Scoping Security Assessments -
A Project Management Approach

GIAC GCPM Gold Certification

Author: Ahmed Abdel-Aziz – CISSP, PMP, aaziz.ahmed@gmail.com
Advisor: Tim Proffitt

Accepted: May, 2011

Abstract

Security assessment projects have a beginning and an end, and produce a unique value to the organization. However, security assessments constitute a special type of project, where it is often a challenge to identify the project objectives, as well as to scope the time and effort needed to complete the security assessment. The goal of this paper is to take a project management approach to scoping security assessments to make scoping easier. The result will be more effective and efficient security assessments, which produce more value to the organization.
1. Introduction

Security assessments can mean different things to different people. This paper will explore what a security assessment is, why it should be done, and how it is different than a security audit. The paper will then cover why it is useful to apply project management principles for security assessment projects, with a specific focus on scope management. Following that foundational knowledge, we will discuss how to improve and facilitate our security assessments by leveraging the scope management processes defined within the Project Management Body of Knowledge (PMBOK).

2. Getting Familiar with Security Assessments

2.1. What is a Security Assessment

Simply put, an information security assessment is a measurement of the security posture of a system or organization (Miles, Rogers, Fuller, Hoagberg, & Dykstra, 2004). The security posture is the way information security is implemented. Security assessments are risk-based assessments, due to their focus on vulnerabilities and impact. Security assessments rely on three main assessment methods that are inter-related. Combined, the three methods can accurately assess the Technology, People, and Process elements of security (SANS, 2008). They are explained as follows.

2.1.1. Reviewing Method

The reviewing method includes passive review techniques and interviews, which are generally conducted manually. They help to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities. They include the review of documentation, architecture, rule-sets, and system configurations. The reviewing method enables understanding what the critical information & systems are, and how the organization wants to focus on security.

2.1.2. Examination Method

Examination 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.
This includes doing technical analysis of the firewalls, intrusion detection systems, and routers. It also includes vulnerability scans of the customer’s networks. The reviewing assessment method provides excellent information that leads into future examinations.

### 2.1.3. Testing Method

Testing, often called penetration testing, is a process whereby someone imitates an adversary looking for security vulnerabilities, which allow the break in to a system or network. Reviewing and examination methods provide excellent information that leads into future testing. The diagram below illustrates the methods’ relationship (Miles et al, 2004).

![Diagram illustrating methods relationship](image)

### Security Assessment Methods

**Figure 1**

### 2.2. Why Perform a Security Assessment

A security assessment is performed to identify the current security posture of an information system or organization. The assessment provides recommendations for improvement, which allows the organization to a reach a security goal that mitigates risk, and also enables the organization.

Ahmed Abdel-Aziz, aaziz.ahmed@gmail.com

© 2011 The SANS Institute

As part of the Information Security Reading Room

Author retains full rights.
The security assessment should enable one to answer the following questions:

- What is the critical information?
- What controls are in place for information systems?
- What is the current security posture of information systems?
- Should more or less stringent countermeasures be instituted?
- What is the prioritized security roadmap to follow that addresses high-priority issues first?

2.3. How is a Security Assessment Different from a Security Audit

There is often confusion on whether a security assessment is the same as a security audit. In fact, they are not the same. Auditing is measuring something against a standard, while assessing is determining how good or bad something is, but not necessarily measuring it against a specific standard (Hoelzer, 2007). An assessment can take place before an audit (to prepare for the audit), or after an audit (to measure how effective the audit was).

Another key difference between security audit & security assessment is the focus. While the main focus of an audit is to check for compliance, the main focus of an assessment is to help the organization improve its security posture (Miles et al, 2004).
3. Project Management for Security Assessments

3.1. Why Project Management for Security Assessments

The PMBOK (Project Management Body of Knowledge) Guide defines a project as a temporary endeavor undertaken to create a unique product, service, or result. When comparing this definition to one’s understanding of a security assessment, we find that security assessments are in fact a project that is temporary (has a definite beginning and end), and creates a unique result (understanding current security posture and how to improve it).

The end of the security assessment project is reached when the project’s objectives have been achieved, or when the project is terminated because its objectives will not or cannot be met. Of course, ending the project when its objectives have been achieved is much more appealing, and that is a key reason why project management processes should be applied for security assessments. Applying proper project management increases the likelihood that the project will succeed and meet its objectives.

Let’s focus on what one is actually trying to do when one conducts a security assessment. An organization has a specific set of security requirements, which are derived from three main sources (Abdel-Aziz, 2010):

1- Security requirements derived from legal, regulatory, and contractual requirements.
2- Security requirements derived from assessing risks to the organization.
3- Security requirements derived from a particular set of objectives for information processing supporting the organization’s operations.

The specific set of security requirements derived from the above three sources constitute the organization’s “Security Goal” in the below figure. By conducting the Security Assessment, one is attempting to define the security gap and to understand how to make it smaller.
Security assessments are considered complex projects (Bernstein, 2010). One can leverage project management processes to increase the success of the attempt to:

1. Define the security gap
2. Understand how to make it smaller

### 3.2. Three-Phase Project Management Approach

One way to reduce project risk and uncertainty in complex projects such as security assessments is to take a phased approach for increased level of project control. In phases, work has distinct focus that differs from any other phase, and work in each phase involves different skill sets (PMI, 2008). By looking back at the three security assessment methods (*Reviewing, Examination, and Testing*), it is clear that each method can fit nicely into a project phase. Each method has a distinct focus, and requires a different skill set. For example, the focus of security assessment Phase-1 (*Reviewing Phase*) would be on understanding what the critical information and systems are, and how organization wants to focus on security (*defensive security*). On the other hand, the focus of security assessment Phase-3 (*Testing Phase*) would be validating a vulnerability existence, or identifying a forgotten vulnerability (*offensive security*). A security consultant skilled in assessing information security policy in Phase-1 may not be as skilled in penetrating a system in Phase-3. Therefore, the skill set needed for each phase is clearly different. Also, the completion of earlier phase(s) provides excellent information that can be used in subsequent phases to
increase the business value of the subsequent phases. The suggested three-phase project management approach is illustrated below.

**Figure 4 – image source: (PMI, 2008)**

In a project, it is important to define specifics about the actual deliverables and how they can be measured. The main deliverable in a security assessment project is a report. A real world example of such a report would list the security weaknesses in the organization in the form of findings. Each finding would have a priority setting (reflecting the associated risk). The finding will map to a recommendation, with multiple options wherever possible. This structure allows building a security improvement roadmap according to available budget and finding priority, ensuring effective use of the security budget. An example of such a report structure is included below for more clarification; this example is for a security assessment consisting of two phases: Reviewing Phase, and Examination Phase.

**Example for Security Assessment Report Structure:**

- Introduction
- Executive Summary

Ahmed Abdel-Aziz, aaziz.ahmed@gmail.com
3.3. Why Focus on Scoping

According to the project management body of knowledge, project management is accomplished through the appropriate application and integration of 42 logically grouped project management processes comprising of 5 process groups: **Initiating, Planning, Executing, Monitoring & Controlling, and Closing**. All 42 processes need not be applied
uniformly on all projects. However, the project manager *(in collaboration with project team)*
is responsible for determining which processes are appropriate for the project (PMI, 2008).
This paper focuses specifically on the scope management knowledge area of project
management. Before stating why the paper focuses on scope management, it is important to
consider the following graph from the PMBOK guide.

![Impact of Variable Based on Project Time](image)

*Figure 5 – image source: (PMI, 2008)*

The graph indicates the cost of change increases as the project time increases. When
one does not properly plan security assessment projects, the project will naturally experience
significant changes later on; these changes will have a high project cost, can lead to project
delay, or even project failure. Changes are inevitable, but a *large number* of changes late in
the project can be prevented with proper project planning.

Ahmed Abdel-Aziz, aaziz.ahmed@gmail.com
The planning process group is the only group out of the five process groups which has a specific process order that should be followed. That means that planning processes that come first are the foundation for the other planning processes. It turns out that these foundational planning processes, which other planning processes rely on, and by extension the rest of the project’s success, are in fact processes related to *scoping*. That is why this paper focuses on the scoping part of project management for security assessment projects.

4. Security Assessment Scope Management

Scope management is the process of defining what work is required, and then making sure that all of that work, and only that work, is done (Mulcahy, 2009). The following five processes will be covered in this project management knowledge area:

1. Collect Requirements Process
2. Define Scope Process
3. Create Work-Breakdown-Structure (WBS) Process
4. Verify Scope Process
5. Control Scope Process

4.1. Collect Requirements Process

Requirements are what stakeholders need from the security assessment project. Stakeholders are simply defined as any person or organization whose interests may be positively or negatively affected by the project; stakeholders may also exert a positive or negative influence over the project.

The Collect Requirements Process is critical. Unless requirements are understood & defined, it will be very difficult for the assessment to meet these requirements, and therefore the assessment will be far from a quality assessment. This is because quality is defined as the degree to which requirements are met (Mulcahy, 2009). There are two main types of requirements for security assessment projects:

1. Requirements Related to The End Result of the Security Assessment
These requirements specify what needs to be achieved and are included in the RFP, if one has been created. In real-life, the RFP usually does not comprehensively cover these requirements (Miles et al, 2004); therefore, these requirements need to be investigated. Some examples of these requirements include:

- Requirements derived from customer expectations about assessment results, timeline, and cost.
- Requirements to determine how well sensitive information is protected from disclosure, or to determine how well policy is achieving its purpose, etc.
- Requirements to use one assessment method \((\text{reviewing, examination, or testing})\), or a combination of them.

2. Requirements Related to How the Work is Managed

These requirements represent high-level rules of engagement. Some examples of these requirements include:

- Adherence to an established assessment methodology used by the organization.
- Organization requirements with which assessments must comply.
- Roles & responsibilities for both assessment team & target organization.
- Assessment logistics, and assessors’ skills & experience.
- Data handling requirements \((\text{data storage, transmission, removal})\).

Now, where do requirements come from, and how can one collect these requirements? Requirements come from the stakeholders, so one needs first to identify stakeholders. Stakeholders can include whoever requested the security assessment, InfoSec personnel, management, and others. After identifying stakeholders, a number of techniques are applied to actually collect the requirements. Two very effective techniques in collecting requirements for security assessments are \textit{Interviews & Questionnaires}.

Ahmed Abdel-Aziz, aaziz.ahmed@gmail.com
Finally, when the requirements are collected, they need to be documented and prioritized based on importance since there may be conflicting requirements. There are ways to handle conflicting requirements; however this is outside of this paper’s scope. When documenting requirements, it is crucial to specify and include acceptance criteria for the various requirements. The importance of including acceptance criteria will become clearer in the “Verify Scope Process” section of the paper.

4.2. Define Scope Process

The Define Scope Process is primarily concerned with what is and is not included in the security assessment and its deliverables. This process makes use of the documentation created in the earlier process - Collect Requirements Process.

While defining scope, areas are clarified where work could easily be misunderstood. The assessment sites are determined, the size and number of systems and components to be assessed are defined. More details about the assessment method(s) to be used are defined. In addition, detailed rules of engagement are defined. For example, specifying project progress reporting details, how emergency communications will take place, acceptable penetration testing times and whether they are announced or not, details regarding the target organization observation of examination/testing activities performed, how denial-of-service (DOS) checks will be performed, etc (SANS, 2008). This scope definition process can take some time. It is advisable to reduce the frequency of visits to the stakeholders during scope definition since assessors can start to lose credibility if assessors cannot efficiently collect the needed information to define scope (Hoelzer, 2007).

The main result of this process is a document called Project Scope Statement. The document in effect says “Here is what we will do in the security assessment”, or “Here is the agreed upon scope for the security assessment”. The Project Scope Statement may include:

- Progressive elaboration of security assessment requirements collected in the previous process – Collect Requirements Process.
- Deliverables
- Progressive elaboration of the acceptance criteria

Ahmed Abdel-Aziz, aaziz.ahmed@gmail.com
• Project exclusions – to reduce likelihood of scope creep
• Constraints & assumptions

4.3. Create Work-Breakdown-Structure (WBS) Process

A project is made more manageable by breaking it down into individual components that together are known as a Work Breakdown Structure or WBS (PMI, 2006). The WBS is illustrated in below figure.

![Work Breakdown Structure (WBS)](image)

**Figure 6: Work Breakdown Structure (WBS) – image source: (Kasti, 2010)**

A work breakdown structure is a very important tool. It increases project understanding, is deliverable-oriented, and divides the project into smaller manageable pieces. A WBS can also be used as a project communication tool. In the process of creating a WBS for a security assessment, we walk through the assessment in our mind and decompose deliverables into their smaller constituents, level by level. This is done until we reach a point where it is easy to estimate the cost, time, and resources to complete the lowest level of the structure. By completing a WBS for the security assessment, we help ensure that nothing in scope slips through the cracks, and nothing out of scope slips into the project.

As the work is decomposed to greater levels of detail, the ability to plan, manage, and control the work is enhanced. However, excessive decomposition can lead to non-productive management effort, and decreased efficiency in performing the work. Also decomposition may not be possible for a deliverable (or project phase) that will be accomplished far into the future, such as a Penetration Test Phase. In this case, we wait until the phase is clarified so the details of that part of the WBS can be developed. The NIST publication 800-53A (Guide...
for Assessing the Security Controls in Federal Information Systems – Building Effective Security Assessment Plans) includes assessment procedures that may be helpful in creating a WBS for a security assessment.

4.4. Verify Scope Process

The Verify Scope Process is the process of formalizing acceptance of the completed project deliverables (PMI, 2008). The key point to note here is that the deliverables are being reviewed and accepted by the customer, and not by the assessment team. The assessment team needs to first review and accept the completed deliverables before the customer reviews the deliverables for acceptance; however, the assessment team review activity is part of quality management and not scope management. Unlike the previous three processes that were part of the Planning Process Group, the Verify Scope Process is part of the Monitoring & Controlling Process Group.

The Requirements Documentation, Project Scope Statement, and Work Breakdown Structure (WBS) created from earlier processes are used during the inspection; these documents are used to compare the completed deliverables against what was agreed upon and documented. The acceptance criteria created in earlier scoping processes are key to facilitating the verification process with the customer. The output of this process is either a formally completed project deliverable (customer is satisfied), or a change request (customer is dissatisfied). The change requests, if any, should then be processed through a Change Control process. Change control is part of the Integration Management knowledge area and is not covered in this paper. The result of properly applying the three previous scoping processes is reaping the rewards of a satisfied customer. At this stage, hopefully there are completed security assessment deliverables, rather than a significant number of change requests coming from a dissatisfied customer. A small number of change requests may be acceptable.

4.5. Control Scope Process

The Control Scope Process is the process of measuring assessment scope performance, and managing Scope Statement & WBS changes. The Control Scope Process is
extremely proactive, but unfortunately rarely applied properly (Mulcahy, 2009). The process helps ensure that at any point in the project, scope is being completed according to plan. To control scope, we need to have assessment activities completed, and a clear definition of the agreed upon requirements and scope. We measure the variance between what was completed and what was planned; and then decide if corrective action or preventive action is required. These needed preventive or corrective actions create change requests. Unlike change requests in the Verify Scope Process which focus on repairing a defect in a completed deliverable, the change requests in the Control Scope Process focus on preventing/correcting a scope deviation before the deliverable is completed – it is proactive. As evident in the below figure, the cost of proactive changes created in the Control Scope Process will be less than the cost of reactive changes created in the Verify Scope Process.

![Impact of Variable Based on Project Time](image)

**Figure 7 – image source:** (PMI, 2008)

Applying the Control Scope Process helps prevent unnecessary problems in security assessment projects. To further clarify the Control Scope Process, a few real world examples will be used to demonstrate cases where deviation from planned scope occurred, and how the Control Scope Process helped to get back on track.

**Case 1:** *(Scope creep due to unexpected outage)*
The security assessor is examining an information system using a vulnerability scanner. Another system on the same network suddenly crashes. The security assessor becomes the prime suspect. Feeling the pressure, the assessor starts to investigate and troubleshoot the other system, which turns out to be a lengthy investigation. Applying the Control Scope Process, it became evident this is scope creep and needs to be controlled. Issue was discussed with customer, project got back on track, and unplanned additional scope was prevented from being added to project.

**Case 2: (Tool problem leading to incomplete scope)**

While performing an assessment activity, the used security tool failed to operate due to a licensing problem. The security assessor moved on to other assessment activities in the work breakdown structure to meet the tight project schedule, and intended to come back to the stalled activity later. With so much to do, the skipped activity was forgotten and led to an incomplete actual scope. This scope deviation was caught early on when the Control Scope Process was applied. Re-visiting the skipped activity after fixing the licensing problem prevented incomplete project scope being delivered to the customer, which certainly would have left a bad impression. Not only that, but catching the skipped activity early led to saving significant costs, since there were many dependencies. All these dependant activities would have had to be redone, adding unnecessary costs to the project.

**Case 3: (Real-time system taken out of scope)**

While examining a real-time system in production as part of a security assessment, the real-time system failed to meet its defined service-level. Every time the scanner sent an uncommon packet to the real-time system, the response time for the real-time system was affected severely. Security examination for the real-time system had to be done in a test environment, instead of the production environment. This caused a scope deviation since no test environment was available. The corrective action taken in the Control Scope Process was to initiate a change request to reduce the project’s scope. The change control process would then evaluate the impact on other project constraints such as cost and schedule. After change request approval, the project scope was redefined to not include the real-time system, thereby eliminating scope deviation. The real-time system would be examined in a future project when a test environment becomes available.

Ahmed Abdel-Aziz, aaziz.ahmed@gmail.com
4.6. Planning Assessments is more than Scoping Assessments

The three scope planning processes (*1-Collect Requirements Process*, *2-Define Scope Process*, and *3-Create WBS Process*) are the foundation of project planning. Although scope planning is the foundation, it is just one aspect of project planning. In addition to scope, planning also includes aspects of time, cost, quality, communication, risk, and procurement. Examples of planning activities in assessments related to these other aspects are:

- Preparing detailed project time plan *(time aspect)*
- Preparing the needed security tools to acquire or build *(procurement/cost aspects)*
- Developing questionnaires, check-lists, and pre-cautions *(time/cost/risk aspects)*
- Scheduling interviews and discussions with organization personnel *(time aspect)*
- Developing communication plan for emergencies and progress update *(communication & risk aspects)*

Imagine how much better a security assessment would be if it could magically be done all over again. This is the power of planning, because it involves walking through the project and getting it organized before it is done. Proper planning can save time, money, and resources (Mulcahy, 2009).

In multi-phase security assessments, a planning technique called rolling-wave planning can be used. In rolling-wave planning, one would not plan subsequent phases *(Testing-phase)*, until some or all work has been completed in earlier phases *(Review/Examination-phase)*. This paper focused on scope management because all planning builds on top of scope planning.

With an understanding of the five scope management processes, one can create a template Scope Management Plan to standardize the scope management effort for future security assessments. The Scope Management Plan would include details about how to define, manage, and control scope for security assessments. The effort put in to develop such a template plan can make scope management even easier for security assessments. That way a tailored way for performing scope management is created – *i.e.: This is how we do scope management for assessment projects here at the XYZ Security Consulting Company.*

Ahmed Abdel-Aziz, aaziz.ahmed@gmail.com
5. Conclusion

The security assessment is a complex security service offered by either a service provider, or by an internal specialized team in the organization. In either case, defining assessment objectives, managing assessment scope, estimating time and budget required, are all significant challenges for this special type of project. The adoption of a project management approach helps overcome all these challenges, and leads to getting more value out of security assessments.

A security assessment is not a security audit; it is a measurement of the security posture using one or more of the three assessment methods: Reviewing, Examination, and Testing. Assessments enable an organization to minimize its security gap. The science of project management can increase the likelihood of success for an assessment, especially when proper scope management and a multi-phase approach are adopted. Proper planning for a security assessment can save time, money, and resources. All planning builds on top of scope planning represented by the three scope management processes: Collect Requirements Process, Define Scope Process, and Create WBS Process. The two remaining scope management processes are for monitoring and controlling and are named: Verify Scope Process and Control Scope Process. These two processes will help take the assessment safely to the other shore of successful completion, once project execution has begun and sailing has started.

A security assessment is a very beneficial security consulting service. The science of project management has proven its value in helping projects succeed. By embracing a Project Management Approach to Scoping Security Assessments the security consultants can get the best of both worlds.

6. References


<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Chicago, ILUS</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit &amp; Training 2020</td>
<td>Munich, DE</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Budapest June 2020</td>
<td>Budapest, HU</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas Summer 2020</td>
<td>Las Vegas, NVUS</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich June 2020</td>
<td>Zurich, CH</td>
<td>Jun 15, 2020 - Jun 20, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London June 2020</td>
<td>OnlineGB</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>

Click here to view a list of all SANS Courses.