.3 Risk Management

D.3.3.1 Review Risk Assessment and Security Plan

The Contractor shall review the appropriate <organization name> risk assessment and <organization name> security plan for the sensitive systems addressed by this SOW. The Contractor shall prepare a report documenting this review. The report shall address the controls and procedures outlined in the plan and the requirements of the referenced regulations and directives. The Contractor shall deliver the <organization name> Risk Assessment and Security Plan Report to the COTR.

D.3.3.2 Select Risk Assessment Methodology for a System

[NOTE: The organization may specify a specific risk assessment methodology or tool is to be used. If the organization does not designate a methodology or tool, then this task should be performed.]

The <Contractor or organization name> shall select the technique for estimating the risk of operating a system. The risk assessment methodology selected should be consistent with the methodology of NIST SP 800-30, Risk Management Guide for Information Technology Systems.

The Contractor shall deliver a Methodology Selection Report to the COTR, explaining the rationale for selecting the methodology.

D.3.3.3 Perform Risk Assessment

The Contractor shall collect the data required to support the risk assessment methodology and perform the risk assessment. The requirements for the risk assessment task are:

- System characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentation.

D.3.3.4 Develop a Risk Mitigation Plan

The Contractor shall develop a plan[15] to mitigate the risks identified in the risk assessment. The plan shall include the following:

- A recommended priority of actions
- Evaluation of recommended control options
- Cost-benefit analysis
- Safeguard implementation plan
- Determination of residual risk.

The Contractor shall deliver the Risk Mitigation Report to the COTR.

[15] Certain key steps of the risk mitigation process have been excluded from this section as they should be in the exclusive domain of the organization. They include the selection of the final controls, assignment of responsibility for implementing controls, and the actual implementation of the selected controls.

D.3.4 Certification and Accreditation

D.3.4.1 Determine Security Requirements

The Contractor shall study the system to gain an overall understanding of the system, its users, functional requirements, and security requirements.

D.3.4.2 Prepare and Review Systems Security Requirements

The Contractor shall prepare a list of system security requirements. The Contractor shall deliver the list of system security requirements to the COTR.

D.3.4.3 Perform Security Test and Evaluation[16] of System

The Contractor shall perform a security test and evaluation to demonstrate through appropriate verification techniques, verification procedures, and procedure refinements, that the management, operational, and technical security controls for the IT system are implemented correctly and are effective in their application.

The Contractor shall prepare a final ST&E report based on the results of the ST&E activities and deliver it to the COTR.

D.3.4.4 Prepare Security Certification Report

The Contractor shall prepare a security certification report summarizing the results of the certification efforts. The statement shall address the adequacy of the security and controls implemented or under development. The Contractor shall deliver the Security Certification Report and Statement to the COTR.

D.3.5 IT Security Product Selection and Evaluation

NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products,* provides guidance to federal organizations on the acquisition and use of security-related IT products. NIST SP 800-23 also provides an introduction to the National Information Assurance Partnership's Common Criteria (CC) Evaluation and Validation Program and NISTs Cryptographic Module Validation Program (CMVP). The following SOW paragraphs are provided if an organization chooses to select a product outside the scope of the CC or CMVP programs. Note however, that for federal agencies that have determined that they need to use cryptography to protect sensitive information they must use FIPS approved cryptography that meets the relevant FIPS standards tested in NIST approved laboratories.

D.3.5.1 Evaluate the Product to Determine Security Features

The Contractor shall determine the security features of the <product name> and/or its interfaces with other security products on the system. When appropriate, this may require direct contact with <product name> vendor's representative. Although purchase of the product may be necessary, obtaining an evaluation copy on a trial basis may be preferable. The Contractor shall draft a report on the security features of the product.

[16] NIST SP 800-37 (Draft) distinguishes between a developmental and an operational ST&E. The type of ST&E depends on whether the system is new, undergoing major modification, or has already been delivered and installed. This SOW paragraph is presented generically and does not differentiate between developmental or operational ST&E.

The Contractor shall deliver a Security Product Report to the COTR.

D.3.5.2 Provide Recommendations and Implementation Plan

The Contractor shall prepare a recommendations report on whether <product name> will meet the organization requirement. Recommendations shall be based on cost, response time, ease of use, ease of implementation and operation, customer support, and quality of documentation. If the recommendation is positive, the Contractor shall prepare a plan for implementing <product name> supporting the organization security objectives. The plan should describe how the objectives are met throughout the implementation process.

The Contractor shall deliver the Recommendations and Implementation Plan Report to the COTR.

D.3.5.3 Review Organization Requirements and Available Products

Evaluate Hardware and Software Products That Perform a Direct IT Security Function

The Contractor shall review the organization's IT security plan and the requirement for a <type of IT security product> IT security product. The review shall document the capabilities that would be most appropriate to meet organization needs. The Contractor shall also assemble a list of the type of products designed for these needs. This list shall include a short general description of each product.

The Contractor shall deliver a Product Requirements Report and Possible Products List to the COTR.

[NOTE: If the organization does not have a specific type of IT security product in mind, the following should be included: When the report is approved, the Contractor shall submit for approval a list of products to be evaluated. The <organization name> will select <N> products for further evaluation.]

Evaluate Available Products

For each product identified as requiring further evaluation, the Contractor shall obtain a working or demonstration copy of the product to test its capabilities. When appropriate, this may require direct contact with <IT security product name> vendor's representative. Although purchase of the product may be necessary, obtaining an evaluation copy on a trial basis may be preferable. The Contractor shall also ensure that the product conforms to relevant existing federal standards.

The report shall address IT security functions performed by the <IT security product>. It shall also address data collection capabilities, utility (e.g., ease of use, error messages, documentation quality), security controls, reporting capabilities, product support, and compatibility with the organization's other IT security products and procedures. The Contractor shall prepare a report documenting advantages and disadvantages of each product.

The Contractor shall deliver a Product Evaluation Report to the COTR.

Conduct Demonstration and Provide Recommendations

The Contractor shall conduct a demonstration of each identified IT security product and emphasize the advantages and disadvantages in the evaluation report. The Contractor shall recommend a product or product(s) and a plan for implementation. Recommendations shall be based on the product's ability to meet specific organization security requirements and on cost, response time, ease of use, ease of implementation and operation, customer support, quality of documentation, and output reports.

The Contractor shall deliver a Recommendations Report to the COTR.

[NOTE: Although identification of the advantages and disadvantages of each identified IT security product, is required, demonstration of each product is optional.]

D.4 Operational Security Services

D.4.1 Contingency Planning

D.4.1.1 Review Contingency Plans

The Contractor shall review the contingency plan[17] for user involvement, practical application, thoroughness, and correctness. The Contractor shall review the most recent test plans and test results, noting identified deficiencies and corrective actions incorporated into the plan. The Contractor shall deliver a Contingency Plan Review Report to the COTR.

D.4.1.2 Review Current Contingency Plan Procedures

The Contractor shall review current contingency plan procedures and evaluate their effect on the continuous operation of the <organization name> systems processing sensitive data. The review shall be a step-by-step look at the planned responses and whether they are adequate to protect lives, limit damage, and maintain the ability to deliver essential services and operations. The Contractor shall also review the results of the most recent contingency plan procedures test results, including the scenarios used. The Contractor shall document the findings of this review in a report. The Contractor shall deliver the Contingency Plan Procedures Review Report to the COTR.

D.4.1.3 Evaluate Damage Assessment Methods

The Contractor shall evaluate the methods used to perform damage assessment, including their impact on security, and document the findings in a report. This report shall cover the methodologies used for damage assessment. The Contractor shall evaluate whether the damage assessment methodology includes the cause of the emergency or disruption, potential for additional disruptions or damage, area affected by the emergency, status of physical infrastructure, inventory and functional status of IT equipment, type of damage to IT equipment or data, items to be replaced, and estimated time to restore services. The Contractor shall deliver the Damage Assessment Methods Evaluation Report to the COTR.

D.4.1.4 Review Backup Procedures

The Contractor shall review the backup procedures, including documentation of the most recent contingency plan test, to assess adequacy of procedures and security of the system throughout the process. The Contractor shall also review the results of the most recent backup procedures test results, including the scenarios used. The test results shall include backup transportation, storage, and specific procedures supporting each system. The Contractor shall deliver the Backup Procedures Review Report to the COTR.

[17] This task assumes that a contingency plan exists. If no such plan exists or it is incomplete, a plan is produced in a separate effort.

D.4.1.5 Evaluate Contingency Plan

The Contractor shall evaluate the contingency plan to determine its ability to deliver sustained operations for the period envisioned. The review shall cover required levels of security to see that they continue in force throughout the process of recovery, temporary operations, and the move back to the original processing site or to the new processing site. The Contractor shall also review the results of the most recent contingency plan test results, including the scenarios used. The Contractor shall document the review in a report. The Contractor shall deliver the Contingency Plan Evaluation Report to the COTR.

D.4.2 Incident Handling

D.4.2.1 Establish Incident Response Team

The Contractor shall form an Incident Response team (the team) to provide direct technical assistance. This aid shall include onsite presence at the <organization name>'s sites request. The objective is for the team to provide to every site requesting aid, sufficient support to solve the technical problems created by the incident.

The team shall establish and maintain an office at <organization name> headquarters that will be the center for conducting team activities. The center shall also house the computers and other hardware needed to handle communications with other sites.

D.4.2.2 Establish a Incident Tracking System

The team shall develop a system for <organization name> to locate pertinent information about previous incidents, links to documentation for known viruses and other malicious code, known vulnerabilities of systems, and key people to contact. The team shall develop an incident tracking system.

The COTR will review the Tracking System.

D.4.2.3 Develop Cooperative Procedures

At the organization's discretion, the team shall form cooperative procedures between <organization name> and other federal organizations. Part of the team's task shall be to develop procedures for incident reporting. These procedures define who is contacted during an incident, what kind of information is shared, who performs a particular task, and how subtasks are divided under different types of incidents and conditions. The team shall develop cooperative relationships with vendors to learn of security vulnerabilities and fixes. The team shall also work with vendors to ensure problems are fixed. The Contractor shall document these cooperative procedures, which will be included in the Incident Handling Guidelines.

The Contractor shall deliver the Cooperative Procedures Report to the COTR.

D.4.2.4 Develop Procedures and Policies for Incident Handling

The team shall develop procedures and policies for incident handling that both the team and technical personnel at the <organization name> sites can follow. These guidelines shall include managerial as well as technical guidance for event handling and the Cooperative Procedures Report developed in Task 3. The team shall define what an incident is and conditions under which the team becomes involved. These guidelines shall be consistent with the <organization name> policy. These guidelines shall also contain the necessary details to solve technical problems, conduct coordinated efforts, and preserve evidence.

Finally, these guidelines shall help those involved in incident handling to categorize events and prioritize responses to those incidents/events.

The Contractor shall deliver the Incident Handling Guidelines to the COTR.

D.4.2.5 Develop Secure Electronic Communications Capabilities

The team shall establish secure electronic communications capabilities with <organization name> sites, so the team can send and receive e-mail from numerous sites, send and receive patches and technical data, etc. This implies that the team shall have to establish controls on dissemination of sensitive and privileged information.

D.4.2.6 Identify Software Tools for Incident Handling

The team members shall determine the types of software tools, which can ease the incident handling process. Tools include intrusion monitoring, detection and recording capabilities, incident analysis and reverse engineering tools, and real-time notification. The Contractor shall write a report on the tools' capabilities. This report shall include recommendations on which tool, if any, would be the most cost effective to aid incident handling by <organization name>.

The Contractor shall deliver the report on Software Tools to Handle Incidents to the COTR.

D.4.2.7 Conduct a Training and Awareness Function

The team shall cooperate with the <organization name> to conduct workshops/training seminars on <topic name>. These activities shall require the team to develop demonstrations of <topic name> methods. The team shall also circulate information about useful software tools to aid in <topic name>.

The COTR will receive the Workshop/Training Seminars Outline and Schedule. The Contractor shall coordinate the dates and places of the Workshops/Training Seminars with the COTR.

D.4.3 Training

D.4.3.1 Develop Course Outline and Master Lesson Plan

The Contractor shall develop a master lesson plan and supporting course material for each audience category within the organization. The guidelines for this task are in the task description section.

The Contractor shall present the Course Outline and Master Lesson Plan to the IT security staff.

D.4.3.2 Develop Lesson Plan for Each Audience Category

The Contractor shall develop a lesson plan and supporting course material for each audience category within the organization.

The Contractor shall present each Lesson Plan and Supporting Course Material for each audience category to the IT security staff.

D.4.3.3 Conduct Pilot Class

The Contractor shall conduct a pilot class for each course developed and use an evaluation methodology approved by the organization to measure the efficacy of course materials and presentation.

The Contractor shall submit the final Instructor Guide and Participant Material Packet to the COTR. This submittal shall include all supporting material developed in the above tasks.

D.5 Technical Security Services

D.5.1 <IT System Name> System Security Support

The contractor shall provide support for the replacement installation, upgrade and integration of <system name> devices at organization sites. The Contractor shall provide the following support:

- **Post-Installation Support.** The Contractor shall provide support for <system name> after installation. This support shall include the upkeep and emergency restoration and/or replacement of the <system name>.
- **Site Installations.** The Contractor shall perform site replacement installations of the <system name> products at the specified locations, upon approval by the <organization>.
- **Documentation.** The Contractor shall author trip reports, including lessons learned, summarizing the outcome of all site installations, to enhance the life-cycle operations of subsequent maintenance and enhancements. The Contractor shall also coordinate any required documentation support for obtaining approval for system installation.
- **Operational Impact.** The Contractor shall perform the above listed support without impact to the critical core functions. This impact assessment is based on existing and available resources; customer support requirements; and any significant incidents, events, exercises, or current operations. The <organization>/<vendor> team will assess the total impact and make an appropriate recommendation to support existing requirements.
- **Site Requirements Analysis.** The Contractor shall request, participate and coordinate site requirements analysis for sites. This analysis will be used to determine the specific level of work to be performed and the quantities and types of equipment and connections needed, during each site installation.

D.6 Contract Management

The following SOW paragraphs are not associated with specific IT security services. Rather, they may be used to support the acquisition of the required service.

D.6.1 Contractor Personnel Requirements

Contractor personnel assigned to this effort shall have appropriate <background screening > up to <screening level>.

The Contractor shall propose staff for assignment to this effort using the skill categories provided.

[NOTE: A background screening specification should be consistent with the information sensitivity designation and required type of background investigation.]

D.6.2 Personnel Qualification Requirements

The Contractor's Site Leads, Technical Leads, and Security Representatives shall be <certification>-certified[18][19] or equivalent within 6 months, and/or have a <degree name> or equivalent.

The Contractor shall propose staff for assignment to this effort using the skill requirements provided.

D.6.3 Contractor Personnel Security Requirements

The Contractor shall ensure contractor, subcontractor, and vendor personnel (hereinafter "contractor personnel") having access to information on <organization name>'s security programs and systems received or generated under this contract, meet <organization requirements>.

The program manager will identify background investigation requirements with each Work Request.

The <organization name> will provide the Contractor with security questionnaire forms, as necessary. All forms shall be completed and submitted and an approval received by the program manager before access to respective information will be granted.

If there are questions concerning the suitability of a contract employee following a background investigation(s), notification and an opportunity to response will be provided to the employee. If the employee is found unsuitable, <organization name> will inform the Contractor and the contracting officer. Upon notification of denied access, the contractor shall ensure immediate action is taken to preclude further access, including disabling access through access control systems, disabling system access privileges, and the return of access identification and media.

[18] Industry certifications do not guarantee that IT security personnel are qualified or technically suitable. Blanket requirements for all personnel to acquire a particular certification can be expensive and needlessly limit the available choices without increasing the value to the organization. Certifications can be used along with other means to develop an understanding of IT security skill levels. General security certifications are useful for positions such as security program manager or systems administrator but may have less value for certain other specialized skill positions such as a protocol or cryptographic engineer. In those areas, specialized certifications can have value. General and specialized certifications alone are not necessarily guarantees of competency or effectiveness and additional evidence will, in general, be needed.

[19] A comprehensive list of security certifications can be found at: searchsecurity.techtarget.com/tip/1,289483,sid14_gci900920,00.html

Appendix E—FREQUENTLY ASKED QUESTIONS

1. **For whom is the guide intended?**
   The *Guide to Information Technology Security Services* is intended for any IT security stakeholder who is responsible for initiating, managing, performing, or terminating an IT security service. Additionally, business managers will find utility in that the document provides a framework that an organization can assess the performance of a current service and service provider and establish whether alternatives will provide a greater return on investment.

2. **Why was this guide written?**
   The guide was written to provide IT security stakeholders with a life-cycle framework for initiating, managing, performing, and terminating IT security services. Organizations are increasingly trying to maximize the return on their investment in security and other IT investments. As organizations seek to find appropriate service providers as well as effective security services, a framework was needed to initiate, manage, perform, and terminate IT security services.

3. **What are IT security services?**

   IT security services can be categorized in a number of ways. In this document they are categorized as either management, operational or technical services. Management IT security services are services that focus on managing the IT security program and risk within the organization, such as security policy development or risk management. Operational security services focus on security controls implemented and executed by people (as opposed to systems), such as network testing or training and awareness. Finally, technical services are services focused on security controls executed by an IT system, such as firewalls and intrusion detection. This document provides a sampling of possible IT security services.

4. **What is the IT security service life cycle?**

   The IT security service life cycle is a six-phased approach to initiating, managing, performing, and terminating IT security services. The six phases are:

   - Initiation
   - Assessment
   - Solution
   - Implementation
   - Operations
   - Closeout

5. **Who has a role in the IT security service life cycle?**

   The list of participants who will select, assessment, implement and manage an IT security service will depend on the type and scope of the service, service arrangement, and type of organization. Key players can include the Chief Information Officer (CIO), contracting officer, contracting officer's technical representative, IT investment board, IT security program manager, IT system security officer, program manager/procurement initiator, and privacy officer, among others.

6. What is an IT security arrangement?

An IT security arrangement is the result of the identification of an IT security service requirement and a decision on the way in which the organization will perform this service requirement. There are any number of service arrangements from which IT security managers may choose. An organization may select its internal employees and teams to provide the service required, it may choose to fully use an external service provider, or it may choose something in between with both external and internal employees performing an IT security service role.

7. Does the IT security services guide recommend "outsourcing" IT security services?

No. The guide does not prescribe a specific service, service level, service mix, service arrangement, service agreement or service provider. Rather, it provides a methodology for assessing, analyzing and selecting IT security services appropriate for each organization. There are too many issues and too many variables for any document to prescribe what is best for a given organization. IT security managers and other senior officials should assess the risks and benefits of each alternative and select the most appropriate alternative for the organization.

8. What are some of the tools managers might use to manage IT security services?

The guide discusses several tools managers might use to manage IT security services including the IT security services life cycle framework, metrics, and service agreements.

9. What are metrics?

Metrics are a management tool that facilitates decision-making and accountability through practical, relevant data collection, data analysis, and performance data reporting. An example of a metric for a management service, a training and awareness program, might be the number of new employees who receive IT security training within their first 30 days on the job. Gathering this metric repeatedly, over time, will allow managers to assess how well the current training service provider performs its task today, to set targets for the service provider in the future, and then to assess how well it met the desired target.

10. What issues/factors affect IT security service decisions?

There are innumerable factors that affect IT security service decisions and will vary by service, service arrangement and type of organization. Generally speaking, the factors and issues can be grouped into the following categories:

- Strategic/Mission–related to the organization's mission and business function.
- Budgetary/Funding–related to cost, funding, and value of IT security
- Technical/Architectural–related to the technical and architectural environment of the organization
- Organizational/Cultural–related to the intangibles of the organization such as image, reputation, and resiliency
- Personnel–related to the organization's contractors and employees
- Policy/Process–related to the organization's business and IT security policies and procedures.

11. How does an organization know which phase of the life cycle its service(s) are in?

The IT security services life cycle is an iterative process in which the IT security services are continually assessed and evaluated. If an organization has not yet implemented IT security services, but needs them, it will be at the initiation phase. All others are likely to be in the operations phase and will be assessing service provider and organizational performance.

12. What triggers the life cycle?

Any number of things can trigger the life cycle, from top-level management choosing to assess the current IT security functions to a new IT security service requirement. The trigger will likely fall into one of the issue categories mentioned in question 10 (see section 4.1 for specific sample triggers from each category), but all triggers have one characteristic in common: it will be an event sufficient to warrant assessing the current IT security environment and identifying viable service solutions.

13. How does an organization know if its current service(s) are adequate?

The second phase of the IT security service life cycle is the assessment phase. During this phase, the IT security managers will assess the existing IT security environment through the use of metrics and the principle of total cost of ownership (TCO). Together they will allow managers to assess the current service level and cost. However, whether this service level and cost is acceptable is beyond the scope of the document. IT security managers will need to determine this for themselves based on their unique IT security and business requirements.

14. How does an organization choose an IT security solution?

An organization chooses an IT security solution based on their assessment of the current environment and business case development of the viable alternatives as compared to their current service. Although the business case may not make the decision-making easy or obvious, it should provide the necessary data for the decision maker to weigh, consider, and select the service arrangement that best suits the organization's needs. There will likely be some discussion and disagreement among the decision makers, but ultimately the selection must be a consensus. A service can succeed only if all business and IT security managers sufficiently buy-in to the implementing solution.

15. How does an organization choose a service provider?

How an organization chooses the service provider may vary depending on the service, service arrangement, and type of organization. If the service arrangement is an internal one, there may be only one internal group who can provide the service. If the service is in a new field or requires highly specialized experience, there may only be a few service providers to choose. Large government agencies may release a formal RFP. Regardless, the organization should identify the service provider evaluation criteria, solicit proposals, and assess potential providers against the criteria.

16. What should a service agreement include?

Service agreements should, as a minimum, specify the following:

- Explicit definitions of both the organization's roles and responsibilities and the service provider's roles and responsibilities.
- Period of performance and/or deliverable due dates
- Defined service levels and service level costs.
- Defined process regarding how the managers will assess the service provider's compliance with the service level and due date targets, rules, and other terms of the agreement
- Specific remedies (e.g., financial, legal) for noncompliance or harm caused by the service provider.
- Explicit rules for handling sensitive data

17. How does an organization monitor service performance?

An organization will need to monitor service provider performance and organizational performance during the operational phase of the IT security service life cycle. The frequency and method for gathering these metrics should be specified in the service agreement between the IT security provider and the client organization. It is likely that the metrics gathered in phase two (assessing the current environment) will be the same metrics gathered during operations, for the future service arrangement will then be the current environment.

18. When does the IT security services life cycle end?

Just as there are innumerable IT security service life cycle triggers, there are many reasons why the IT security service may end, including service provider insolvency, contract closeout, changing requirements, poor service provider performance, or new technology requirements. The common characteristic among all potential service closeouts would be an event significant enough to require implementation of a different security solution.