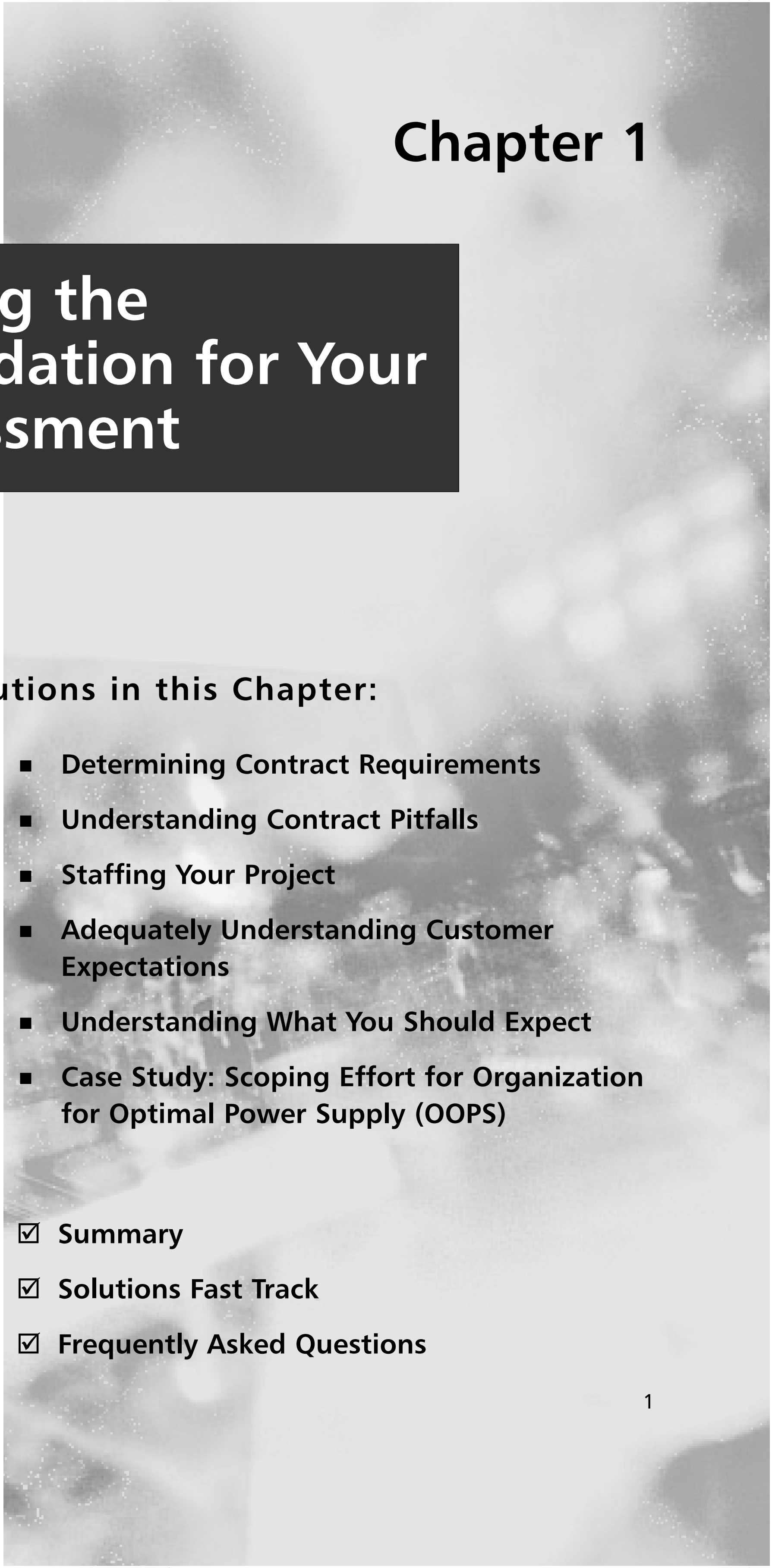


Chapter 1

Laying the Foundation for Your Assessment

Solutions in this Chapter:

- Determining Contract Requirements
- Understanding Contract Pitfalls
- Staffing Your Project
- Adequately Understanding Customer Expectations
- Understanding What You Should Expect
- Case Study: Scoping Effort for Organization for Optimal Power Supply (OOPS)

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

The National Security Agency (NSA) Information Security (INFOSEC) Assessment Methodology (IAM) is a detailed and systematic method for examining security vulnerabilities from an organizational perspective as opposed to a only a technical perspective. Often overlooked are the processes, procedures, documentation, and informal activities that directly impact an organization's overall security posture but that might not necessarily be technical in nature. The IAM was developed by experienced NSA and commercial INFOSEC assessors and has been in practice within the U.S. government since 1997. It was made available commercially in 2001.

NSA developed the IAM to give organizations that provide INFOSEC assessments a repeatable framework for conducting organizational types of assessments as well as provide assessment consumers appropriate information on what to look for in an assessment provider. The IAM is also intended to raise awareness of the need for organizational types of assessment versus the purely technical type of assessment. In addition to assisting the government and private sectors, an important result of supplying baseline standards for INFOSEC assessments is fostering a commitment to improve an organization's security posture.

As with any project, the first step is to identify a need; in this case, it's the need for an assessment. This identification can happen in two ways. An organization's leaders may realize they need an assessment, or a potential provider can convince them that they need an assessment. The justification for an assessment can include legislative requirements, response to a security incident, part of good security engineering practice, requirements for contracts or insurance, or simply because it's the right thing to do. This book does not focus on selling the IAM to customers, since that is a specific business practice. Instead, it focuses on the process of conducting the IAM within a customer environment. In this chapter, we examine the beginning of the process, focusing on establishing the scope and contractual requirements for an assessment.

Understanding Why…

Contracting and the NSA IAM

NSA intentionally does not specifically address business processes in the IAM methodology. The IAM was originally designed as a government methodology (NSA providing services to other government agencies) and therefore had no need for contract considerations. Once it was discovered that the methodology had applicability in the commercial world, NSA decided to stay out of the contracting side and let each entity handle contracting-related obligations. NSA is not generally involved with developing contract requirements, formats, or contents. The information contained in this chapter comes primarily from the authors' experience in preparing contracts and scoping the efforts for IAM assessments. Each individual IAM provider must address contracting requirements without NSA assistance.

Determining Contract Requirements

The process doesn't truly start at writing the contract.The process probably starts one or two months earlier, when the customer decides that they need to do something related to information security, and they need to do it soon.The provider company or another company probably spent some time trying to convince the customer of the type of assessment they need. Somewhere during this process, either a basic set of requirements is set or a request for proposal (RFP) is written.

At this point, it can officially be said that the need for an assessment has been identified.The time has come to develop the scope and contract for the assessment. Every IAM-related assessment starts with documentation that describes the requirements and expectations between those that are conducting the assessment and those that are receiving the assessment. In the commercial environment, the contracting process lays the foundation for the effort. In the government environment, it can be a contract or a memorandum of agreement (MOA) or memorandum of understanding (MOU) between two organizations that can drive the assessment effort. Ultimately, the majority of information is the same in either case. In the following sections, we examine the considerations that should be included in a contracted or other associated documentation.

What Does the Customer Expect?

Meeting expectations is critical in completing a successful assessment. Understanding customer expectations from the beginning of the process will be of tremendous assistance in defining the project's scope, making estimates to complete the work, and finalizing the effort. Which expectations are you as the assessor concerned about? The expectations you need to address include:

- Customer definition of an assessment
- Customers' "other" needs for the assessment
- Qualifications of the assessment team
- Customer timeline requirements
- Customer contracting process
- Customer cost limitations

Customer Definition of an Assessment

A critical first step for an assessment project is to come to a common understanding on what composes an assessment. Often you have to spend a great deal of time with potential customers just defining what they are looking to accomplish with the "assessment" process. The term *assessment* has been used loosely for years to describe everything from an audit to "attack and penetration" testing. NSA has broken up what has been traditionally called assessments into a three-phase, top-down approach (see Table 1.1):

1. **Assessment** The assessment is an organizational-level process that focuses on the nontechnical security functions within an organization. In the assessment, we examine the security policies, procedures, architectures, and organizational structure that are in place to support the organization. Although there is no hands-on testing (such as scans) in an assessment, it is a very hands-on process, with the customer working to gain an understanding of critical information, critical systems, and how the organization wants to focus the future of security.

2. **Evaluation** The evaluation is a hands-on technical process that looks specifically at the organization from a system/network level to identify security vulnerabilities that exist in those systems and can be mitigated through technical, managerial, or operational means. Evaluations are often confused with assessments. The IAM specifically focuses on the assessment, but elements of evaluations can be included in the IAM process. NSA calls this a Level 1+ assessment. This includes doing technical analysis of the firewalls, intrusion detection systems, guards, and routers. It may also include some basic vulnerability scans of the customer's networks. In addition, the IAM process provides excellent information that leads into future evaluations.
3. **Red teaming** Red teaming, often called *attack and penetration testing,* is a process whereby someone imitates an adversary looking for security vulnerabilities to make it easy to break into a system or network. This is often called the *low-hanging fruit* because these vulnerabilities are the easiest means into the customer network.

Table 1.1 NSA TRIAD Comparison

Assessment (Level I)	Evaluation (Level II)	Red Team (Level III)
Cooperative high-level overview	Hands-on process	Adversarial
Information/mission-criticality analysis (includes policy, procedures, and information flow)	Cooperative testing	External
No hands-on testing	Diagnostic tools	Penetration tests
Not overly technical	Penetration tools	Simulation of appropriate adversary
	Technical in nature required	Specific technical expertise

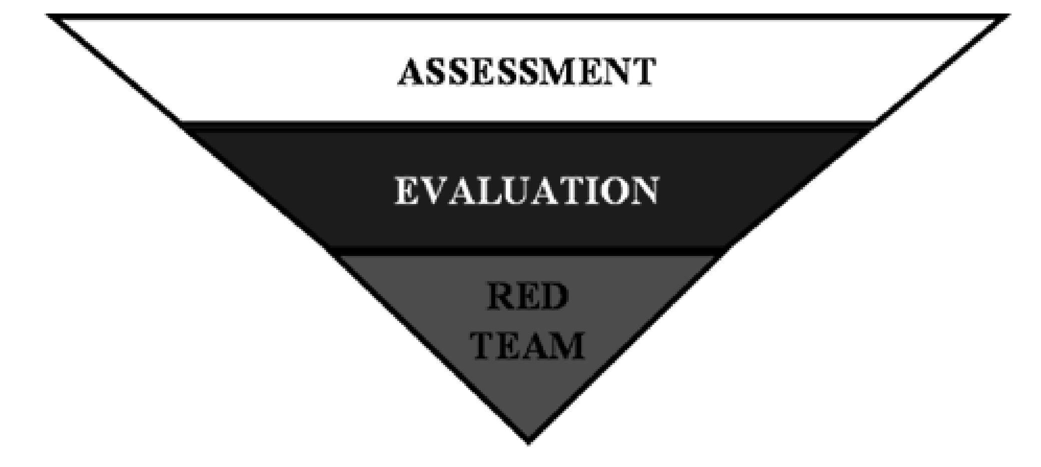
NSA's Triad is a top-down approach that starts with a high-level overview of the target organization's security posture. The approach then focuses specifically on critical systems that carry the organization's critical information. The final step is testing what has been implemented as part of the assessment and evaluation processes by taking a look from the "hacker's eye" view.

In days of old (and even today), security was addressed (when it was addressed at all) by first locking down a critical system, then locking down the network around the system, then documenting what had been done. Almost as an afterthought, it was decided that some policy was needed to enforce the security in the future. This process is completely opposite of what the IAM prescribes as a top-down approach. The IAM prescribes an approach of identifying critical information and critical systems, putting in place the policies and procedures to protect the critical information and systems, then addressing the technical security of the network. Figure 1.1 shows Level 1, Level 2, and Level 3 in the top-down approach model.

Terminology Alert

Assessment NSA defines an INFOSEC assessment as "A review of the Information System Security (INFOSEC) posture of a specified, operational system for the purpose of identifying potential vulnerabilities. Once identified, recommendations will be provided for the elimination or mitigation of the vulnerability."

Figure 1.1 The NSA Triad



Sources for Assessment Work

The request for an assessment can come from many different sources. Common methods include an RFP, referral from a partner, referral from a previous customer, trade-show contact, a Web site search, and cold calling. The source of the request will often determine the level of effort necessary to win the work. For example, a referral already has some credibility behind it for your organization. A cold call or trade-show contact will probably to require some additional effort to convince an organization you are the right people to do the work for them.

A great deal of effort goes into building relationships that help strengthen opportunities with potential customers. It can honestly take an organization several weeks to more than a year to work opportunities into a sale. So be prepared for the sales cycle that may occur. The best opportunities are from referrals.

Contract Composition

Every organization has its own contracting format, proposal methodology, and bidding process. The following information is not intended to replace those elements, but it is included here to assist you in ensuring that a minimum set of information is included. In all cases, consult with your contracting department and/or legal counsel on appropriate and acceptable contents of the contract. In today's business market, contracting is a combination of multiple skills to include project management, negotiation, financial analysis, risk management, and intellectual property management.

Minimum Contract Contents

The following is a list of items that should be included in all contracts for assessments in some form. Assessment companies may want to consider these elements in proposals and statements of work as well; many times, these documents roll directly into a contract or agreement:

- **Purpose** This section describes, in simple terms, the purpose of the assessment, how it relates to the customer, and the benefits the organization will receive from the assessment process. It is essential that you use common terminology relevant to the organization to assure that the purpose is understood.
- **Methodology** This section describes the methodology that will be used to conduct the assessment. This is a good place to emphasize the IAM as a standard methodology to conduct INFOSEC assessments,

developed and approved by the National Security Agency. This includes the phases, processes, and steps that will be used during the assessment.

- **Scope** This section is a detailed demonstration of the level of effort, boundaries, and limitations of the assessment. Appropriate assumptions are a critical part of the scoping process. The scope section provides a detailed listing of known assumptions affecting the assessment. Assumptions are critical in demonstrating an understanding of the customer environment and detailing how that environment will affect the assessment. The types of assumptions may include number of physical locations, number and types of system, number and types of network, relevant point of contact (POC) information, information about availability of personnel to be interviewed, and any associated constraints that can be listed as assumptions.
- **Roles and responsibilities of customer staff** This section identifies the participation expected of the customer's staff to support the assessment effort. Activities can include introductions, scheduling, coordination, and communications. Utilize this space to ensure that the customer has an understanding of what they need to do to support the assessment effort.
- **Deliverables** An accurate list of deliverables with a brief description of the deliverable will assist in managing expectations. Often the customer's expectations of a deliverable will be different than planned by the assessment team. Assuring an accurate description of the deliverables in the signed agreement is important to the process.
- **Period of performance** The necessary schedule for the assessment can be extremely important. Gaining an understanding of customer availability and the consultant's availability is key to planning a successful assessment. Depending on the schedule requirements, it may not be possible to list specific dates at this point. If this is the case, be sure to include the expectation of time for activities so the customer can look at their calendars and begin to plan when the assessment makes sense.
- **Location of the work** Work location figures directly into the cost of the assessment. In this section, be sure to list where the onsite work is to be conducted, where offsite work is to be conducted, if multiple locations will need to be visited, and where the analysis and reporting will be conducted. Be sure to take into account whether the assessment team

will be dealing with classified information and the potential necessity for additional security controls while conducting assessment activities.

- **Service fees with any relevant quotation notes** This is your pricing table for the effort. Be as detailed as possible to show the plan of action along with associated costs. (The actual cost of your assessment service depends entirely on your own organization's policy and is not addressed in this book.)
- **Payment schedule** Generally, net 30 days or net 45 days is common. However, with some customers, you might have to work out a special agreement for payment. This is a business process specific to your organization and is not covered in detail within this book.
- **Acceptance** This is the signature section of the contract, addressing your organization's approved statement of terms and conditions. The acceptance section may include information on the length of the agreement, scheduling coordination requirements, termination terms and costs, any other related penalties for cancellation, and acceptance of the terms of the proposal/agreement.
- **Organizational qualifications** This section describes and demonstrates how your organization is best qualified to execute the work the customer requires. This will likely be a detailed background of your organization, qualifications of the organization, qualifications of the members of the team being proposed, and how those qualifications will assist the customer in meeting their goals.

Additional Contract Contents

As we discussed earlier, organizations should follow their own contracting processes when bidding and contracting work with customers. Many more items can be included in a contract; we presented only a sampling of items you may find. Consult with the appropriate legal and contractual experts for purposes of creating the contracts that will meet your organization's needs. Some of the additional items you may find in your contracts or that may e required by the customer include:

- **Insurance information** Many organizations require specific levels of insurance, both general liability and professional liability, in order to work with them. This information will need to be included in any final agreement.

- **Personnel qualifications** The contracting organization may require proof of qualifications for personnel proposed to work a contract. This proof may include certifications, number of years of experience, and specific types of insurance.
- **Warranties** Include any associated warranty information for products or services provided.
- **Representations** Generally used to identify that there are no other representations other than the written contract or agreement.
- **Independent contractor statement** To avoid tax issues, many contracts include independent contractor statements and associated responsibilities for wages and benefits for each organization.
- **Assignment of rights** This section normally does not allow for the contract rights to be assigned to another entity without the express written approval of the contracting organization.
- **Confidentiality statements** This section focuses on protecting the confidential information of both the contracting and the contracted parties.
- **Document ownership statements** For our purposes, this section generally specifically identifies that all documents belong to the customer.
- **Indemnification** An indemnification statement may look like the following: "The contractor and contractee agree that they shall indemnify and hold harmless the other and its respective officers and employees from any loss, cost, damage, expense, or liability of every kind and nature which they may incur, arising out of, or in connection with performance under this Agreement, occasioned in whole or in part, by the negligent actions or willful misconduct of other, or by its lower-tier subcontractors." This is a legal protection mechanism to avoid huge lawsuits for normally acceptable problems that may arise for anything other than neglect or misconduct.
- **Survival of obligations** This section focuses on the length of time that obligations within the contract will persist. This section also states that if one section of the contract is deemed unusable, the other sections still remain intact.
- **Waiver and severability** This section states that if any provision or portion thereof of the contract is held to be invalid under any applicable

statute or rule of law, it shall be, to that extent, deemed omitted without invalidating the remaining portions of the contract.

- **Governing law** This section addresses what federal and state laws shall govern the legal aspects of the contract.
- **Force majeure** This section addresses failure of a contract due to circumstances beyond the contractor's control. Wording may look like the following: "Neither party to the Subcontract shall be considered to be in default of its obligations under this Subcontract to the extent that failure to perform any such obligation arises out of causes beyond the control and without the fault or negligence of the affected party. Examples of these causes are (1) acts of God or of the public enemy, (2) acts of the Government in either its sovereign or contractual capacity, (3) fires, (4) floods, (5) epidemics, (6) quarantine restrictions, (7) strikes, (8) freight embargoes, and (9) unusually severe weather. In each instance, the failure to perform must be beyond the control and without the fault or negligence of the affected party. 'Default' includes failure to make progress in the work so as to endanger performance. However, Subcontractor shall not be excused for failure to perform any obligation under this Subcontract if such failure is caused by a subcontractor of the Subcontractor's at any tier and the cause of such failure was not beyond the control of both the Subcontractor and its lower-tier subcontractor, and without the fault or negligence of either."

What Does the Work Call For?

A good understanding of what the customer is asking for is essential. As we said before, to ultimately set the boundaries for the assessment, you may have to spend some time educating the customer as to what makes up an IAM assessment. Expectations will be different for each customer that you work with. Things to consider are:

- Level of detail the customer requires for recommendations in order to ascertain the level of effort required to develop and document the recommendations that are created as part of the process. Level of detail includes the amount of technical detail put into each recommendation and determining whether saying something as simple as "upgrade the server operating system to Windows 2000 or higher" is enough of a recommendation or if step-by-step "how-to" instructions will be required.

- Knowledge of any regulations or legislation that the customer will have to comply with at the end of the assessment. This information is used to determine some of the organization's security objectives and directly affects the recommendations that are made to the customer.
- Knowledge of any assessments that were conducted in the past is useful to show the level of detail in previous assessments as well as provide a good indicator of whether the customer will implement recommendations provided.

What Does the Statement of Work Say?

Statements of work (SOWs) and RFPs are very common mechanisms via which you will receive a request for an assessment. The intent of these documents is to detail the customer's requirements for the assessment. Depending on who develops the SOW or RFP, the packages can contain a wide range of detail. These documents can be very short (one page) or very long and detailed, with a great deal of legal jargon. At times, you may have the opportunity to assist in writing an SOW or an RFP for a potential work effort. If this is the case, you can gain a greater understanding of requirements for the work.

More on Scope

The most important and defining section of the contract is the Scope section. A detailed and true representation of the scope of the effort is essential for estimating level of effort and overall pricing for the project. Scope also establishes the framework for customer satisfaction. A poorly defined scope can result in an unhappy customer and/or an unhappy assessment team—not to mention the financial impact a company will feel if the project is poorly scoped and runs over the expected level of effort. What "value add" does the scope bring to the project?

- Defines approved areas to be covered for the assessment
- Sets limitations on the assessment efforts
- Defines appropriate dates and times for all specific assessment efforts
- Lists actions that will be taken during the assessment
- Defines expectations for the project
- Defines concerns from both the customer and the consultant perspective

- Establishes and details the logical and physical boundaries for the project
- Sometimes called "rules of engagement"

Scope is the mutual understanding between the assessment team and the customer as to the actions that will take place during the assessment. An effective scope requires an agreement between the customer and the assessment team. In many cases, the scope will require a legal review by the customer's legal department. The scope is also intended to limit the impact on the customer as much as possible. This level of acceptable impact needs to be addressed as part of the scoping effort.

Source of Scope Information

Scope information can come from multiple sources. One of the obvious sources for scoping is the SOW or RFP that the customer issued to obtain the assessment services. Generally this information is truncated and requires additional details to properly determine the scope. Additional sources of scoping information can include the customer representative assigned to the project. That person will generally provide additional nonproprietary information that is specifically requested. If it is a competitive bid, the customer representative will generally be required to provide this information to all potential bidders.

Additionally, customer documentation is an excellent source of information about the organization and any related security programs, if the information is available. Useful documentation can include acceptable-use policies, security policies, network architecture diagrams, and results of previous assessments. Another excellent way to get scoping information is to ask the right questions on a scoping questionnaire. We discuss this procedure in the next section.

Collecting Scope Information

Obtaining the information you need to properly scope an effort can be a challenge for the proposal or assessment team. More often than not, we have found that customer SOWs or RFPs are poorly scoped when they are developed. They do not contain enough information, or they are boilerplate RFPs and contain erroneous information. Usually we have to go back to the customer to collect additional information to finalize any bidding or scoping process we are working on.

This is one situation in which we have found that a questionnaire can be useful in obtaining the information we need. Figure 1.2 contains a set of sample questions that could help you obtain the basic information needed to properly scope the effort. A scoping questionnaire provides customers with an easy-to-complete form that asks the relevant questions relating to information needed to properly scope the level of effort for a project. The questionnaire will give a good baseline of information and may lead to additional necessary questions to finalize the details. The scoping questionnaire will answer many of the typical questions up front to provide the necessary clarification needed on the project.

Figure 1.2 Scoping Questionnaire Questions

These are information areas in which to consider asking questions to obtain information about the customer's environment.

How many physical sites do you have?

Where are they located?

How many employees are located at each site?

What are the core hours for the site?

Is shift work involved? Will the assessment information gathering cover all shifts?

What networking protocols are you running? (IP, IPX, etc.)

What is the layout of the network architecture? Please provide an up-to-date network diagram.

How many workstations are located at each site?

What operating systems are on the workstations?

How many servers at each site?

What services are running on the servers? (Web, DNS, etc.)

What operating systems are on the servers?

Do you have a firewall(s)? How many? What kind?

Do you have an active network- and/or host-based intrusion detection system(s)?

How many? What kind?

How many Web servers are active and accessible to the public?

What type of Web servers are they? (Apache, IIS)

How many Web servers are active and for internal use only?

What type of Web servers are they? (Apache, IIS)

Do you currently utilize a RAS server for external access?

If so, what product?

Continued

Figure 1.2 Scoping Questionnaire Questions

Do you currently utilize a remote VPN product for external access? (e.g., Altiga VPN concentrator)

If so, what product?

Who will be the primary point of contact (POC) at your organization for this work?

Name, phone, cell phone, e-mail address, job title:

Do you utilize a Windows NT-based domain architecture?

Do you utilize a Windows 2000 Active Directory-based architecture?

Do you utilize a Novell NDS-based architecture?

Do you have wireless networking?

Do you have mainframe environments?

What types of mainframes?

Is there third-party connectivity?

Are you using Voice over IP (VoIP) or IP telephony? How many stations are there?

Are you using a converged network architecture?

NOTE

You should create your own scoping questionnaire based on your INFOSEC experience. This gives you the information you need to develop your contractual scope and make estimates of level of effort and pricing for the contract. We've merely provided examples to help get you started.

Defined Credential Requirements

In defining credential requirements for the assessment work, you may experience a huge difference between government and commercial organizations. From a commercial perspective, as the provider of the security assessment you have hopefully gained and documented value-added skills that you can highlight to your customer. These skills may include specific work experience, specific training, and specific certifications. These credentials may include but certainly are not limited to Certified Information System Security Professional (CISSP, www.isc2.org), Certified Information Security Manager (CISM, www.isaca.org), and Certified Information Systems Auditor (CISA, www.isaca.org). You may also find it valuable in commercial contracting to highlight government experience because, from a process and procedure standpoint, it is generally recognized that the government has been ahead of the commercial arena for some time.

From the government perspective, there may be requirements specifically for certain types of clearances (for example, Secret or Top Secret), background investigations of employees, or specific required certifications. Clearances are especially prevalent with Department of Defense (DoD) and Department of Energy (DoE) relationships, but they could be required in other forums as well. Organizations may also find it useful to be a member of relevant security membership organizations such as the Information System Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the American Society of Industrial Security (ASIS). Many more industry-specific professional associations should be taken into consideration.

What Are the Timelines?

Establishing expectations of the timelines for the assessment effort is an important step to be coordinated with the customer. If the customer believes the work can be done in two weeks and you think the work will take two months, somewhere along the way someone does not have a complete understanding of the processes involved or what the customer is looking for in the assessment.

NSA allows for three to four months for the entire IAM process to allow for differences in the size and complexity of an organization. Obviously, the methodology is flexible enough to allow for smaller, less complex organizations or larger, more complex organizations. Some of the time, very extensive activities are taking place. At other times, a waiting period is occurring. The contracting process is not estimated by NSA and is therefore not included in NSA estimates.

NSA's IAM timeline is presented in Figure 1.3. As you are bidding the work, here are the activities you must take into account:

- **The contracting process** Generally not billable to the customer or estimated in the costs. This is generally considered company overhead.
- **Pre-assessment site visit** Estimated at one to three days, depending on organization size, this step will require full-time dedication of two or

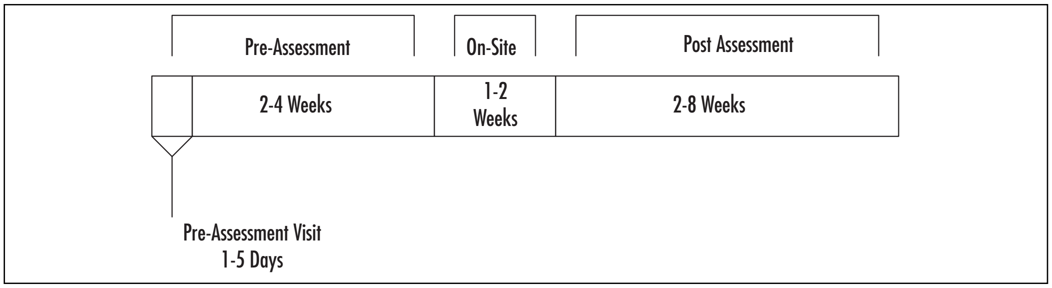
three staff members for the duration. The pre-assessment process is covered in detail in Chapters 2–6.

- **Pre-assessment coordination** Estimated at two to four weeks, this step allows the team to prepare for the onsite assessment. The equivalent of one full-time person is likely sufficient for this step. Pre-assessment coordination is covered in Chapter 6.
- **Onsite assessment** NSA estimates the onsite portion of the assessment to take one to two weeks. The actuality of length of time and number of people on the assessment team is completely dependent on the complexity of the organization you are assessing, the number physical sites you have to deal with, and the agreed-on scope of the assessment. The supplement to contractual scope will be the assessment plan discussed in Chapter 6.
- **Post-assessment** The post-assessment process deals with the analysis of findings and writing the final report. When estimating the time required for this effort, take into account the level of detail the customer requires for recommendations and the complexity of the organization (number of physical sites, number of systems, number of different types of systems, etc.).

NOTE

Timelines provided here are only guides. Actual time frames will depend on the size, industry, and complexity of the organization being assessed.

Figure 1.3 IAM Timeline



Understand the Pricing Options

Fixed price or hourly? What is a reasonable price for the customer to handle from a scoping perspective? Can a customer endure three to four months of hourly billing at a standard rate? How do you know how long the assessment is going to take before you have completed the pre-assessment process? These are all pricing challenges that make the commercial contracting world different from the government contracting world.

Government Contracting

In federal government contracting, most work is done on an hourly rate. Government contracting generally programs for a certain number of people to work a certain period of time to execute the scope of the statement of work. Rates in government contracting are generally lower; however, there is generally more flexibility from the time frame perspective to accomplish activities necessary to complete the assessment. However, be cautious to ensure that you are meeting customer expectations with what you are putting together from a scoping and expectations perspective.

The strategy with government contracting is to be involved as a prime contractor or as a subcontractor on various possible contract vehicles to include indefinite delivery, indefinite quantity (IDIQ) contracts or a Government Services Administration (GSA) schedule. Although these are common ways to gain government contracts for assessments, they are not the only mechanism to get a government contract. Ultimately it comes down to contacts, being at the right place and right time. Keep in mind that generally labor and other direct costs (such as travel and equipment) must be billed under "different colors of money" with the government.

Terminology Alert

A *prime contractor* is an organization that has a direct contract with the government to provide services or products. A *subcontractor* is an organization that has an agreement with a prime contractor to provide services supporting the prime's contract with the government.

Commercial Contracting

Commercial contracting is a different situation than government contracting. Corporations take multiple avenues to accomplish their contracting needs. This includes basic purchase orders, signed proposals, and extensive contracts with page after page of stipulations and requirements. Be sure to include the minimum amount of specific project-related data that is needed to meet your needs, and have your legal counsel review any information with which you might not be familiar. It's always a good idea to include your legal counsel in the process, especially when something changes from standard templates. The actual contracting process is a specific business-related process for your organization and varies from company to company.

Fixed Price vs. Hourly Rate

So what's the best choice? Obviously, we cannot tell you what is best for your organization. Table 1.2 outlines the pros and cons of each pricing type. There are obviously other contract avenues that are not addressed here. Fixed price is popular with many customers, since they will know what they are getting for the money. Open-ended and hourly rate contracts tend to be scary at a time when organizations are keeping a tight rein on their pocketbooks.

Table 1.2 Fixed vs. Hourly Pricing

	Pro	Con
Fixed price	Flexibility with staffing Flexibility with charge rates Incentive to keep down costs	All major and minor scope changes require a change order. Difficult to bill until the assessment is complete, unless specific interim payments are authorized in the contract. Generally a higher risk and therefore higher cost for same level of effort vs. hourly rate
Hourly rate	Typically lower cost for same level of effort vs. fixed price Flexibility with scope changes since any increase in effort will just result in more hours burned (until max hours run out)	More closely monitored in both labor hours and other direct costs Loss of staffing flexibility since rates are based on labor categories and skill sets

WARNING

The assessment plan that results from the pre-assessment process may change the level of effort thought to be needed for the assessment. You should consider including a clause in the contract that allows for rescoping for significant changes once the assessment plan is completed and accepted. Another approach is to contract the pre-assessment as a separate agreement from the remaining phases of the IAM assessment. This allows the assessment plan to be used as the scoping input for the onsite assessment contract.

Understanding Scoping Pitfalls

Common mistakes during the scoping process can derail the assessment effort. Although it is impossible to address every possible scenario, taking into consideration these concerns will help you avoid the common pitfalls associated with scoping the assessment.

Common Areas of Concern

The following discussion outlines common areas in which the scoping process can head off into the wrong direction. These areas are not all-inclusive, and the team developing the contract will need to ensure that additional brainstorming is added to the process to create a complete listing.

Customer Concerns

Generally, a customer has specific reasons for asking for an assessment. It will be important to understand the specific concerns the customer wants to address as part of this process. This understanding helps meet customer expectations. Some of the reasons customers ask for an assessment are:

- Legislative/regulatory requirements
- Insurance requirements
- Protection of critical infrastructure
- To provide the system owners a certain level of confidence that their information is protected
- As part of a good security engineering and management practice
- In response to suspected threats, security incidents, and red team activities
- For an independent review to validate internal reviews
- It is the right thing to do

Customer Constraints

All customers have constraints of some kind, whether time, financial or other resources, political, or third-party involvement. Failure to discuss, recognize, and clarify constraints with the customer up front and throughout the assessment process can result in failure of the assessment project. Some common constraints that might be missed or ignored include:

- Available time frames to execute the assessment
- Drivers for the assessment
- Financial constraints on the organization to conduct the assessment
- Personnel resources to support the effort

- Company politics
- Third-party control of resources (boundaries)
- Physical and logical boundaries associated with the organization

"Scope Creep" and Timelines

Unplanned and unbid scope changes in projects are often called *scope creep*. This occurs when a project deviates from the written scope to a higher level of effort. Effectively controlling scope creep can assist in effectively managing the overall project. Scope creep not only has an impact on the financial aspects of the project—it also has an impact on the project's timelines and the assessment team's ability to complete the job on time.

Scope creep can be caused by poor planning, unknown areas of the organization that need to assessed, or the customer's desire to further investigate a certain security area that is being analyzed by the assessment team. Scope creep can also occur when a customer wants to get more out of the effort than they are paying for.

From the Trenches…

Common Scope Creep

The most common example of scope creep occurs when more systems or more locations need assessed than were originally identified by the customer. This is generally due to the lack of full communication by the customer with their technical staff or a communications disconnect between the assessment company and the customer. This is why it is extremely important to be detailed in the assumptions section. Another example of scope creep occurs with the discovery of additional systems that need to be reviewed as part of the assessment that were not originally part of the effort.

Restricting Scope Slippage in the Contract

The project manager, team lead, and customer representative should work closely together to avoid scope creep. Any agreed-on changes need to appropriately documented and, if necessary, repriced into the project. This doesn't mean that all scope changes have to be considered negative or even require a cost increase. But it does recommend an evaluation of the change on a case-by-case basis to ensure that expectations are being met.

Uneducated Salespeople

Educate your security sales staff on the assessment process before they are sent out to the field to sell an assessment. They do not have to be experts on the entire process, but they do need to understand what an assessment is composed of, expectations from the process, involvement of the customer in the process, and the impact of customer complexity on the process. Then, working in conjunction with the assessment "experts," they can put together a quality sales presentation and proposal. Ensure that your salespeople understand not to make promises that they are not sure the organization can keep. This includes level of effort of the cost and unreasonable expectations in terms of time frames.

Assessments 101

An INFOSEC assessment:

- Determines which information is critical to the organization
- Identifies the systems that process, store, or transmit that critical information
- Determines the current INFOSEC posture for these systems
- Determines the proper INFOSEC posture for these systems
- Identifies potential vulnerabilities
- Recommends solutions to mitigate or eliminate those vulnerabilities

Planning & Coordinating…

Sold Up the River

This is not intended as a general criticism of salespeople; however, we have experienced several incidents in which an uninformed salesperson sold a service without knowledge of what the effort entailed or how it could be accomplished. Package-pricing a security assessment without knowledge of who the assessment is for or how the assessment is conducted can result in serious mission and financial failure for the organization conducting the assessment. Success is not only measured by how well you do your job but also whether the customer is content with the service they were provided at the price they paid.

Bad Assumptions

Curiosity may have killed the cat, but bad assumptions will kill your contract. A great deal of effort needs to be put into developing and reviewing the assumptions that are made for each contract. Assumptions list the understood environment in which the assessment will be conducted. They will also identify the expected involvement of the customer in the process in terms of staff availability, scheduling requirements, and time frames.

Assumption Topic Areas

The following are examples of information that needs to included in the assumptions section and that must be as accurate as possible to avoid confusion and poor scoping:

- Location at which the assessment will be conducted
- Number of sites at which the assessment will conducted
- Availability of customer personnel for the assessment
- Scheduling of assessment interviews to include shift work
- Travel requirements
- Documentation availability

- Necessary support from the customer in managing the assessment
- Availability and currency of the network architecture diagrams
- Operating system types for servers and workstations
- The customer's technical expertise

Poorly Written Contracts

Poorly written contracts are the basis of poor assessments. Generally, poor contracts are based on bad information, bad assumptions, and lack of attention to detail. A boilerplate assessment contract can be dangerous if not properly tailored to the current customer. Every organization has different expectations and requirements to meet. The worst kind of assessment contract has no specific detail related to the customer being assessed.

Poor Scope Definition

Poor scope definition generally results from a poor understanding of the requirements and expectations associated with the project. From a provider perspective, poor scope definition could mean a loss of revenue and profits for an effort. Poor scoping can result in your consultants having to spend unplanned hours on the job and eventual cost overruns. Another major mistake in the scoping effort is not having the customer approve the agreed-on scope with a signature. Having the customer sign for approval of the scope will help avoid future issues of the customer denying that they agreed with the scope or possibly forcing additional work for no additional money. Be sure to protect your company. Don't assume anything. Document in detail the terms of the agreement.

NOTE

Contracts are one area in which large companies generally have an advantage over smaller companies. They normally have years of experience, a dedicated contracting staff, and strong legal counsel that supports their needs in the contracting process.

Underbid or Overbid: The Art of Poor Cost Estimating

Pricing of a bid can be as critical as the quality of the information put into the bid. Understanding the customer environment and limitations from a financial perspective will help you properly price the effort. This closely ties into the assumptions section of the project. The assumptions help determine the level of effort. It's always dangerous to bid a project low to win the bid. Bidding low cuts into the flexibility and profit margin the project may carry. On the other hand, bidding high can price you out of contention for the project. True pricing has to come from actual expected effort and what your experience tells you it will take to complete the effort.

Many outside influences can impact the costing efforts. As mentioned previously, a poor understanding of the requirements and expectations associated with the project is one influencer. Another is salesperson influence on the process—trying to force undue pressure on the process in an attempt to win the bid. This pressure may result in mistakes being made in costing the effort. Another pressure from the sales staff is, "I said we could do this assessment for $25,000, so we have to do it for $25,000."

Notes from the Trenches…

Contracting Differences

Don't assume that your experience with either government contracting or commercial contracting fully prepares you for all aspects of contracting for the other arena. Government contracts and commercial contracts are unique in nature, as are the differences between the various government agencies or commercial industries. Be prepared to learn something new with the different entities you will be working with, and don't get frustrated when one entity does contracting differently than another.

Staffing Your Project

Deciding on the right composition of the assessment team is important in making your project a success or failure. Putting together the wrong mix for the team can result in an unsatisfied customer and, potentially, the failure of the project. In this section, we look at how the composition of the team for each assessment is important and some of the assurances needed when naming the assessment leader and the assessment team.

Job Requirements

The actual scope of the project determines the team composition for the assessment. It is important for the team leader and the team members to be knowledgeable of the industry the customer works in, the related regulations and guidance that govern the customer, and any legislative requirements that drive the customer's business. For example, if your team has been contracted to perform an assessment on a medical institution, it would be most beneficial to have team members who are familiar with the Healthcare Information Privacy and Portability Act (HIPPA). A close examination of the customer's environment will also determine the technical composition of the assessment team.

Networking and Operating Systems

Gaining an understanding of the technical operating environment is critical in selecting the best team members. A major failure in many assessments relates to having the wrong technical expertise on the team. Having an individual with primarily strong UNIX skills interview the customer's Windows team of the customer would probably prove to be a bad decision; as would having a Cisco networking expert talk to the UNIX team. The technologies are not the same, and in order to garner respect and cooperation in the assessment efforts, the assessment team needs to "speak the same language" as the person or team being assessed. This is not to say that you cannot have an individual on your team with strong skills in multiple technical areas. In fact, your assessment will most likely be more successful if you have technical team members with multiple applicable skills that can be utilized during the assessment process.

Some of the most critical experts to have involved on your team could include those proficient in Windows Server and WorkStation Operating Systems (Win NT, Win 2000, Win 2003, Win XP); UNIX (Sun Solaris, HPUX); Linux (Red Hat, Slackware, Mandrake), Cisco IOS, and possibly mainframes (such as

AS400, VAX, or VMS). Each customer will have a different combination of technical networking and computer operating systems. A good source of this information is from the network architecture descriptions and current network diagrams.

Hardware Knowledge

Understanding the various types of hardware the customer has in use can also be helpful. This hardware can include the types of firewalls, intrusion detection systems, server platforms, routers and switches, and phone systems. This information will also be useful in conducting the assessment. If you have a customer that is purely a Cisco shop, you will want a Cisco-versed individual on the team. If the customer has a combination of hardware and software, you must consider having a very knowledgeable generalist on the team.

Picking the Right People

Final selection of the assessment team is a process of matching the understood needs of the customer with the expertise of available team members. Finding the right match for the pre-assessment phase and ultimately the onsite phase is critical to team success.

Matching Consultants to Customers

Consultants are matched to each customer based on the industry the customer is working in and the specific technologies the customer utilizes in their operational environment:

- **Team leader** The team leader is the single most critical member of the assessment team and should be planned as the team leader for both the pre-assessment and onsite phases. This individual is responsible for constant communication and coordination with both the assessment team and the customer. The team leader should have a minimum of three security assessments supporting other team leaders to ensure that they understand the dynamics involved and have adequate experience to fall back on and share with the customer.

  This individual must be an extremely dynamic person who is capable of facilitating discussion in multiple types of environments and multiple political situations. The team leader should be knowledgeable in the industry in which the customer is primarily working. The team leader does not necessarily have to be a technical expert, but it's important that he or she be capable of understanding the organization's terminology and industry. It is wise to assign a dynamic technical team member to back up the team leader in case of emergency or some other sudden situation.

- **Technical team members** Technical team members need to be experienced in a variety of technologies specifically related to the customer's technical environment. Industry expertise would be a value-add, but the technical expertise is more essential in this case. Technical team members need to be dynamic enough to communicate well with the customer team to obtain the information needed to fully assess the customer security environment.
- **Documentation security specialists** Documentation review and analysis are a large part of the IAM assessment process. It is useful to have expertise in security documentation on the assessment team. These individuals will assist the team leader in identifying documentation issues and providing analysis of inclusions and exclusions of the current documentation.

Personality Issues

Any effort includes the possibility of personality conflicts between team members or with employees of the customer company. The team leader needs to understand this dynamic and attempt to avoid these situations or implement buffers to prevent the situation from becoming an issue. This is more a political issue than anything. Customers will sense tension between team members, which can detract from the overall success of the assessment. When a conflict does arise and the issues cannot be resolved in a less restrictive manner, team member reassignment may be necessary. Since the effort is about customer satisfaction, the team members need to attempt to adjust to the customer first before trying to force a change in the customer.

Adequately Understanding Customer Expectations

The true success of a project is driven by whether the customer is happy with the process and end result of the project. This management of expectations starts from the initial introduction to the customer to the end of the project life cycle, in which the assessment team answers any remaining questions about the results. If at any point the customer appears not to be satisfied with the process, the assessment team needs to make extra efforts to understand the dissatisfaction and come to some resolution.

The Power of Expectations

Expectations drive the customer's sense of satisfaction from the assessment process and the resulting final deliverables. Managing customer expectations and ultimately satisfaction is critical to the success of the assessment.

What Does the Customer Expect for Delivery?

Many assessments start with the customer not understanding what they are truly looking to gain from the assessment process. For this reason, providing customer satisfaction can be difficult. This requires an understanding of the level of detail for the recommendations, the boundaries desired for the assessment, and a strong understanding of the desired use of the results.

Understanding the desired use of the assessment results assists in determining how the final report can be focused to meet customer needs. For example, if a department within a company requested the assessment for the purpose of enlightening senior company management of issues they are not currently addressing, the assessment can be sure to address those areas of concern. Or the assessment may be done as proof of due diligence for the organization's insurance company in the current liability insurance renewal process.

Understanding what the customer expects for delivery will assist the assessment team with the proper focus for the effort.

Adjusting Customer Expectations

Expectations will change throughout the assessment process. The customer will gain a greater understanding of the assessment process and the value the assessment adds to the organization. This understanding will result in a few more desires from the customer and a slightly expanded scope, which could include adding systems to the list of systems to be assessed, increasing the number of sites or divisions to be included in the process, and increasing the number and type of personnel to be interviewed. Changing expectations may also change some of the details of the final deliverable. The business process for changes will determine if pricing or timelines will need to change as well. Ultimately, the deliverable will be a combination of the original expectations, combined with the changing expectations or desires as the assessment process moves forward.

Educating the Customer

Customer education provides the baseline understanding between customer desires and the approach the assessment team takes. Education is an ongoing process, and some education must be addressed at each interview or other customer meeting to keep everyone on the same understanding level. This includes helping the customer understand the level of effort and timelines in which the assessment will occur.

Helping the Customer Understand the Level of Effort

Customers generally do not understand the level of effort required by the assessment team to conduct an INFOSEC assessment. Use some of the training information to help inform the customer of methodology and what it entails. Take time to explain past experiences and give examples of activities that work or do not work during the process. The customer needs to understand what is expected of them to ensure that they can make themselves available during the process.

Explaining Timeline Requirements

Many customers will not have an understanding of the amount of time required to conduct an IAM assessment. Some may think your company will come in for a week and be done. Giving the customer a full understanding of the process, including timelines that outline with what happens in each phase, will be helpful. The education process requires reminders throughout every phase; we recommend that you include timeline discussions as part of each inbriefing (opening meeting) and outbriefing (closing meeting).

Understand the Commitment

The assessment team must understand the level of commitment they are facing while conducting the assessment. Ensure that the assessment team understands the expectations for their time, especially while onsite. Managing the team's expectations as well as the customer's expectations is important for the effort's success.

Project Leadership

For the assessment team, the primary responsibility is to conduct the assessment in an organized, professional, and productive manner. This includes ensuring that the process is on track from a project standpoint. The assessment team is a facilitator helping the customer through the process of identifying critical information, critical systems, and the customer's security objectives. The team leader also needs to work closely with the customer representative to ensure that details are considered in the scheduling process.

Constant Communication with the Customer

As in every relationship, communication is a key component of IAM project success. Keeping the customer involved and informed throughout the effort helps prevent misunderstandings, confusion, and misinformation from occurring throughout the assessment process.

During the contracting process, work closely with the customer to put the final information together; doing so will provide you with a great deal of needed information. It is also an opportunity to set a good communication standard with the customer so they can gauge what to expect.

During the pre-assessment phase, good communication is needed to establish schedules for the pre-assessment site visit and to arrange receiving the relevant documentation for the assessment. It is important to communicate items such as arrival times, number of people, names of people, how to contact you while you're traveling, where you are staying, and so on. This will help avoid surprises. During the pre-assessment site visit, constant communication with the customer is necessary, especially since many of the relevant decisions to be made as part of the assessment process are customer decisions. If communications break down during this process, failure is almost guaranteed. Good communication during preparation for the onsite visit before the actual assessment is also critical for the purpose of scheduling interviews and ensuring that there is time between interviews to make notes and reflect as appropriate.

Communication during the onsite phase of the assessment revolves around keeping the customer informed of progress, initial findings, and any challenges encountered. As always, the goal for customer communication is that there be no surprises. During the onsite phase, it is recommended that the team leader meet with the customer contact a minimum of once per day, and more often as needed. Periodic communications should be considered for the senior leadership. If you were doing a multiweek assessment, for example, the end of each week would be appropriate, highlighting the progress and initial findings of the assessment. An informed customer is a happy customer.

During the post-assessment phase, communication with the customer must continue. It is important to include discussion on progress of the final report, analysis findings, and discussion on any questions arising from the analysis process.

From the Trenches…

Communication Breakdown

Communication breakdown is the number-one reason for customer dissatisfaction. Overlooking seemingly simple details can result in making a poor impression on the customer. A simple example of a communication failure that had significant impact on the assessment process occurred when one assessor overlooked requirements to access customer facilities and the need for a visit request with appropriate clearances. This oversight resulted in a two-day delay in starting the onsite portion of the assessment. The team leader's failure to coordinate all the team's clearances had a significant impact on the start of the assessment, especially since it was the team leader's clearance that did not get passed to the customer. This glitch obviously did not start the assessment off on the right foot, cost the assessment team time and money, and required a great deal of action to regain customer support. Attention to detail at all levels is critical to a successful assessment.

Constant Communication with Team Members

Communication isn't important only between the assessment team and the customer. It is also important between team members and the team leader. Miscommunication among team members, especially considering the intense schedule and stress the team will be under, can result in poor work, hurt feelings, and general disgruntlement. These results will not only affect the team members—the customer will also know there are problems, which could create a negative perception that will be difficult to change.

During the initial contracting of the project, it may be wise to notify personnel who you're bidding on the effort that they are bid and give them a general idea of the time frame for the assessment to occur so that they can keep an opening in their schedules, if possible. When establishing timelines with the customer, take into consideration the team schedule that is already in place and who are the key players for the assessment, and take steps to ensure their availability.

Team communication during the pre-assessment phase is crucial to prepare for and conduct the pre-assessment activities. To prevent overlap and frustration, the team members need to fully understand their roles and responsibilities throughout every step of the process. During the pre-assessment site visit, the team members present are likely to be working very closely to accomplish the tasks. There may be some separate meetings, but those are few in the pre-assessment. During the pre-assessment preparation activities, it is wise to meet on a minimum weekly basis to ensure that everyone is on track with their roles and responsibilities in preparing to go to the customer site.

The same applies for the onsite phase—you must ensure that everyone understands and executes their roles and responsibilities. During this phase, the team leader needs to make sure that the team meets daily to discuss progress and challenges that are occurring. This will help the team leader keep the customer informed during the customer communication sessions and work to resolve any roadblocks to the assessment's successful completion.

During the post-assessment phase, team member communication will help keep the analysis and recommendation activities on track. Strong communication will also help reduce the duplication of effort and provide a better-quality deliverable for the customer. The team leader must communicate to keep the team focused on the task of doing the analysis and providing the recommendations.

Timeliness of the Effort

Meeting customer expectations from a timeliness perspective can sometimes be a challenge. A significant activity to better meet customer expectations involves educating the customer on what to expect. Through experience, we have found that government customers are more understanding about the length of time required for an assessment than are commercial customers.

NSA places a great deal of emphasis on the timeliness of the assessment effort. Ideally, the entire process will be completed in three to four months, if not sooner. The value of the findings and recommendations is greater if the process is completed as quickly as possible. Each assessment is a snapshot in time. The longer the effort takes to complete, the older and possibly more out of date the information will be when it's delivered. Each customer will have a different definition of timeliness based on that customer's needs. Timeliness for a customer may be driven by any of the following:

- Funding
- Audit or inspection schedule
- Renewal of insurance policies
- Contract requirements with the customer's customers
- Certification and accreditation (C&A) requirements

Long Nights, Impossible Odds

The assessment team will be faced with the dilemma of too much to do and not enough time to do it. Performing an assessment is not an eight-hour-a-day job, especially while conducting the pre-assessment site visit and the onsite assessment phase of the project. Extensive time is needed in the evenings to review documentation and notes related to each day's activities and to prepare for the following day. It is also important to begin formulating findings based on the information obtained during each day. Should you not plan for this time, you might miss something because it wasn't noted appropriately during the process. Often forgotten in the scheduling process is the need to interview and spend time with shift workers from all shifts, night staff, night security guards, and the like. The team leader must take this need into consideration in the scheduling process to ensure that team members are not scheduled for 24 straight hours of interviews.

Initial Resistance Fades to Cooperation

In dealing with the customer's employees, the assessment team will find some initial concerns and misunderstandings about the function of the assessment. Some may see the assessment as an invasion of their territory or a threat to their jobs. With the right leadership dynamics from the assessment team and support from the organization's leadership, this initial resistance will fade into cooperation. People involved with the assessment process begin to see the value of the IAM process and the information it helps to pull out of the organization. Items that help with this cooperation are the basic characteristics of the IAM assessment:

- Nonattribution
- Not an audit or inspection
- Team-offered recommendations to help with findings
- Nonconfrontational approach to the assessment

Case Study: Scoping Effort for the Organization for Optimal Power Supply

The Organization for Optimal Power Supply (OOPS) issued an RFP on October 1, 2003, following a regional blackout. Concern was raised that the outage may have been associated with a security problem within the system. OOPS is regulated by the DoE and must be concerned about being a critical infrastructure by providing power for the nation's power grids. *DoE is requiring OOPS to have a third-party assessment* to examine security for the OOPS organization and determine the organization's current security posture. The RFP describes the OOPS operating environment as follows:

"The Organization for Optimal Power Supply (OOPS) provides electricity to one-twentieth of the United States' citizens. They constantly monitor power consumption and redirect power according to demands. This includes initiating or terminating operations of generator stations. Historically, *OOPS has had a difficult time starting up idle generator stations when they are needed. Therefore, they have decided to place servers in each station to control the generator's output and status.* To activate a generator station, the regional office calls into the server and logs onto the machine. After a generator station has been activated, it updates its status and output to the regional server by hourly dialup connections. The control of all the OOPS generators is run through a main control center at the corporate headquarters. The control center decides when to activate any generators and which areas are in need of power. All the regional offices are connected to the main server via Frame Relay lines, which allows rapid updates of the current situation. All updates are done automatically by the servers but can be initiated by authorized users if necessary. The technical environment includes a combination of a

Sun Solaris 9 UNIX Server, 6 Windows 2000 Servers, 72 Windows 2000 Workstations, Cisco routers, and a Windows 98 backup server. *All systems are 100% secure.*"

What can we tell about this organization from this brief description?

- OOPS is being "required" by the DOE to do the assessment.
- They feel they are secure on their technical systems.
- They don't understand the purpose of the assessment because they don't mention anything about the security structure of the organization or any existing policy related to security.
- They have implemented some technology workarounds to make their generator control stations work.

Upon analysis of the RFP and discussion with the OOPS technical representative, we were given permission to submit a scoping questionnaire to gather more information about the requirement. OOPS made it clear that they had to publish and distribute any questions and answers provided to all bidding vendors. The questions submitted to OOPS are focused only on needed information not yet provided in the RFP. The additional information gained through the scoping questionnaire is used to prepare the proposal. As a result of the additional information gained, the scope of the assessment is defined as:

- **Scope** OOPS has requested an assessment of their security posture. Included locations in the assessment are the corporate HQ located in Colorado Springs, Colorado. Also included are the regional sites located in Albuquerque, New Mexico; Provo, Utah; Seattle, Washington; and Boise, Idaho. There are eight (8) generator stations located across the region. Access to the generator stations is through dialup modem**.** OOPS has agreed that the assessment will review information from the HQ and regional sites, but all interviews are to be conducted on site at the HQ location, which is located on one campus covering no more than a one-square-block area. Regional site staff will be made available via telephone for discussion. OOPS operates over three (3) shifts and has requested that a subset of users be interviewed on each shift to cover all areas. The organizational security assessment is based on the IAM developed by NSA. The organizational assessment process helps customers focus on the mission of the organization, the processes used to meet mission objectives, the data contained within those processes, and the systems that process, transport, manipulate, and store data. The result of the assessment process is documentation defining the current organizational security posture versus the perceived posture, the critical data within the organization, the prioritization of impact on the organization due to loss of integrity, availability, or confidentiality of data assets, and recommendations for mitigating security issues.

- **Assumptions** Assumptions will be included in the Customer Concerns and/or Constraints section of the assessment plan, which is covered in more detail in Chapter 6 of this book. The following assumptions are made based on information provided by OOPS:

1. Travel will be required while conducting the onsite portion of the evaluation to the HQ location only. Regional sites will be contacted via phone as necessary.
2. The regional sites will not require travel beyond the OOPS HQ to access.
3. Security documentation will be provided to the evaluation team prior to the commencement of the onsite phase of the effort, where possible.
4. The assigned OOPS POC will arrange the interview schedules based on input from the assessment team.
5. The assigned OOPS POC will send out assessment information to the OOPS organization to assist with expectations and education prior to the arrival of the assessment team.

Summary

Taking the time to effectively scope your assessment will save a great deal of headache as the assessment moves forward. This basic foundation sets the tone for the entire assessment process, gives the assessment team its first opportunity to gain experience with the customer, and gives the customer its first opportunity to communicate with the assessment team. Creating "good karma" throughout the scoping and contracting process generally leads to positive results throughout the entire process.

The first necessary action is to get the customer to understand they need an assessment and, in our case, specifically an IAM style of assessment. This may require work on the part of the offering company to educate the customer on the composition of a security assessment and the differences among an assessment, an evaluation, and red teaming. This understanding is essential in meeting the customer's needs and expectations. Spending time with the customer to identify the benefit of an IAM style of assessment will increase your chances to be contracted for the work.

Once the customer is convinced that an assessment is needed, they may begin working with you directly or may be required to go out for competitive bid through an RFP or some other proposal solicitation process. The RFP will contain important information necessary to write a proposal or a contract. The most critical challenge is establishing the scope of the effort and related assumptions to determine the level of effort and costing required to execute the project.

Another challenge is avoiding the normal pitfalls that can occur with any scoping process. The pitfalls come from lessons learned over years in the contracting process. Unfortunately, the pitfall information is made up of primarily "thou shalt not" statements:

- Thou shalt not miss addressing specific customer concerns in your scoping process.
- Thou shalt not make bad scope assumptions.
- Thou shalt not allow outside influences to affect the accuracy of the scoping process.
- Thou shalt not let "scope creep" go unmanaged.
- Thou shalt not write bad contracts that either underbid or overbid a project.

Be sure to use recommendations from your legal staff and experienced team members in putting together your final scope and contract.

Selecting your project staff depends on the size of the customer organization being assessed, the industry in which the customer works, and the technologies the customer employs. The number of people necessary to conduct the assessment depends on similar factors and also must take into consideration the customer's desired timeline and the geographic separation of the customer's organizational components. Technical drivers to consider include the types of hardware and software the customer is using as well as the operating systems in use on the servers, workstations, and network components. Experience will drive the process of matching the consultants to the customers.

Throughout the entire process of scoping and preparing for the assessment, never lose sight of your number-one goal: meeting customer expectations. How do you do this? Through effective communication with the customer, communication with the assessment team, customer education, working with customer timelines, and gaining a common understanding of the level of commitment required to complete the assessment process.

Best Practices Checklist

Determining Contract Requirements

☑ Understand what the customer is asking for and confirm it in writing.

☑ Ensure a common understanding of definitions in relation assessment, evaluation, and red teaming.

☑ Ensure that critical contract elements are addressed, then apply them to your organization's contracting process.

Understanding Contract Pitfalls

☑ Gain an understanding of the customer's constraints in relation to financial and technical implementation.

☑ Assumptions need to be comprehensive and help establish boundaries.

☑ Closely monitor the assessment to avoid undocumented "scope creep."

☑ Avoid overbidding or underbidding contracts. Don't let outside influences taint your logical decision process for determining expected cost.

Staffing Your Project

☑ Select the team leader based on facilitator and leadership skills as well as knowledge of the customer's industry area being assessed.

☑ Select team members based on technical knowledge and the ability to effectively communicate with the customer.

☑ Have a backup plan for team member augmentation or replacement, in case a situation arises.

Adequately Understanding Customer Expectations

☑ Customer expectations drive customer satisfaction. Pay close attention to expectations.

☑ Understand the customer's purpose for requesting an assessment. This drives the focus the final report will have to take to meet these customer needs.

☑ Confirm periodically with the customer that their expectations are being met.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form. You will also gain access to thousands of other FAQs at ITFAQnet.com.

Q: How many hours does it take to do an IAM assessment?

A: Obviously, the amount of time required for an assessment is completely dependent on the size and complexity of the organization being assessed. Added complicating factors can be multiple sites and multiple shifts that need to be covered. Travel can also be an issue. We have found that most organizations' assessments can be completed in between 200 and 450 person hours. This seems like a wide range, but many factors play into this total.

Q: How much should I charge the customer for an IAM assessment?

A: This is completely a business process, and pricing is 100 percent up to your company to decide. We have found that fixed-price contracts with a very detailed scope and set of assumptions are the way to go. They give the team more flexibility in deciding how to execute the effort. We have heard of assessments costing over $100,000 to conduct, but in our experience the assessments are in the $20,000 to $50,000 range.

Q: How can a potential customer check our IAM credentials as part of their vendor selection process?

A: NSA's IATRP.com Web site contains a listing of individuals certified in the IAM. This is a public Web site available to anyone who wants to view it. Another option is to include a copy of the individual certificate of completion for NSA with the provided résumés.

Q: How are the IAM certification and the IAM methodology selling points to the customer?

A: The IAM is a value-added credential showing prospective customers that an individual is recognized for understanding a methodology that was developed and supported by NSA, one of the most prominent security organizations in the world.

Q: Who should I select as the team leader for the assessment?

A: Team leader selection is a process that should be based on the knowledge of the individual in the industry being assessed as well as proven ability to communicate with customers, assessment teams, and other management. A person with proven ability and training as a facilitator will help this process tremendously. The team leader must be an excellent organizer, politician, and communicator.

Q: Should I ever replace team members once I've assigned them?

A: Let's face it—the necessity to replace a team member or even a team leader may arise. Although it's not ideal, replacing a team member is an option, should there be an irresolvable conflict between the team member and the customer or team leader. Replacement may also be necessary should an emergency arise with the team member. The team leader should be prepared with a backup person should this situation occur. It is also important to ensure that your team does not have a single point of failure in leadership or technical capabilities. Have backups ready to deploy in case of need. Make every effort to minimize the impact to the customer as this replacement occurs.

Q: What happens when I don't win the contract?

A: Worst case, you have just spent a few "all-nighters" with nothing to show for your efforts. A better way to look at it is that you have learned a little process improvement, developed better contract templates, and have learned more lessons for the next time you write a contract. Additionally, you are more than likely going to make some additional good contacts in the process. If you win one in10 competitive bids, you are doing well.

Q: Are references important, and if so, how do I get started obtaining references to win work?

A: References are extremely important, but gaining references at the start can be difficult. Start small; gain some references by doing an outstanding job for small organizations. Also consider making a low- or no-cost effort to gain the experience, apply the developed templates, and gain the recommendation before trying to openly compete for assessment work. Start somewhere to gain the references needed to compete for larger, paid efforts.