Systems Security Engineering

SSE CMM

Capability Maturity Model

Appraisal Method

Version 2.0

April 16, 1999

Systems Security Engineering Capability Maturity Model (SSE-CMM) Appraisal Method – Version 2.0

Table of Contents

Acknowledgments

Sponsoring Organizations

Organizations have sponsored the SSE-CMM Project through provision of technical support staff as well as the infrastructure for sustaining the continuing efforts. These organizations include National Security Agency, Office of the Secretary of Defense, and Communications Security Establishment (Canada).

Participating Organizations

The Systems Security Engineering Capability Maturity Model (SSE-CMM) is a community-owned model, and is a result of the dedicated work of many individuals. The following list acknowledges the efforts and support of those organizations that contributed to the effort through participation in Working Groups or as reviewers:

Arca Systems, Inc.
AverStar, Inc.
BDM International, Inc.
Booz-Allen & Hamilton, Inc.
Cisco Systems
Communications Security Establishment (Canada)
Computer Sciences Canada
Computer Sciences Corporation
Critical Information Assurance Office
Data Systems Analysts, Inc.
Defense Information Systems Agency
Domus Software
E-Systems
Electronic Data Systems
Electronic Warfare Associates – Canada, Ltd.
Fites and Associates
Fuentez Systems Concepts, Inc.
G-J Consulting
GRC International, Inc.
Harris Corporation
Hughes Aircraft
IIT Research Institute
Institute for Computer & Information Sciences
Institute for Defense Analyses
Internal Revenue Service
ITT Aerospace
JOTA System Security Consultants, Inc.
Lockheed Martin Management and Data Systems
Lockheed Martin Mission Systems
Merdan Group, Inc.
MITRE Corporation
Mitretek Systems
Motorola
National Center for Supercomputing Applications
National Institute for Standards and Technology
National Security Agency
Naval Research Laboratory
Navy Command, Control, Operations Support Center Research, Development, Testing & Evaluation Division (NRaD)
Northrop Grumman
Office of the Secretary of Defense
Okiok Data
Oracle Corporation
pragma Systems Corporation
Predicate Logic, Inc.
Rapid Systems Solutions, Inc.
San Antonio Air Logistics Center
Science Applications International Corporation
Signal 9 Solutions
Software Engineering Institute
SPARTA, Inc.
Stanford Telecom
Systems Research & Applications
Tax Modernization Institute
The Sachs Groups
tOmega Engineering
Trusted Information Systems
TRW
Unisys Government Systems
United States Agency for International Development (USAID)

SSE-CMM Project Team Members

Since January 1995, the SSE-CMM Project team members have participated in the development of the SSE-CMM Model Description and Appraisal Method, and have promoted the adoption of the SSE-CMM. The following are members of the SSE-CMM Project team:

Abzug, Charles	Institute for Computer & Information Sciences
Adams, John	Trusted Information Systems
Aldrich, Mark	GRC International, Inc.
Bacoyanis, Gus	TRW
Barrett, Claire	Arca Systems, Inc.
Bass, Frank	tOmega Engineering
Bratton, Vicky	E-Systems
Burke, Karen	Lockheed Martin Management and Data Systems
Campbell, Chris	Motorola Govt. & Space Technology Group
Cartier, Gene	Systems Research & Applications Corp.
Casimir, Michael	National Security Agency
Cheetham, Chris	National Security Agency
Childers, Susy	Computer Sciences Corporation
Cohen, Aaron	JOTA System Security Consultants, Inc.
Craft, Jim	Systems Research & Applications
Danner, Bonnie	TRW Government Information Services Division
Dawson, Bill	BDM International, Inc.
DeGrafft, Hart	Sparta, Inc.
DeMello, Jeff	Oracle Corp.
Diggs, Galina	Predicate Logic, Inc.
Emery, Patrick	GRC International, Inc.
Ferraiolo, Karen	Arca Systems, Inc.
Filsinger, Jarrellann	Trusted Information Systems
Fordham, Mal	IIT Research Institute
Fowler, Joan	Data Systems Analysts, Inc.
Gallagher, Lisa	Arca Systems, Inc.
Gambel, Dan	Mitretek
George, Bruce	National Security Agency
Gibson, Virgil	Computer Sciences Corporation
Gilmore, Linda	Computer Sciences Corporation
Gove, Ron	SAIC
Hart, Tom	GRC International, Inc.
Heaney, Jody	MITRE Corporation
Hefner, Rick	TRW
Henning, Ronda	Harris Corporation
Hopkinson, John	Electronic Warfare Associates - Canada, Ltd.
Hsiao, David	GRC International, Inc.
Jelen, George	GJ Consulting
Klein, Penny	DISA/CISS

Knode, Ron	Computer Sciences Corporation
Koepnick, Glenn	San Antonio Air Logistics Center
Landoll, Doug	Arca Systems, Inc.
Lorenz, Natalie	Booz-Allen & Hamilton
Menk, Chuck	National Security Agency
Monroe, Warren	Hughes Aircraft
Nickel, James	ITT
Niemeyer, Robert	Stanford Telecom
Obenza, Ray	Software Engineering Institute
Payne, Charles	Secure Computing Corporation
Pearson, Dallas	National Security Agency
Robbins, James	Electronic Warfare Associates - Canada, Ltd.
Rowe, Kenneth	National Center for Supercomputing Applications
Sachs, Joel	The Sachs Groups
Sacksteder, Julie	Merdan Group, Inc.
Schanken, Mary	National Security Agency
Schwartz, Robert	TRW
Shafer, Rob	Systems Research & Applications
Simmons, Marty	Lockheed Martin Mission Systems
Thompson, Victoria	Arca Systems, Inc.
Toth, Pat	National Institute of Standards and Technology
Wager, Gene	CPSG/San Antonio Air Force Logistics Center
Weaver, Gary	Harris Corporation
Weiss, Howard	Sparta, Inc.
West, Charles	Science Applications International Corporation
Wichers, Dave	Arca Systems, Inc.
Williams, Jeff	Arca Systems, Inc.
Wilson, William	Arca Systems, Inc.
Zola, Marty	Rapid Systems Solutions, Inc.

Reviewers

Several expert reviewers commented on intermediate releases of SSE-CMM Project work products and participated in formal Project Reviews. Their comments and suggestions were important in ensuring the quality and validity of the model and the appraisal method. This group includes:

R. Batie	Northrop Grumman
D. Busson	Booz-Allen & Hamilton
K. Cusick	SECAT
B. Danner	TRW
D. Evans	Unisys Govt. Systems
S. Garcia	SEI
L. Gates	NRaD
T. Havighurst	NSA
G. Miller	BDM Federal
W. Pearce	TRW
D. Preston	IIT Research Institute
B. Riski	Hughes Information Technology Systems
M. Shupack	US Navy/SPAWAR
G. Stephens	GTE
S. Welke	IDA
D. Werling	BDM International

To the Reader

Abstract

The purpose of this document is to present the major elements of the Systems Security Engineering Capability Maturity Model (SSE-CMM) Appraisal Method (SSAM). The SSAM is the method for using the SSE-CMM to evaluate the process capability of an organization or enterprise's systems security engineering function. The SSE-CMM is described in SSE-CMM version 2.0 [SSE-CMM]. This document describes the four phases of the SSE-CMM appraisal method and provides guidance for the preparation and conduct of an appraisal.

Who Should Use the SSAM?

Any organization wishing to evaluate the capability of another organization to perform systems security engineering activities should consider using the SSAM. The SSAM can be used to evaluate the processes of product developers, service providers, system integrators, system administrators, and security specialists to obtain a baseline or benchmark of actual practices against the standards detailed in the SSE-CMM.

Why was the SSAM the Developed?

The SSAM was developed to provide the systems security engineering community with a publicly-accessible method for preparing for and performing SSE-CMM appraisals.

What is the Scope of the SSAM?

Although the basic concepts in the SSAM are adaptable for other appraisal contexts, the SSAM is specifically designed to support the SSE-CMM. This document is a process description for the SSAM, not a training manual. Some of the material may support appraisal training or the development of appraisal training materials; however, this document is *not* intended as a substitute for appraisal training.

How Should the SSAM be Used?

This version of the SSAM description is written to support the needs of third-party evaluations. However, the document does in some cases include guidance for using the SSAM for self-appraisals.

Additional Information

Questions, further information, or contacts concerning this model or pilot appraisals using this model can be referred to the SSE-CMM Web Site <http://www.sse-cmm.org>.

Data Rights Associated with the SSE-CMM

The members of the SSE-CMM Project are committed to free use of project materials by the systems engineering, and security engineering communities. Participants have agreed that this and future versions of this document, when released to the public, will retain the concept of free access via a permissive copyright notice. Permission to reproduce this work and to prepare derivative works from this product is granted royalty-free, provided the copyright is included with all reproductions and derivative works.

Chapter 1 Introduction to the SSE-CMM Appraisal Method (SSAM)

1.1 Document Overview

The SSAM contains the information and direction required to conduct an appraisal of an organization’s system security engineering process capability and maturity as defined in the System Security Engineering - Capability Maturity Model. This document is divided into four chapters and supported by nine appendices.

- **Chapter 1** introduces readers to the SSAM as well as important general information required to conduct a successful appraisal.
- **Chapter 2** presents the 4 phases of the appraisal process and the steps within each phase.
- **Chapter 3** contains guidance for Sponsors of an appraisal.
- **Chapter 4** contains guidance for teams conducting the appraisal
- The **Appendices** include templates, guidance, checklists, references and other information useful for conducting successful appraisals.

1.2 SSAM Overview

Phases

Table 1–1 lists the phases of the appraisal process. The process elements for each phase are fully described in Chapter 2. A typical schedule is included in Appendix B.

Phase	Description
Planning	Establish the framework under which the appraisal will be conducted as well as to prepare the logistical aspects for the On-Site Phase
Preparation	Prepare the Appraisal Team for the On-Site activities, and conduct a preliminary gathering and analysis of data through the Questionnaire.
On-Site	Explore the results of the preliminary data analysis, and provide an opportunity for practitioners at the appraised entity to participate in the data gathering and validation process
Reporting	Appraisal Team performs its final analysis of all data gathered during the previous three phases and presents its findings to the Sponsor.

Table 1–1. Appraisal Process Phases

Results

The primary work products of the SSAM process are the findings briefing and appraisal report. The findings briefing includes the rating profile and list of appraisal findings. The rating profile indicates the capability level of each PA for the organization. The findings address both the strengths and weaknesses of the Appraised Organization. It is generally developed for the Sponsor, but may be presented to the Appraised Organization at the Sponsor’s request. The appraisal report is written solely for the Sponsor and includes additional detail on each of the findings and their implications for the Sponsors needs. In addition, the final report addresses any Sponsor driven reporting requirements.

Guidance for how to develop the rating profile and writing SSAM reports is addressed in Chapter 4.

1.3 Appraisal Participant Roles and Descriptions

Appraisal participants are grouped according to the three types of organizations involved in the appraisal - Sponsor, Appraiser, and Appraised. Each plays an important role in ensuring that the appraisal goals are met. The following tables outline the primary participants, their qualifications and typical responsibilities in an appraisal. It should be noted that individuals within an organization may perform multiple functions.

For self-appraisals, all appraisal participants are most likely members of the same overall entity, but for the purposes of the appraisal, function as if from the three separate Appraisal Organizations. However, organizations interested in performing a self-assessment may hire outside contractors to assist them.

Sponsor Organization

The Sponsor Organization is the initiator of the appraisal process. It is responsible for defining the appraisal’s scope and purpose, selecting applicable projects from the Appraised Organization, and tailoring the SSE-CMM to meet its needs. The Sponsor Organization may also provide funding to the Appraiser Organization for the conduct of the appraisal. Guidance for the Sponsor Organization can be found in Chapter 3. Table 1–2 lists the roles for the Sponsor Organization personnel during the appraisal process.

Title	Description	Primary Responsibilities	Qualifications
Sponsor	Initiates requirement for appraisal process	Define purpose and goals of appraisal Act as conduit between Appraiser (Facilitator) and Appraised (Site Coordinator) Organizations	Ability to support appraisal activities

Table 1–2. Sponsor Organization Roles

Appraiser Organization

The Appraiser Organization supplies the personnel that will actually conduct the appraisal. In most cases the Appraiser Organization will assist the Sponsor in selecting appropriate projects and tailoring the SSE-CMM to meet their needs. It is essential that the personnel selected to perform the appraisal remain objective throughout the process and have no bias towards or against the Appraised Organization. Table 1–3 lists the roles for the Appraisal Organization personnel during the appraisal process.

Title	Description	Primary Responsibilities	Qualifications
Appraisal Team	All Appraiser Organization personnel participating in the appraisal effort	Participate in Appraisal	See Section 4.2.3
Facilitators	Shared leadership of the Appraisal Team Non-voting participant of Appraisal Team	Ensure appraisal is carried out correctly Coordination of activities with Sponsor Organization (Sponsor) Development and maintenance of appraisal schedule.	See Section 4.2.3
Evidence Custodian[*]	Maintains custody chain of evidence	Request, collect, secure, and dispose of evidence provided by Appraised Organization	Strong configuration management skills
Voting Members	Decision makers of the Appraisal Team	Identify and analyze data and evidence Develop findings and rating reports	See Section 4.2.3
Observers	Non-voting Participant of Appraisal Team	Assist Voting Members and Facilitators Gain experience using the SSAM	SSE-CMM knowledgeable SSAM knowledgeable

Table 1–3. Appraisal Organization Roles

Appraised Organization

The Appraised Organization is the entity that is undergoing the appraisal. It may be a unit within a larger organization, or it may be the organization as a whole. What is meant by Appraised Organization is usually determined by the Sponsor when the requirement for an appraisal is announced or by the organization that will be bidding on the proposal. It depends on the company and how it is organized. Table 1–4 lists the roles for the Appraised Organization personnel during the appraisal process.

[*] The role of Evidence Custodian is fulfilled by one of the Facilitators.

Title	Description	Primary Responsibilities	Qualifications
Site Personnel	All members of the Appraised Organization involved in the appraisal effort	Attend briefings Answer questions during interviews	Employee of Appraised Organization
Site Coordinator	Contact person	Coordinate Appraised Organization's activities during appraisal process Liasse with Appraiser Organization (Facilitator) and Sponsor Organization (Sponsor)	Knowledge of Appraised Organization structure, functioning, policies, procedures Authority to make decisions Familiarity with appraisal efforts (if possible)
Executives	High level authority figures within the Appraised Organization	Show support for appraisal	Ability to compel employee participation in appraisal
Executive Spokesperson	Spokesperson for Executives	Address Site Personnel during Open Meeting	Executive of Appraised Organization
Project Lead	In charge of project activities and personnel	Complete SSAM Questionnaire Respond to interview questions	Identified as having responsibility for oversight of security engineering aspects of an approved project
Practitioner	Member of project team	Respond to interview questions	Support, directly or indirectly, a relevant project

Table 1–4. Appraised Organization Roles

Labor Requirements

Table 1–5 defines the typical labor requirements for a complete appraisal (e.g., all SSE-CMM process areas applied to three projects).

Appraisal Role	Recommended Number of People	Hours per Person	Total Hours for this Role
Sponsor*	1	80	80
Facilitators	2	160	320
Voting team members	4	80	320
Observer	1	80	80
Site Coordinator	1	100	100
Project Leads	1 per project	10	30
Practitioners	6 per project	4	72
Total	**30**	**n/a**	**1002**

Table 1–5. Labor Requirements for an Appraisal

1.4 Appraisal Types

Appraisal for Acquisition

The SSAM was written to facilitate appraisals conducted by third parties, but contains some guidance for interpreting the method for self-appraisals.

The specific objectives of the appraisal will vary according to the needs of the appraisal initiator or Sponsor. These objectives will impact the selection of projects to be appraised and the information presented in the appraisal work products.

Third-party appraisals are conducted for many reasons including:

- qualification for contract consideration
- independent comparative analysis of qualified vendors
- evaluation of existing vendors for purposes of oversight
- assure customer expectations are understood and met
- management of program risk through having an understanding of provider’s weak areas

Appraisal for Self-Improvement

A SSE-CMM appraisal performed for the purpose of self-improvement can provide an organization valuable insights into its own capability to practice security engineering. However, an appraisal demands a substantial commitment of resources and entails a certain unavoidable level of intrusion into the Appraised Organization. Establishing a sound rationale for the appraisal can help the Sponsor to obtain the necessary corporate buy-in and resource commitments. The rationale can also form the basis for an efficient and cost-effective appraisal

* The labor requirements for the Sponsor will vary depending upon their level of involvement in the Planning and Preparation stages of the appraisal.

effort by supporting proper scoping and planning. The choice of SSE-CMM Process Areas and capability levels, the appraisal deadlines, the method for reporting results, and the projects to be included in the appraisal are all influenced by the goals established by the Sponsor. For example, if the primary goal of an appraisal is to improve their ability to provide assurance, the appraisal may place a heavier emphasis on the quality and completeness of evidence than an appraisal performed for the purpose of overall process improvement.

Typical goals for an appraisal performed for self-improvement are:

- to gain an understanding of domain-related issues,
- to understand deployment of new organizational practices,
- to determine overall capability of the organization,
- to determine progress of process improvement activities.

The Sponsor should consider the relevance of the SSE-CMM to the organization and to the particular projects to be appraised in setting goals for the appraisal:

Does the organization practice security engineering in the course of integrating systems, developing applications or products, or providing services?

Does the organization want to improve its practice of security engineering to achieve repeatability, continuity, efficiency and greater assurance? Or is the organization seeking to establish its competency for source selection purposes?

Which projects demonstrate the security engineering process areas that are to be included in the appraisal?

The Sponsor should also recognize that a SSE-CMM appraisal would not prescribe good processes or teach organizations how to improve their capability to perform specific processes. Nor is it a substitute for product evaluation or system certification. On the other hand, a SSE-CMM appraisal can provide important insights and guidance that will lead to process improvements over time, and it can contribute to assurance arguments for products and systems. The Sponsor needs to weigh the value of the potential benefits of an appraisal against its cost before proceeding.

Chapter 2 Appraisal Method Phases

The SSAM is divided into four phases: Planning, Preparation, On-Site and Reporting. Each phase consists of multiple steps which must be carried out before the next phase can begin. Chapter 2 describes each phase and its steps in detail, including it purpose, major participants, typical duration, tailorable parameters, and exit criteria. In addition for several of the steps additional information on how the major participants should proceed is provided. The Notes section at the conclusion of each step includes guidance on how to achieve the best possible results from each step. Figure 2–1 shows the four phases of the SSAM and the primary steps involved with each.

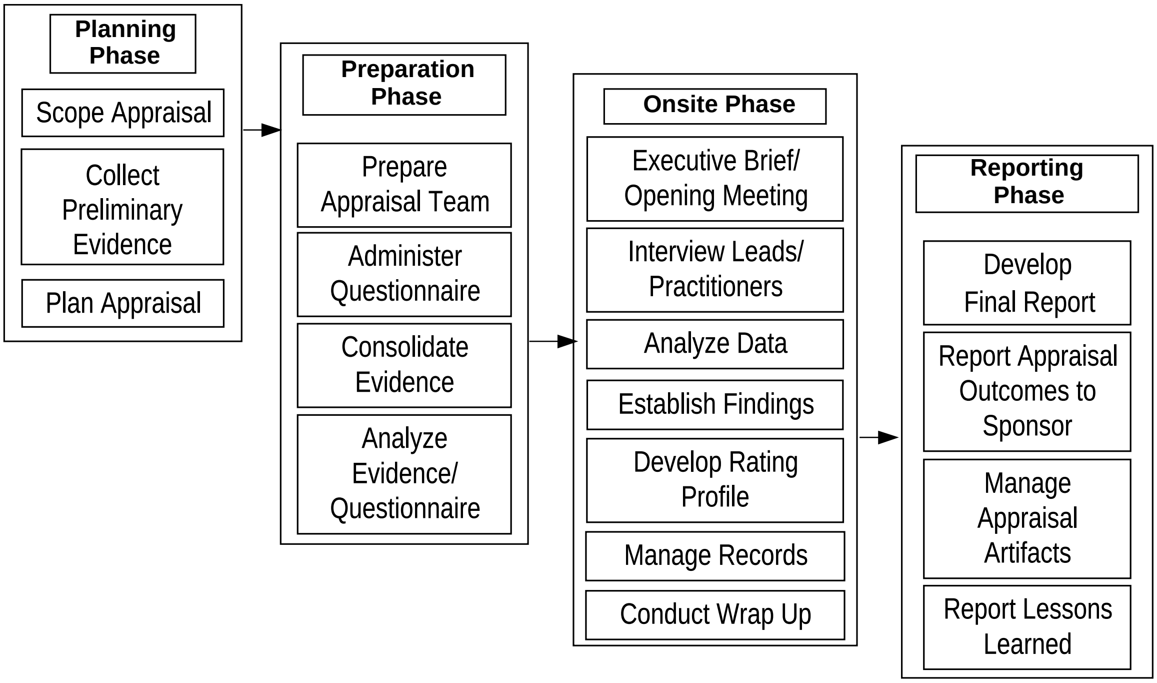


Figure 2–1. SSAM Phases

2.1 Planning

Purpose

The purpose of the Planning Phase is to establish the framework under which the appraisal will be conducted as well as to prepare the logistical aspects for the On-Site Phase. Figure 2–2 shows the steps in the Planning Phase.

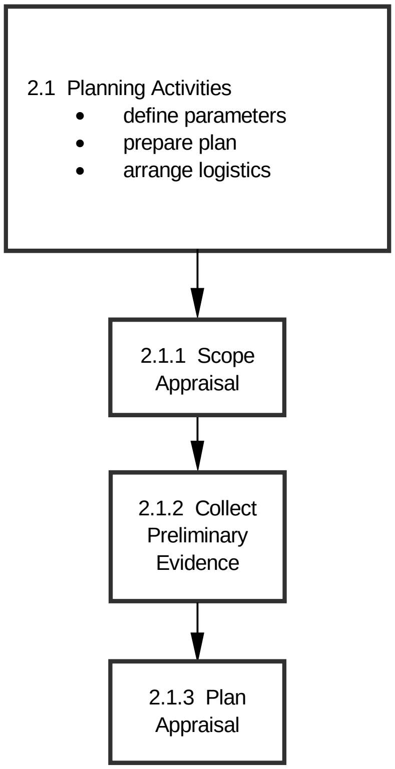


Figure 2–2. SSAM Phases

Summary Description

Table 2–1 lists the major activities of the Planning Phase and the expected output of each. Each element is described more fully in the summaries that follow.

ID	Activity	Description	Outputs
2.1.1	Scope Appraisal	The purpose and goals of the appraisal are established.	Understanding of Sponsor goals
2.1.2	Collect Preliminary Evidence	Evidence is collected from the Appraisal Organization based on their answers to the Questionnaire.	Completed Questionnaires Evidence
2.1.3	Plan Appraisal	A structured plan and agreed upon approach to conducting the appraisal is developed and approved.	Team members Appraisal Plan and Questionnaire

Table 2–1. Summary Description of the Planning Phase

2.1.1 Scope Appraisal

Purpose

The purpose of Scope Appraisal is to define and agree upon the limits and purpose of the appraisal to meet the goals established for the appraisal by the Sponsor.

Summary Description

Scope Appraisal involves defining the application of the model to meet Sponsor goals, setting overall project deadlines, establishing how results are reported, assisting in the determination of acceptable projects, and any other high level information or decisions needed from the Sponsor.

Major Participants

Table 2–2 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	**Summary**
Facilitator	Assists in refinement of appraisal parameters and the establishment of realistic targets.
Sponsor	Defines purpose and goals of appraisal.
Appraised Organization	Provides current information on the organization and applicable projects.

Table 2–2. Participants for Scope Appraisal

Typical Duration

1-2 days depending on number and complexity of appraisal sites and number of teams used

Steps

Table 2–3 shows the steps for this process element.

Step	Guidance
Determine appraisal goals	This activity involves determining the reason/need for the appraisal. Typical appraisal purposes include: confirmation of known flaws, to achieve a rating that can be used in a procurement, to enhance the organizations capabilities (identify specific areas of improvement based on known general areas of deficiency), to obtain buy-in for change, etc. The Sponsor may choose to have the Facilitator assist with this step.
Select Appraisal Team	Choosing an Appraisal Team is critical to both the quality and efficiency of the appraisal. Chapter 3 provides guidance to the Sponsor in selecting a team. The Sponsor will typically select a company that performs SSE-CMM appraisals while the team Facilitator will put together the team in the Planning step. Chapter 3 also provides guidelines that were defined by the SSE-CMM Project for selecting Appraisal Team members.
Define Appraised Organization Factors	As part of scoping the appraisal, specific organizational aspects are addressed. This includes first determining the organization or part of the organization that is to be appraised. Also, a list of acceptable projects is prepared. At this time it should also be decided the number of interviews to be conducted and who specifically will be interviewed including the Project Leads and practitioners. In addition, procedures for reporting results to the Appraised Organization need to be determined.
Define use of the model and appraisal method	Users of CMMs should note that the SSE-CMM Project does not produce, evaluate, or endorse interpretations of the SSE-CMM model and appraisal method. However, particular communities may produce interpretations to fit their particular needs. The Sponsor may have a set Capability Level that is required of the Appraised Organization. The SSE-CMM Appraisal Method defines criteria for attaining Capability Levels, but the Sponsor may wish to redefine the criteria based on the importance they place on meeting a specific level.

Table 2–3. Steps for Scope Appraisal.

Tailorable Parameters

- Use of model for the particular appraisal
- Required capability level

Exit Criteria

- Definition of model application according to Sponsor goals
- Overall deadlines
- Reporting method
- List of acceptable projects
- Criteria for the attaining capability levels
- Other outputs as determined by Facilitator and Sponsor

Notes

None

2.1.2 Collect Preliminary Evidence

Purpose

The purpose of Collect Preliminary Evidence is to ensure that any preliminary evidence, as decided upon in Scope Appraisal, is collected.

Summary Description

Collect Preliminary Evidence includes determining what evidence needs to be collected to support any Sponsor requirements and collecting that evidence prior to the appraisal. This evidence typically includes completed questionnaires for each project and evidence to support questionnaire responses.

Major Participants

Table 2–4 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	**Summary**
Facilitator	Assists Sponsor in defining requirements and collecting evidence.
Sponsor	Defines requirements for preliminary evidence and method of collecting evidence. Coordinates with Facilitator and Site Coordinator.
Site Coordinator	Provides evidence as required.

Table 2–4. Participants for Collect Preliminary Evidence.

Typical Duration

- 1-2 days

Steps

Table 2–5 shows the steps for this process element.

Step	Guidance
Define evidence requirements	The Sponsor defines what evidence will be collected prior to the appraisal and collects and stores the evidence at the Sponsor site. The Sponsor may choose to have the Facilitator assist with this step.
Collect evidence	The Appraised Organization's Site Coordinator ensures that the Sponsor receives the required evidence. A completed Questionnaire accompanied by supporting evidence may be required for submitted as part of a proposal package. All supporting evidence should be catalogued at this point, indicating which requirements the evidence supports. For efficiency purposes, the Site Coordinator should provide this information.

Table 2–5. Steps for Collect Preliminary Evidence.

Tailorable Parameters

- This is a Sponsor driven step and may be tailored out.

Exit Criteria

Notes

- See Chapter 3.

2.1.3 Plan Appraisal

Purpose

The purpose of Plan Appraisal is to produce and obtain approval for the final Appraisal Plan, which documents the parameters and details of the appraisal.

Summary Description

Plan Appraisal involves development of the Appraisal Plan, establishing the availability of planned interviewees during the On-Site period, planning the logistic requirements of the appraisal (meeting rooms, support staff availability, etc.), establishing the Appraisal Team, and verifying the appraisal schedule with all affected parties. It also involves verifying who will receive data upon appraisal conclusion.

Major Participants

Table 2–6 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	Summary
Facilitator	Oversees production of and approval for final Appraisal Plan. Provides Appraisal Team Notebooks.
Appraisal Team	Produces assigned sections of plan.
Sponsor	Approves final Appraisal Plan. Maintains contact with Site Coordinator on progress of preparation and assists in removing obstacles to the appraisal. Ensures Non-Disclosure Agreements are available and signed before any evidence is analyzed by the Appraisal Team.
Site Coordinator	Verifies the schedules of the intended participants and arranges logistics details for the appraisal.

Table 2–6. Participants for Plan Appraisal

Typical Duration

- 2-6 weeks, depending on the complexity of the Appraisal Plan

Steps

Table 2–7 shows the steps for this process element.

Step	Guidance
Choose Appraisal Team	The Facilitator selects the members of the Appraisal Team based on the guidelines in Chapter 4.
Define reporting procedures	The Sponsor specifies how and to whom appraisal results are to be reported. Alternatives range from no report, to a high level presentation to members of the organization by the Appraisal Team at the conclusion of the on-site phase, to a detailed written report provided after the appraisal.
Define schedule	The Sponsor determines the time frame of the appraisal. The Facilitator and Site Coordinator assist in this step by agreeing to details of the schedule. Appendix B provides example schedules for the Preparation and On-Site Phases.
Define logistics	The Site Coordinator arranges all logistics for the appraisal including: rooms for the Appraisal Team, briefings, and interviews; access to the facilities, people, and evidence; any supplies needed by the team; providing meals on site; and suggesting lodging for the team.
Document Appraisal Plan	The Appraisal Plan documents all of the decisions made with regard to all of the previous steps in this process element. Appendix A provides a template for the Appraisal Plan.

Table 2–7. Steps for Plan Appraisal.

Tailorable Parameters

- Degree to which details are planned (dependent on appraisal complexity)
- Contents of the questionnaire, based on the appraisal goals

Exit Criteria

- Appraisal schedule established
- Appraisal Team established
- Appraisal participant availability confirmed
- Appraisal Plan approved
- Logistics of appraisal prepared
- Appraisal questionnaire defined
- Appraisal Team Notebooks prepared
- Evidence collected
- Non-Disclosure Agreements prepared

Notes

Appendix A provides a template for the Appraisal Plan. During this step the actual schedule for the On-Site Phase is produced. Model schedules are provided in Appendix B. Appendix C, provides details on preparing the appraisal logistics.

Logistics Notes:

<u>Space for the Appraisal Team</u>: The space should be large enough to comfortably accommodate the team for the duration of the appraisal (typically five days). The space should contain:

- conference table and chairs adequate for meetings of the entire team
- telephone
- power outlets for one or more computers and a projector
- white boards or walls to which post-its can be attached

In addition, interview rooms and a briefing room will be needed periodically during the appraisal.

<u>Access to facilities, people and evidence</u>: The Site Coordinator should arrange all necessary access to avoid wasting valuable time. If possible, the Appraisal Team should be allowed reasonable access to the facility in which the appraisal is conducted, to minimize time lost arranging escort. The Sponsor should also make sure that the interviewees, briefing audiences, and other people involved in the appraisal are available as required by the Appraisal Plan. Required evidence should be gathered and inventoried prior to the appraisal. Any clearance requirements or non-disclosure agreements should be provided to the Appraisal Team as far in advance of the appraisal as possible.

<u>Supplies</u>: The Site Coordinator may be asked to supply:

- colored paper (to facilitate identification and control of proprietary information)
- appropriate containers for disposal of proprietary or sensitive working papers
- reproduction capability
- display capability (including view graph foils and pens if necessary)
- white boards, flip charts, or other such surface if placing adhesive note pages on walls is not acceptable

<u>Food and Lodging</u>: The Site Coordinator should assist in arranging lodging for the Appraisal Team convenient to the appraisal site. In addition, because of the tight appraisal schedule, it is advisable to make meals available for the Appraisal Team at the appraisal site.

Notes for Appraisal Notebook

The Facilitator should prepare the Appraisal Notebook for each of the team members for use during the appraisal. The notebook should include:

- SSE-CMM Model Description
- SSE-CMM Appraisal Method
- Appraisal Plan
- Schedule
- Ground Rules
- Project Descriptions

- Completed Questionnaires
- Biographies of Leads and Practitioners

2.2 Preparation

Purpose

The purpose of the Preparation Phase is to prepare the Appraisal Team for the On-Site activities and conduct a preliminary gathering and analysis of data through the Questionnaire. Figure 2–3 shows the steps in the Preparation Phase.

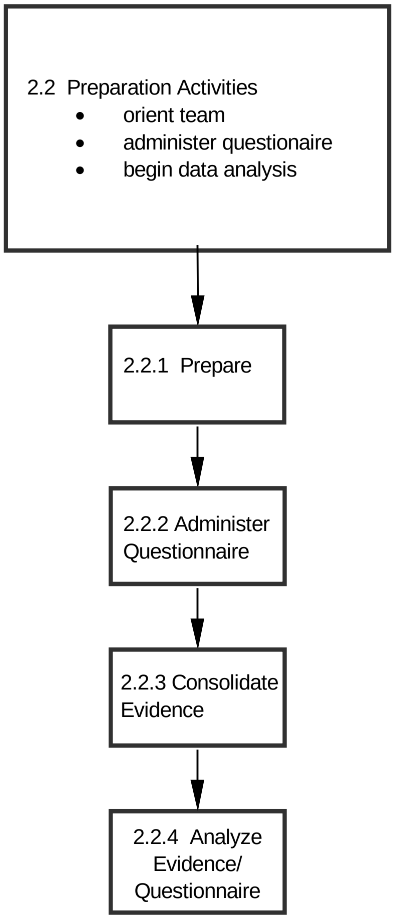

2.2 Preparation Activities
• orient team
• administer questionaire
• begin data analysis
2.2.1 Prepare
2.2.2 Administer Questionnaire
2.2.3 Consolidate Evidence
2.2.4 Analyze Evidence/ Questionnaire

Figure 2–3. Preparation Phase.

Summary Description

Table 2–8 lists the major activities of the Preparation Phase and the expected output of each. Each element is described more fully in the summaries that follow.

ID	Activity	Description	Outputs
2.2.1	Prepare Appraisal Team	This step ensures that all Appraisal Team members are familiar with the SSE-CMM and that they receive the same instructions regarding the conduct of the appraisal.	Team support for appraisal
2.2.2	Administer Questionnaire	A predefined questionnaire administered to Project Leads to obtain preliminary information about the Appraised Organization.	Completed Questionnaire
2.2.3	Consolidate Evidence	Supporting evidence to answers indicated in the questionnaire responses is collected and questionnaire data is compiled.	Evidence gathered Questionnaire data transcribed
2.2.4	Analyze Evidence/ Questionnaire	The team conducts a thorough review of all evidence collected to this stage and prepares questions to ask Project Leads during the On-Site Phase.	Questions for Project Leads

Table 2–8. Summary Description of the Preparation Phase

2.2.1 Prepare Appraisal Team

Purpose

The purpose of Prepare Appraisal Team is to familiarize the team with the details of the appraisal.

Summary Description

Prepare Appraisal Team involves reviewing the details of the appraisal with the team. The Facilitator reviews with the team the SSE-CMM and Appraisal Method in relation to this appraisal, Appraisal Plan, schedule, information about the organization to be appraised (including the specific projects), model interpretations for the organization, and any Sponsor-tailored parameters. Responsibilities for each team member are assigned.

Major Participants

Table 2–9 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	**Summary**
Facilitator	Reviews appraisal details with team and answers questions.
Appraisal Team	Understands appraisal method tailoring and responsibilities in the appraisal.

Table 2–9. Participants for Prepare Appraisal Team.

Typical Duration

- 1-2 days

Steps

Table 2–10 shows the steps for this process element.

Step	Guidance
Review SSE-CMM	During the SSE-CMM review, the Facilitator reviews all of the GPs and BPs, as well as associated work products, capability levels, and how to generate findings and rating profiles. It is assumed that all members will have received SSE-CMM training prior to their selection as part of the Appraisal Team. This should not be a model training session, but a high level review of the content and concepts.
Review SSAM	The SSAM review should include coverage of the four phases and their steps. The time allotted for SSAM review is dependent upon the Team's overall SSAM knowledge and general appraisal experience. Again, this should not be an SSAM training session, but a high level review of the methods and concepts.
Review Appraisal Plan	Before the Appraisal Team is introduced to the Appraisal Plan, any confidentiality related issues must be discussed and if necessary non-disclosure agreements signed. No Appraised Organization specific information should be discussed until all confidentiality related topics, agreements, and consequences are aired. After distributing the Appraisal Notebook, the Facilitator details the specific interpretations of the SSE-CMM and the SSAM for this appraisal, appraisal schedules, acceptable work-products, Sponsor goals and concerns, with an emphasis on those components which have been tailored to meet Sponsor needs. The Facilitator should spend a significant amount of time reviewing how the model has been tailored to meet the needs of the Sponsor. Any questions regarding interpretation/application of the model must be cleared up before initiating the next step otherwise the appraisal will fall behind schedule.
Assign Roles	Team members are also assigned specific duties - focus on particular PAs. Issues of team conduct and performance - voting, discussion format, etc. are defined.

Table 2–10. Steps for Prepare Appraisal Team.

Tailorable Parameters

- More experienced teams may require less preparation time (may not need in-depth review of model and appraisal method)

Exit Criteria

- Appraisal Team understands the use of the SSE-CMM in the appraisal
- Appraisal Team understands the use of the SSAM in the appraisal
- Appraisal Team members understand their roles in the appraisal

- Appraisal Team commits to performing the appraisal as structured in the Planning Phase
- Signed Non-Disclosure Agreements

Notes

This activity should not be performed at the Appraised Organization site. If the Sponsor uses more than one Appraiser Organization to conduct the appraisals, this step should be conducted at the Sponsor Organization's site. Having the teams receive training together promotes consistency among the appraisals.

The review session is led by a Facilitator and should take one to two days, depending upon the team's SSE-CMM knowledge. The more familiar the team members are with the SSE-CMM and its concepts the more thorough, accurate, and relevant the evidence gathering and analysis will be.

2.2.2 Administer Questionnaire

Purpose

The purpose of Administer Questionnaire is to obtain information on the appraised entity through the administration of the questionnaire and the collection of data based on the responses.

Summary Description

Administer Questionnaire involves administering and collecting the results from the questionnaire used to access the organization. Results are used to focus the On-Site data gathering efforts of the appraisal.

Major Participants

Table 2–11 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	Summary
Project Leads	The selected leads provide data on projects and the organization via the questionnaire.
Facilitator	Administers the questionnaire in a meeting with the Project Leads.
Site Coordinator	Ensures that all participants are made available for data collection.

Table 2–11. Participants for Administer Questionnaire.

Typical Duration

- 4-8 hours per participant

Steps

Table 2–12 shows the steps for this process element.

Step	Guidance
Administer Questionnaire	The Facilitator, in a meeting with the Project Leads administers the Questionnaire. The Facilitator remains available with the Project Leads to answer any questions and provide guidance. It is recommended that the questionnaire be administered as a group, with the Facilitator or other person with knowledge about the SSE-CMM present to answer questions of terminology, etc
Collect responses	The Facilitator collects completed questionnaires and all evidence cited.

Table 2–12. Steps for Administer Questionnaire.

Tailorable Parameters

- Time, depending upon how questionnaire is administered
- Who questionnaire is administered to (Sponsor may direct Appraisal Team to administer questionnaire to persons in addition to Project Leads)

Exit Criteria

- Completed questionnaires received by Appraisal Team

Notes

A copy of the questionnaire for all 22 PAs can be found in Appendix D.

The Questionnaire, Appendix D of the SSAM, is the preliminary data gathering tool used in SSE-CMM appraisals. Its purpose is to determine the extent to which the 22 PAs are applied throughout the Appraised Organization. The questionnaire is not a test; it is not "scored." The results of the Questionnaire are used to create a preliminary ratings profile and form the basis for the questions asked during the Project Lead and Practitioner interviews.

The Questionnaire is administered to the Project Leads by the Facilitator at the Appraised Organization site over the course of two half days. It is possible to administer the Questionnaire in one day, however, splitting the process over two days decreases questionnaire fatigue and results in more accurate responses.

Project Leads are asked to determine if the base and generic practices of each PA are performed for their project. For positive responses to the Questionnaire, the Project Leads must indicate evidence, training manuals, official memoranda, etc., that substantiates their answers. The Facilitator should reference the Work Products section for each BP in the SSE-CMM model and the Appraisal Plan as guidance for anticipated evidence. Project Leads may cite evidence other than that indicated in the model or Appraisal Plan, but it is the responsibility of the Appraisal Team during the Analyze Evidence/Questionnaire step to determine if the evidence is valid.

At the Sponsor's discretion, during this step, the Questionnaire may also be administered to personnel in addition to the Project Leads. If the Appraisal is the basis for awarding contracts, a completed Questionnaire, accompanied by supporting evidence, may have been required as part of an RFP response.

2.2.3 Consolidate Evidence

Purpose

The purpose of Consolidate Evidence is to compile the questionnaire data in an analyzable form and to identify and collect supporting evidence.

Summary Description

Consolidate Evidence involves consolidating the responses to the questionnaire. The identification and collection of supporting evidence is also included in this step.

Major Participants

Table 2–13 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	Summary
Appraisal Team	The team collects the questionnaire data in a form that can be analyzed by the team. Any identified evidence is requested through the Evidence Custodian and received from the Site Coordinator. If any preliminary evidence was received, the Appraisal Team can begin analysis of that evidence.
Site Coordinator	Provides evidence requested by Appraisal Team along with an inventory of the evidence.
Facilitator	Coordinates activities among team members.
Evidence Custodian	Tracks evidence requests and usage.

Table 2–13. Participants for Consolidate Evidence.

Typical Duration

- 2-3 hours.

Steps

Table 2–14 shows the steps for this process element.

Step	Guidance
Transfer questionnaire responses to data tracking mechanism	In order facilitate the analysis of the Questionnaire answers, the Project Leads' responses should be consolidated and transferred to an electronic tracking mechanism. The use of a data tracking tool assists the Appraisal Team during the analysis process to recognize patterns and inconsistencies in responses both within projects and across the Appraised Organization as a whole. Appendix E provides a Data Tracking Sheet (DTS) for questionnaire/interview consolidation.
Gather evidence and track in Evidence Tracking Tools	As the Appraisal Team consolidates the Questionnaire answers, a list of supporting evidence requiring review will develop. It is the job of the Evidence Custodian with the assistance of the Site Coordinator to collect the evidence. However, the Evidence Custodian alone is responsible for documenting the receipt, use, and disposal of the evidence once it is received from the Site Coordinator. Appendix F provides templates of Evidence Tracking Tools that can be used to assist the Evidence Custodian accomplish these tasks. All evidence must be kept secure, but remain accessible to the Appraisal Team and interviewees as necessary.

Table 2–14. Steps for Consolidate Evidence.

Tailorable Parameters

- Data tracking format
- Time, based on number of PAs

Exit Criteria

- Questionnaire data is transferred to data tracking mechanism
- Supporting evidence is gathered

Notes

Appendix E provides a model Data Tracking Sheet which will be referred to throughout this document, that may be used to consolidate questionnaire responses. Appendix F provides sample forms and logs useful in tracking the request, receipt, use, and disposal of evidence.

2.2.4 Analyze Evidence/Questionnaire

Purpose

The purpose of Analyze Evidence/Questionnaire is to analyze the results of the Questionnaire responses and supporting evidence provided by the Appraised Organization to develop a set of Exploratory Questions for use during the Project Lead interviews.

Summary Description

The Appraisal Team analyzes the responses to the Questionnaire and determines areas for practice validation, identifies potential discrepancies in responses, and performs a gap analysis against the SSE-CMM. This process element results in a set of Exploratory Questions and anticipated responses for use during the Project Lead interviews. Anticipated responses are called "listen fors" and may refer to procedures or documents, or both. Evidence cited in support of Questionnaire responses is analyzed for corroboration to answers and is used to provide direction for Exploratory Question development.

Major Participants

Table 2–15 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	**Summary**
Facilitator Evidence Custodian	Provides guidance in the formulation of Exploratory Questions. Makes requests for evidence and tracks its use.
Appraisal Team	Analyzes DTS and available evidence.
Voting Members	Develop and agree upon a set of interview questions for each Project Lead and identifies evidence requirements.
Site Coordinator	Gathers evidence requested by Voting Members through the Evidence Custodian.

Table 2–15. Participants for Analyze Evidence/Questionnaire.

Typical Duration

- 4-8 hours

Steps

Table 2–16 shows the steps for this process element.

Step	**Guidance**
Analyze DTS	The Appraisal Team reviews the DTS for inconsistencies, gaps and contradictions in Questionnaire responses.

Step	Guidance
Review Evidence	The Voting Members review evidence referenced in the Questionnaire responses and determines if it supports the Organization's process claims. If the cited evidence is not provided in advance to the Appraisal Team, the Evidence Custodian should request the evidence from the Site Coordinator.
Generate Exploratory Questions	Based on its analysis of the DTS and available evidence the Voting Members, with guidance from the Facilitator generates 20-40 Exploratory Questions for each Project Lead.

Table 2–16. Steps for Analyze Evidence/Questionnaire.

Tailorable Parameters

- Location where analysis is conducted (Appraised or Appraiser Organization site)
- Number of Exploratory Questions developed

Exit Criteria

- Exploratory Questions are prepared for each Project Lead
- Requests for supporting evidence are made

Notes

When analyzing the DTS and supporting evidence, the Appraisal Team should look both within and across projects to gain a clearer understanding of the Appraised Organization's processes. Particular, but not exclusive attention should be given to the areas of greater interest to the Sponsor. Typical areas of interest for the Appraisal Team when conducting their analysis and developing the Exploratory Questions are; discrepancies in cited evidence for positive responses; failure of supplied evidence to support process claims; existence of anticipated work products for each GP and PA; mix of *yes*, *no*, and *don't know* responses across projects for individual GPs and for an individual Project Leads; and claims of higher GP compliance without lower level fulfillment.

Although non voting members of the Appraisal Team may take part in the evidence discussion and analysis and may assist in the generation of Exploratory Questions, the Voting Members are responsible for determining the final content of the questions and deciding who they will be asked of.

Guidance on evidence analysis and question generation is located in Chapter 4.

2.3 On-Site

Purpose

The purpose of the On-Site Phase is to explore the results of the preliminary data analysis, and provide an opportunity for practitioners at the appraised entity to participate in the data gathering and validation process. Figure 2–4shows the steps in the On-Site Phase.

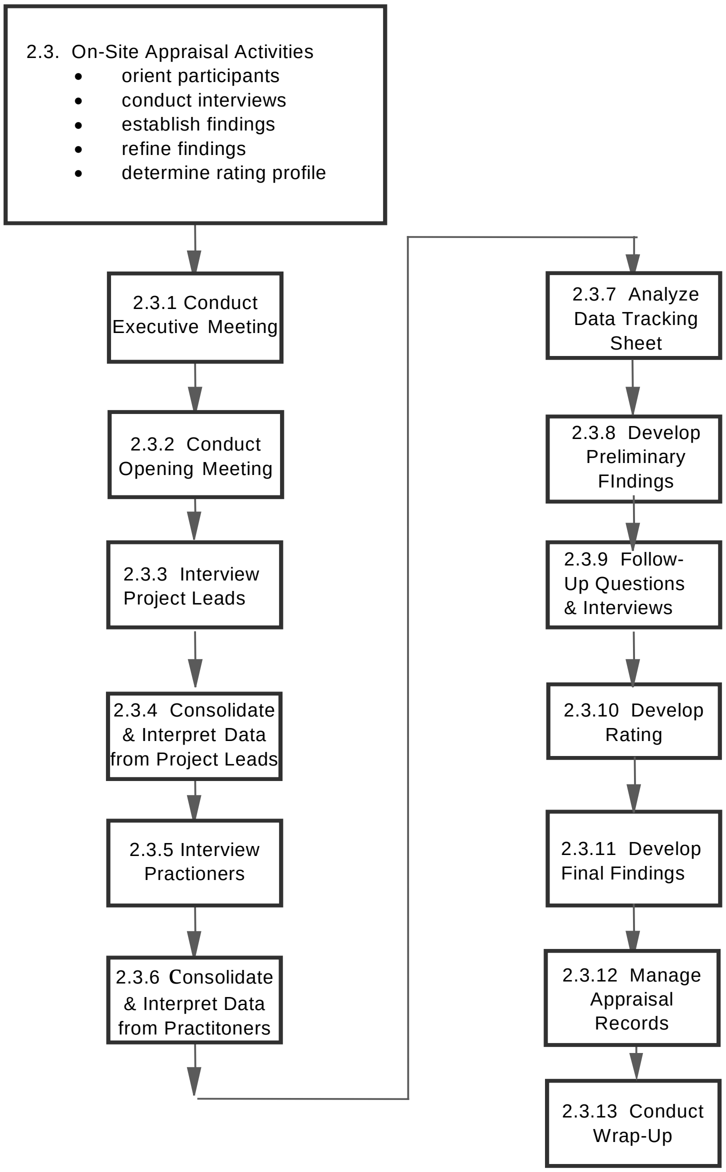

2.3. On-Site Appraisal Activities
• orient participants
• conduct interviews
• establish findings
• refine findings
• determine rating profile
2.3.1 Conduct Executive Meeting
2.3.2 Conduct Opening Meeting
2.3.3 Interview Project Leads
2.3.4 Consolidate & Interpret Data from Project Leads
2.3.5 Interview Practioners
2.3.6 Consolidate & Interpret Data from Practitoners
2.3.7 Analyze Data Tracking Sheet
2.3.8 Develop Preliminary FIndings
2.3.9 Follow-Up Questions & Interviews
2.3.10 Develop Rating
2.3.11 Develop Final Findings
2.3.12 Manage Appraisal Records
2.3.13 Conduct Wrap-Up

Figure 2–4. On-Site Phase.

Summary Description

Table 2–17 lists the major activities of the On-Site phase and the expected output of each. Each element is described more fully in the summaries that follow.

ID	Activity	Description	Outputs
2.3.1	Conduct Executive Meeting	The executive meeting provides management with an overview of the appraisal and provides the Appraisal Team with a view of the organization that gives a context for the appraisal.	Supported appraisal effort Answered questions
2.3.2	Conduct Opening Meeting	The opening meeting provides participants with an overview of the appraisal. It is also the time where management expresses support of the appraisal.	Supported appraisal effort Answered questions
2.3.3	Interview Project Leads	Through structured interview techniques using the Exploratory Questions, the Appraisal Team gathers corroborating data regarding the project's systems security engineering practices.	Interview notes Data requests
2.3.4	Consolidate & Interpret Data from Project Leads	The team members review their notes, discuss any issues, and update the data tracking sheet.	Updated data tracking sheet Adjustments to practitioner interviews
2.3.5	Interview Practitioners	Through structured interview techniques using the Exploratory Questions, the Appraisal Team gathers corroborating data regarding the project's systems security engineering practices.	Interview notes Data requests
2.3.6	Consolidate & Interpret Data from Practitioners	The team members review their notes, discuss any issues, and update the data tracking sheet.	Completed data tracking sheet
2.3.7	Analyze Data Tracking Sheet	The team conducts a zero-based review of the current data tracking sheet and adjusts the entries as appropriate.	Analyze data tracking sheet
2.3.8	Develop Preliminary Findings	Using all data sources available, the team generates a preliminary list of findings with regard to the organization's systems security engineering practices.	Preliminary findings
2.3.9	Follow-Up Questions & Interviews	The team determines if any additional questions should be asked and to who.	Additional questions and interviews
2.3.10	Develop Rating	The team members review their notes, discuss any issues, update the data tracking sheet and formulate the rating profile.	Updated data tracking sheet Rating

ID	Activity	Description	Outputs
2.3.11	Develop Final Findings	The team prioritizes and provides working for findings that fit the appraisal context.	Prioritized findings
2.3.12	Manage Appraisal Records	The team forwards new evidence to the Sponsor for storage and disposes of non-deliverable work products as agreed to in the contract.	Appraisal evidence and interim work products disposed
2.3.13	Conduct Wrap-Up	The Facilitator presents the Ratings and Findings to the Appraised Organization.	Rating and Findings presented

Table 2–17 Summary Description of the On-Site Phase

2.3.1 Conduct Executive Meeting

Purpose

The purpose of Conduct Executive Brief is to present the appraisal process and schedule to executive level management.

Summary Description

Conduct Executive Brief involves gathering executive level managers together to review the appraisal process and reaffirm corporate commitment to the appraisal.

Major Participants

Table 2–18 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator	Presents brief overview of the model and appraisal.
Appraisal Team	Supports Facilitator.
Executives	Learn their role in the On-Site phase of appraisal activities.

Table 2–18. Participants for Conduct Executive Meeting

Typical Duration

- 0.5 hour

Steps

Table 2–19 shows the steps for this process element.

Step	Guidance
Appraisal Discussion	The Facilitator gives a brief introduction to the SSE-CMM, SSAM, and Appraisal Plan.
Question and Answer	The Facilitator responds to any questions or concerns raised by the Executives.

Table 2–19. Steps for Conduct Executive Meeting

Tailorable Parameters

- The presentation will vary based on the purpose of the appraisal.

Exit Criteria

- Opening briefing delivered
- Management questions answered

Notes

The briefing to the Executives should cover the following topics; introduction to SSE-CMM and SSAM, the parameters/details of the appraisal as outlined in the Appraisal Plan, benefits of appraisal, and how ratings will be used.

2.3.2 Conduct Opening Meeting

Purpose

The purpose of Conduct Opening Meeting is to present the appraisal process and schedule all appraisal participants. An additional purpose is for the executives to express support for the appraisal activities.

Summary Description

Conduct Opening Meeting involves gathering all the appraisal participants together, to review the appraisal process and reaffirm corporate commitment to the appraisal.

Major Participants

Table 2–20 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Executive Spokesperson	Welcomes participants and introduces Facilitator Shows management support for the appraisal
Facilitator	Presents brief overview of the Model, Appraisal Method and Appraisal Plan
Appraisal Team	Supports Facilitator
Appraisal Participants	Learn their role in the On-Site phase of appraisal activities

Table 2–20. Participants for Conduct Opening Meeting.

Typical Duration

- 1 hour

Steps

Table 2–21 shows the steps for this process element.

Step	Guidance
Executive Comments	The Executive Spokesperson expresses support for the appraisal.
Facilitator Presentation	The Facilitator gives a presentation on the SSE-CMM and SSAM focusing on the On-Site phase and Site Personnel responsibilities.
Question & Answer	The Facilitator answers any questions from the Appraisal Participants.

Table 2–21. Steps for Conduct Opening Meeting

Tailorable Parameters

- The presentation will vary based on the purpose of the appraisal.

Exit Criteria

- Opening briefing delivered
- Questions of Site Personnel answered

Notes

Refer to Appendix G for a sample Opening Briefing.

2.3.3 Interview Project Leads

Purpose

The purpose of Interview Project Leads is to provide the Project Leads with the opportunity to elaborate on their responses to the Questionnaire through the exploration of issues that the Appraisal Team wishes to have clarified.

Summary Description

Interview Project Leads involves eliciting additional information and evidence from the Project Leads that aids the Appraisal Team in making a ratings determination. The Project Lead may be asked to respond to questions, demonstrate activities, and or explain the use of individual pieces of evidence..

Major Participants

Table 2–22 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	**Summary**
Facilitator	Conducts interview.
Project Lead	Responds to Exploratory Questions.
Appraisal Team	Takes notes.

Table 2–22. Participants for Interview Project Leads.

Typical Duration

- 1½ hours per interview + 15 minutes for Appraisal Team discussion/break per interview

Steps

Table 2–23 shows the steps for this process element.

Step	**Guidance**
Conduct Interview	The Facilitator asks the interview questions developed from the analysis of the Questionnaire responses, while the members of the Appraisal Team take notes.
Follow Up Questions	Voting Members of the Appraisal Team ask additional questions for issues still requiring clarification.
Process Check	The Appraisal Team conducts a quick process check to ensure that the interview is generating needed information and adjusts appropriately for next interview.

Table 2–23. Steps for Interview Project Leads.

Tailorable Parameters

- Number of Exploratory Questions asked
- Number of additional Voting Member questions asked

Exit Criteria

- Project Lead answers all questions

Notes

Before beginning the interview, the Facilitator should introduce themselves and the members of the Appraisal Team and briefly explain the purpose of the interview. The interviewee should be reminded that the issues discussed in the interview and interview notes are not shared with anyone outside of the Appraisal Team and that all information/comments/responses are covered by the Non Disclosure Agreement.

The Facilitator should follow the interview script as developed during step 2.2.4 Consolidate Evidence. However, the Facilitator is encouraged to introduce follow-up or clarifying questions where appropriate; interviewee doesn’t understand concept being addressed, a different interpretation of previously discussed evidence is given, response clearly contradicts that of other interviewees, etc.

Depending upon the number of Exploratory Questions developed for an individual Project Lead, and the need for additional questions by the Facilitator, it is possible that not all scripted questions will be asked, or that the Voting Members of the Appraisal Team members will have the opportunity to pose their individual questions. Unaddressed questions should be recorded during the process check for possible incorporation in later interviews.

2.3.4 Consolidate & Interpret Data from Project Leads

Purpose

The purpose of Consolidate & Interpret Data from Project Leads is to assimilate the information gathered during the Project Lead interviews and translate it into the DTS so that it can be analyzed

Summary Description

Consolidate & Interpret Data from Project Leads involves updating the DTS to reflect the information gathered during the Project Lead interviews and interpreting that information to develop questions for the Participant Interviews.

Major Participants

Table 2–24 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	**Summary**
Facilitator	Provides guidance and model expertise for the Appraisal Team’s deliberations.
Appraisal Team	Reviews notes, discusses issues and formulates observations.
Voting Members	Update the DTS.

Table 2–24. Participants for Consolidate Data from Project Leads.

Typical Duration

- 2 hours

Steps

Table 2–25 shows the steps for this process element.

Step	**Guidance**
Review notes	Each team member privately reviews his/her notes from the interviews with the Project Leads.
Update DTS	The Appraisal Team discusses as a whole the responses of each Project Lead on a question by question basis. The DTS is updated based on the decisions of the Voting Members
Interpret Data	The Appraisal Team reviews the available information (DTS, interview notes, questionnaire responses, cited evidence) and discusses what areas require further investigation during the Practitioner interviews.
Update Interview Questions	Based on the data interpretations, interview scripts for use during the Practitioner interviews are developed by the Voting Members.

Table 2–25. Steps for Consolidate Data from Project Leads.

Tailorable Parameters

- None

Exit Criteria

- Questions for Practitioner interviews are developed.

Notes

See Appendix E for details on the DTS

The process for developing Practitioner interview questions is the same as that used for developing Exploratory Questions for the Project Leads. The new scripts should incorporate, where appropriate, any Exploratory Questions not addressed during previous interviews, as well as any additional questions recorded during the lead-interview process check.

2.3.5 Interview Practitioners

Purpose

The purpose of Interview Practitioners is to meet with the practitioners of each project to obtaining corroboration of the key issues previously asserted and to identify new issues.

Summary Description

The session Facilitator introduces the team, explains the purpose of the session, and asks the practitioner the Exploratory Questions. A session recorder tracks the responses and, along with the rest of the Appraisal Team, takes notes. As a result of some responses, practitioners may be asked to supply documents for review. There is a separate session for each practitioner. This interview typically provides corroborating and clarifying data in relation to other sources.

Table 2–26 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator	Conducts interview.
Project Lead	Responds to interview questions.
Appraisal Team	Takes notes

Table 2–26. Participants for Interview Project Leads.

Typical Duration

- 45 minutes per interview + 15 minutes for Appraisal Team discussion/break per interview

Steps

Table 2–27 shows the steps for this process element.

Step	Guidance
Conduct Interview	The Facilitator asks the interview questions developed from the analysis of the Project Lead interview responses, while the members of the Appraisal Team take notes.
Follow Up Questions	Voting Members ask additional questions for issues still requiring clarification.
Process Check	The Appraisal Team conducts a quick process check to ensure that the interview is generating needed information and adjusts appropriately for next interview.

Table 2–27. Steps for Interview Project Leads.

Tailorable Parameters

- Number of scripted questions asked

- Number of follow-up questions asked
- Number of Appraisal Team members present during interview

Exit Criteria

- Practitioner answers scripted and follow-up Questions.

Notes

Before beginning the interview, the Facilitator should introduce themselves and the members of the Appraisal Team and briefly explain the purpose of the interview. The interviewee should be reminded that the issues discussed in the interview and interview notes are not shared with anyone outside of the Appraisal Team and that all information/comments/responses are covered by the Non Disclosure Agreement.

The Facilitator should follow the interview script as developed during step 2.3.4. Consolidate and Interpret Data from Project Leads. However, the Facilitator is encouraged to introduce follow-up or clarifying questions where appropriate; interviewee doesn't understand concept being addressed, a different interpretation of previously discussed evidence is given, response clearly contradicts that of other interviewees, etc.

Depending upon the number of questions developed for an individual Practitioner, and the need for follow-up questions by the Facilitator, it is possible that not all scripted questions will be asked, or that the Voting Members will have the opportunity to pose their individual questions. Unaddressed questions should be recorded during the process check for possible incorporation in later interviews.

2.3.6 Consolidate Data from Practitioners

Purpose

The purpose of Consolidate Data from Practitioners is to assimilate the Appraisal Team's notes from the practitioner interviews and form preliminary ratings for each process area.

Summary Description

Consolidate Data from Practitioners involves updating the DTS to reflect the information gathered in the interviews with the practitioners. It also allows Voting Members to verify their understanding of the information obtained in the interviews with fellow team members. Finally, this data consolidation step allows the Appraisal Team to determine any needed changes in the schedule or other aspect of the remaining data gathering process.

Major Participants

Table 2–28 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator	Provides guidance and model expertise for the team's deliberations.
Appraisal Team	Reviews notes, discuss any issues, formulate observations.
Voting Members	Update the DTS.

Table 2–28. Participants for Consolidate Data from Practitioners.

Typical Duration

- 2 hours

Steps

Table 2–29 shows the steps for this process element.

Step	Guidance
Review Notes	Each team member privately reviews his/her notes from the practitioner interviews.
Update DTS	The Appraisal Team discusses as a whole the response of each Practitioner on a question by question basis. The DTS is updated based on the decision of the Voting Members.
Preparation	The team discusses the upcoming events and any adjustments to the schedule that they may wish to make based on the previous steps. In particular, the Voting Members may wish to add a few Exploratory Questions or findings to the preliminary findings in order to resolve conflicting evidence, especially where the ratings are affected.

Table 2–29. Steps for Consolidate Data from Practitioners

Tailorable Parameters

- None

Exit Criteria

- DTS is updated
- Scheduling and data gathering changes are agreed to where necessary

Notes

See Appendix E for details on the format and suggested use of the DTS.

2.3.7 Analyze Data Tracking Sheet

Purpose

The Purpose of Analyze Data Tracking Sheet is to conduct a zero-based review of the current DTS.

Summary Description

The Appraisal Team analyzes the evidence, provided by the Appraised Organization in support of its processes

Major Participants

Table 2–30 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	Summary
Facilitator	Provides guidance and model expertise for the Appraisal Team's deliberations.
Appraisal Team	Reviews interview notes and, discusses issues, formulates observations.
Voting Members	Updates DTS.

Table 2–30. Participants for Analyze Data Tracking Sheet.

Typical Duration

- 1-3 hours

Steps

Table 2–31 shows the step for this process element.

Step	Guidance
Review Notes	Each team member privately reviews his/her notes from all activities.
Discuss Issues	Team members raise issues that they have encountered during the review step. The Facilitator moderates the discussion to ensure that all issues are aired.
Update DTS	At the end of the discussion, the DTS is updated based on Voting Member consensus.

Table 2–31. Steps for Analyze Data Tracking Sheet.

Tailorable Parameters

- None

Exit Criteria

- Updated DTS

Notes

None

2.3.8 Develop Preliminary Findings

Purpose

The purpose of Develop Preliminary Findings is to formulate a set of findings that reflect an initial synthesis of the accumulated data from all data sources used in the appraisal.

Summary Description

During Develop Preliminary Findings, the Voting Members systematically analyze the data from all sources to generate a list of preliminary findings related to the process areas and capability levels under investigation.

Major Participants

Table 2–32 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator	Leads team in brainstorm activities and oversees the preparation of the preliminary findings.
Voting Members	Synthesize the accumulated data into preliminary findings in the context of the appraisal.

Table 2–32. Participants for Develop Preliminary Findings

Typical Duration

- 4 or more hours

Steps

Table 2–33 shows the steps for this process element.

Step	**Guidance**
Develop Candidate Findings	Voting Members record their candidate preliminary findings according to process areas/common features.
Review Candidate Findings	Findings are collated and redundancies and trivial findings are eliminated, and common threads grouped. Findings are presented to all Voting Members for consensus on which to include in the final report.
Record Findings	Preliminary findings are recorded.
Develop Follow-Up Questions	The findings development process may indicate areas or issues that require further clarification through interviews of Project Leads and Practitioners. The Appraisal Team should develop any necessary Follow-Up questions based on the processes used during the evidence consolidation steps.

Table 2–33. Steps for Develop Preliminary Findings.

Tailorable Parameters

- Level of granularity of preliminary findings
- Number of preliminary findings

Exit Criteria

- 40-60 preliminary findings
- Follow-Up Questions and list of interviewees

Notes

2.3.9 Follow-Up Questions and Interviews

Purpose

The purpose of Follow-Up Questions and Interviews is to resolve issues as a result of preliminary findings which influence the development of ratings.

Summary Description

During Follow-Up Questions and Interviews, the Appraisal Team gathers clarifying information from Project Leads and/or Practitioners.

Major Participants

Table 2–34 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator	Conducts session and asks Follow-Up Questions.
Appraisal Team	Records responses.
Project Lead or Practitioners	Responds to questions.

Table 2–34. Participants for Follow-Up Questions and Answers

Typical Duration

- 1-2 hours (as necessary)

Steps

Table 2–35 shows the steps for this process element.

Step	Guidance
Conduct Interview	The Facilitator asks the interview questions developed from the analysis of the Project Lead interview responses, while the members of the Appraisal Team take notes.
Follow Up Questions	Voting Members ask additional follow up questions for issues still requiring clarification.
Process Check	The Appraisal Team conducts a quick process check to ensure that the interview is generating needed information and adjusts appropriately for next interview.

Table 2–35. Steps for Follow-Up Interviews and Questions

Tailorable Parameters

- Depth of follow-up on individual issues

- Not all appraisals will require this step

Exit Criteria

- All Follow-Up questions are answered

Notes

None

2.3.10 Develop Rating

Purpose

The purpose of Develop Rating is to assimilate in the DTS the notes taken during the review of preliminary findings and any additional information gathered during the follow-up interviews. The translation of the DTS results into a profile that shows the capability level achieved for each process area.

Summary Description

Develop Rating involves synthesizing the DTS into a rating profile. The team reviews notes and achieves consensus on the capability level for each process area.

Major Participants

Table 2–36 lists the primary participants involved in this process element and the summary or their activity during this process.

Role	**Summary**
Facilitator	Provides guidance and model expertise for the team's deliberations
Appraisal Team	Review their notes, discuss any issues, formulate observations.
Voting Members	Update the DTS and formulate ratings.

Table 2–36. Participants for Develop Rating.

Typical Duration

- 4 - 6 hours.

Steps

Table 2–37 shows the steps for this process element.

Step	**Guidance**
Review Notes	Each team member privately reviews his/her notes from the interview with the Project Leads and practitioners.
Update DTS	The Appraisal Team discusses as a whole the responses given in the Follow-Up interviews on a question by question basis. The Facilitator moderates the discussions to give each issue a chance to be aired. The DTS is updated based on the consensus decision of the Voting Members.
Ratings	Based on the DTS, the Voting Members form a rating for each process area based on consensus.

Table 2–37. Steps for Develop Rating.

Tailorable Parameters

- None

Exit Criteria

- Consensus is obtained on the rating profile

Notes

At this point in the appraisal process, team consensus on the ratings is necessary. The Facilitator leads the process of building consensus.

2.3.11 Develop Final Findings

Purpose

The purpose of Develop Final Findings is to focus on the process areas and rating profile to provide observations for the overall results of the appraisal activity. The Final Findings are refinements of the Preliminary Findings.

Summary Description

Develop Final Findings involves analyzing the Preliminary Findings and DTS in light of the contents of the capability levels, determining the estimated process capability for each process area investigated, and synthesizing the Preliminary Findings for presentation to the Sponsor.

Major Participants

Table 2–38 lists the primary participants involved in this process element and the summary of their activities during this process.

Role	Summary
Facilitator	Provides SSE-CMM expertise and guides the Voting Members in forming consensus.
Voting Members	Develop final findings.

Table 2–38. Participants for Develop Final Findings.

Typical Duration

- 1-3 hours.

Steps

Table 2–39 shows the steps for this process element.

Step	Guidance
Review Data	The Appraisal Team reviews the preliminary findings, DTS and new data recovered from the Follow-Up Questions step. This information allows the Voting Members to identify the primary areas of interest to the Appraisal.
Prioritize Findings	The Finding are prioritized based on Sponsor identified concerns, if available, and on the Voting Member's consensus of the strengths and weaknesses identified in the Appraised Organization.
Approve Findings	Each finding is presented to the Voting Members for final edit and approval. The Voting Members must *unanimously* agree with each finding.
Develop Presentation	Findings are captured for presentation to Sponsor

Table 2–39. Steps for Develop Final Findings.

Tailorable Parameters

- Level of granularity of findings
- Depth of analysis for determining capability level
- Identification of strengths and weaknesses

Exit Criteria

- Unanimous acceptance is obtained for each finding
- Findings briefing is completed

Notes

Findings may be presented in the context of process area categories, process areas, base practices, generic practices, common features, or capability levels, depending on the appraisal goals.

Findings can be reported at the PA or Capability level. At the PA level, the findings indicate the BP of GP failures that prevented the attainment of the next level within the PA. At the Capability level, findings indicate common trends that have prevented the "general" attainment of a specific level across PAs. To report a Capability level deficiency, the specific GP or set of GPs must be found as inadequate for more than 50% of the PAs.

2.3.12 Manage Appraisal Records

Purpose

The purpose of Manage Appraisal Records is to properly dispose of all records relating to the appraisal.

Summary Description

Managing Appraisal Records involves the proper disposal of all materials gathered and created during the appraisal. Most intermediate work products and inputs will be destroyed while any evidence gathered or work products developed during the On-Site Phase are sent to the Sponsor.

Major Participants

Table 2–40 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator Evidence Custodian	Ensures that all records are properly disposed of. Provides for the secure handling of any records that will remain in the possession of the team. Packages new evidence and sends to Sponsor.
Appraisal Team	Gathers all notes and other intermediate work products.
Site Coordinator	Destroys all notes and other intermediate work products.
Sponsor	Receives new evidence and work products.

Table 2–40. Participants for Manage Appraisal Records.

Typical Duration

- 1-2 hours

Tailorable Parameter

- None

Exit Criteria

- Records not needed are destroyed
- New evidence is forwarded to Sponsor

Notes

The exact means of record disposal should be established in the Appraisal Plan and should include which items the team will take away from the On-Site facility How new evidence (evidence collected during the On-Site Phase) is forwarded is at the discretion of the Sponsor and should also be established in the Appraisal Plan. If the Sponsor does not wish the Appraised

Organization to be made aware of the team's evaluation rating, the Site Coordinator should not be involved in destroying the team's notes and intermediate work products, and this function should be taken over by the Evidence Custodian. All parties should be reminded of the procedures before the On-Site activities begin.

2.3.13 Conduct Wrap-Up

Purpose

The purpose of Conduct Wrap-Up is to provide the results of the appraisal to the Appraised Organization.

Summary Description

Brief Results involves the Appraisal Team, Sponsors, and Appraised Organization having an open discussion of the appraisal results, process, and/or the next steps, as appropriate. No confidentiality rules are abrogated in this meeting. In the event that the Sponsor directs the team to provide the details of the appraisal to the site personnel, the rating and findings will be provided to the site without discussion.

Major Participants

Table 2–41 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator	Present appraisal results as directed by the Sponsor.
Appraisal Team	Attend briefing.
Site Personnel	Attend briefing.

Table 2–41. Participants for Conduct Wrap-Up.

Typical Duration

- 30 minutes to 1 hour

Tailorable Parameter

- This is an optional process element, which may be tailored out at the Sponsor's request, if appropriate.

Exit Criteria

- Brief results and depart site

Notes

This is a Sponsor driven optional step and any presentation given must reflect the Sponsor's tailoring requirements.

2.4 Reporting Phase

Purpose

The Reporting Phase is the concluding phase of the appraisal process in which the team performs its final analysis of all data gathered during the previous three phases and presents its findings to the Sponsor. Figure 2-5 shows the steps in the Reporting Phase.

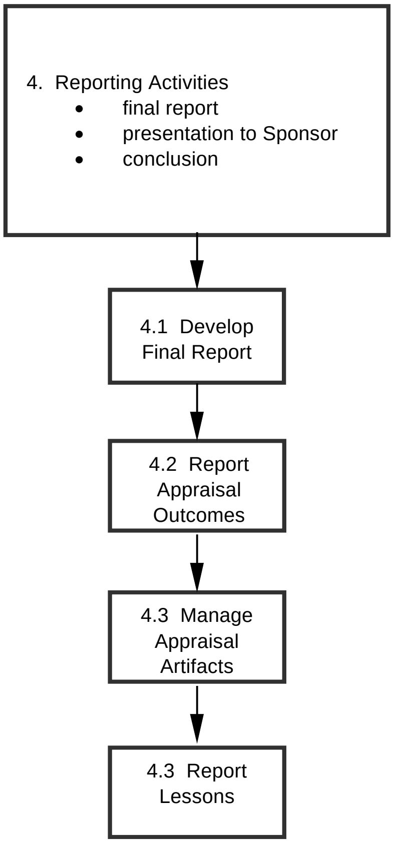


Figure 2-5. Post-Appraisal Phase

Summary Description

Table 2–42 lists the major activities of the post-appraisal phase and the expected output of each. Each element is described more fully in the summaries that follow.

ID	Activity	Description	Outputs
2.4.1	Develop Final Report	Finalize findings report and develop briefing for Sponsor.	Findings Report
2.4.2	Report Appraisal Outcomes	Present appraisal results to Sponsor.	Sponsor is briefed
2.4.3	Manage Appraisal Artifacts	Work products are disposed of.	All work products are properly disposed of
2.4.4	Report Lessons Learned	Team members discuss appraisal process.	Lessons are reported out

Table 2–42. Summary Description of Reporting Phase

2.4.1 Develop Final Report

Purpose

The purpose of Develop Final Report is to ensure that the final appraisal report accurately reflects the information obtained during the appraisal process.

Summary Description

Develop Final Report involves synthesizing the findings developed during the On-Site phase and knowledge of the Appraised Organization, into the final report.

Major Participants

Table 2–43 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator	Reviews findings report.
Appraisal Team	Synthesizes knowledge of organization and appraisal findings into final report

Table 2–43. Participants for Develop Final Report.

Typical Duration

- 1-2 hours

Steps

Table 2–44 lists the primary participants involved in this process element and a summary of their activities during this process.

Step	Guidance
Review Data	The Appraisal Team reviews the findings, DTS and any new data recovered from the Follow-Up Questions and Interviews section.
Write Report	The initial findings report is refined to include Sponsor specific concerns and any additional information brought out in the review process.
Develop Briefing	The final briefing for the Sponsor is developed.

Table 2–44. Steps for Develop Final Report.

Tailorable Parameters

- Level of detail and number of findings reported

Exit Criteria

- Final report is written
- Briefing for Sponsor is developed

Notes

Because at this point, the Sponsor has all of the relevant material gathered or produced during the appraisal, the final report must be written at the Sponsor site. The final report may be presented in several different formats. Often it is given in the form of an oral presentation for which slides are developed, but it may only consist of a written document without an oral presentation or discussion. The report format, length, and audience should be outlined in the appraiser - Sponsor contract and should be developed as soon as possible after the completion of the On-Site phase activities. This step is different than 2.3.11 because here the team writes to the specifics of the Sponsor requirements. The report also addresses any decisions made by the Sponsor and or Appraisal Team during the Planning and Preparation Phases that may have had an impact on the appraisal outcomes. The team may also include recommendations to the Sponsor such as how to manage contracts awarded to the Appraised Organization.

2.4.2 Report Appraisal Outcomes to Sponsor

Purpose

The purpose of Report Appraisal Outcomes to Sponsor is to present the results of the appraisal to the Sponsor.

Summary Description

Report Appraisal Outcomes to Sponsor involves the presentation and explanation of the appraisal results by the Appraisal Team, to the Sponsor.

Major Participants

Table 2–45 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	**Summary**
Facilitator	Present and discuss results as directed by the Sponsor. Suggest follow-on assignments.
Sponsor	Attend briefing. Ask questions of Appraisal Team. Make follow-on assignments.
Appraisal Team	Attend briefing. Answer Sponsor questions as appropriate.

Table 2–45. Participants for Report Appraisal Outcomes to Sponsor.

Typical Duration

- 0.5 - 1 hour

Tailorable Parameters

- Type of briefing (i.e. Written report, open session, Facilitator only discussion)
- Amount of discussion with Sponsor
- Additional follow-up tasks

Steps

Table 2–46 shows the steps for the Sponsor brief of the appraisal results.

Step	Guidance
Brief Results	Facilitator presents the results as directed by Sponsor.
Question & Answer	The Sponsor may wish to ask questions for clarification of particular findings or judgments, which may be asked of the Facilitator or Appraisal Team as a whole.

Table 2–46. Steps for Report Appraisal Outcomes to Sponsor.

Exit Criteria

- Results briefed
- Follow-on activities assigned

Notes

The format for the final briefing should be laid out in the original contract between the Appraisal and Sponsor Organizations. At no time should questions from the Sponsor or responses given by the Facilitator and Appraisal Team violate any confidentiality agreements signed with the Appraised Organization. If an in-person briefing is not required by the Sponsor, the Facilitator should send a letter to the Sponsor with the written appraisal document highlighting the results of the appraisal, a list of Appraisal Team members, any contractual obligations that could not be met in the given time frame/resources, and an offer to explain the report at a later time if requested. Even if the Sponsor has no specific questions, this is a good time to gauge the Sponsor's reaction and receive the Sponsor's acknowledgment that the appraisal is complete. The style of the report is determined by the Sponsor and may only include a written report without an oral presentation or discussion with Appraisal Team. If briefing the results in an oral presentation copies of the presentation should be made available for all attendees. Often the Sponsor has questions of clarification that they prefer to ask the Facilitator or team members individually, outside of the group setting.

2.4.3 Manage Appraisal Artifacts

Purpose

The purpose of Manage Appraisal Artifacts is to properly dispose of all final work products and records material still in the possession of the Appraisal Team after the On-Site Phase.

Summary Description

Managing Appraisal Artifacts involves the proper destruction or storage of the appraisal work products; DTS, Ratings, Findings and any other documentation (other than appraisal related contracts) that may still be in the possession of the Appraisal Team.

Major Participants

Table 2–47 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	**Summary**
Facilitator	Ensures that all material is properly disposed of. Provides for the secure handling of any records that will remain in the possession of the team.
Appraisal Team	Secures all records being kept by the Appraisal Organization
Sponsor	Secures all records being kept by the Sponsor organization

Table 2–47. Participants for Manage Appraisal Artifacts.

Typical Duration

- 1-2 hours

Tailorable Parameter

- Records to be kept by team
- How records are secured

Exit Criteria

- Records not needed are destroyed
- Records remaining with the appraisal and Sponsor organizations are secured

Notes

The exact means of work product disposal/storage should be established in the Appraisal Plan and should include what documents the Appraisal Organization will keep for its own records. The Appraisal Organization may wish to keep some work products and other documents - i.e., Facilitator notes and team notebooks, for later reference. The Sponsor is responsible for keeping copies of all work products, contracts, and evidence generated during the appraisal process.

2.4.4 Report Lessons Learned

Purpose

The purpose of Report Lessons Learned is to facilitate the passing-on of knowledge regarding the appraisal method to future Appraisal Teams. It provides an opportunity for the Appraisal Team to provide feedback to and receive feedback on the process itself from the Sponsor.

Summary Description

Report Lessons Learned involves synthesizing information about what did and did not work during the appraisal and suggestions for improvement. It may also incorporate any feedback from the Sponsor on the appraisal process received during Brief Results (Sponsor).

Major Participants

Table 2–48 lists the primary participants involved in this process element and a summary of their activities during this process.

Role	Summary
Facilitator	Leads discussion and records issues
Appraisal Team	Individually raise issues (positive and negative) encountered during the appraisal

Table 2–48. Participants for Report Lessons Learned.

Typical Duration

- 1-2 hours

Steps

Table 2–49 shows the steps for Reporting Lessons Learned.

Step	Guidance
Discussion	Led by the Facilitator, individual team members discuss their appraisal experience. Team members should be encouraged to make suggestions for improvements in the future and or formalize processes that were particularly helpful. Team members should reference their project notebooks for specific references. The discussion should take place soon after the final brief is delivered to the Sponsor.
Report	The most significant issues raised should be recorded in a formal manner, without attribution to individual members. Report types include, but are not limited to, lists of dos and don’ts for subsequent Appraisal Teams, suggestions for changes in the method, or open-ended questions for Sponsors.

Table 2–49. Steps for Report Lessons Learned

Tailorable Parameters

- Report type
- Report audience
- Notification to Sponsor

Exit Criteria

- Lessons recorded/delivered

Notes

This is an Appraiser Organization optional step, although the Sponsor may request that it be conducted as part of a formal follow-up requirement. (If the Sponsor directs the Appraisal Team to conduct such a review, the results should be forwarded to the Sponsor as soon as possible.) It is requested that the results of this step be forwarded to the SSAM maintenance group, using for possible incorporation in future updates to the method. Appendix I is a template for forwarding comments to the SSAM Maintenance Group.

Chapter 3 Sponsor Organization Guidance

3.1 Introduction

In the case of appraisals performed for the purpose of source selection, the Sponsor is the acquisition authority or other individual responsible for obtaining secure products, systems or services. The challenge is to ensure an acceptable level of objectivity and consistency in what is often an essential subjective effort. For SSE-CMM appraisal and other related services, it is recommended that individuals and organizations that have been active participants in the SSE-CMM Project be contacted. A well-planned and executed SSE-CMM appraisal, with clearly expressed requirements and performed by an experienced and expert Appraisal Team, can provide a solid basis for source selection. There are a number of considerations confronting the Sponsor of a SSE-CMM appraisal that bear on the success of the effort. The Appraisal Team must be able to assume that the Sponsor prior to the start of the appraisal has addressed these issues. This chapter is designed to help potential Sponsors consider and deal with those critical issues, including establishing parameters and a rationale for the appraisal, specifying requirements, and supporting the execution of the appraisal. Typically, the Sponsor will delegate many of the activities and responsibilities described in this chapter to the Facilitator. If the Sponsor wishes, the Appraisal Team may also assist in working through the issues.

3.2 Establishing Appraisal Goals

An SSE-CMM appraisal is an effective tool for source selection, providing a sound basis for comparison of bidder capability, as well as knowledge that can be invaluable for managing program risk after contract award. However, an appraisal demands a substantial commitment of resources and entails a certain unavoidable level of intrusion into the Appraised Organization. Establishing sound rationale for the appraisal can help the Sponsor to obtain the necessary corporate buy-in and resource commitments. The rationale, stated as appraisal goals, can also form the basis for an efficient and cost-effective appraisal effort by supporting proper scoping and planning, since the choice of SSE-CMM Process Areas and Capability Levels, the appraisal deadlines, the method for reporting results, and the projects to be included in the appraisal are all influenced by the goals established by the Sponsor. For example, if the primary goal of an appraisal is to demonstrate the organization's ability to provide assurance, the appraisal may place a heavier emphasis on the quality and completeness of evidence than an appraisal performed for the purpose of overall process improvement.

The primary goal of appraisal for source selection is usually to determine the overall capability of the organization for the purpose of qualifying or differentiating bidders. A secondary goal is often the identification of the engineering organization's strengths and weaknesses in order to anticipate and manage program risk. The goals should be explicitly stated in the request for proposal (RFP).

Capability maturity against the SSE-CMM can be demonstrated in several different ways, with very different resource demands, depending upon the requirements of the RFP:

- The Sponsor may be willing to accept the organization's assertion of security engineering capability. In this case, RFP requirements may be general, requiring that the bidder simply comment in their proposal on their ability to meet a particular SSE-CMM profile without an explicit demand for formal appraisal. The bidder may feel confident enough to respond without any appraisal effort at all (perhaps based on previous appraisal results).

- The Sponsor may wish to conduct an appraisal that is abbreviated or limited in scope to obtain insight into capability maturity. The RFP may, for example, require bidders to merely respond to an SSE-CMM questionnaire. (Obviously, the accuracy and value of such an "appraisal" is likely to be limited.)

The RFP may require the bidder to perform a self-appraisal against a given SSE-CMM profile and provide the results as part of their proposal.

- The RFP may require that the bidder undergo a third-party appraisal by a team designated by the acquisition organization. In this case, at least some of the cost of the appraisal is borne by the acquisition organization, since it provides the Appraisal Team. The team is likely to be experienced and knowledgeable, and therefore efficient, minimizing the requirement for the bidders' resources. Since an appraisal is resource intensive as well as complex, an experienced third party team can save both the Sponsor and the Appraised Organization valuable time and dollars.

- The RFP may also include a request for the Appraised Organization to provide in its contract proposal any evidence that would be required by Appraisal Organization when conducting an appraisal. Providing the Appraisal Team with as much information as possible prior to the On-Site Phase increases the efficiency of the appraisal process and the accuracy of its results.

The Sponsor should consider the relevance of the SSE-CMM to the organization and to the particular projects to be appraised in setting goals for the appraisal:

- Does the organization practice security engineering in the course of integrating systems, developing applications or products, or providing services?

- Is the organization seeking to establish its competency for source selection purposes?

- Is the organization hoping to gain insights that will help mitigate program risk?

- What kinds of projects demonstrate the security engineering process areas that are to be included in the appraisal?

The Sponsor should recognize that an SSE-CMM appraisal will *not* prescribe good processes or teach organizations how to improve their capability to perform specific processes. Nor is it a substitute for product evaluation or system certification. On the other hand, an SSE-CMM appraisal *can* provide important insights and guidance that will lead to process improvements over time, and it *can* contribute to assurance arguments for products and systems. The Sponsor needs to weigh the value of the potential benefits of an appraisal against its cost before proceeding.

3.3 Choosing an Appraiser Organization

Choosing an Appraisal Team is critical to both the quality and efficiency of the appraisal. An inexperienced or inexpert Appraisal Team can undermine the objectivity of the effort and waste precious time and resources in the process. Chapter 3 provides guidelines for a qualified SSECMM Appraisal Team. Using an experienced Appraisal Team should ensure that the following key skills and characteristics are present:

- previous experience with organizational appraisals or process improvement activities, particularly for source selection
- credibility with both management and participants
- experience in action planning and subsequent improvement efforts
- good communication skills
- positive and encouraging attitude

3.4 Tailorable Parameters

There are several components of the appraisal that may be tailored during the planning phase to suit the Sponsor.

3.4.1 Process Areas [PAs]

While all PAs are considered applicable to all security engineering efforts, the Sponsor may choose to focus on specific PAs and exclude others from the appraisal. In addition, while the PAs are generic, the Sponsor may tailor some aspects of PAs to satisfy particular needs. For instance, the Sponsor may wish to offer as evidence work products that are not among those listed as examples in a given PA. Terminology that would otherwise be unfamiliar may also be adapted to the appraised organization.

3.4.2 Target Capability Level

The Sponsor may identify goal or target capability levels for the PAs included in the appraisal. In appraisals performed for source selection, minimum capability levels may be specified in the RFP. The target may be a single level across all PAs or a specific level for each PA.

The SSAM defines the requirement for achieving level 1 as, 100% performance of the base practices. All other capability levels are considered achieved if 100% of the previous level and at least 80% of the current level is achieved.

The Sponsor may have a set Capability Level that is required of the Appraised Organization. The SSE-CMM Appraisal Method defines criteria for attaining Capability Levels, but the Sponsor may wish to redefine the criteria based on the importance they place on meeting a specific level.

3.4.3 Questionnaire

The questionnaire may be tailored to reflect the decision to eliminate specific PAs from consideration.

3.4.4 Projects

The Sponsor may specify particular projects or types of projects for the appraisal. For example, it may be desirable to include projects that are very similar in technology, size, and scope to that for which the source selection is to be made. Other factors, such as geographic proximity (to minimize Appraisal Team travel) or project "life cycle phase," may be considerations in project selection. The choice of projects is often influenced by the appraisal goals. Table 3-1 offers some considerations for project selection:

Goal of the Appraisal	**Project Type**
Understand domain-related issues.	Select projects within desired domain. Note that the domain can be focused on industry, technology base, customer type, project complexity, etc.
Understand deployment of new organizational practices.	Select new projects that have started since deployment of new practices.
Determine overall capability of the organization, e.g., for source selection.	Select projects that are expected to be representative of the organizational capability.
Determine progress of process improvement activities.	Select projects that have been pilots for process improvements.

Table 3–1. Project Selection

Selected projects should be led by individuals or teams with responsibility for resource planning, allocation, and monitoring, as well as responsibility for the quality, quantity, and security of products delivered by the project. Projects performed by integrated product development teams also lend themselves to SSE-CMM appraisal.

Although the SSAM does not require that appraised projects be located near each other geographically, the logistics considerations associated with a multi-site appraisal should be carefully considered. Due to the intensity of the appraisal schedule, it may be impractical to accommodate travel required to conduct interviews and examine evidence at multiple sites.

3.4.5 Interviewees

The Sponsor may specify functional role, seniority, level of responsibility or involvement, or other such qualifications for interviewees. "Project Leads," though they may be known by different titles, should be single points of information for a broad base of topics related to the systems security engineering functions of projects. If it is infeasible to find individual "project leads" with the broad information on specific projects needed for the appraisal, the Sponsor may allow interviewees to be selected from a larger group of questionnaire takers, based on the breadth of knowledge exhibited by their questionnaire responses.

3.4.6 Reporting Method

The Sponsor may specify how and to whom appraisal results are to be reported within the appraised organization. Alternatives range from no report, to a high level presentation to Imembers of the organization by the Appraisal Team at the conclusion of the on-site phase, to a detailed written report provided after the appraisal.

3.4.7 Evidence

The RFP should include any evidence requirements (ideally in the form of an evidence matrix) and an appropriately tailored SSE-CMM questionnaire for use in the appraisal. The Appraised Organization can use this information to help select projects and personnel to participate in the appraisal and to begin putting together an evidence library for use by the Appraisal Team. The RFP should indicate any permissible alternative forms of evidence, and should clearly identify acceptable evidence "types" if the appraised organization is permitted to select specific examples. The RFP should also address the issue of evidence disposition, indicating, for example, whether evidence is to be returned to the appraised organization for retention at the end of the on-site phase or retained by the Appraisal Team. If the evidence or other working papers are to be destroyed, the RFP should state when and by whom.

3.4.8 Relationship with Site Coordinator

The Site Coordinator is the appraised organization’s representative and Appraisal Team interface throughout the appraisal process. The Sponsor should require that the site coordinator have the authority necessary to help ensure the appraisal goes smoothly. The Site Coordinator will probably be responsible for satisfying the appraisal logistics requirements specified in the RFP. These might include space for the Appraisal Team; access to facilities, people, and evidence; supplies; and arrangements for food and lodging during the appraisal.

Chapter 4 Appraiser Organization Guidelines

4.1 Introduction

This chapter provides guidelines to an organization that is performing a third party appraisal. As stated earlier, there are numerous differences between the self-assessment and the third party assessment. The organization providing the third party appraisal must be very cognizant of the Sponsor's legal and organizational issues in order that they do not compromise the appraisal process.

4.2 Planning Phase Guidance

4.2.1 Defining the Appraisal Scope

The Sponsor is ultimately responsible for defining the scope of the third party appraisal. However, the Appraisal Organization (especially the Facilitator) should be available to assist the Sponsor in this effort. Depending on the Sponsor's experience performing appraisals, it is strongly urged that experienced appraisers be involved in the appraisal scope definition – those appraisers from the Appraisal Organization, if the Sponsor does not have the in-house experience.

4.2.2 Planning the Appraisal Specifics

It is also the Sponsor's responsibility to plan the specifics of the appraisal with the organization that will be appraised. This includes the selection of a date and time, location, people to be interviewed, resources necessary during the appraisals, and projects to be assessed. However, the Appraisal Organization should be involved in this planning stage to be better prepared for the appraisal. Also, using their appraisal experience, the Appraisal Organization can better refine the list of interviewees and projects to be assessed.

4.2.3 Selecting Appraisal Team Members

The SSE-CMM Appraisal Team should include no more than one member who has not previously participated on a prior CMM appraisal. The SSE-CMM Project developed guidelines for choosing an Appraisal Team. Each member of the Appraisal Team should fully meet at leas one of the following criteria and collectively the Appraisal Team should meet all of the criteria:

- Active membership in an SSE-CMM Project Working Group
- 10 years security engineering experience
- 2 years process improvement experience
- training or experience in some form of CMM appraisal, preferably SSE-CMM.

SSE-CMM Appraisal Team Facilitators should meet most of the above criteria, and ideally should have facilitated a precious SSE-CMM appraisal. The Facilitators and other Appraisal

Team members work as a single team during the entire On-Site phase. The Appraisal Team will analyze data, perform all of the interviews, and develop the findings. They are also responsible for developing the recommendations to the findings that are published in the appraisal report. To assure success in the appraisal effort, the Appraisal Team members should

- Be credible with both Sponsor and participants.
- Be involved in action planning.
- Have good communication skills.
- Have a positive and encouraging attitude.

The Appraisal Organization has been selected for their organizational appraisal experience, therefore those with CMM appraisal (and especially SSE-CMM appraisal experience) will be involved in these activities. It is especially important that an experienced individual be SSAM Facilitator. Note that there may also be observers present on Appraisal Teams, for example a member of the Sponsor organization or a trainee from the Appraisal Organization.

The typical composition of an Appraisal Team is 3 voting members and 1 observer in addition to the 2 Facilitators. Section 1.2 reviews typical labor requirements.

4.3 Preparation Phase Guidance

4.3.1 Selecting Appropriate Questionnaire Recipients

The questionnaire is, at a minimum, distributed to the Project Leads. However, depending upon the responsibilities and visibility of the leads within the organization, the questionnaires for some process areas may also be distributed to others more familiar with that particular process area. When choosing to distribute the questionnaire to additional respondents, it is recommended that these individuals possess the skill mix expressed in Table 4–1.

Process Area	Recommended Skills
PA 01:Administer Security Controls	Systems Security Administrator
PA 02: Assess Impact	Any senior practitioner
PA 03: Assess Security Risk	Any senior practitioner
PA 04: Assess Threat	Any senior practitioner
PA 05: Assess Vulnerability	Any senior practitioner
PA 06: Build Assurance Argument	Project manager
PA 07: Coordinate Security	Project manager
PA 08: Monitor System Security Posture	System Operators, Configuration Managers, System Administrators, System Security Administrator
PA 09: Provide Security Input	Any senior practitioner with requirements and design experience
PA 10: Specify Security Needs	Any senior practitioner with requirements and design experience
PA 11: Verify and Validate Security	System verification manager or senior test engineers
PA 12: Ensure Quality	Senior project-level quality manager or lead (in environments with shared quality leadership responsibility, Project Lead for the project) Organizational quality manager, total quality management coordinator
PA 13: Manage Configurations	Senior project-level CM manager for the projects selected for appraisal
PA 14: Manage Project Risk	Project manager
PA 15: Monitor and Control Technical Effort	Project manager
PA 16: Plan Technical Effort	Project manager
PA 17: Define Organization's Security Engineering Process	Individuals responsible for defining organization-level processes; may be part of the quality leadership area, policies/procedures area, or other support group
PA 18: Improve Organization's Security Engineering Processes	Individuals responsible for deploying organization-level process improvement activities; may be part of the quality leadership area, policies/procedures area, or other support group
PA 19: Manage Security Product Line Evolution	Individuals at organization level responsible for strategic product line positioning and advancement; may be in R&D, technical marketing, or other support structure
PA 20: Manage Security Engineering Support Environment	Individuals at organization level involved in deploying new development technologies
PA 21: Provide Ongoing Skills and Knowledge	Individuals responsible for organization-level training planning, development, and deployment; may be part of an R&D group, training department, or other support structure
PA 22: Coordinate with Suppliers	Project manager

Table 4–1. Questionnaire Distribution

4.3.2 Analyze Questionnaire

In order to facilitate the analysis of the Questionnaire answers, the Project Leads' responses should be consolidated and transferred to an electronic tracking mechanism. The use of a data tracking tool assists the Appraisal Team during the analysis process to recognize patterns and inconsistencies in responses both within projects and across the Appraised Organization as a whole.

Appendix E presents the questionnaire/interview consolidation tool developed by the SSE-CMM Project, the Data Tracking Sheet (DTS). The answers to the Questionnaire, consolidated in the DTS, present an overall picture of an Appraised Organization’s system security engineering practices and give an early indication of the direction of the appraisal. The Appraisal Team analyzes the DTS and supporting evidence to develop interview questions designed to elicit additional information about and insight into the Appraised Organization. Analyzing the data involves looking for discrepancies, inconsistencies, and inadequacy in responses and sited evidence, and areas of questionable performance internal to and across projects.

4.3.3 Exploratory questions

Exploratory questions are developed to discover the reason for any issues identified in the questionnaire responses. This is the first step in eliciting supporting or conflicting information on the performance of base or generic practices. Exploratory questions:

- Should be limited to approximately 40 per Project Lead, and should be prioritized due to interview time limitations.
- Should be linked to the individual process areas or generic practices in order to maintain traceability to the model, and facilitate the data management that needs to occur throughout the On-Site phase.
- Are typically a mix of some specific questions that are designed to address inconsistencies on a specific project, or general questions aimed at possible consistent misinterpretations of the questionnaire.

If the exploratory question generation process is not well managed, it can easily exceed the typical four hour duration. A method for quickly generating a pool of questions follows:

- Facilitator demonstrates, using questionnaire data for one PA, how to generate exploratory questions.
- To provide balance in the workload, PAs can be divided among the Appraisal Team members.
- For each PA, team members review the questionnaire responses for inconsistencies between and within projects, and request evidence to support any areas of interest.
- Where discrepancies are determined, team members generate exploratory questions referencing the Project Lead(s) or Practitioner(s) for whom question is intended and the particular PA in question.

In developing exploratory questions, the Appraisal Team identifies any potential issue areas in the questionnaires that need to be further investigated. The team needs to look for:

- *Inconsistencies:* apparent contradictory responses from the same project to two or more questions
- *Anomalies:* contradictory responses to the same question by two or more projects
- *Unsupported answers*: “yes” responses to questions with no cited evidence

The interview questions that are developed should be open-ended and non-accusatory, although they may “push” the interviewee. Often, the team may be searching for or anticipating particular answers i.e. references to internal memoranda or other documents etc. These pre-identified answers are known as “listen-fors”.

After the candidate questions are developed they are discussed by the Team as a whole. From the pool of questions, the Team then decides which questions to ask individual Project Leads.

4.3.4 Types of Evidence

The team must gather evidence across projects being appraised as well as up and down the organization’s hierarchy. The following are categories of information that need to be analyzed:

- Organizational Policies (for example directives and standards)
- Organizational Procedures (for example resource allocation, training)
- Project Plans (for example, configuration management, engineering, project and test plans)
- Project Procedures (for example reviews, document development, analysis)
- Process Implementation (for example project folders)
- Audit Trail (for example meeting minutes, action items, reports)

4.3.5 Collecting Evidence

The Appraisal Team needs to be able to justify any decisions that are made with regard to findings or ratings for the Appraised Organization. The team must determine whether the evidence provided is appropriate and sufficient to make a judgment about the organization. The team is required to analyze a number of sources of evidence (e.g., interview, document) before a decision can be made. The section on Developing Findings in this chapter lists the requirements for sources of supporting evidence before a finding can be considered validated.

As the Appraisal Team consolidates the Questionnaire answers, a list of supporting evidence requiring review will develop. It is the job of the Evidence Custodian with the assistance of the Site Coordinator to collect the evidence. However, the Evidence Custodian alone is responsible for documenting the receipt, use, and disposal of the evidence once it is received from the Site Coordinator. Appendix F provides templates of the Evidence Tracking Tools to assist the Evidence Custodian accomplish these tasks.

The ETTs are the companion tools to the DTS. Their purpose is to aid the Evidence Custodian in the request, collection, tracking, use, and disposal of all evidence collected and work product developed during the Appraisal. It consists of four spreadsheets: an evidence request form, and evidence request, usage and disposal tracking sheets.

4.3.6 Analyzing Evidence

Evidence is required to support the Appraised Organization’s claims of process compliance and institutionalization. The evidence is used to create, confirm and/or re-enforce appraisal findings. An evidence review strategy is generally prepared in the planning stages of an appraisal. Considerations for the artifact review strategy include appraisal goals, scope, and constraints; reference model and organizational scope; results of instrument analysis (questionnaire); “expected” maturity of the organization; team size; and time on-site.

The evidence strategy is based on verifying the existence of evidence and should consider the review as a means of verifying:

- Coverage, that is across the lifecycle and between organizational levels;
- Corroboration, that is validating the observations through the quantity and source of data (rules for corroboration are provided in the section on developing findings); and
- Completeness, that is including indicators of distribution lists, date, responsibility, purpose, decisions and other components as required.

Note that the team is not only analyzing the evidence to determine whether specific elements of a process or procedure are being followed, but also to evaluate the ability of the process or procedure work products to meet the Sponsor's requirements.

The existence of supporting evidence is generally determined through Questionnaire and Interview responses. The lack of evidence confirmation to positive responses, or conflicting evidence citation in the questionnaire points to potential issues areas for further query during the interview phases. Interviews are used to explain/confirm evidence as well as to gain an overall understanding of the organization's processes. Processes are implemented by activities that are performed by people. Artifacts, usually documents, are items associated with those enacting these activities. For this reason, interviewees should be selected based on process "function" served and the scope of the appraisal.

Evidence must be "weighted" by the Appraisal Team in that the source of the information is taken into consideration when the evidence is considered. For example, evidence from questionnaires or interviews may be considered less "valid" in that they are more prone to misuse or misunderstanding. Thus, the team might look for a certain amount of corroborating evidence from other sources, such as documents. Conflicting evidence might indicate weaknesses and or findings to be reported out with the appraisal results.

4.3.7 Handling Evidence

The handling of evidence in a third party appraisal is very important. All evidence must be kept secure, but remain accessible to the Appraisal Team and interviewees as necessary. Because evidence collection often involves proprietary information, it is crucial that all aspects of evidence collection be discussed, agreed to, and documented in the Appraisal Plan.

4.4 On-Site Phase Guidance

4.4.1 Conducting Meetings

The meetings that are conducted during the On-Site phase of the appraisal should be conducted within the bounds defined by the Sponsor. The Appraisal Team should not inform the interviewees or any other representatives of the Appraised Organization any information that has not been approved by the Sponsor.

4.4.2 Managing Appraisal Records

Since appraisal records produced by the Appraisal Team and the evidence provided to the Appraisal Team may very well be considered proprietary to the organization being appraised and acquisition confidential to the Sponsor, it is important that the Appraisal Team handle any material correctly. When the evidence is on site, it should be left under lock and key when the Appraisal Team is not in the same room with it. Any evidence received should be cataloged and packaged to be sent to the Sponsor prior to the team leaving the site. Any data produced by the Appraisal Team should be shredded or packaged and treated as evidence.

4.4.3 Conducting Wrap-Up

The Wrap Up meeting is a meeting that is very beneficial in the self-assessment process. It is meant to feed back to those interviewed the findings of the appraisal. For a third party appraisal, it might not be possible for a variety of reasons (e.g., procurement process issues) to provide feedback to the Appraised Organization directly from the Appraisal Team. This is an issue that should be carefully considered by the Sponsor, and the Appraisal Organization should follow the Sponsor's guidance to the letter.

4.4.4 Developing the Rating Profile

One of the results of the On-Site phase is a rating profile covering the appraised process areas. The rating profile correlates closely with the appraisal findings, and the two are developed in a closely coupled process.

The rating profile can be viewed at specific points in the appraisal process, as detailed in the process element summaries in Chapter 2. The DTS is a support tool introduced in Appendix E to help organize the data obtained by the Appraisal Team. The tool supports the Appraisal Team by providing a preliminary view of the ratings for each PA, allowing the Team to identify areas where the Appraised Organization is very close to meeting a capability level. Ratings are based on the degree to which the appraised entity performs all of the practices at a given level, in the judgment of the Appraisal Team.

The final rating profile is developed prior to developing the final findings. They serve as a starting point for developing the final findings. There is generally a close correlation between the final findings and the process areas with a low rating profile.

4.4.5 Rating presentation formats

Results of SSE-CMM appraisals can be presented in a variety of formats. The following formats are some examples for presenting the rating profile:

- Pie chart: shows the number of PAs at specific levels (works well for organizations primarily in the level 2-3 maturity range).
- Figure 4–1 illustrates the Bar chart: the score for each PA is shown on a bar graph which allows the option to use quartiles for PAs below level 1 (good option for the organization in the 0-2 maturity range).
- Figure 4–2 illustrates the Tabular format.

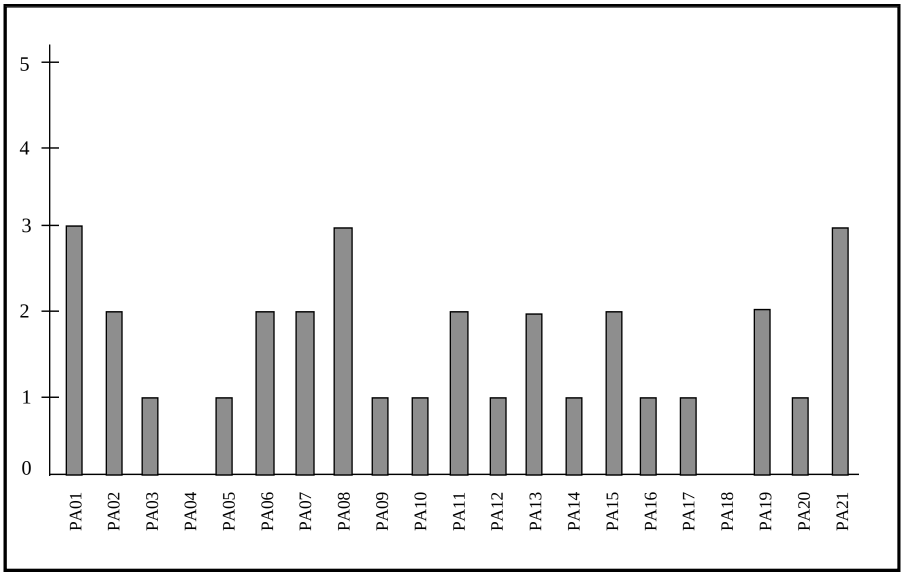


Figure 4–1. Example PA Bar Chart

PA Title	Rating
Administer Security Controls	1
Assess Impact	3
Assess Security Risk	3
Assess Threat	3
Assess Vulnerability	3
Build Assurance Argument	1
Coordinate Security	3
Monitor System Security Posture	2
Provide Security Input	1
Specify Security Needs	3
Verify and Validate Security	2
Ensure Quality	1
Manage Configurations	1
Manage Project Risk	0
Monitor & Control Technical Effort	1
Plan Technical Effort	1
Define Organization’s Security Engineering Process	0
Improve Organization’s Security Engineering Processes	0
Manage Security Product Line Evolution	1
Manage Security Engineering Support Environment	1
Provide Ongoing Skills and Knowledge	0
Coordinate with Suppliers	3

Figure 4–2. Example PA Table

4.4.6 Developing Findings

The appraisal findings are a key product of the appraisal. They are the result of synthesizing all of the data collected throughout the On-Site phase, along with the questionnaire responses.

Findings are usually limited to approximately seven, highlighting the most important findings of the appraisal. Findings include both strengths and weaknesses.

The preliminary findings are a synthesis of the primary issues that Appraisal Team members have collected from the Project Leads, and the practitioner groups. Confirmed preliminary findings are clustered using a technique such as affinity diagram, and a set of 5 to 10 themes or underlying factors are derived which forms the draft findings. Draft findings can be presented via briefing charts in the format of finding, cause, and consequence.

The findings typically fall into one of three categories:

- General barriers to the next level.
- Weaknesses in the base practices.
- Weaknesses in the generic practices.

In developing the findings, the Appraisal Team must make judgements to determine:

- that each observation is:
- accurate and
- sufficiently corroborated; and
- that the set of observations is:
- consistent and
- fully covers the areas required for the appraisal.

The SSAM has identified the following rules for corroboration, that is validation of the observations through the quantity and source of data:

- must come from multiple sources (not including the questionnaire); or
- must come from multiple sessions, where one must be a direct process user.

In addition, a minimum of 50% of the observations for each Process Area must have documentation as a source.

The main findings should be carefully worded to reflect what the team has actually heard from the participants. The finding is usually a single observation; it may be thought of as a characterization of a symptom. Use of organizational objectives or appraisal goals as defined by the Sponsor and the risks to meeting those goals is recommended as part of determining the findings. Characteristics of good findings include:

- concise, yet specific,
- non-attributing, yet actionable,
- in Appraised Organization terms, yet traceable to the SSE-CMM.

Final findings are an edited version of the draft findings based upon comments from the practitioners and Project Leads. These are used to develop the appraisal report and recommendations.

4.5 Reporting Phase Guidance

4.5.1 Reporting on the Appraisal

There are many methods that the Appraisal Team may report on the appraisal to the Sponsor. These include a formal report, a briefing to the Sponsor, or both. During the Appraisal Planning Phase, the reporting method will be defined by the Sponsor. It is important that the confidentiality of any appraisal data and findings be observed by the Appraisal Team and their organization. Additionally, the Sponsor's reporting requirements should be followed so that the Appraisal Organization does not prejudice the appraisal.

The content of the report should be in concert with the planned use of appraisal results as documented in the Appraisal Plan. Recommended contents for the report include:

- All findings where each one should be described by text and cite supporting evidence.
- Appraisal information including: the Appraisal Plan; all presentations, and all annotated worksheets and checklists.

4.5.2 Managing Artifacts

During the Post-Appraisal Phase, the artifacts of the appraisal include any evidence provided by the Appraised Organization and any data produced by the proposal team. This information should be cataloged and used to produce the findings. When that process is completed, the data should be stored at a Sponsor selected site until the data is no longer legally required (e.g., subsequent to the protest phase of an acquisition).

4.5.3 Utilizing Lessons Learned

A lessons learned activity can be useful to the Appraisal Organization to provide information to improve their appraisal activities. In every activity, some things are done exceptionally and others could have been done better. Process improvement can be applied to the process of appraising too. However, it is important to maintain the confidentiality of the appraisal specifics as agreed upon by the Appraisal Team. The Appraisal Organization should encourage the Sponsor to participate in this activity. But, with or without the Sponsor, the Appraisal Organization should perform this last important step.

Appendix A Appraisal Plan

1 Introduction

The introductory section of the Appraisal Plan (the Plan) describes the primary purpose and use of the document

1.1 Purpose

Statement of use and development..

1.2 Application

Summation of contract between Sponsor and Appraiser Organizations, include dates of appraisal, contract number for Appraisal. A copy of the contract may be attached as an Appendix

1.3 Handling

Include if document is proprietary/classified and procedures for protecting. Also include the document's distribution list.

1.4 Changes

Explain who is responsible for the Plan and how any changes will be disseminated to the Plan recipients.

2 Appraisal Information

2.1 Appraisal Purpose

High level explanation of why is appraisal being conducted. Include references to RFP etc. Do not include specific information regarding tailoring the method or model.

2.2 Appraisal Organizations

Contact information (Organization name, address, contact person, contact means)

2.3 Sponsor Organization

2.4 Appraiser Organization

2.5 Appraised Organization

3 Appraisal Application

Document information specific to this appraisal including tailoring of model and method, Sponsor goals and other areas of interest

3.1 Sponsor Goals

A definition of Sponsor Goals provides all Appraisal Participants a unified picture of the purpose of the Appraisal. Include Sponsor expectations, uses of results, and reasons for conducting appraisal.

3.2 PA Refinement

Describe in detail any tailoring/interpretations made of the SSE-CMM Model.

3.3 SSAM Refinement

Although the SSAM is a defined method, Appraiser Organizations may need to further refine particular aspects of the Method to meet individual sponsor goals and expectations. All refinements must be documented and agreed upon by the Sponsor and the Appraiser Organization.

3.3.1 Steps

Some steps may be expanded, reduced, or eliminated based on Sponsor requirements. All modifications to the SSAM steps, including those that address ‘Tailorable Parameters’ should be documented here along with an explanation of why the modification was necessary. Refinements should be documented in order of the steps.

3.3.2 Reports

Reports, including presentations, may be developed for use by the Sponsor, Appraised Organization, or both. Document the level of detail, frequency, format and deadlines for submission.

3.3.3 Evidence

Describe what will and will not be considered ‘evidence’ for this appraisal, be a specific as possible. This section may also include a brief description of how evidence should be evaluated.

3.3.4 Other

This section should include information regarding special tools etc. being used by the team etc.

4 Appraisal Participants

List all appraisal participants, their role in the Appraisal and how they may be contacted. Contact information may include phone/fax numbers, e-mail addresses, building and room numbers etc.

4.1 Sponsor Organization

Role	**Name**	**Contact Information**
Sponsor		

4.2 Appraiser Organization

Primary Role	**Name**	**Contact Information**
Facilitator –1		
Facilitator – 2		
Team Member – 1		
Team Member – 2		
Team Member – 3		
Team Member – 4		

4.3 Appraised Organization

Primary Role	**Name**	**CONTACT INFORMATION**
Site Coordinator		
Executive – 1		
Project Lead – 1		
Practitioner –1		
Practitioner – 2		
Practitioner – 3		

5 Appraised Organization

5.1 General Description

Provide a general description of the Appraised Organization for use as a reference. The description should include typical customers and work products, size, age, any CMM history. Additional information may include management style, notable staffing.

5.2 Organization Chart

Include a pictorial reference of the structure of the Appraised Organization. If the Appraised Organization has a mixed management style this should also be explained in this section.

6 Projects

Describe the projects chosen for inclusion in the appraisal. Enough detail should be given to allow anyone reading the Appraisal Plan to understand why the project was chosen, how it functions internally as well as within the Appraised Organization as a whole, and typical customers and work products. A list of all project participants, including those not scheduled for interviews should be included.

6.1 Project 1

6.1.1 Description

Provide a description of Project 1 including project purpose/scope/goals, customer, and work products.

6.1.2 Applicability to Appraisal

Provide a brief explanation of how Project 1 is applicable to this appraisal. The explanation may include special skill mix requirements for the project, specific tools used, processes etc.

6.1.3 Organization Chart

If possible, provide an organization chart for the project indicating how the staff are organized for Project 1.

6.1.4 Participants

Provide a list of all Project 1 participants their function on the project and contact information. Include those not slated for direct involvement in this appraisal, and any staff members that have left the organization since completion of their assignment, and any outside consultants involved.

7 Schedules

7.1 Overall Deadlines

7.2 Appraisal Schedules

See Appendix C for suggested schedules

7.2.1 Planning Phase

7.2.2 Preparation Phase

7.2.3 On-Site Phase

7.2.4 Reporting Phase

8 Resource Requirements

Logistical requirements should be developed referencing the steps of each phase and Appendix C.

8.1 Planning Phase

8.2 Preparation Phase

8.3 On-Site Phase

8.4 Reporting Phase

9 Information Handling

9.1 Confidentiality Agreements

Document any requirements for confidentiality agreements. Different agreements may be required between the Appraiser and Sponsor Organizations, the Appraiser and Appraised Organizations and Appraised and Sponsor Organization. A complete copy of the text of each agreement should be included in the appendix to the Plan.

9.2 Evidence

Different types of evidence (based on source) may have different handling requirements. Document instructions and procedures for ensuring that it is handled correctly

9.3 Assessed Organization Proprietary

This includes any evidence – documents, videos, e-mail, source code etc. that the Assessed Organization provides to the Appraisal Organization either directly or through the Sponsor Organization. This does not include Appraisal Team interview notes which are considered Appraisal Team Work Products.

9.3.1 Collection

9.3.1.1. Direct

Principally this is a description of how the Evidence Custodian and Site Coordinator will coordinate their efforts.

9.3.1.2. Indirect

Detail how information sent to the Sponsor during the Planning Phase will be forwarded to the Appraisal Team. Include specific method – registered mail, encrypted e-mail etc., and responsible parties

9.3.2 Tracking

Name specific tools used to track evidence. If no specific tool will be used describe the process used.

9.3.3 Use

Indicate parameters of use of any collected information. Such as where it can be used and when. Include restrictions on copying, marking up etc.

9.3.4 Storage

Document how the Appraisal Team or Appraised Organization will store the evidence during the appraisal. The method chosen should ensure unrestricted access and ease of use for both parties.

9.3.5 Disposal

The Sponsor may require that some evidence must be forwarded to the Sponsor. Details of how this is to be accomplished should be documented.

9.4 Appraisal Team Work Products

Appraisal Team Work Products include, completed questionnaires, interview notes, meeting minutes/notes, DTS and draft and final copies of all reports and briefings.

9.4.1 Production

Indicate how the Appraisal Team will identify their work products as being separate from those of the Appraised Organization. (use of colored paper etc.)

9.4.2 Use

Indicate who will have access to intermediate and final work products and where these products will be developed.

9.4.3 Storage

Document how the Appraisal Team will secure its appraisal work products during all Phases of the appraisal.

9.4.4 Disposal

The Sponsor may require that some evidence must be forwarded to the Sponsor. Details of how this is to be accomplished should be documented.

Appendix A: Questionnaire

Document the exact questionnaire to be used in the appraisal

Appendix B: Opening Briefing

Document the specific briefing on the process to be given to the Appraised Organization

Appendix C: Final Briefing

Outline the requirements of the final briefing.

Appendix B Schedules

The schedules provided below indicate rough estimates of the time required to complete the tasks in the Preparation and On-Site Phases. It assumes that the Preparation activities will take 3 days and that the On-Site activities require 5 days to complete. The schedules indicate the step involved for each designated block of time and the personnel required for each day.

Preparation Phase

Steps 2.2.1 – 2.2.4

Day 1

Personnel Required Appraisal Team

					Preparation Activity #
8:30 AM	-	9:00 AM	00:30	Review of SSE-CMM - general	1
9:00 AM	-	10:30 AM	01:30	Review of SSAM - general	1
10:30 AM	-	10:45 AM	00:15	Break	
10:45 AM	-	11:30 AM	00:45	Discussion of Sponsor goals and objectives	1
11:30 AM	-	12:00 PM	00:30	SSE-CMM and SSAM interpretation for specific appraisal	1
12:00 PM	-	1:00 PM	01:00	Lunch	
1:00 PM	-	3:00 PM	02:00	Review of Appraisal Plan	1
3:00 PM	-	3:15 PM	00:15	Break	
3:15 PM	-	4:00 PM	00:45	Review of appraisal schedule	1
4:00 PM	-	5:00 PM	01:00	Assignment of responsibilities	1

Day 2

Personnel Required Project Leads, Site Coordinator, Site Support Staff, Appraisal Team

					Preparation Activity #
8:30 AM	-	9:30 AM	01:00	Introduce team and purpose of questionnaire	
9:30 AM	-	10:00 AM	00:30	Administer Questionnaire/Review evidence	2/4
10:00 AM	-	10:15 AM	00:15	Break	
10:15 AM	-	12:00 AM	01:45	Administer questionnaire/Review evidence	2/4
12:00 PM	-	1:00 PM	01:00	Lunch	
1:00 PM	-	2:15 PM	01:15	Consolidate Evidence	3
2:15 PM	-	2:30 PM	00:15	Break	
2:30 PM	-	4:00 PM	01:30	Analyze Evidence/Questionnaire	3/4
4:15 PM	-	4:30 PM	00:15	Break	
4:30 PM	-	7:00 PM	02:30	Analyze Evidence/Questionnaire	3/4
7:00 PM	-	7:30 AM	00:30	Team Meeting	

Day 3

Personnel Required: Project Leads, Site Coordinator, Site Support Staff, Appraisal Team

					Preparation Activity #
8:00 AM	-	8:30 AM	00:30	Team Meeting	
8:30 AM	-	10:30 AM	02:00	Administer Questionnaire/Review evidence	2/3
10:30 AM	-	10:45 AM	00:15	Break	
10:45 AM	-	12:00 AM	01:15	Administer questionnaire/Review evidence	2/3
12:00 PM	-	1:00 PM	01:00	Lunch	
1:00 PM	-	2:15 PM	01:15	Consolidate Evidence	4
2:15 PM	-	2:30 PM	00:15	Break	
2:30 PM	-	4:00 PM	01:30	Analyze Evidence/Questionnaire	3/4
4:15 PM	-	4:30 PM	00:15	Break	
4:00 PM	-	5:30 PM	01:30	Analyze Evidence/Questionnaire	3/4
5:30 PM	-	6:00 PM	00:30	Team Meeting	

On-Site Phase

Steps 2.3.1 – 2.3.13

Day 1

Personnel Required: Project Leads, Site Coordinator, Facilitators, Appraisal Team

					On-Site Activity #
8:00 AM	-	8:30 AM	00:30	Team Meeting	
8:30 AM	-	9:00 AM	00:30	Executive Brief	1
9:00 AM	-	10:00AM	01:00	Opening Meeting	2
10:00 AM	-	10:15 AM	00:15	Break	
10:15 AM	-	11:45 PM	01:30	Interview Lead	3
11:45 AM	-	12:00 PM	00:15	Break	
12:00 PM	-	1:00 PM	00:45	Lunch	3
1:00 PM	-	2:30 PM	01:30	Interview Lead	
2:30 PM	-	2:45 PM	00:15	Break	
2:45 PM	-	4:15 PM	01:30	Interview Lead	3
4:15 PM	-	4:30 PM	00:15	Break	
4:30 PM	-	6:00 PM	01:30	Consolidate Lead Data/ Interpret Lead Data	4
6:00 PM	-	6:15 PM	00:15	Break	
6:15 PM	-	7:00 PM	02:00	Consolidate Lead Data/ Interpret Lead Data	4
7:00 PM	-	7:30 PM	00:30	Team Meeting	

Day 2

Personnel Required: Project Practitioners Site Coordinator, Facilitators, Appraisal Team

			On-Site Activity #
7:30 AM - 8:00 AM	00:30	Team Meeting	
8:00 AM - 8:45 AM	00:45	Interview Practitioner	5
8:45 AM - 9:00 AM	00:15	Break	
9:00 AM - 9:45 AM	00:45	Interview Practitioner	5
9:45 AM - 10:00 AM	00:15	Break	
10:00 AM - 10:45 AM	00:45	Interview Practitioner	5
10:45 AM - 11:00 AM	00:15	Break	
11:00 AM - 12:00 PM	01:00	Consolidate Data, DTS, New Questions	6
12:00 PM - 1:00 PM	01:00	Lunch	
1:00 PM - 1:45 PM	00:45	Consolidate Data, DTS, New Questions	6
1:45 PM - 2:00 PM	00:15	Break	
2:00 PM - 2:45 PM	00:45	Interview Practitioner	5
2:45 PM - 3:00 PM	00:15	Break	
3:00 PM - 3:45 PM	00:45	Interview Practitioner	5
3:45 PM - 4:00 PM	00:15	Break	
4:00 PM - 4:45 PM	00:45	Interview Practitioner	5
4:45 PM - 5:00 PM	00:15	Break	
5:00 PM - 6:30 PM	01:30	Consolidate Data, DTS, New Questions	6
6:30 PM - 7:00 PM	00:30	Team Meeting	

Ratio of Appraisers to Practitioners 4:1

Day 3

Personnel Required: Project Practitioners, Site Coordinator, Facilitators, Appraisal Team

						On-Site Activity #
7:30 AM	-	8:00 AM	00:30	Team Meeting		
8:00 AM	-	8:45 AM	00:45	Interview Practitioner	X2	5
8:45 AM	-	9:00 AM	00:15	Break		
9:00 AM	-	9:45 AM	00:45	Interview Practitioner	X2	5
9:45 AM	-	10:00 AM	00:15	Break		
10:00 AM	-	10:45 AM	00:45	Interview Practitioner	X2	5
10:45 AM	-	11:00 AM	00:15	Break		
11:00 AM	-	12:00 PM	01:00	Consolidate Data, DTS, New Questions		6
12:00 PM	-	1:00 PM	01:00	Lunch		
1:00 PM	-	1:45 PM	00:45	Consolidate Data, DTS, New Questions		6
1:45 PM	-	2:00 PM	00:15	Break		
2:00 PM	-	2:45 PM	00:45	Interview Practitioner	X2	5
2:45 PM	-	3:00 PM	00:15	Break		
3:00 PM	-	3:45 PM	00:45	Interview Practitioner	X2	5
3:45 PM	-	4:00 PM	00:15	Break		
4:00 PM	-	4:45 PM	00:45	Interview Practitioner	X2	5
4:45 PM	-	5:00 PM	00:15	Break		
5:00 PM	-	6:30 PM	01:30	Consolidate Data, DTS, New Questions		6
6:30 PM	-	7:00 PM	00:30	Team Meeting		

Ratio of Appraisers to Practitioner 2:1

Day 4

Personnel Required: Interviewees as designated, Site Coordinator, Site Support Staff, Facilitators, SSE

					On-Site Activity #
8:00 AM	-	12:00 PM	04:00	Analyze DTS, Develop/Review Preliminary Findings	7/8
12:00 PM	-	1:00 PM	01:00	Lunch	
1:00 PM	-	3:00 PM	02:00	Develop and Review Preliminary Findings	8
3:00 AM	- -	4:00 PM	01:00	Follow-up Interview (as necessary)	9
4:00 PM	-	5:00 PM	01:00	Follow-up Interview (as necessary)	9
5:00 AM	-	7:00 PM	02:00	Analyze DTS, Develop/Revise Preliminary Findings	7/8
7:00 PM	-	7:30 PM	00:30	Team Meeting	

Ratio of Appraiser to Practitioners 2:1

Day 5

Personnel Required: Site Coordinator, Site Support Staff, Facilitators, SSE

					On-Site Activity #
8:00 AM	-	12:00 PM	04:00	Develop Rating	10/11
12:00 PM	-	1:00 PM	01:00	Working Lunch	
1:00 PM	-	4:30 PM	03:30	Develop Rating	10/11
4:30 PM	-	5:00 PM	00:30	Manage Artifacts	12
5:00 PM	-	5:30 PM	00:30	Conduct Wrap-Up	13

Appendix C Appraisal Planning Checklist

This checklist is used to support the SSE-CMM appraisal Facilitator in preparing for the on-site portion of the SSAM.

Preparation Tasks

The table below describes the major events that must be completed before the on-site phase of the appraisal can proceed. The time frames presented are approximations and are relative to the commencement of the on-site phase, not in terms of how long they should take to accomplish.

✔	Task	Description	Responsibility	Time Frame
	Set parameters and define limits of appraisal	Meeting/Discussion to manage expectations in which the purpose, goals, parameters, and targets of appraisal are defined	Facilitator Sponsor	1-1.5 mo.
	Establish requirements for handling sensitive/proprietary material	Draft/approve/sign any necessary non-disclosure agreements as well as establish procedures for storage and disposal of evidence collected by Appraisal Team.	Facilitator Sponsor	1-1.5 mo.
	Initial Contract	Approve/Sign contract between appraisal entity and Sponsor covering purpose, goals, parameters, targets of appraisal as established in 2.1.1 and 2.1.2 and verify who will receive data on the conclusions of the appraisal. .	Facilitator Sponsor	1-1.5 mo.
	Establish Appraisal Team	Choose members of Appraisal Team based on qualifications/standards laid out in Chapter 4 and provide them with complete copies of the SSE-CMM and SSAM.	Facilitator Sponsor	1-1.5 mo.
	Select Projects for Appraisal	Using contract, RFP, and another relevant guidance material choose projects for evaluation and submit to Sponsor.	Facilitator Sponsor	1.5 mo.
	Establish Appraisal Schedule	Working with on-site coordinator to confirm the availability of project leads,	Facilitator Site Coordinator	1 mo.

✔	Task	Description	Responsibility	Time Frame
		participants and managers, and Appraisal Team, establish schedule to include preparation, on-site, and post-assessment phases including dates for submissions and final task completion.	Sponsor	
	Logistics	Arrangements are made on-site for appropriate facilities for the Appraisal Team to conduct its work. Several meeting rooms of various size will be required, including a large meeting hall for the opening and closing briefs, 3-4 smaller rooms for project lead and practitioner interviews, and a conference room for regular meetings and working sessions of the whole Appraisal Team. If the appraisal site does not allow outside computing equipment to be brought into its facility, or if the Appraisal Team does not have the appropriate equipment in its possession, then arrangements also need to be made for computing facilities (hardware, software and peripherals). These will include computers in all interview, conference, and meeting rooms, access to printers, copiers and faxes and possibly an overhead projector or LCD panel. Additionally the team may require other office supplies such as flip charts, markers, notepads, transparencies, post-it notes, white boards, writing paper, etc. Escorts, if required for the Appraisal Team, should also be arranged at this time.	Site Coordinator Facilitator	2-4 wks

✔	Task	Description	Responsibility	Time Frame
		Other requirements may be determined by the Sponsor.		
	Prepare Appraisal Team	Review the SSAM with Appraisal Team members to ensure that they are comfortable with the methodology used in the appraisal and understand their roles in its conduct.	Facilitator Appraisal Team	1 mo.
	Tailor Appraisal Questionnaire	Based on the goals of the appraisal a SSE-CMM questionnaire, to be completed by the project leads, is tailored.	Facilitator Appraisal Team	1 mo.
	Prepare Appraisal Team Notebook	Each team member should have copies of all completed questionnaires, descriptions of each project, resumes of leads and participants as well as copies of the SSE-CMM, SSAM, and tailored questionnaire.	Facilitator	1 wk
	Administer Questionnaire	In a group setting the project leads are given the questionnaire in a face-to-face setting.	Facilitator Site Coordinator Project Leads	2 days

Appendix D   Questionnaire

The following questionnaire is administered to the project leads during the Preparation Phase of the appraisal. A Facilitator should be made available to assist project leads in interpreting questions. The PAs are presented in the same order that they are found in the SSE-CMM model. The questionnaire is organized such that for each PA the respondent is first asked if the Base Practices are performed. If all Base Practices are performed, then the project lead is asked to answer questions regarding the maturity and institutionalization of those processes.

PA01 Administer Security Controls

Process area summary: The purpose of Administer System Security Controls is to ensure that the intended security for the system that was integrated into the system design, is in fact achieved by the resultant system in its operational state.

Goals

- Security controls are properly used and configured.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.	____________
Yes	**No**	**Don't Know**	Manage the configuration of system security controls.	____________
Yes	**No**	**Don't Know**	Manage security awareness, training, and education programs for all users and administrators.	____________
Yes	**No**	**Don't Know**	Manage periodic maintenance and administration of security services and control mechanisms.	____________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	____________
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	____________
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	____________

					Evidence
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	

Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________

					Evidence
Yes	**No**	**Don’t Know**	5.2.4	Continuously improving the process area by changing the organization’s standard process definition to increase its effectiveness?	____________________

PA02 Assess Impact

Process area summary: The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.

Goals

- The security impacts of risks to the system are identified and characterized.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system.	____________
Yes	**No**	**Don't Know**	Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system.	____________
Yes	**No**	**Don't Know**	Select the impact metric to be used for this assessment.	____________
Yes	**No**	**Don't Know**	Identify the relationship between the selected metrics for this assessment and metric conversion factors if required.	____________
Yes	**No**	**Don't Know**	Identify and characterize impacts.	____________
Yes	**No**	**Don't Know**	Monitor ongoing changes in the impacts.	____________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	____________

					Evidence
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	____________________
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	____________________
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	____________________
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	____________________
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	____________________
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	____________________
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	____________________
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	____________________
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	____________________
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	____________________
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	____________________

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	____________________

Yes **No** **Don't Know** 3.1.2 Tailor the organizational standard process definition to meet the needs of a specific use? ____________________

Yes **No** **Don't Know** 3.2.1 Follow the tailored version of the organizational standard process definition? ____________________

Yes **No** **Don't Know** 3.2.2 Perform defect reviews of appropriate work products? ____________________

Yes **No** **Don't Know** 3.2.3 Use data on performing the defined process to manage the defined process? ____________________

Yes **No** **Don't Know** 3.3.1 Coordinate communication within the security engineering group? ____________________

Yes **No** **Don't Know** 3.3.2 Coordinate communication among the various groups within your project/organization? ____________________

Yes **No** **Don't Know** 3.3.3 Coordinate communication with external groups? ____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

Evidence

Yes **No** **Don't Know** 4.1.1 Establishing measurable quality goals for the work products of the organization's standard process family? ____________________

Yes **No** **Don't Know** 4.2.1 Determine the process capability of the defined process quantitatively? ____________________

Yes **No** **Don't Know** 4.2.2 Take corrective action as appropriate when the defined process is not performing within its process capability? ____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

Evidence

Yes **No** **Don't Know** 5.1.1 Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability? ____________________

					Evidence
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	

PA03 Assess Security Risk

Process area summary: The purpose of Assess Security Risk is to identify the security risks involved with relying on a system in a defined environment. This process area focuses on ascertaining these risks based on an established understanding of how capabilities and assets are vulnerable to threats. Specifically, this activity involves identifying and assessing the likelihood of the occurrence of exposures. “Exposure” refers to a combination of a threat, vulnerability, and impact which could cause significant harm. This set of activities is performed any time during a system’s life-cycle to support decisions related to developing, maintaining, or operating the system within a known environment.

Goals

- An understanding of the security risk associated with operating the system within a defined environment is achieved.
- Risks are prioritized according to a defined methodology.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don’t Know**	Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared.	
Yes	**No**	**Don’t Know**	Identify threat/vulnerability/impact triples (exposures).	
Yes	**No**	**Don’t Know**	Assess the risk associated with the occurrence of an exposure.	
Yes	**No**	**Don’t Know**	Assess the total uncertainty associated with the risk for the exposure.	
Yes	**No**	**Don’t Know**	Order risks by priority.	
Yes	**No**	**Don’t Know**	Monitor ongoing changes in the risk spectrum and changes to their characteristics.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	____________________
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	____________________
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	____________________
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	____________________
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	____________________
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	____________________
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	____________________
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	____________________
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	____________________
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	____________________
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	____________________
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	____________________

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	____________________
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	____________________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	____________________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	____________________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

PA04 Assess Threat

Process area summary: The purpose of the Assess Threat process area is to identify security threats and their properties and characteristics.

Goals

- Threats to the security of the system are identified and characterized.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Identify applicable threats arising from a natural source.	
Yes	**No**	**Don't Know**	Identify applicable threats arising from man-made sources, either accidental or deliberate.	
Yes	**No**	**Don't Know**	Identify appropriate units of measure, and applicable ranges, in a specified environment.	
Yes	**No**	**Don't Know**	Assess capability and motivation of threat agent for threats arising from man-made sources.	
Yes	**No**	**Don't Know**	Access the likelihood of threat manifestation.	
Yes	**No**	**Don't Know**	Monitor ongoing changes in the threat spectrum and changes to their characteristics.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	

					Evidence
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	____________________
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	____________________
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	____________________
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	____________________
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	____________________
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	____________________
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	____________________
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	____________________
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	____________________
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	____________________

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	____________________
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	____________________

Yes **No** **Don't Know** 3.2.1 Follow the tailored version of the organizational standard process definition? ____________________

Yes **No** **Don't Know** 3.2.2 Perform defect reviews of appropriate work products? ____________________

Yes **No** **Don't Know** 3.2.3 Use data on performing the defined process to manage the defined process? ____________________

Yes **No** **Don't Know** 3.3.1 Coordinate communication within the security engineering group? ____________________

Yes **No** **Don't Know** 3.3.2 Coordinate communication among the various groups within your project/organization? ____________________

Yes **No** **Don't Know** 3.3.3 Coordinate communication with external groups? ____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

Evidence

Yes **No** **Don't Know** 4.1.1 Establishing measurable quality goals for the work products of the organization's standard process family? ____________________

Yes **No** **Don't Know** 4.2.1 Determine the process capability of the defined process quantitatively? ____________________

Yes **No** **Don't Know** 4.2.2 Take corrective action as appropriate when the defined process is not performing within its process capability? ____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

Evidence

Yes **No** **Don't Know** 5.1.1 Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability? ____________________

Yes **No** **Don't Know** 5.2.1 Perform causal analysis of defects? ____________________

					Evidence
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

PA05 Assess Vulnerability

Process area summary: The purpose of Assess Vulnerability is to identify and characterize system security vulnerabilities. This process area includes analyzing system assets, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability. The terms associated with security risk and vulnerability assessment are used differently in many contexts. For the purposes of this model, “vulnerability” refers to an aspect of a system that can be exploited for purposes other than those originally intended, security holes, or implementation bugs within a system that are likely to be attacked by a threat. These vulnerabilities are independent of any particular threat instantiation or attack. This set of activities is performed any time during a system’s life-cycle to support the decision to develop, maintain, or operate the system within the known environment.

Goals

- An understanding of system security vulnerabilities within a defined environment is achieved.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don’t Know**	Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized.	____________________
Yes	**No**	**Don’t Know**	Identify system security vulnerabilities.	____________________
Yes	**No**	**Don’t Know**	Gather data related to the properties of the vulnerabilities.	____________________
Yes	**No**	**Don’t Know**	Assess the system vulnerability and aggregate vulnerabilities that results from specific vulnerabilities and combinations of specific vulnerabilities	____________________
Yes	**No**	**Don’t Know**	Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.	____________________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	____________________
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	____________________
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	____________________
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	____________________
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	____________________
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	____________________
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	____________________
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	____________________
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	____________________
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	____________________
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	____________________
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	____________________

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	

PA06 Build Assurance Argument

Process area summary: The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.

This process includes identifying and defining assurance related requirements; evidence production and analysis activities; and additional evidence activities needed to support assurance requirements. Additionally, the evidence generated by these activities is gathered, packaged, and prepared for presentation.

Goals

- Work products and processes meet customer security needs.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Identify the security assurance objectives.	____________________
Yes	**No**	**Don't Know**	Define a security assurance strategy to address all assurance objectives.	____________________
Yes	**No**	**Don't Know**	Identify and control security assurance evidence.	____________________
Yes	**No**	**Don't Know**	Perform analysis of security assurance evidence.	____________________
Yes	**No**	**Don't Know**	Provide a security assurance argument that demonstrates the customer's security needs are met.	____________________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

PA07 Coordinate Security

Process area summary: The purpose of Coordinate Security is to ensure that the appropriate parties are aware of and involved with security engineering activities. This activity is critical, as security engineering cannot succeed in isolation. This coordination involves maintaining open - communications between security groups, other engineering groups, and external groups. Various mechanisms may be used to coordinate and communicate the security engineering decisions and recommendations between these parties, including memoranda, documents, e-mail, meetings, and working groups.

Goals

- All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions.
- Decisions and recommendations related to security are appropriately communicated and coordinated.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note you do not have to personally be involved in performing the practice it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Define security engineering coordination objectives and relationships.	___________________
Yes	**No**	**Don't Know**	Identify coordination mechanisms for security engineering.	___________________
Yes	**No**	**Don't Know**	Facilitate security engineering coordination.	___________________
Yes	**No**	**Don't Know**	Use the identified mechanisms to coordinate decisions and recommendations related to security.	___________________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	___________________

					Evidence
Yes	**No**	**Don’t Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don’t Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don’t Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don’t Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don’t Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don’t Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don’t Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don’t Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don’t Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don’t Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don’t Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	

Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	____________________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	____________________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	____________________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________

					Evidence
Yes	**No**	**Don’t Know**	5.2.1	Perform causal analysis of defects?	__________
Yes	**No**	**Don’t Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	__________
Yes	**No**	**Don’t Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	__________
Yes	**No**	**Don’t Know**	5.2.4	Continuously improving the process area by changing the organization’s standard process definition to increase its effectiveness?	__________

PA08 Monitor Security Posture

Process area summary: The purpose of Monitor Security Posture is to ensure that all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security are identified and reported. The external and internal environments are monitored for all factors that may have an impact on the security of the system.

Goals

- Both internal and external security related events are detected and tracked.
- Incidents are responded to in accordance with policy.
- Changes to the operational security posture are identified and handled in accordance with the security objectives.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note you do not have to personally be involved in performing the practice -- it’s enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don’t Know**	Analyze event records to determine the cause of an event, how it proceeded, and likely future events.	
Yes	**No**	**Don’t Know**	Monitor changes in threats, vulnerabilities, impacts, risks, and the environment.	
Yes	**No**	**Don’t Know**	Identify security relevant incidents.	
Yes	**No**	**Don’t Know**	Monitor the performance and functional effectiveness of security safeguards.	
Yes	**No**	**Don’t Know**	Review the security posture of the system to identify necessary changes.	
Yes	**No**	**Don’t Know**	Manage the response to security relevant incidents.	
Yes	**No**	**Don’t Know**	Ensure that the artifacts related to security monitoring are suitably protected.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	____________
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	____________
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	____________
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	____________
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	____________
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	____________
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	____________
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	____________
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	____________
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	____________
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	____________
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	____________

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	____________________
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	____________________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	____________________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	____________________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	

PA09 Provide Security Input

Process area summary: The purpose of Provide Security Input is to provide system architects, designers, implementers, or users with the security information they need. This information includes security architecture, design, or implementation alternative and security guidance. The input is developed, analyzed, and provided to and coordinated with the appropriate organization members based on the security needs identified in PA01 Specify Security Needs.

Goals

- All system issues are reviewed for security implications and are resolved in accordance with security goals.
- All members of the project team have an understanding of security so they can perform their functions
- The solution reflects the security input provided.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.	
Yes	**No**	**Don't Know**	Determine the security constraints and considerations needed to make informed engineering choices.	
Yes	**No**	**Don't Know**	Identify alternative solutions to security related engineering problems.	
Yes	**No**	**Don't Know**	Analyze and prioritize engineering alternatives using security constraints and considerations.	
Yes	**No**	**Don't Know**	Provide security related guidance to the other engineering groups.	
Yes	**No**	**Don't Know**	Provide security related guidance to operational system users and administrators.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don’t Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don’t Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don’t Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don’t Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don’t Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don’t Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don’t Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don’t Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don’t Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don’t Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don’t Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	____________________
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	____________________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	____________________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	____________________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	

PA10 Specify Security Needs

Process area summary: The purpose of Specify Security Needs is to explicitly identify the needs related to security for the system. Specify Security Needs involves defining the basis for security in the system in order to meet all legal, policy, and organizational requirements for security. These needs are tailored based upon the target operational security context of the system, the current security and systems environment of the organization, and a set of security objectives are identified. A set of security-related requirements is defined for the system that becomes the baseline for security within the system upon approval.

Goals

- A common understanding of security needs is reached between all applicable parties, including the customer.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Gain an understanding of the customer's security needs.	
Yes	**No**	**Don't Know**	Identify which laws, policies, standards, external influences and constraints govern the system.	
Yes	**No**	**Don't Know**	Identify the purpose of the system in order to determine the security context.	
Yes	**No**	**Don't Know**	Capture a high-level security oriented view of the system operation.	
Yes	**No**	**Don't Know**	Capture high-level goals that define the security of the system.	
Yes	**No**	**Don't Know**	Define a consistent set of statements which define the protection to be implemented in the system.	
Yes	**No**	**Don't Know**	Obtain agreement that the specified security meets the customer's needs.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	____________________
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	____________________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	____________________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	____________________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

PA11 Verify and Validate Security

Process area summary: The purpose of Verify and Validate Security is to ensure that solutions are verified and validated with respect to security. Solutions are verified against the security requirements, architecture, and design using observation, demonstration, analysis, and testing. Solutions are validated against the customer's operational security needs.

Goals

- Solutions meet security requirements.
- Solutions meet the customer's operational security needs.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Identify the solution to be verified and validated.	
Yes	**No**	**Don't Know**	Define the approach and level of rigor for verifying and validating each solution.	
Yes	**No**	**Don't Know**	Verify that the solution implements the requirements associated with the previous level of abstraction.	
Yes	**No**	**Don't Know**	Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs.	
Yes	**No**	**Don't Know**	Capture the verification and validation results for the other engineering groups.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	

					Evidence
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't**	3.1.2	Tailor the organizational standard process	

		Know		definition to meet the needs of a specific use?	____________________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	____________________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	____________________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________

					Evidence
Yes	**No**	**Don’t Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don’t Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don’t Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don’t Know**	5.2.4	Continuously improving the process area by changing the organization’s standard process definition to increase its effectiveness?	

PA12 Ensure Quality

Process area summary: The purpose of Ensure Quality is to address not only the quality of the system, but also the quality of the process being used to create the system and the degree to which the project follows the defined process. The underlying concept of this process area is that high-quality systems can only be consistently produced on a continuous basis if a process exists to continuously measure and improve quality. In addition, this process must be adhered to rigorously and throughout the system life cycle. Key aspects of the process required to develop high-quality systems are measurement, analysis, and corrective action.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Ensure the defined systems security engineering process is adhered to during the system life cycle.	
Yes	**No**	**Don't Know**	Evaluate work product measures against the requirements for work product quality.	
Yes	**No**	**Don't Know**	Measure the quality of the systems security engineering process used by the project	
Yes	**No**	**Don't Know**	Analyze quality measurements to develop recommendations for quality improvement or corrective action as appropriate.	
Yes	**No**	**Don't Know**	Obtain employee participation in identifying and reporting quality issues.	
Yes	**No**	**Don't Know**	Initiate activities that address identified quality issues or quality improvement opportunities	
Yes	**No**	**Don't Know**	Establish a mechanism or a set of mechanisms to detect the need for corrective actions processes or products.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	

PA13 Manage Configurations

Process area summary: The purpose of Manage Configurations is to maintain data on and status of identified configuration units, and to analyze and control changes to the system and its configuration units. Managing the system configuration involves providing accurate and current configuration data and status of developers and customers.

This process area is applicable to all work products that are placed under configuration management. An example set of work products that may be placed under configuration management could include hardware and software configuration items, design rationale, requirements, product data files, or trade studies.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Decide among candidate methods for configuration management.	
Yes	**No**	**Don't Know**	Identify configuration units that constitute identified baselines.	
Yes	**No**	**Don't Know**	Maintain a repository of work product baselines.	
Yes	**No**	**Don't Know**	Control changes to established configuration units.	
Yes	**No**	**Don't Know**	Communicate status of configuration data, proposed changes, and access information to affected groups.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don’t Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don’t Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don’t Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don’t Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don’t Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don’t Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don’t Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization’s Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	4.1.1	Establishing measurable quality goals for the work products of the organization’s standard process family?	
Yes	**No**	**Don’t Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don’t Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization’s Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	
Yes	**No**	**Don’t Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don’t Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don’t Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don’t Know**	5.2.4	Continuously improving the process area by changing the organization’s standard process definition to increase its effectiveness?	

PA14 Manage Program Risk

Process area summary: The purpose of Manage Risk is to identify, assess, monitor, and mitigate risks to the success of both the security engineering activities and the overall technical effort. This process area continues throughout the life of the project. Similar to the Plan Technical Effort (PA12) and Monitor and Control Technical Effort (PA11) process areas, the scope of this process area includes both the security engineering activities and the overall technical project effort, as the security engineering effort on the project cannot be considered successful unless the overall technical effort is successful.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided..

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Develop a plan for risk-management activities that is the bases for identifying, assessing, mitigating, and monitoring risks for the life of the project.	
Yes	**No**	**Don't Know**	Identify project risks by examining project objectives with respect to the alternatives and constraints, and identifying what can go wrong.	
Yes	**No**	**Don't Know**	Assess risks and determine the probability of occurrence and consequence of realization.	
Yes	**No**	**Don't Know**	Obtain formal recognition of the project risk assessment.	
Yes	**No**	**Don't Know**	Implement the risk-mitigation activities.	
Yes	**No**	**Don't Know**	Monitor risk-mitigation activities to ensure that the desired results are being obtained.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

PA15 Monitor and Control Technical Effort

Process area summary: The purpose of Monitor and Control Technical Effort is to provide adequate visibility of actual progress and risks. Visibility encourages timely corrective action when performance deviates significantly from plans.

Monitor and Control Technical Effort involves directing, tracking, and reviewing the project’s accomplishments, results, and risks against its documented estimates, commitments, and plans. A documented plan is used as the basis for tracking the activities and risks, communicating status, and revising plans.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don’t Know**	Direct technical effort in accordance with technical management plans.	
Yes	**No**	**Don’t Know**	Track actual use of resources against technical management plans.	
Yes	**No**	**Don’t Know**	Track performance against the established technical parameters.	
Yes	**No**	**Don’t Know**	Review performance against the technical management plans.	
Yes	**No**	**Don’t Know**	Analyze issues resulting from the tracking and review of technical parameters to determine corrective actions.	
Yes	**No**	**Don’t Know**	Take corrective actions when actual results deviate from plans.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don’t Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don’t Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don’t Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don’t Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don’t Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don’t Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don’t Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don’t Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don’t Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don’t Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don’t Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	

PA16 Plan Technical Effort

Process area summary: The purpose of Plan Technical Effort is to establish plans that provide the basis for scheduling, costing, controlling, tracking, and negotiating the nature and scope of the technical work involved in system development, manufacturing, use, and disposal. System engineering activities must be integrated into comprehensive technical planning for the entire project

Plan technical effort involves developing estimates for the work to be performed, obtaining necessary commitments from interfacing groups, and defining the plan to perform the work.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided.

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Identify resources that are critical to the technical success of the project.	
Yes	**No**	**Don't Know**	Develop estimates for the factors that affect the magnitude and technical feasibility of the project.	
Yes	**No**	**Don't Know**	Develop cost estimates for all technical resources required by the project.	
Yes	**No**	**Don't Know**	Determine the technical process to be used on the project.	
Yes	**No**	**Don't Know**	Identify technical activities for the entire life cycle of the project.	
Yes	**No**	**Don't Know**	Determine specific processes to support effective interaction with the customer(s) and supplier(s).	
Yes	**No**	**Don't Know**	Develop technical schedules for the entire project life cycle.	
Yes	**No**	**Don't Know**	Establish technical parameters with thresholds for the project and the system.	

Yes	**No**	**Don't Know**		Use the information gathered in planning activities to develop technical management plans that will serve as the bases for tracking the salient aspects of the project and the security engineering effort.	
Yes	**No**	**Don't Know**		Review the technical management plans with all affected groups and individuals, and obtain group commitment.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	

					Evidence
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	________

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	________
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	________

					Evidence
Yes	**No**	**Don’t Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________
Yes	**No**	**Don’t Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________

5. Continuously Improving

Are the following characteristics visible in the organization’s Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________
Yes	**No**	**Don’t Know**	5.2.1	Perform causal analysis of defects?	____________
Yes	**No**	**Don’t Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________
Yes	**No**	**Don’t Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________
Yes	**No**	**Don’t Know**	5.2.4	Continuously improving the process area by changing the organization’s standard process definition to increase its effectiveness?	____________

PA17 Define Organization’s Systems Engineering Processes

Process area summary: The purpose of Define Organization’s Systems Engineering Process is to create and manage the organization’s standard systems security engineering process, which can subsequently be tailored by a project to form the unique processes that it will follow in developing its systems or products.

Define Organization’s Systems Engineering Process involves defining, collecting, and maintaining the process that will meet the business goals of the organization, as well as designing, developing, and documenting systems-engineering process assets. Assets include example processes, process fragments, process-related documentation, process architecture, process-tailoring rules and tools, and process measurements.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided..

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don’t Know**	Establish goals for the organization’s systems security engineering process from the organization’s business goals.	
Yes	**No**	**Don’t Know**	Collect and maintain systems-engineering process assets.	
Yes	**No**	**Don’t Know**	Develop; a well-defined standard systems security engineering process for the organization.	
Yes	**No**	**Don’t Know**	Define guidelines for tailoring the organization’s standard systems security engineering process for project use in developing the project’s defined process.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don’t Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don’t Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don’t Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don’t Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don’t Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don’t Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don’t Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don’t Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don’t Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don’t Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don’t Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	____________
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	____________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	____________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	____________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

PA18 Improve Organization’s System Engineering Processes

Process area summary: The purpose of Improve Organization’s System Engineering Processes is to gain competitive advantage by continuously improving the effectiveness and efficiency of the systems security engineering processes used by the organization. It involves developing and understanding of the organization’s processes in the context of the organization’s business goals, analyzing the performance of the processes, and explicitly planning and deploying improvements to those processes.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided..

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don’t Know**	Appraise the existing processes being performed in the organization to understand their strengths and weaknesses.	____________
Yes	**No**	**Don’t Know**	Plan improvements to the organization’s processes based on analyzing the impact of potential improvements on achieving the goals of the processes.	____________
Yes	**No**	**Don’t Know**	Change the organization’s standard systems security engineering processes to reflect targeted improvements.	____________
Yes	**No**	**Don’t Know**	Communicate process improvements to existing projects and to other affected groups, as appropriate.	____________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t**	2.1.1	Allocate adequate resources (including	____________

					Evidence
		Know		people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	

Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	___________________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	___________________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	___________________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	___________________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	___________________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	___________________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	___________________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	___________________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	___________________
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	___________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	___________________

					Evidence
Yes	**No**	**Don’t Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don’t Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don’t Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don’t Know**	5.2.4	Continuously improving the process area by changing the organization’s standard process definition to increase its effectiveness?	

PA19 Manage Product Line Evolution

Process area summary: The purpose of Manage Product Line Evolution is to introduce services, equipment, and new technology to achieve the optimal benefits in product evolution, cost, schedule, and performance over time as the product line evolves toward its ultimate objectives.

An organization must first determine the evolution of a product. Then the organization has to decide how it will design and build those products including critical components, cost-effective tools, and efficient and effective processes.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided..

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Define the types of products to be offered.	____________________
Yes	**No**	**Don't Know**	Identify new product technologies or enabling infrastructure that will help the organization acquire, develop, and apply technology for competitive advantage.	____________________
Yes	**No**	**Don't Know**	Make the necessary changes in the product development cycle to support the development of new products.	____________________
Yes	**No**	**Don't Know**	Ensure critical components are available to support planned product evolution.	____________________
Yes	**No**	**Don't Know**	Insert new technology into product development, marketing, and manufacturing.	____________________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization’s Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don’t Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	
Yes	**No**	**Don’t Know**	5.2.1	Perform causal analysis of defects?	
Yes	**No**	**Don’t Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	
Yes	**No**	**Don’t Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	
Yes	**No**	**Don’t Know**	5.2.4	Continuously improving the process area by changing the organization’s standard process definition to increase its effectiveness?	

PA20 Manage Systems Engineering Support Environment

Process area summary: The purpose of Manage Systems Engineering Support Environment is to provide the technology environment needed to develop the product and perform the process. Development and process technology is inserted into the environment with a goal of minimizing disruption of development activities while upgrading to make new technology available.

The technology needs to an organization change over time, and the efforts described in this process area must be re-executed as the needs evolve.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided..

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Maintain awareness of the technologies that support the organization's goals.	
Yes	**No**	**Don't Know**	Determine requirements for the organization's systems security engineering support environment based on organizational needs.	
Yes	**No**	**Don't Know**	Obtain a systems security engineering support environment that meets the requirements established in Determine Support Requirements by using the practices in the Analyze Candidate Solutions process area.	
Yes	**No**	**Don't Know**	Tailor the systems security engineering support environment to individual project's needs.	
Yes	**No**	**Don't Know**	Insert new technologies into the systems security engineering support environment based on the organization's business goals and the project's needs.	

Yes	**No**	**Don't Know**		Maintain the systems security engineering support environment to continuously support the projects dependent on it.	
Yes	**No**	**Don't Know**		Monitor the systems security engineering support environment for improvement opportunities.	

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that	

					Evidence
				planned?	____________

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	____________
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	____________
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	____________
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	____________
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	____________
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	____________
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	____________
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	____________

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	____________
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	____________

					Evidence
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	____________________

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

PA21 Provide Ongoing Skills and Knowledge

Process area summary: The purpose of Provide Ongoing Sills and Knowledge is to ensure that projects and the organization have the necessary knowledge and skills to achieve project and organizational objectives. To ensure the effective application of these critical resources that are predominantly available only from people, the knowledge and skill requirements within the organization need to be identified as well as the specific project's or organization's needs (such as those relating to emergent programs or technology, and new products, processes, and policies.)

Needed skills and knowledge can be provided both training within the organization and by timely acquisition from sources external to the organization. Acquisition form external sources may include customer resources, temporary hires, new hires, consultants, and subcontractors. In addition, knowledge may be acquired from subject matter experts.

Goals

- Ensure appropriate training of personnel, within the specified community, is provided..

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Identify needed improvements in skill and knowledge throughout the organization using the projects' needs organizational strategic plan, and existing employee skills as guidance.	
Yes	**No**	**Don't Know**	Evaluate and select the appropriate mode of acquiring knowledge or skills with respect to training or other sources.	
Yes	**No**	**Don't Know**	Ensure that appropriate skill and knowledge are available to the systems security engineering effort	
Yes	**No**	**Don't Know**	Prepare training materials based upon the identified training needs.	
Yes	**No**	**Don't Know**	Train personnel to have the skills and knowledge needed to perform their assigned roles.	
Yes	**No**	**Don't Know**	Assess the effectiveness of the training to meet the identified training needs.	

Yes	**No**	**Don't Know**		Maintain records of training and experience.	__________
Yes	**No**	**Don't Know**		Maintain training materials in an accessible repository.	__________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	__________
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	__________
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	__________
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	__________
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	__________
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	__________
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	__________
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	__________
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	__________
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	__________
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	__________
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	__________

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

PA22 Coordinate with Suppliers

Process area summary: The purpose of Coordinate with Suppliers is to address the needs of organizations to effectively manage the portions of product work that are conducted by other organizations. Decisions made as a part of this process area should be made in accordance with the Analyze Candidate Solutions process area (PA01). The general term supplier is used to identify an organization that develops, manufactures, tests, supports, etc., a component of the system. Suppliers may take the form of vendors, subcontractors, partnerships, etc., as the business organization warrants.

In addition to coordination of schedules, processes, and deliveries of work products, affected organizations must have a share vision of the working relationship. Relationships can range from integrated developer/supplier product teams, to prime-contractor/subcontractor, to vendors, and more. A successful relationship between an organization and a supplier depends on the capability of both organizations, and on a mutual understanding of the relationship and expectations.

Goals

-

1. Base Practices

Comments: Are the practices identified below performed as part of your project? Please note: you do not have to personally be involved in performing the practice -- it's enough that it is known who performs it. For any questions answered in the affirmative, please indicate supporting evidence.

				Evidence
Yes	**No**	**Don't Know**	Identify needed system components or services that must be provided by other/outside organizations	____________________
Yes	**No**	**Don't Know**	Identify suppliers that have shown expertise in the identified areas.	____________________
Yes	**No**	**Don't Know**	Choose suppliers in accordance with the Analyze Candidate Solutions process area (PA01).	____________________
Yes	**No**	**Don't Know**	Provide to suppliers the needs, expectations, and measures of effectiveness held by the organization for the system components or services that are to be delivered.	____________________
Yes	**No**	**Don't Know**	Maintain timely two-way communication with suppliers.	____________________

2. Planned and Tracked

Do those involved in performing the base practices of the Administer Security Controls process area also perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	2.1.1	Allocate adequate resources (including people) for performing the process area?	
Yes	**No**	**Don't Know**	2.1.2	Assign responsibilities for developing the work products and/or providing the services of the process area?	
Yes	**No**	**Don't Know**	2.1.3	Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?	
Yes	**No**	**Don't Know**	2.1.4	Provide appropriate tools to support performance of the process area?	
Yes	**No**	**Don't Know**	2.1.5	Ensure that the individuals performing the process are appropriately trained in how to perform the process?	
Yes	**No**	**Don't Know**	2.1.6	Plan the performance of the process?	
Yes	**No**	**Don't Know**	2.2.1	Follow documented plans and policies, standards, and/or procedures	
Yes	**No**	**Don't Know**	2.2.2	Place work products under version control or configuration management, as appropriate?	
Yes	**No**	**Don't Know**	2.3.1	Verify compliance of the process with applicable policies, standards and/or procedures?	
Yes	**No**	**Don't Know**	2.3.2	Verify compliance of work products with the applicable standards and/or requirements?	
Yes	**No**	**Don't Know**	2.4.1	Track the status of the process against the plan using measurement?	
Yes	**No**	**Don't Know**	2.4.2	Take corrective action as appropriate when progress varies significantly from that planned?	

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	3.1.1	Documenting of a standard process or family of processes in an organizational standard process definition which describes how to implement the base practices of the process area?	
Yes	**No**	**Don't Know**	3.1.2	Tailor the organizational standard process definition to meet the needs of a specific use?	
Yes	**No**	**Don't Know**	3.2.1	Follow the tailored version of the organizational standard process definition?	
Yes	**No**	**Don't Know**	3.2.2	Perform defect reviews of appropriate work products?	
Yes	**No**	**Don't Know**	3.2.3	Use data on performing the defined process to manage the defined process?	
Yes	**No**	**Don't Know**	3.3.1	Coordinate communication within the security engineering group?	
Yes	**No**	**Don't Know**	3.3.2	Coordinate communication among the various groups within your project/organization?	
Yes	**No**	**Don't Know**	3.3.3	Coordinate communication with external groups?	

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	4.1.1	Establishing measurable quality goals for the work products of the organization's standard process family?	
Yes	**No**	**Don't Know**	4.2.1	Determine the process capability of the defined process quantitatively?	
Yes	**No**	**Don't Know**	4.2.2	Take corrective action as appropriate when the defined process is not performing within its process capability?	

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes? For any questions answered in the affirmative, please indicate supporting evidence.

					Evidence
Yes	**No**	**Don't Know**	5.1.1	Establishing quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability?	____________________
Yes	**No**	**Don't Know**	5.2.1	Perform causal analysis of defects?	____________________
Yes	**No**	**Don't Know**	5.2.2	Eliminate the causes of defects in the defined process selectively?	____________________
Yes	**No**	**Don't Know**	5.2.3	Continuously improve performance of the defined process, incorporating all changes in its process definition?	____________________
Yes	**No**	**Don't Know**	5.2.4	Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?	____________________

Appendix E Data Tracking Sheet [DTS]

Purpose

The Data Tracking Sheet (DTS) is a spreadsheet tool used to assist the team in recording and analyzing information gathered throughout the appraisal. Although there are some automated calculations of ratings included in the DTS, all of the data inputs and analysis must be conducted by the team. The structure of the DTS allows for attribution of information to those that provide it. This is done so that the team may properly determine if responses are an indicator of individual knowledge and practice, or truly reflective of an organization.

Description

The DTS has four major sections PAs, Questionnaire Responses, Interview Responses, and Evidence Acceptance. Each of these sections is further broken down into several subsections.

"SSAMv2_0 DTS.xls"

PAs

All of the PAs covered in the appraisal are listed in the far-left columns of the spreadsheet. Each Base and Generic Practices are listed in individual rows. The Generic Practices are listed for each PA.

Questionnaire Responses

The Questionnaire Response columns are used to record responses given by the Appraised Organization to the Questionnaire, and provide a preliminary view of the Appraised Organization’s rating profile. This preliminary view gives the Appraisal Team an idea of how close the Appraised Organization is to meeting a particular level. This Questionnaire section of the DTS is divided into two sections; Preparation and On-Site Phase. It is expected that an Appraised Organization as a whole, or individual projects involved in the assessment will generate the responses for the administration of the questionnaire during the Preparation phase so the column headings are labeled O1, O2, and O3. During the On-Site Phase the Questionnaire is administered to individual project leads, so the response columns are identified as L1, L2, and L3.

Recording Questionnaire Responses

Respondent answers to the Questionnaire are transferred to the electronic DTS in the following manner:

- *A yes* answer is entered as a *1*,
- *A no* answer is entered as a *0*,and
- *A don't know* or *blank* answer is entered as a*?*.

The same translation scheme is used for transferring responses gathered in both the Preparation and On-Site Phases.

Preliminary/Guidance Rating

A preliminary/guidance rating is calculated as the percentage of *yes* and *no* responses that are *yes*. *Blank* and *don't know* responses are not included in the calculation. This view of the ratings, particularly those generated from the On-Site section, serve as a starting point for the Team's development of questions for the Interview Project Leads (2.3.5) stage.

Interview Reponses

The same tracking sheet is used to record responses given during the three interview stages (Project Lead, Practitioner, and Follow-Up). Like the Questionnaire responses, the interview responses are tracked by respondent, and are grouped according to project. However, the method for recording that information differs significantly from the previous process. The purpose of the Project Lead and Practitioner Interviews is to verify not only that a particular systems security engineering process is practiced by an organization, but that there is evidence to support the claim.

Recording Responses

To accomplish this verification task, interview responses are tracked according the evidence provided by the interviewee. The team uniquely labels all evidence with an alphanumeric identifier (see Appendix F). Evidence sited by an interviewee that the team determines is credible, relevant, and proven to exist, is entered into the DTS for the BP or GP being addressed. (Guidance for evidence is found in Chapter 4.) If the cited evidence is proved not to exist or determined to be irrelevant, or the interviewee is unable to answer the question, then a zero is entered into the DTS for that person for the BP or GP being discussed. If the interviewee is not asked a question about a particular BP or GP, then the corresponding cell is left blank.

Evidence Acceptance

By analyzing all of the evidence supplied and how it is used by the Appraised Organization the Appraisal Team makes a determination as to the Appraised Organization's Final Rating.

Pass/Fail

The Appraisal Team determines if the evidence supplied by Appraised Organization and the interpretations of its use, as reflected in the DTS, is sufficient to give the Appraised Organization credit for implementing a BP or GP.

Evidence Acceptance

- For BPs and GPs where provided evidence is deemed sufficient enter the identifier for the corresponding evidence that proves compliance in the corresponding cell.
- For BPs and GPs where provided evidence is deemed insufficient or no evidence is provided enter a 0.
- For BPs and GPs where no questions were asked during the interview stages, and lower dependant BPs or GPs have an evidence determination of 0, enter a 0 in the corresponding cell.
- For BPs and GPs where no questions were asked during the interview stages, and no lower dependant BPs or GPs have an evidence determination of 0, leave the corresponding cell blank.

Final Rating

The final rating is automatically calculated for each PA at each level.

Appendix F Evidence Tracking Sheet [ETS]

Because evidence identification, collection, use and disposal is such an important element of the appraisal process, four tools have been developed to assist the Evidence Custodian track the flow of evidence materials; Evidence Request Form, Evidence Request Tracking Sheet, Evidence Use Tracking Sheet, and Evidence Disposal Tracking Sheet. At the end of the appraisal the Evidence Request Form may be destroyed, but the completed tracking sheets must be forwarded to the Sponsor.

Evidence Request Form

This form is used by the Appraisal Team to request documents from the Site Coordinator. To maintain the confidentiality of the appraisal participants and team members, the request form does not identify who identified the existence of a particular piece of evidence or who on the Appraisal Team requested to see it.

Evidence Request Tracking Sheet

Used in conjunction with the Request Form, this spreadsheet allows the Evidence Custodian to track the Appraised Organization’s compliance with all requests for evidence.

Evidence Use Tracking Sheet

This sheet logs the use of each piece of evidence by the Appraisal Team.

Evidence Disposal Tracking Sheet

This sheet logs the disposal (forwarding to Sponsor or destruction) of evidence and intermittent work products of the Appraisal Team.

Evidence Request Form

Evidence Custodian: ______________________________________

Site Coordinator: ______________________________________

Date Requested: ______________________________________

Evidence Format: ______________________________________

Evidence Title: ______________________________________

____

Evidence Description: ______________________________________

____

____

Date Received: ______________________________________

Evidence Request Tracking Sheet

Evidence #	Title	Description	Appraisal Team Member	Date/Time Requested	Date/Time Received	Date/Time Returned
1	SSE-CMM Handbook for XYZ Company	Description of SSE-CMM as interpreted by XYZ Company	SSAM guy	12/9/1998 12:00pm	12/9/98 12:30pm	12/10/1998 2:30pm

Evidence Use Tracking Sheet

Appraisal Team Member	PA	BP/CL	Project Member	Type	Title	Description	Date Received	Evidence #
SSAM guy	PA 01	BP1	PL1	Document	SSE-CMM Handbook for XYZ Company	Description of SSE-CMM as interpreted by XYZ Company	12/10/98	1

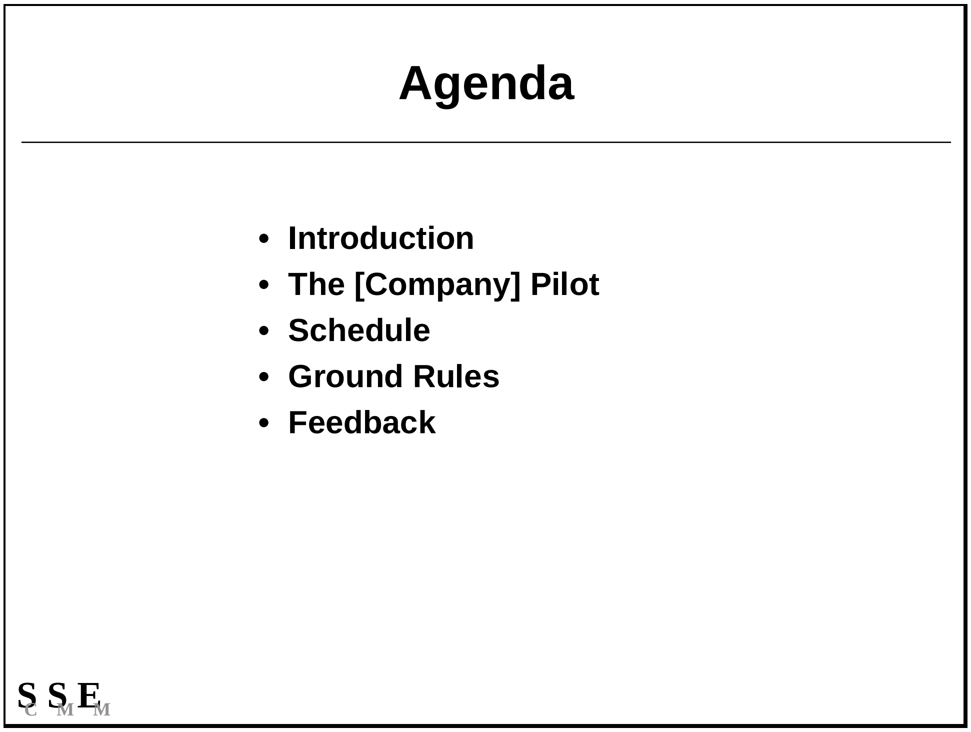
Evidence Disposal Tracking Sheet

Evidence #	Title	Description	Date/Time Destroyed	Means	Date/Time To Sponsor	Means	Date/Time Received by Sponsor
1	SSE-CMM Handbook for XYZ Company	Description of SSE-CMM as interpreted by XYZ Company	N/A	N/A	12/12/1998 12:00pm	FedEx	12/13/98 12:30pm
2	Appraisal Team notes	Internal notes of Appraisal Team taken during meeting	12/13/1998 1:00am	Burn Bag	N/A	N/A	N/A

Appendix G Opening and Closing Briefings

Opening Briefing

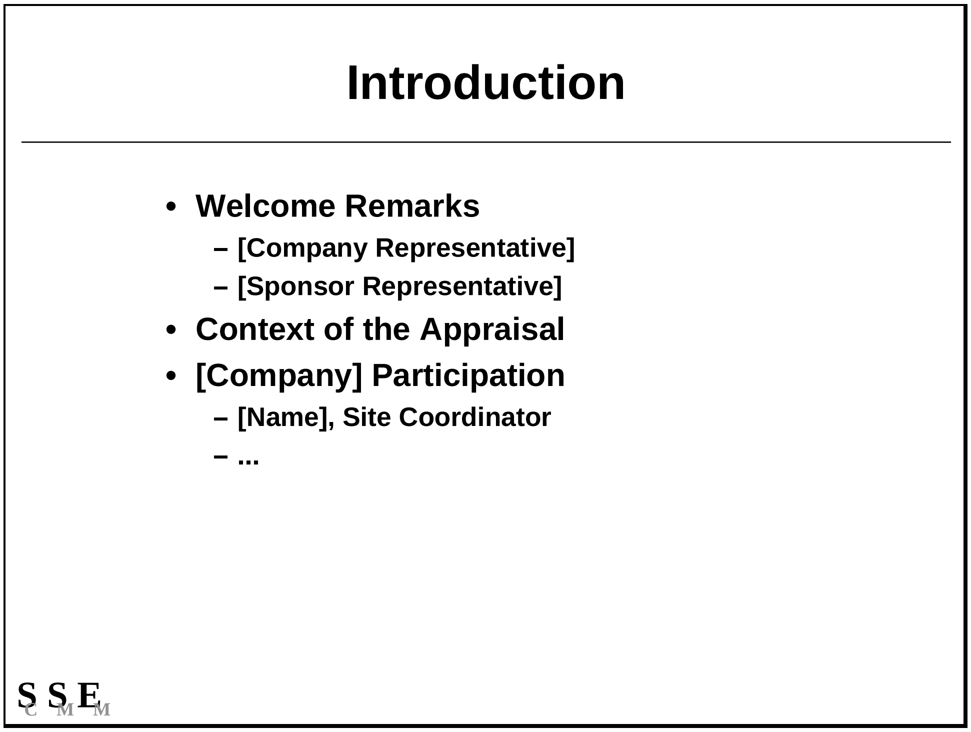
The Appraisal Plan provides the specific information for the Opening Briefing.



Agenda

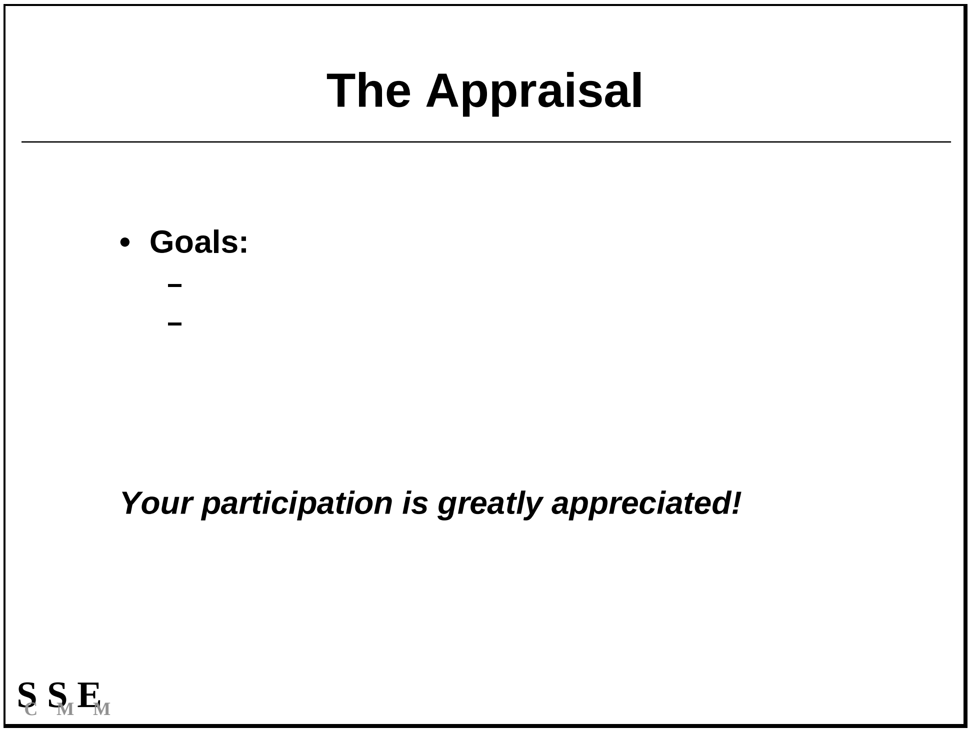
- Introduction
- The [Company] Pilot
- Schedule
- Ground Rules
- Feedback

SSE CMM



Introduction

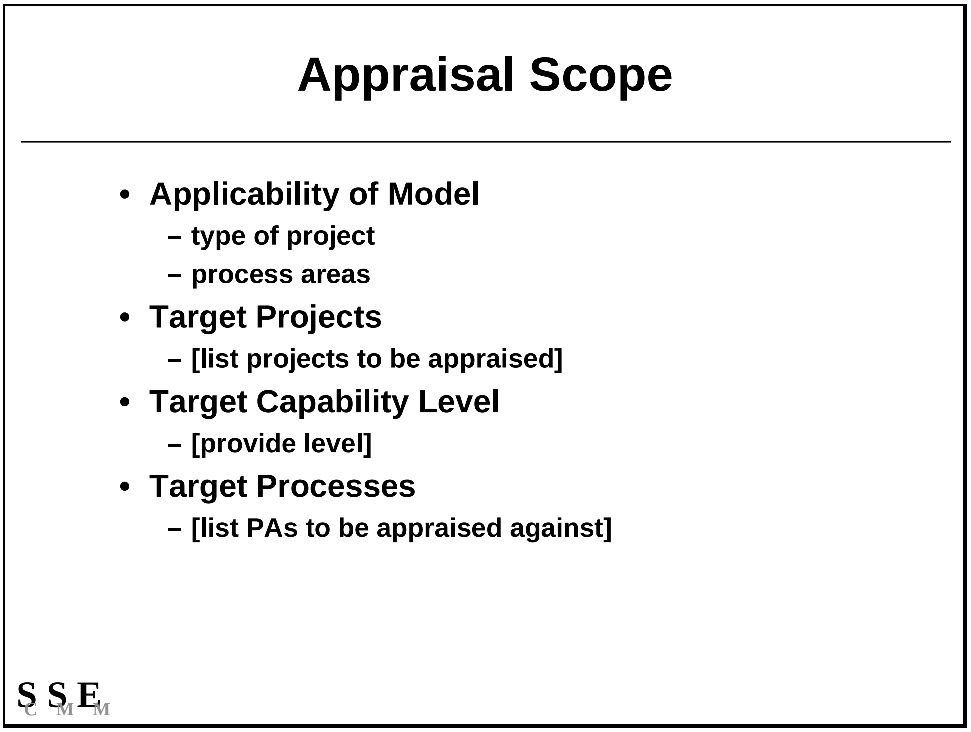
- Welcome Remarks
  - [Company Representative]
  - [Sponsor Representative]
- Context of the Appraisal
- [Company] Participation
  - [Name], Site Coordinator
  - ...



The Appraisal

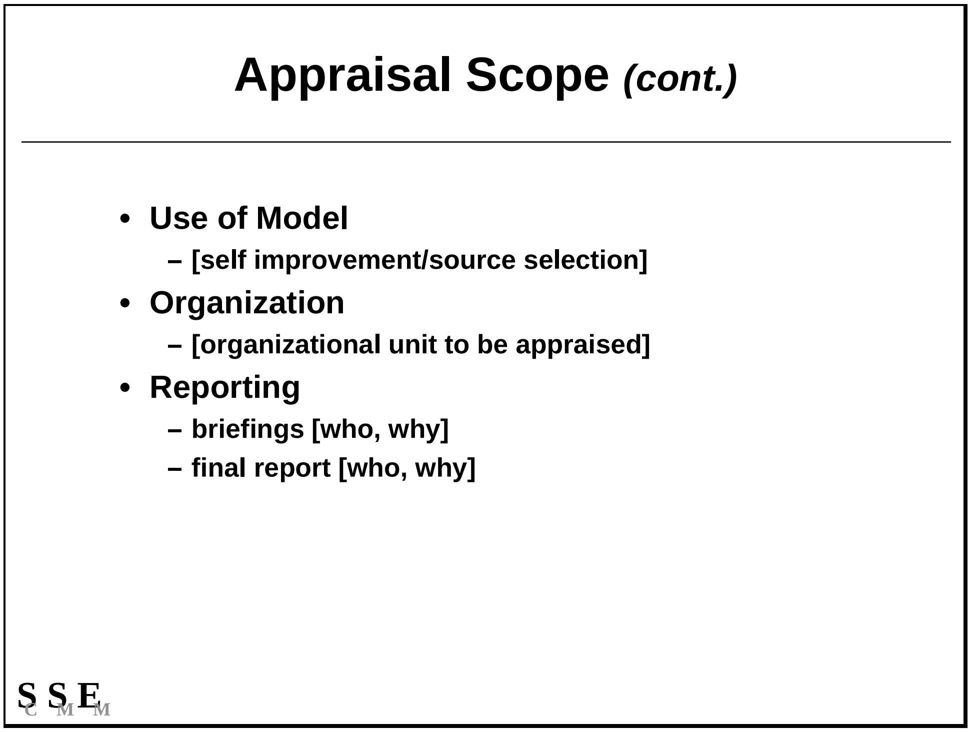
- Goals:
  -
  -

Your participation is greatly appreciated!



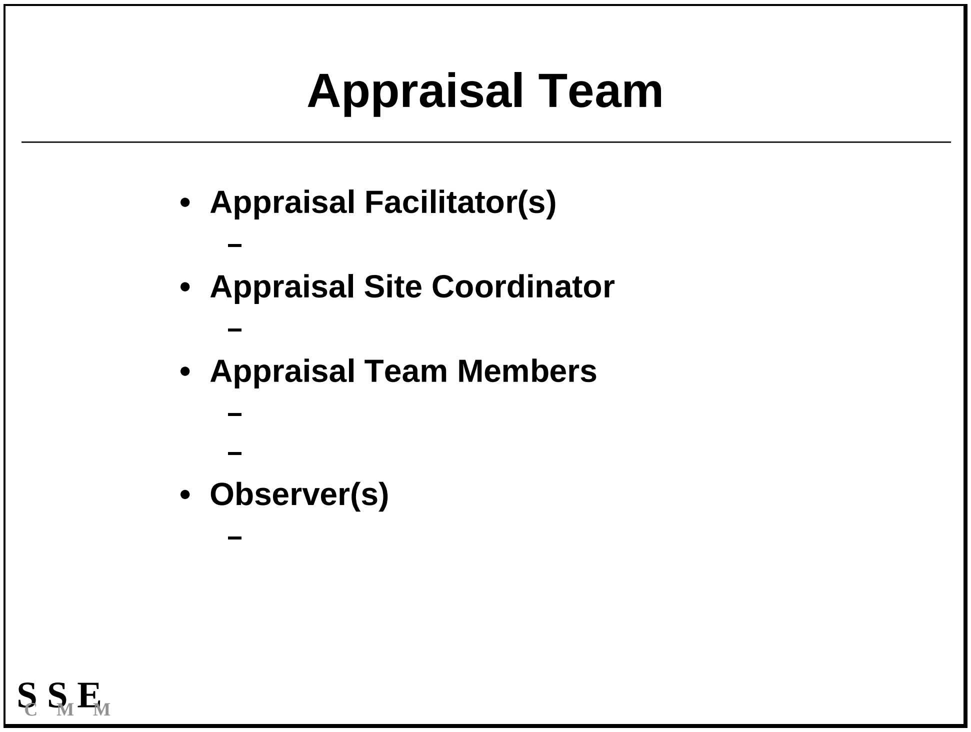
Appraisal Scope

- Applicability of Model
  - type of project
  - process areas
- Target Projects
  - [list projects to be appraised]
- Target Capability Level
  - [provide level]
- Target Processes
  - [list PAs to be appraised against]



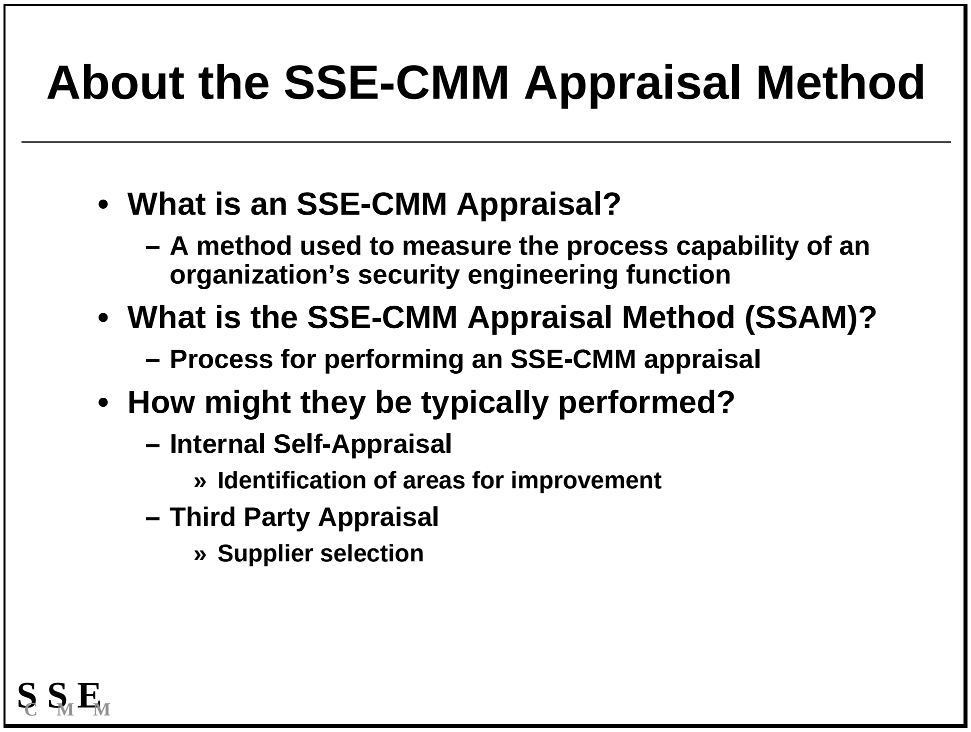
Appraisal Scope *(cont.)*

- Use of Model
  - [self improvement/source selection]
- Organization
  - [organizational unit to be appraised]
- Reporting
  - briefings [who, why]
  - final report [who, why]



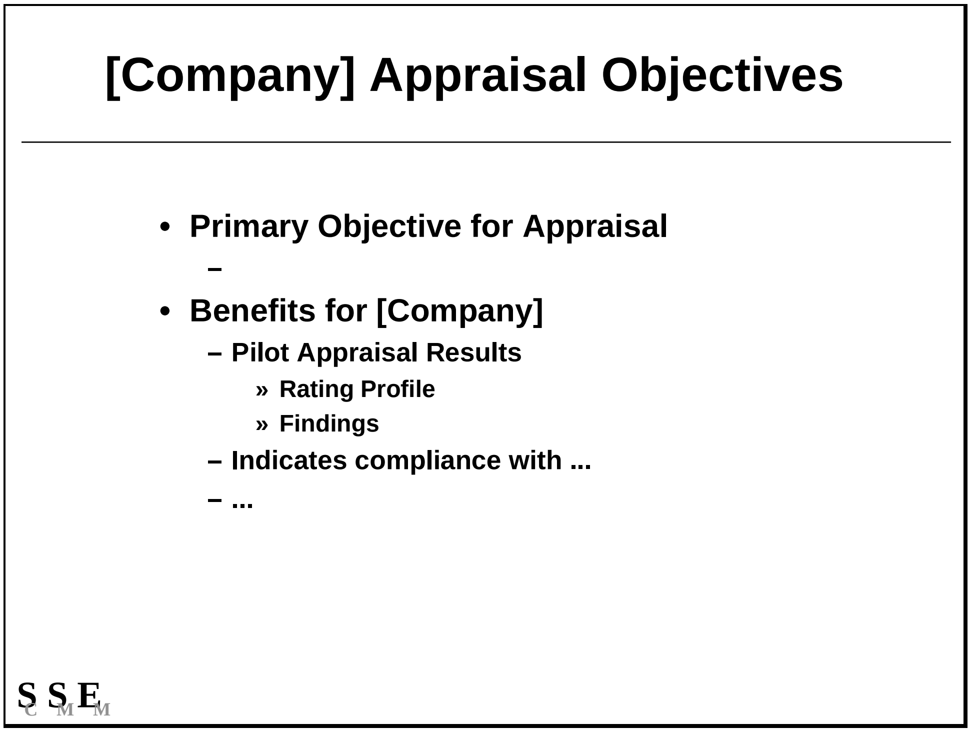
Appraisal Team

- Appraisal Facilitator(s)
  - –
- Appraisal Site Coordinator
  - –
- Appraisal Team Members
  - –
  - –
- Observer(s)
  - –



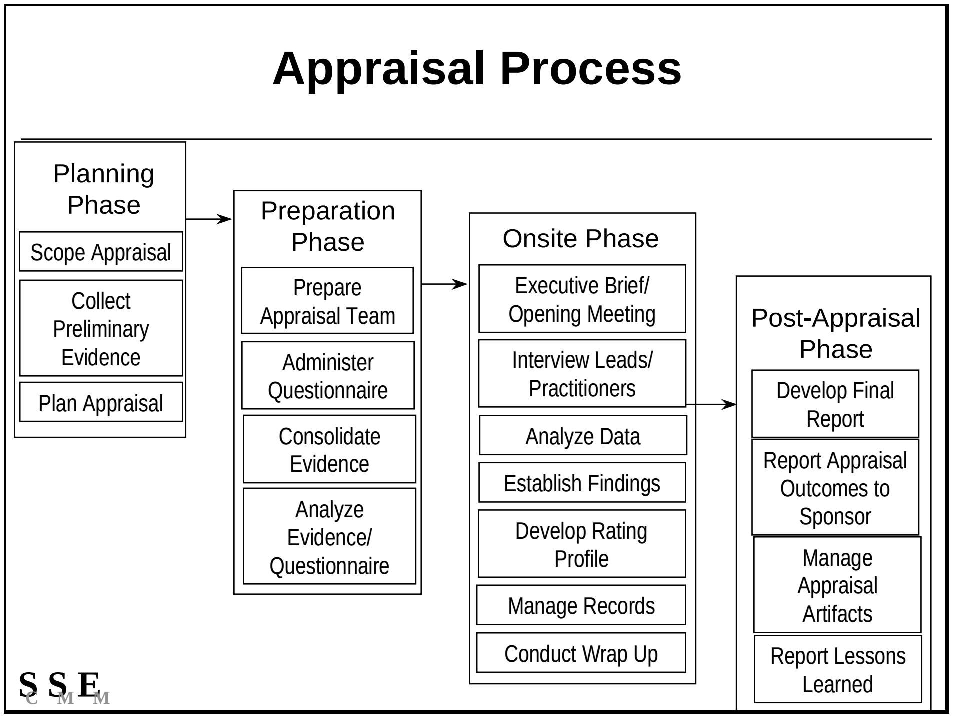
About the SSE-CMM Appraisal Method

- What is an SSE-CMM Appraisal?
  - – A method used to measure the process capability of an organization’s security engineering function
- What is the SSE-CMM Appraisal Method (SSAM)?
  - – Process for performing an SSE-CMM appraisal
- How might they be typically performed?
  - – Internal Self-Appraisal
    - » Identification of areas for improvement
  - – Third Party Appraisal
    - » Supplier selection



[Company] Appraisal Objectives

- Primary Objective for Appraisal
  - –
- Benefits for [Company]
  - Pilot Appraisal Results
    - » Rating Profile
    - » Findings
  - Indicates compliance with ...
  - ...



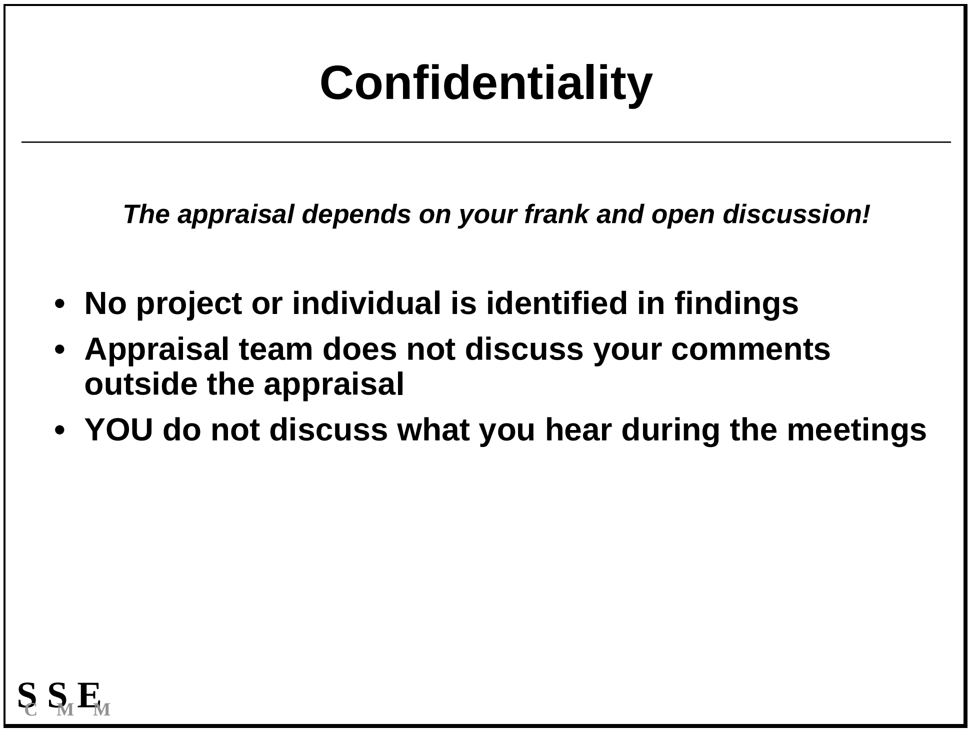
Appraisal Process

Planning Phase
- Scope Appraisal
- Collect Preliminary Evidence
- Plan Appraisal

Preparation Phase
- Prepare Appraisal Team
- Administer Questionnaire
- Consolidate Evidence
- Analyze Evidence/ Questionnaire

Onsite Phase
- Executive Brief/ Opening Meeting
- Interview Leads/ Practitioners
- Analyze Data
- Establish Findings
- Develop Rating Profile
- Manage Records
- Conduct Wrap Up

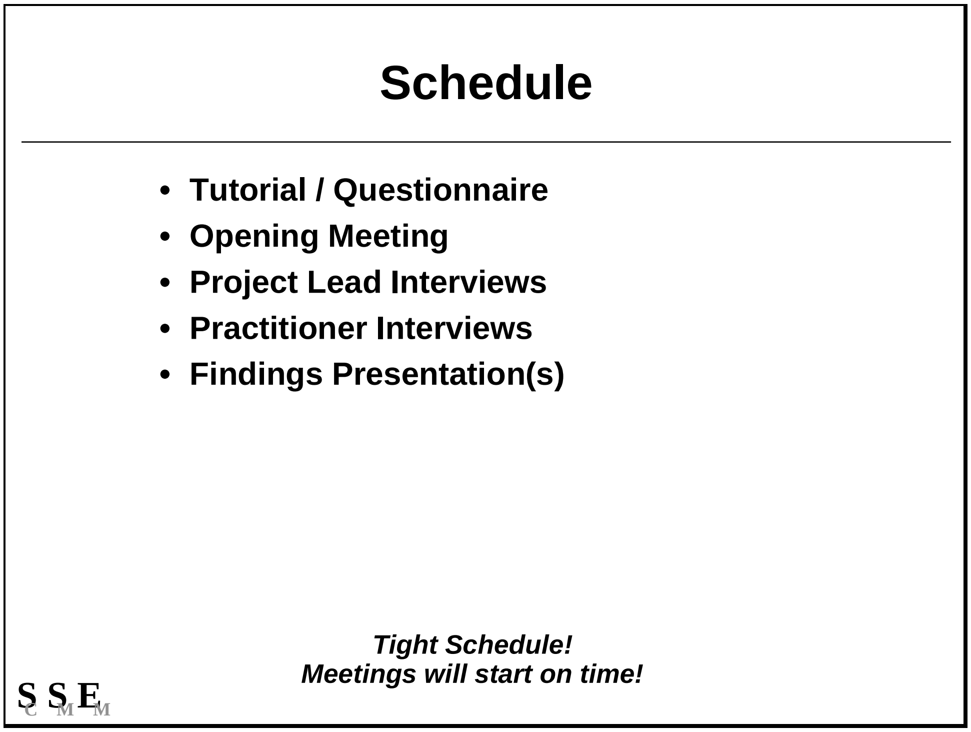
Post-Appraisal Phase
- Develop Final Report
- Report Appraisal Outcomes to Sponsor
- Manage Appraisal Artifacts
- Report Lessons Learned



Confidentiality

The appraisal depends on your frank and open discussion!

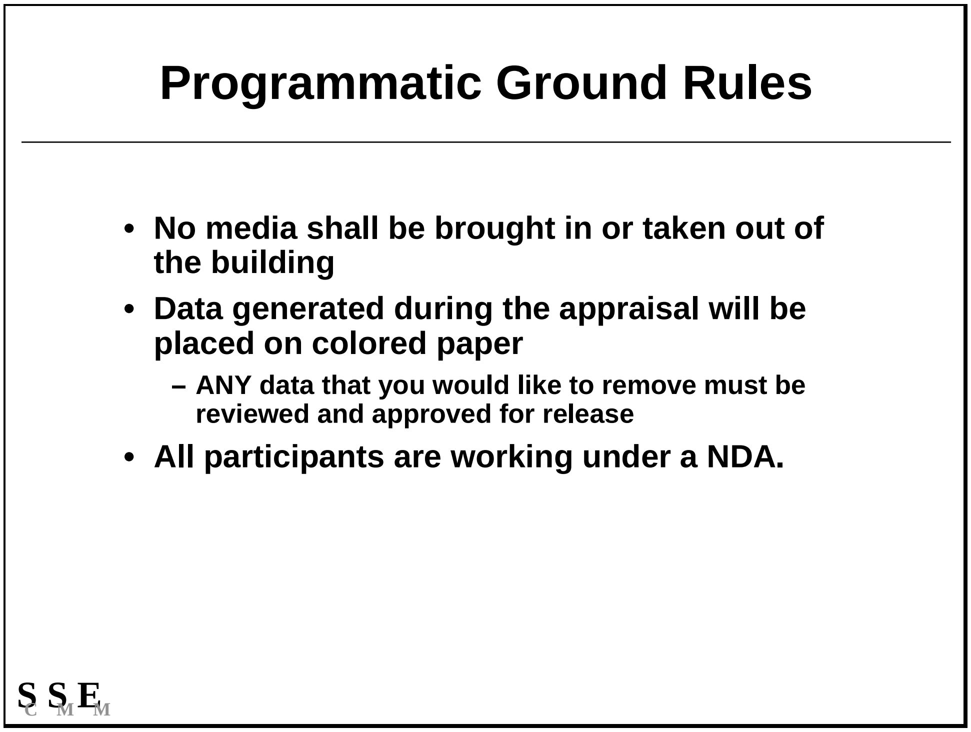
- **No project or individual is identified in findings**
- **Appraisal team does not discuss your comments outside the appraisal**
- **YOU do not discuss what you hear during the meetings**



Schedule

- **Tutorial / Questionnaire**
- **Opening Meeting**
- **Project Lead Interviews**
- **Practitioner Interviews**
- **Findings Presentation(s)**

Tight Schedule!
Meetings will start on time!



Programmatic Ground Rules

- No media shall be brought in or taken out of the building
- Data generated during the appraisal will be placed on colored paper
  - ANY data that you would like to remove must be reviewed and approved for release
- All participants are working under a NDA.

S S E C M M

Closing Briefing

Systems Security Engineering

S S E C M M

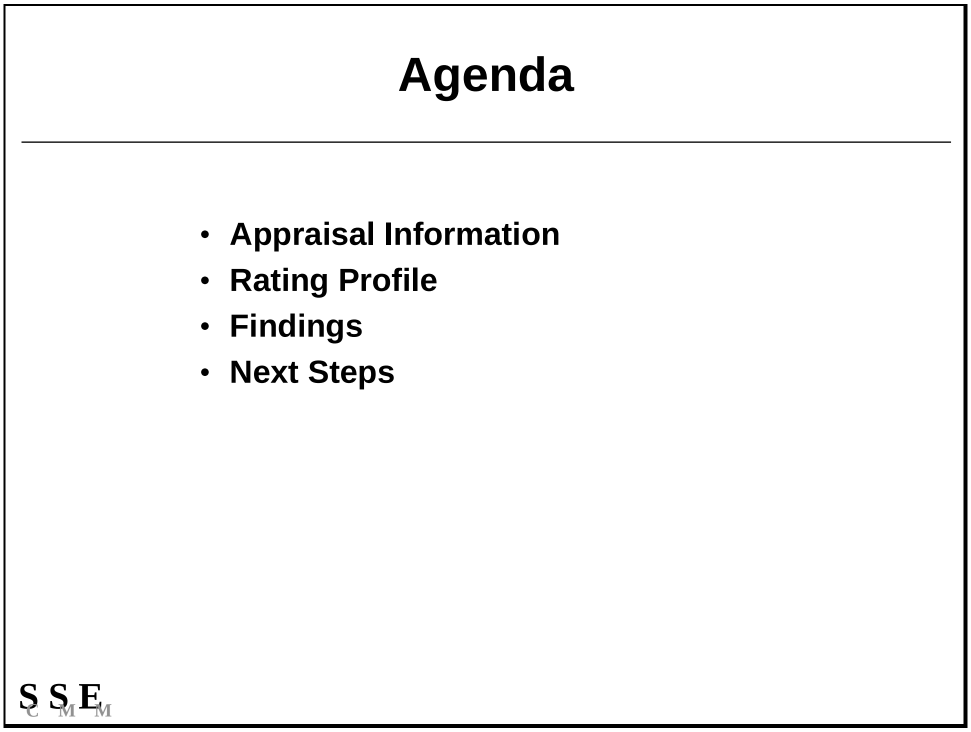
Capability Maturity Model

[Company Name]
SSE-CMM Appraisal

Closing Briefing

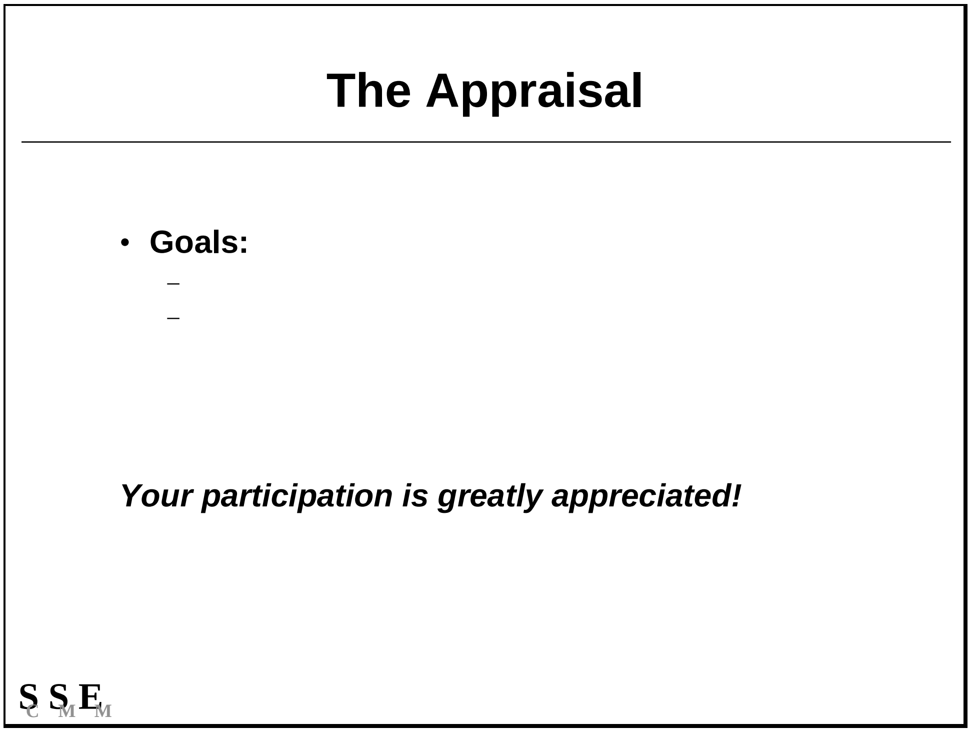
[Date]

S S E C M M



Agenda

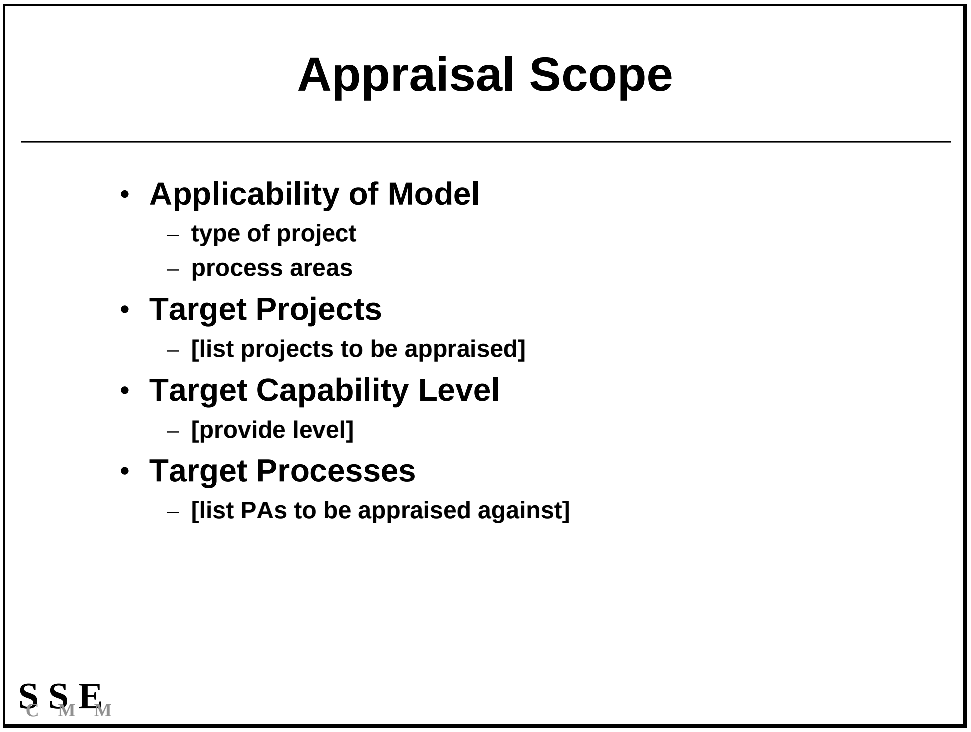
- Appraisal Information
- Rating Profile
- Findings
- Next Steps



The Appraisal

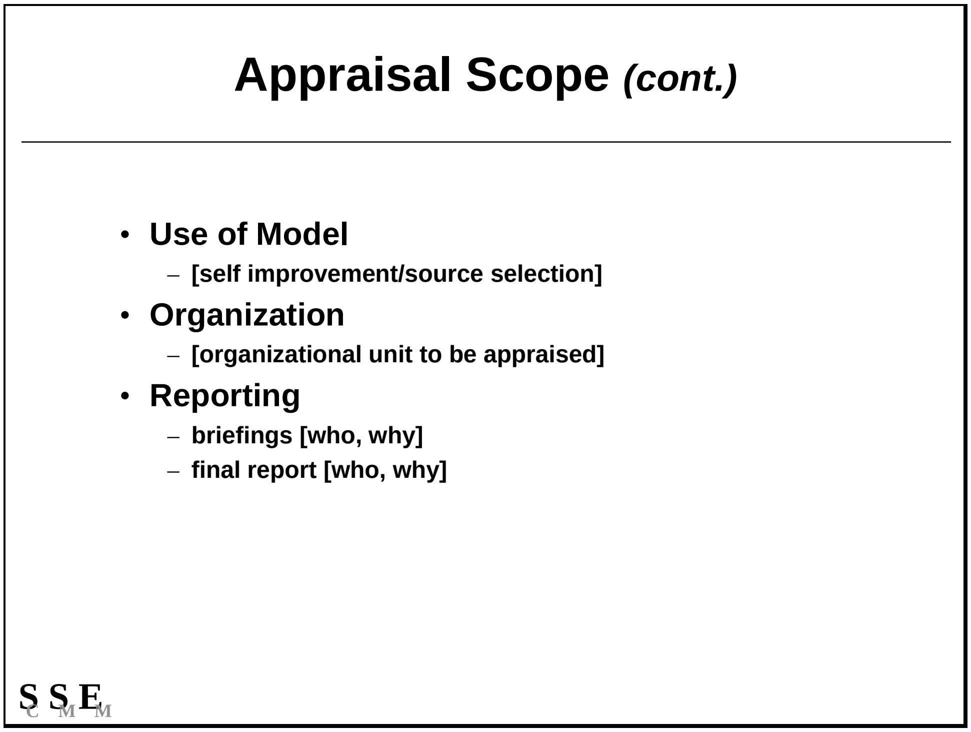
- Goals:
  - –
  - –

Your participation is greatly appreciated!



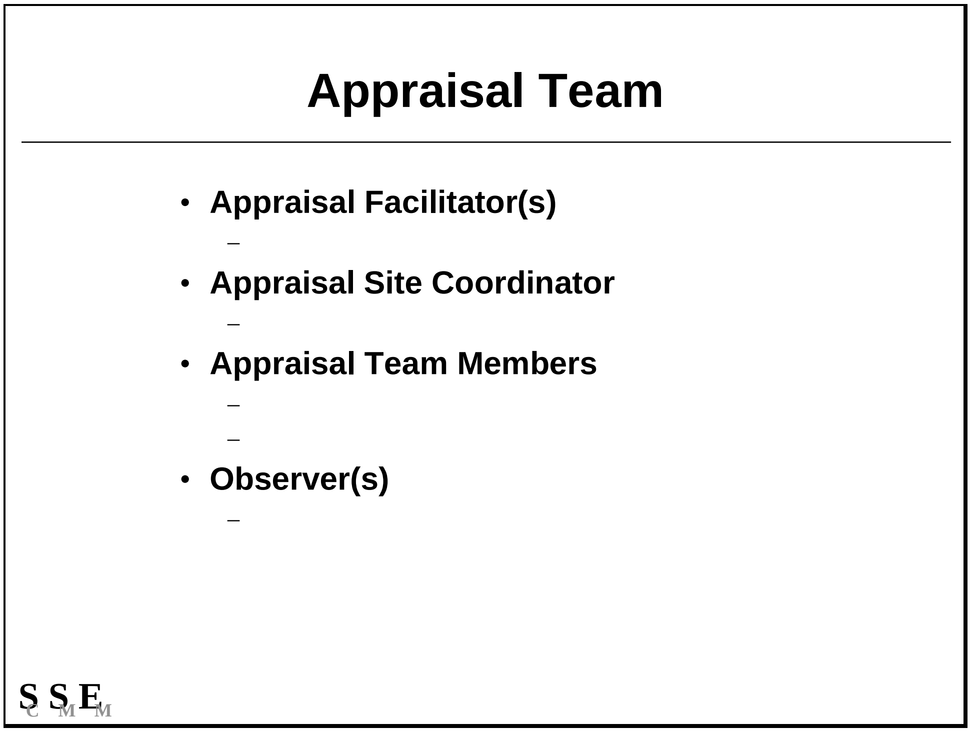
Appraisal Scope

- Applicability of Model
  - type of project
  - process areas
- Target Projects
  - [list projects to be appraised]
- Target Capability Level
  - [provide level]
- Target Processes
  - [list PAs to be appraised against]



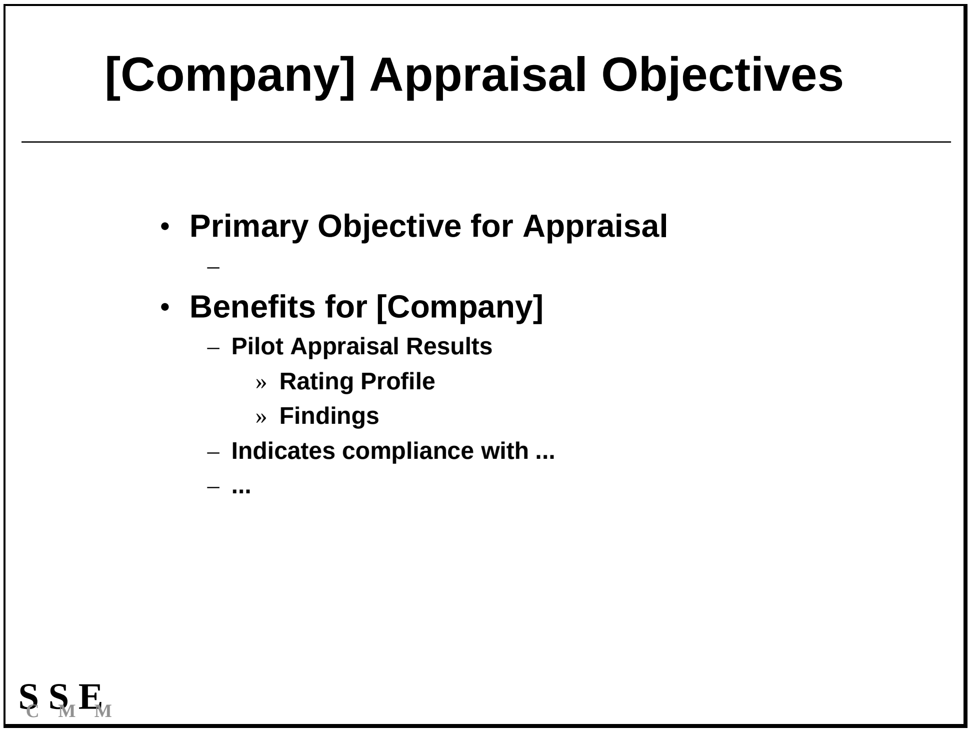
Appraisal Scope *(cont.)*

- Use of Model
  - [self improvement/source selection]
- Organization
  - [organizational unit to be appraised]
- Reporting
  - briefings [who, why]
  - final report [who, why]



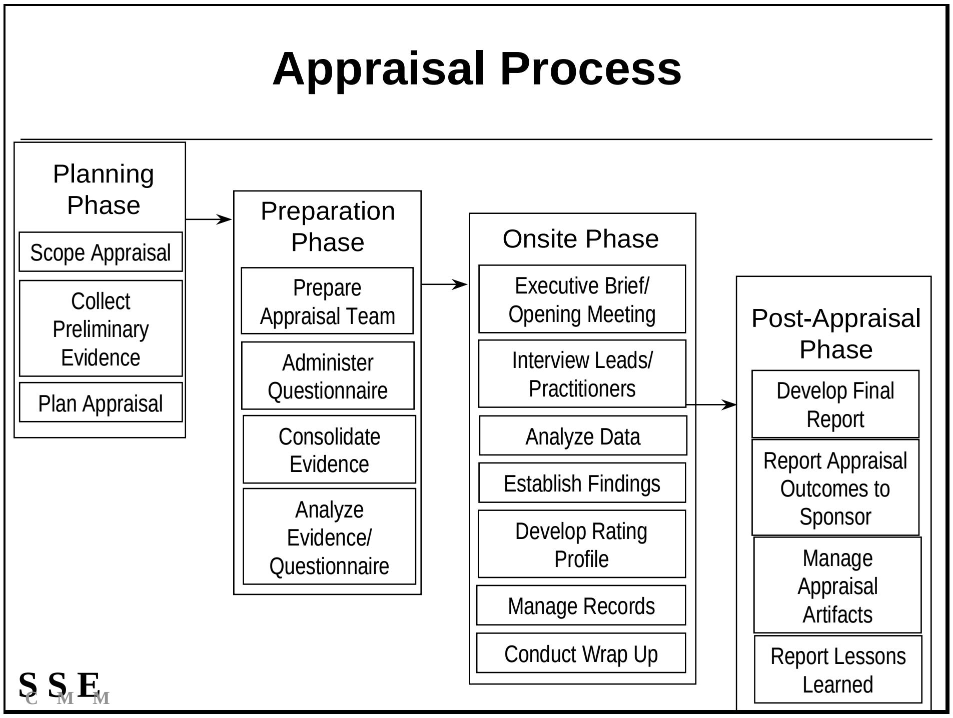
Appraisal Team

- Appraisal Facilitator(s)
  - –
- Appraisal Site Coordinator
  - –
- Appraisal Team Members
  - –
  - –
- Observer(s)
  - –



[Company] Appraisal Objectives

- Primary Objective for Appraisal
  - –
- Benefits for [Company]
  - Pilot Appraisal Results
    - » Rating Profile
    - » Findings
  - Indicates compliance with ...
  - ...



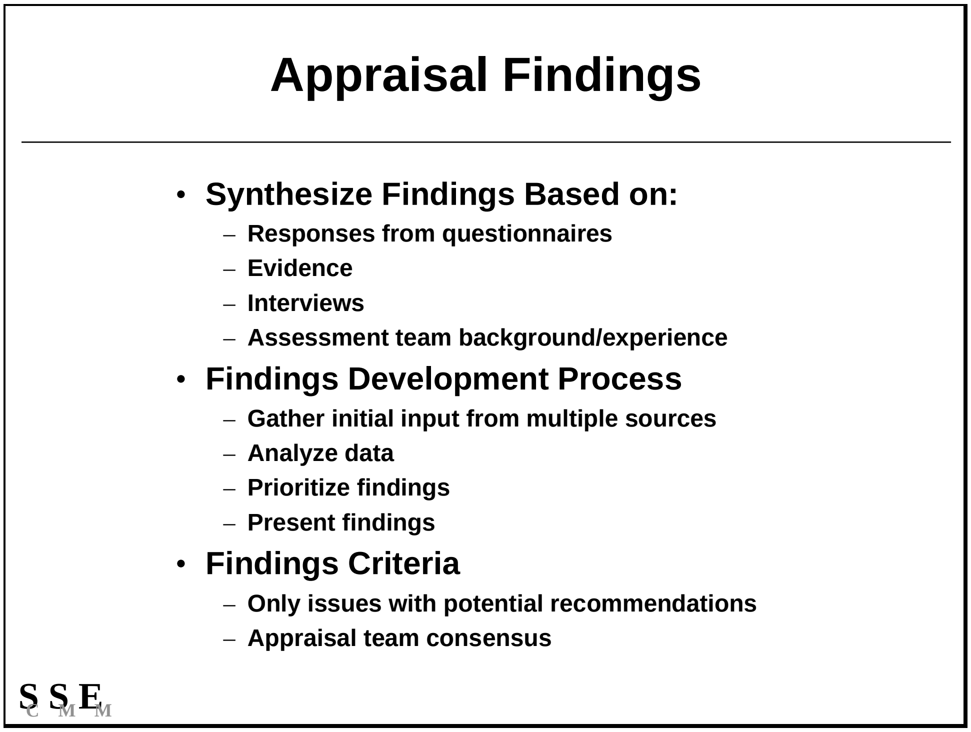
Appraisal Process

Planning Phase
- Scope Appraisal
- Collect Preliminary Evidence
- Plan Appraisal

Preparation Phase
- Prepare Appraisal Team
- Administer Questionnaire
- Consolidate Evidence
- Analyze Evidence/ Questionnaire

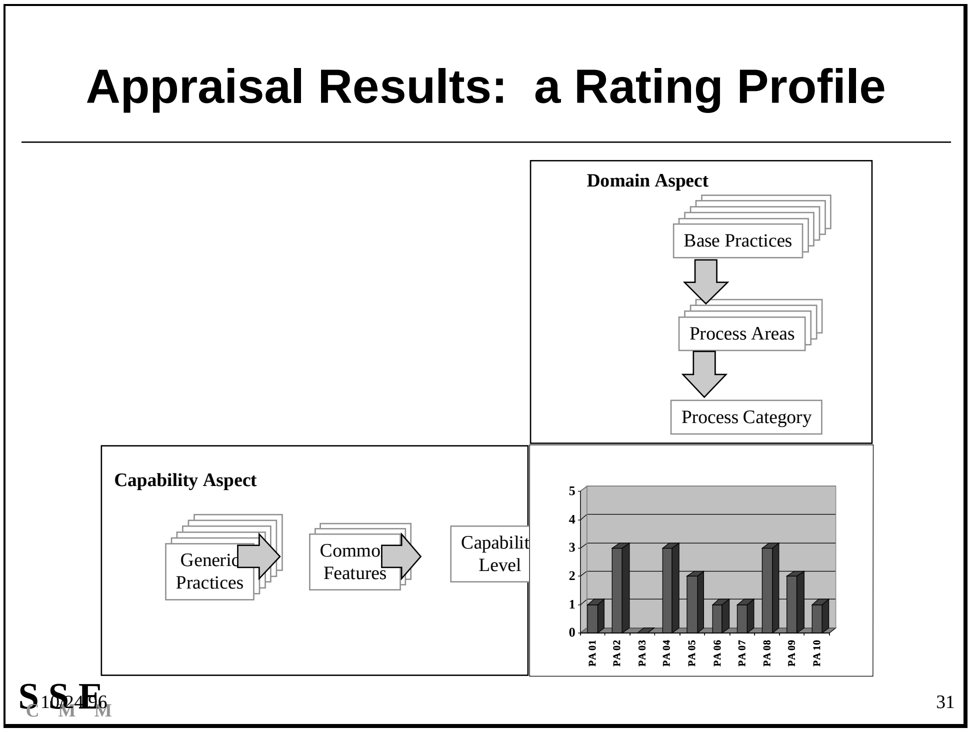
Onsite Phase
- Executive Brief/ Opening Meeting
- Interview Leads/ Practitioners
- Analyze Data
- Establish Findings
- Develop Rating Profile
- Manage Records
- Conduct Wrap Up

Post-Appraisal Phase
- Develop Final Report
- Report Appraisal Outcomes to Sponsor
- Manage Appraisal Artifacts
- Report Lessons Learned



Appraisal Findings

- **Synthesize Findings Based on:**
  - **Responses from questionnaires**
  - **Evidence**
  - **Interviews**
  - **Assessment team background/experience**
- **Findings Development Process**
  - **Gather initial input from multiple sources**
  - **Analyze data**
  - **Prioritize findings**
  - **Present findings**
- **Findings Criteria**
  - **Only issues with potential recommendations**
  - **Appraisal team consensus**



Appraisal Results: a Rating Profile

Domain Aspect

Base Practices

Process Areas

Process Category

Capability Aspect

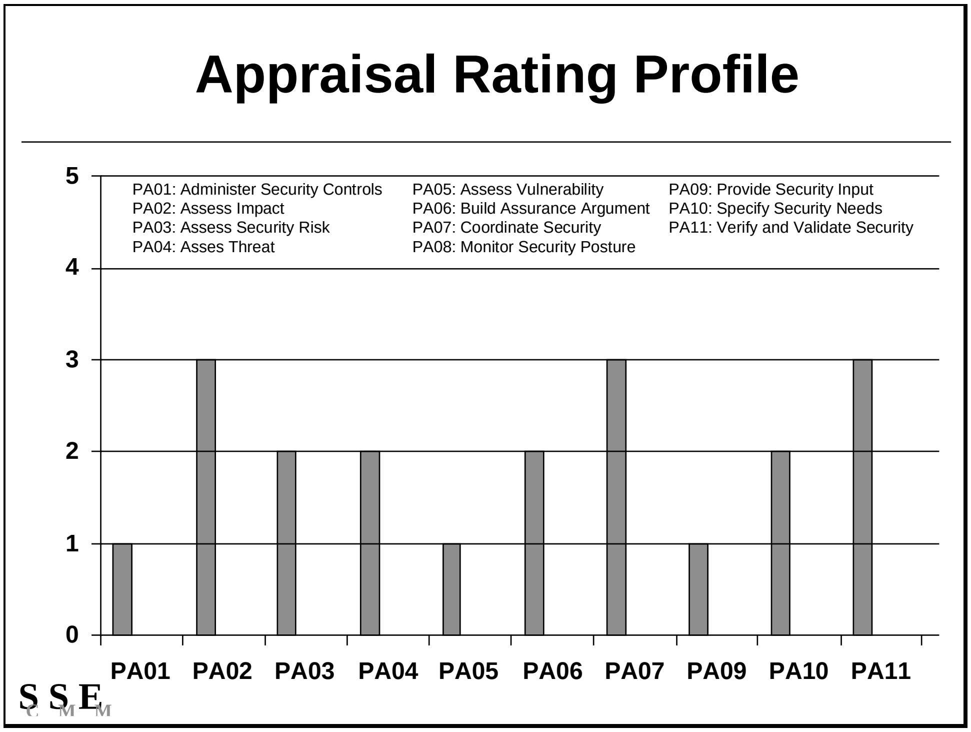
Generic Practices

Common Features

Capability Level

SSE CMM 10/24/96

31



Appraisal Rating Profile

PA01: Administer Security Controls
PA02: Assess Impact
PA03: Assess Security Risk
PA04: Asses Threat
PA05: Assess Vulnerability
PA06: Build Assurance Argument
PA07: Coordinate Security
PA08: Monitor Security Posture
PA09: Provide Security Input
PA10: Specify Security Needs
PA11: Verify and Validate Security

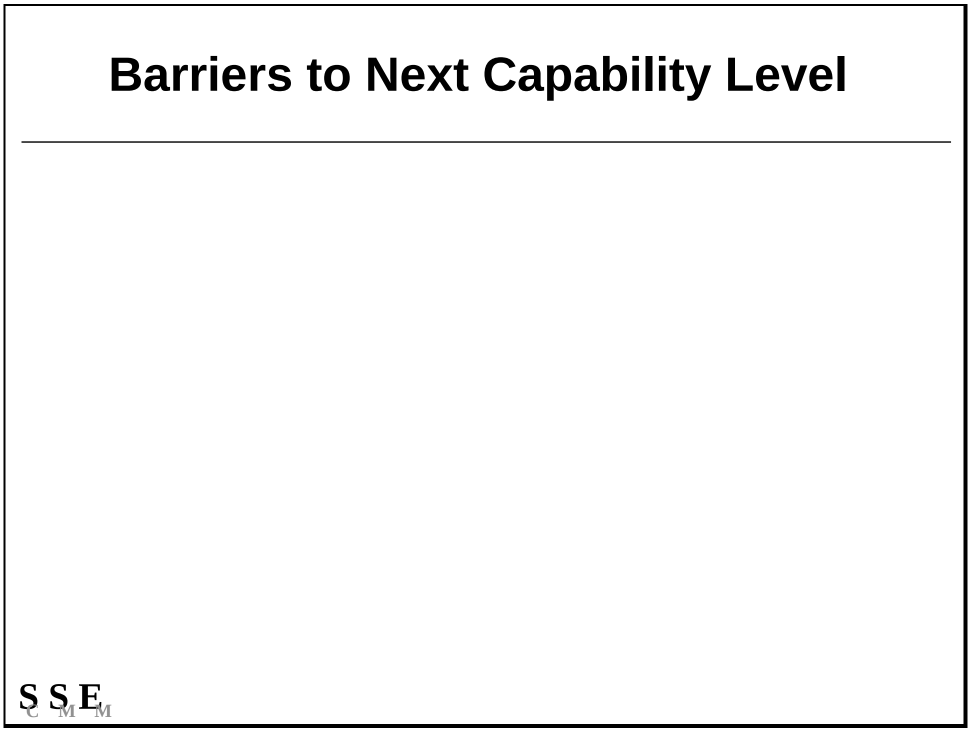
SSE CMM

Findings

•

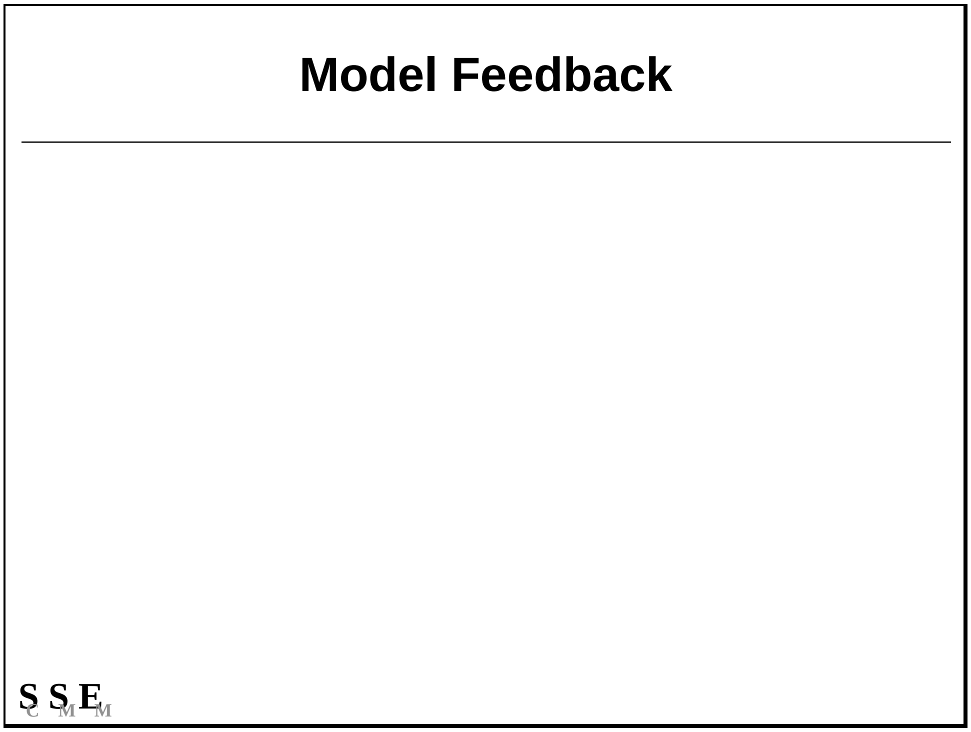
–

S S E
C M M

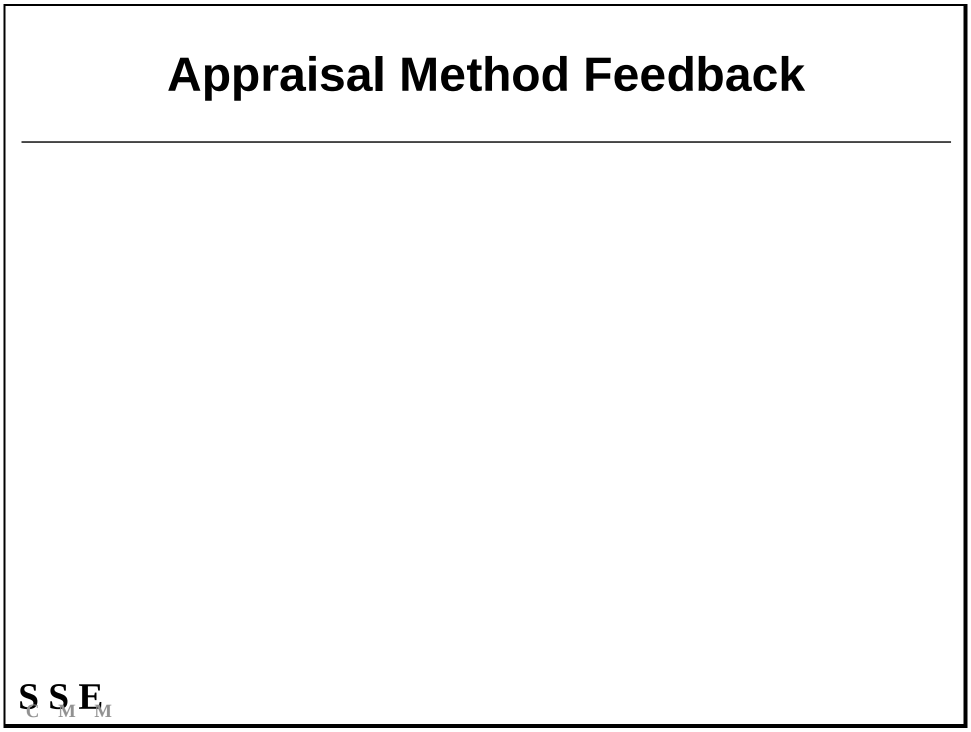


Barriers to Next Capability Level

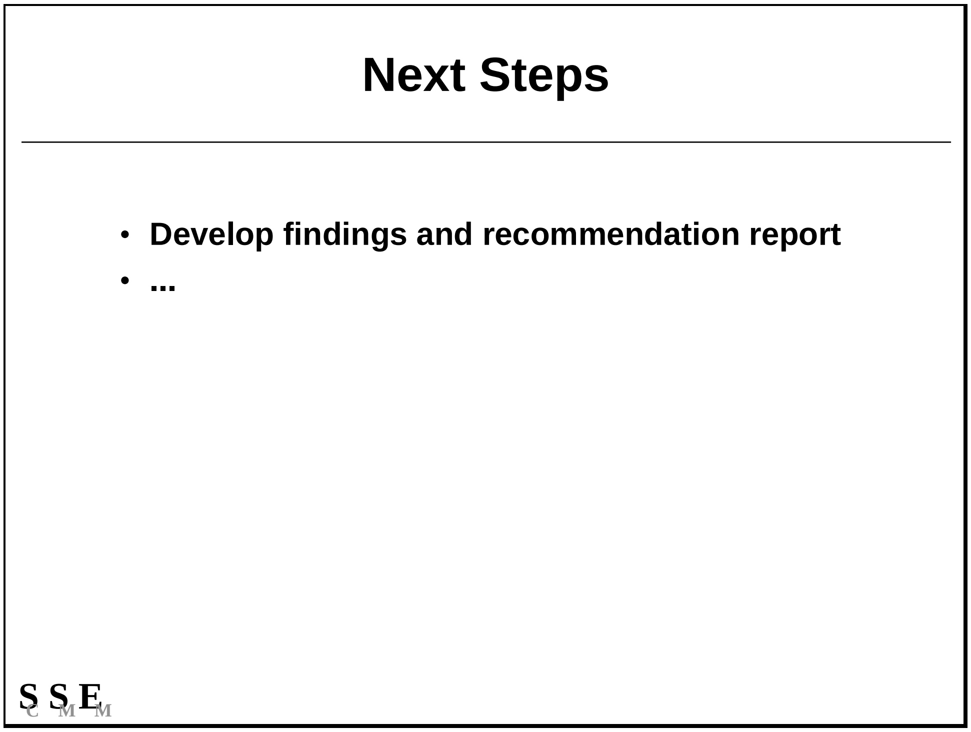
S S E
C M M



Model Feedback

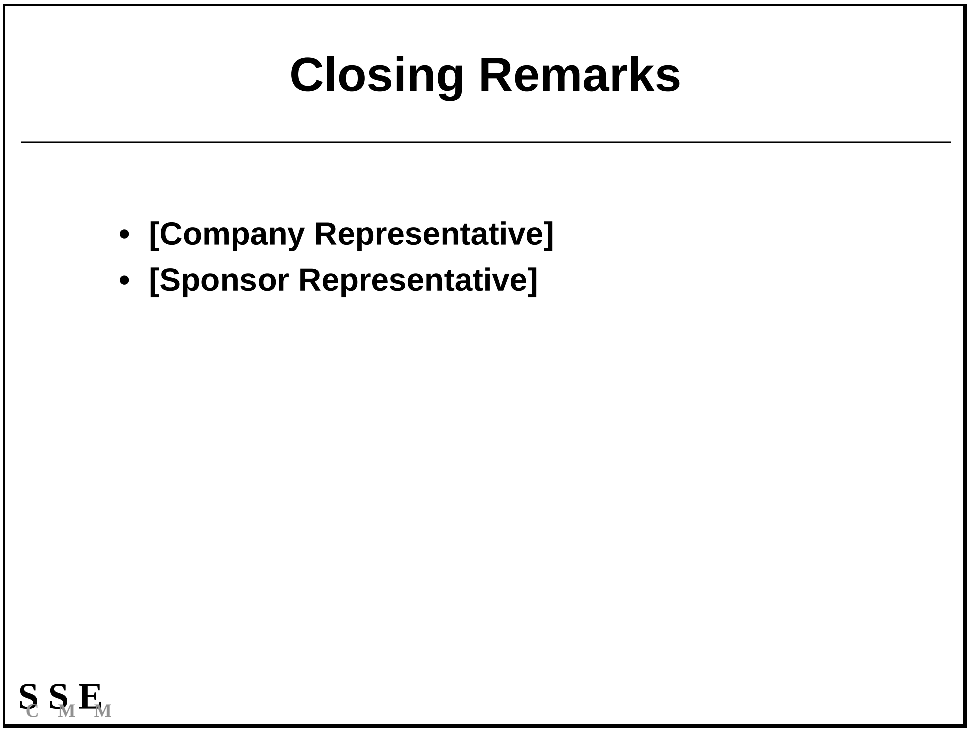


Appraisal Method Feedback



Next Steps

- Develop findings and recommendation report
- ...



Closing Remarks

- [Company Representative]
- [Sponsor Representative]

Appendix H References

Introduction

This appendix provides the references for documents cited within the SSAM.

Reference List

[SSECMM] *Systems Security Engineering Capability Maturity Model, Model Description Document, Version 2.0b*, October 5, 1998.

[SECMM] Kuhn, Dorothy A., Wells, Curtis, et. al., *A Systems Engineering Capability Maturity Model, Version 1.1,* (SECMM-94-06|CMU/SEI-96-HB-04). Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute: March 1996.

[CAF] Masters, S. *CMM Appraisal Framework, Version 1.0,*" (ESC-TR-95-001|CMU/SEI-95-TR-001). Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute: 1995.

Appendix I Request for Comments

SECTION I: TO BE COMPLETED BY APPRAISER		
Name/Organization:	Phone:	Email:
Reference to section or page:	Problem Title:	
Description of problem (use back if needed):		
Impact if the problem is not resolved:		
Possible solutions:		
SECTION II: TO BE COMPLETED BY SSE-CMM STEERING GROUP		
❒ Accepted ❒ Rejected	Priority: ❒ High ❒ Medium ❒ Low	
Rationale:		
Action Required:		
Disposition:		
Assigned to:		
Due Date:		