References

1. Security Concerns in Licensing Agreements
   http://www.securityfocus.com/infocus/1636
   Last retrieved in April 2009

2. SSE-CMM – Model Website
   http://www.sse-cmm.org/model/model.asp
   Last retrieved in November 2009

3. SSE-CMM – Model Description Document Version 3.0
   http://www.sse-cmm.org/docs/ssecmmv3final.pdf
   Last retrieved in July 2009

4. Do We Really Need a Security Industry?
   Bruce Schneier (2007)
   http://www.wired.com/politics/security/commentary/securitymatters/2007/05/securitymatters_0503
   Last retrieved in April 2009

5. Process based information systems evaluation: towards the attributes of "PRISE".
   Journal of Enterprise Information Management.
   Ozkan, S., Hackney, R., Bilgen, S. (2007).
   20(6). Pp. 700-725.

6. Assessing Software Development Practices in Sudan
   Research by Nahla Murtada Ahmed (2008)

7. Tech Mahindra leads SSE CMM implementation in India
   http://www.prdomain.com/companies/M/Mahindra&Mahindra/newsreleases/20066633290.htm
   Last retrieved in July 2009

8. Sobha Renaissance Information Technology
   http://www.renaissance-it.com
   Last retrieved in July 2009

9. SSE-CMM Appraisal Method Document Version 2
   http://www.sse-cmm.org/
   Last retrieved in May 2009

10. How can security be measured?
    Information Systems Control Journal, Volume 2, 2005.
    Chapin, D.A., Akridge, S. (2005).
    http://www.isaca.org/Content/ContentGroups/Journal1/20058/jpdf052-how-cansecurity.pdf
    Last retrieved in March 2009

11. The Governance, Risk Management, and Compliance Spending Report.
AMR Research, 2008
http://www.amrresearch.com/
Last retrieved in May 2009

12. Metrics based Security Assessment. In Information Security and Ethics: Social and Organizational (pp 261-287). IRM Press. Goldman, J.E, Christie, V.R. (2004).

13. COBIT
***http://*www.isaca.org/cobit/**
Last retrieved in May 2009

14. Unified Modeling Language (UML)
http://www.uml.org/
Last retrieved in September 2009

Appendix

Organization Appraisal Questionnaires

Organization Name : _____

Respondent Name : _____

Number of Employees Working : _____

Number of Developers Working : _____

Years Organization has been working in this field : _____

Overview of Process Areas

Process areas (PA) listed below are related to security engineering practices. Check all that your organization is practicing during software development.

PA01 - Administer Security Controls

PA02 - Assess Impact

PA03 Assess Security Risk

PA04 - Assess 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

Note: You only need to answer the questions of process area that you believe is being practiced by your organization in rest of this book.

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.

Goal

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.

- **Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.**

Example Work Products

• An organizational security structure chart – identifies the organization members related to security and their role.
• Documents describing security roles – describes each of the organizational roles related to security and their responsibilities.
• Documents describing security responsibilities – describes each of the security responsibilities in detail, including what output is expected and how it will be reviewed and used.
• Documents detailing security accountabilities – describes who is accountable for security related problems, ensuring that someone is responsible for all risks.
• Documents detailing security authorizations – identifies what each member of an organization is allowed to do.

a) Yes b) No c) Don't Know

- **Manage the configuration of system security controls.**

Example Work Products

- records of all software updates – tracks licenses, serial numbers, and receipts for all software and software updates to the system, including date, person responsible, and a description of the change.
- records of all distribution problems – contains a description of any problem encountered during software distribution and a description of how it was resolved.
- system security configuration – a database describing the current state of the system hardware, software, and communications, including their location, the individual assigned, and related information.
- system security configuration changes – a database describing any changes to the system security configuration, including the name of the person making the change, a description of the change, the reason for the change, and when the change was made.
- records of all confirmed software updates – a database tracking software updates which includes a description of the change, the name of the person making the change, and the date made.

- periodic summaries of trusted software distribution – describes recent trusted software distribution activity, noting any difficulties and action items.
- security changes to requirements – tracks any changes to system requirement made for security reasons or having an effect on security, to help ensure that changes and their effects are intentional.
- security changes to design documentation – tracks any changes to the system design made for security reasons or having an effect on security, to help ensure that changes and their effects are intentional.

a) Yes b) No c) Don't Know

- **Manage security awareness, training, and education programs for all users and administrators.**

Example Work Products

- user review of security training material – describes the effectiveness, applicability, and relevance of the security awareness and training material.
- logs of all awareness, training and education undertaken, and the results of that training – tracks user understanding of organizational and system security.
- periodic reassessments of the user community level of knowledge, awareness and training with regard to security – reviews the organizational understanding of security and identifies possible areas to focus on in the future.
- records of training, awareness and educational material – collection of security relevant training material which can be reused throughout an organization. Can be integrated with other organizational training materials.

a) Yes b) No c) Don't Know

- **Manage periodic maintenance and administration of security services and control mechanisms.**

Example Work Products

- maintenance and administrative logs – record of maintenance, integrity checks, and operational checks performed on system security mechanisms.

- periodic maintenance and administration reviews – contains analysis of recent system security administration and maintenance efforts.
- administration and maintenance failure – tracks problems with system security administration and maintenance in order to identify where additional effort is required.
- administration and maintenance exception – contains descriptions of exceptions made to the normal administration and maintenance procedures, including the reason for the exception and the duration of the exception.
- sensitive information lists – describes the various types of information in a system and how that information should be protected.
- sensitive media lists – describes the various types of media used to store information in a system and how each should be protected.
- sanitization, downgrading, and disposal – describes procedures for ensuring that no unnecessary risks are incurred when information is changed to a lower sensitivity or when media are sanitized or disposed.

a) Yes b) No c) Don’t Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

***Common Feature: A.* Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

***Common Feature: B.* Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

Common Feature: A. **Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

Common Feature: B. **Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

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.

Goal

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.

- **Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system.**

Example Work Products

- System priority lists and impact modifiers
- System capability profile – describes the capabilities of a system and their importance to the objective of the system.

a) Yes b) No c) Don't Know

- **Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system.**

Example Work Products

- Product asset analysis – contains an identification of the product assets and their significance to the operation of the system.
- System asset analysis – contains an identification of the system assets and their significance to the operation of the system

a) Yes b) No c) Don't Know

- **Select the impact metric to be used for this assessment.**

Example Work Products

- selected impact metrics

a) Yes b) No c) Don't Know

- **Identify the relationship between the selected metrics for this assessment and metric conversion factors if required.**

Example Work Products

- impact metric relationships lists – describes the relationships between the metrics
- impact metric combination rules – describes the rules for combining impact metrics

a) Yes b) No c) Don’t Know

- **Identify and characterize impacts.**

Example Work Products

- exposure impact lists – a list of potential impacts and the associated metrics

a) Yes b) No c) Don’t Know

- **Monitor ongoing changes in the impacts.**

Example Work Products

- impact monitoring reports – describes the results of monitoring impacts
- impact change reports – describes changes to impacts

a) Yes b) No c) Don’t Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature:* *A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature:* *B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

Common Feature: A. **Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

Common Feature: B. **Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

Common Feature: A. **Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

Common Feature: B. **Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

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.

Goal

- 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.

- **Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared.**

Example Work Products

- risk assessment method – describes the approach for identifying and characterizing risks.
- risk assessment formats – describes the format in which risks will be documented and tracked, including a description, significance, and dependencies.

a) Yes b) No c) Don't Know

- **Identify threat/vulnerability/impact triples (exposures).**

Example Work Products

- system exposure lists – describes the exposures of the system

a) Yes b) No c) Don't Know

- **Assess the risk associated with the occurrence of an exposure.**

Example Work Products

- exposure risk list – a list of the calculated risks
- exposure priority table – a prioritized table of the calculated risks

a) Yes b) No c) Don't Know

- **Assess the total uncertainty associated with the risk for the exposure.**

Example Work Products

- exposure risk with associated uncertainty – a list of risks showing the measure of risk along with a measure of the uncertainty

a) Yes b) No c) Don't Know

- **Order risks by priority.**

Example Work Products

- risk priority lists – a list prioritizing the risks
- safeguard requirement lists – lists of potential safeguards that can help mitigate the risks
- rationale for prioritization – a description of the prioritization scheme

a) Yes b) No c) Don't Know

- **Monitor ongoing changes in the risk spectrum and changes to their characteristics.**

Example Work Products

- risk monitoring reports – reports describing the current risk spectrum
- risk change reports – describes the operational capabilities of a system and their importance to the objective of the system.

a) Yes b) No c) Don't Know

---

2. Planned & 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.

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the Administer Security Controls base practices perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's Administer Security Controls processes?

***Common Feature: A.* Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

***Common Feature: B.* Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's Administer Security Controls processes?

***Common Feature: A.* Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

***Common Feature: B.* Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

PA04 Assess Threat

Process area summary:

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

Goal

- 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.

- **Identify applicable threats arising from a natural source.**

Example Work Products

- applicable natural threat tables – tables documenting the character and likelihood of natural threats

a) Yes b) No c) Don't Know

- **Identify applicable threats arising from manmade sources, either accidental or deliberate.**

Example Work Products

- threat scenario descriptions – descriptions of how the threat works
- threat severity estimates – measurements of likelihood associated with a threat

a) Yes b) No c) Don't Know

- **Identify appropriate units of measure, and applicable ranges, in a specified environment.**

Example Work Products

- threat table with associated units of measure and location ranges.

a) Yes b) No c) Don't Know

- **Assess capability and motivation of threat agent for threats arising from man-made sources.**

Example Work Products

- threat agent descriptions – capability assessments and descriptions

a) Yes b) No c) Don't Know

- **Access the likelihood of threat manifestation.**

Example Work Products

- threat event likelihood assessment – report describing the likelihood of threats

a) Yes b) No c) Don’t Know

- **Monitor ongoing changes in the threat spectrum and changes to their characteristics.**

Example Work Products

- threat monitoring reports – documents describing the results of the threat monitoring effort
- threat change reports – documents describing changes in the threat spectrum

a) Yes b) No c) Don’t Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

Common Feature: A. **Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

Common Feature: B. **Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

***Common Feature: A.* Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

***Common Feature: B.* Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

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, weaknesses, security holes, or implementation flaws within a system that are likely to be attacked by a threat. These vulnerabilities are independent of any particular threat instance 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.

Goal

- 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.

- **Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized.**

Example Work Products

- vulnerability analysis method – identifies the approach for finding and addressing system security vulnerabilities, including the analysis, reporting, and tracking process.
- vulnerability analysis formats – describes the format of the results of a vulnerability analysis to ensure a standardized approach.
- attack methodology and philosophy – includes objectives and the approach for performing the attack testing
- attack procedures – detailed steps for performing the attack testing
- attack plans – includes resources, schedule, description of the attack methodology
- penetration study – the analysis and implementation of attack scenarios targeted at identifying unknown vulnerabilities
- attack scenarios – description of the specific attacks that will be attempted

a) Yes b) No c) Don't Know

- **Identify system security vulnerabilities.**

Example Work Products

- vulnerability list describing the vulnerability of the system to various attacks
- penetration profile includes results of the attack testing (e.g., vulnerabilities)

a) Yes b) No c) Don't Know

- **Gather data related to the properties of the vulnerabilities.**

Example Work Products

- vulnerability property tables – tables that document the characteristics of vulnerabilities of the product or system

a) Yes b) No c) Don't Know

- -

- **Assess the system vulnerability and aggregate vulnerabilities that results from specific vulnerabilities and combinations of specific vulnerabilities**

Example Work Products

- vulnerability assessment report – includes a quantitative or qualitative description of the vulnerabilities that result in a problem for the system, including the likelihood of attack, likelihood of success, and the impact of the attack.
- attack reports – documents the results and analysis of the results including vulnerabilities found, their potential for exploitation, and recommendations

a) Yes b) No c) Don't Know

- -

- **Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.**

Example Work Products

- vulnerability monitoring reports – documents describing the results of the vulnerability monitoring effort
- vulnerability change reports – documents describing new or changed vulnerabilities

a) Yes b) No c) Don't Know

- -

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- Plan the performance of the process?

a) Yes b) No c) Don't Know

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

***Common Feature: A.* Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

***Common Feature: B.* Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

***Common Feature: A.* Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

***Common Feature: B.* Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

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.

Goal

- 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.

- **Identify the security assurance objectives.**

Example Work Products

- statement of security assurance objectives – identifies the customer's requirements for the level of confidence needed in a system's security features

a) Yes b) No c) Don't Know

- **Define a security assurance strategy to address all assurance objectives.**

Example Work Products

- Security assurance strategy – describes the plan for meeting the customer's security assurance objectives and identifies the responsible parties.

a) Yes b) No c) Don't Know

- **Identify and control security assurance evidence.**

Example Work Products

- Security assurance evidence repository (e.g., database, engineering notebook, test results, evidence log) – stores all evidence generated during development, testing, and use. Could take the form of a database, engineering notebook, test results, or evidence log.

a) Yes b) No c) Don't Know

- **Perform analysis of security assurance evidence.**

Example Work Products

- assurance evidence analysis results – identifies and summarizes the strengths and weaknesses of evidence in the repository.

a) Yes b) No c) Don't Know

- **Provide a security assurance argument that demonstrates the customer's security needs are met.**

Example Work Products

- assurance argument with supporting evidence – a structured set of assurance objectives supported by various pieces of assurance evidence.

a) Yes b) No c) Don’t Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

***Common Feature: A.* Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

***Common Feature: B.* Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

Common Feature: A. **Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

Common Feature: B. **Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

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.

Goal

- 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.

- **Define security engineering coordination objectives and relationships.**

Example Work Products

- information sharing agreements – describe a process for sharing information between groups, identifying the parties involved, media, format, expectations, and frequency.
- working group memberships and schedules – describe the organization's working groups, including their membership, roles of members, purpose,3 agenda, and logistics
- organizational standards – describe the processes and procedures for communicating security related information between the various working groups and with the customer.

a) Yes b) No c) Don't Know

- **Identify coordination mechanisms for security engineering.**

Example Work Products

- communication plans – include the information to be shared, meeting times, processes and procedures to be used between members of working groups and with other groups.
- communication infrastructure requirements – identify the infrastructure and standards needed to share information between working group members and with other groups effectively.
- templates for meeting reports, message, memoranda – describe the format for various documents, to ensure standardization and efficient work.

a) Yes b) No c) Don't Know

- **Facilitate security engineering coordination.**

Example Work Products

- procedures for conflict resolution – identifies the approach for efficiently resolving conflicts within and between organizational entities.

- meeting agendas, goals, action items – describes the topics to be discussed at a meeting, emphasizing the goals and action items to be addressed.
- action item tracking – identifies the plan for working and resolving an action item, including responsibility, schedule, and priority.

a) Yes b) No c) Don't Know

- **Use the identified mechanisms to coordinate decisions and recommendations related to security.**

Example Work Products

- decisions – communication of security related decisions to affected groups via meeting reports, memoranda, working group minutes, e-mail, security guidance, or bulletin boards
- recommendations – communication of security related recommendations to affected groups via meeting reports, memoranda, working group minutes, e-mail, security guidance, or bulletin boards

a) Yes b) No c) Don't Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

***Common Feature: A.* Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

***Common Feature: B.* Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

Common Feature: A. **Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

Common Feature: B. **Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

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.

Goal

- 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.

- **Analyze event records to determine the cause of an event, how it proceeded, and likely future events.**

Example Work Products

- descriptions of each event – identifies the source, impact, and importance of each detected event.
- constituent log records and sources – security related event records from various sources.
- event identification parameters – describe which events are and are not being collected by various parts of a system
- listing of all current single log record alarm states – identifies all requests for action based on single log records.
- listing of all current single event alarm states – identifies all requests for action based on events which are formed from multiple log records.
- periodic report of all alarm states that have occurred – synthesizes alarm listings from multiple systems and does preliminary analysis.
- log analysis and summaries – performs analysis on the alarms that have occurred recently and reports the results for broad consumption.

a) Yes b) No c) Don't Know

- **Monitor changes in threats, vulnerabilities, impacts, risks, and the environment.**

Example Work Products

- report of changes – identifies any external or internal changes that may affect the security posture of the system
- periodic assessment of significance of changes – performs analysis on changes in security posture to determine their impact and need for response

a) Yes b) No c) Don't Know

- **Identify security relevant incidents.**

Example Work Products

- incident list and definitions – identifies common security incidents and describes them for easy recognition
- incident response instructions – describes the appropriate response to security incidents that arise
- incident reports – describes what incident occurred and all relevant details, including source of the incident, any damage, response taken, and further action required
- reports related to each intrusion event detected – describes each intrusion event detected and provides all relevant details, including the source, any damage, response taken, and further action required
- periodic incident summaries – provides a summary of recent security incidents, noting trends, areas that may require more security, and possible cost savings from lowering security

a) Yes b) No c) Don't Know

- **Monitor the performance and functional effectiveness of security safeguards.**

Example Work Products

- periodic safeguard status – describes the state of the existing safeguards in order to detect possible misconfiguration or other problems
- periodic safeguard status summaries – provides a summary of the state of existing safeguards, noting trends, needed improvements, and possible cost savings from lowering security

a) Yes b) No c) Don't Know

- **Review the security posture of the system to identify necessary changes.**

Example Work Products

- security review – contains a description of the current security risk environment, the existing security posture, and an analysis of whether the two are compatible
- risk acceptance review – a statement by the appropriate approval authority that the risk associated with operating the system is acceptable

a) Yes b) No c) Don't Know

- **Manage the response to security relevant incidents.**

Example Work Products

- system recovery priority list – contains a description of the order in which system functions will be protected and restored in the case of an incident causing failure
- test schedule – contains the dates for periodic testing of the system to ensure that security related functions and procedures are operational and familiar
- test results – describes the results of periodic testing and what actions should be taken to keep the system secure
- maintenance schedule – contains the dates for all system maintenance, both upgrades and preventative and is typically integrated with the test schedule
- incident reports – describes what incident occurred and all relevant details, including source of the incident, any damage, response taken, and further action required.
- periodic reviews – describes the procedure to be performed during periodic reviews of the security of the system, including who is to be involved, what checks will be made, and what the output will contain
- contingency plans – identifies the maximum acceptable period of system downtime, the essential elements of the system, a strategy and plan for system recovery, business resumption, situation management, and procedures for testing and maintenance of the plan

a) Yes b) No c) Don’t Know

- **Ensure that the artifacts related to security monitoring are suitably protected.**

Example Work Products

- a listing all archived logs and associated period of retention – identifies where artifacts associated with security monitoring are stored and when they can be disposed
- periodic results of spot checks of logs that should be present in archive – describes any missing reports and identifies the appropriate response
- usage of archived logs – identifies the users of archived logs, including time of access, purpose, and any comments
- periodic results of testing the validity and usability of randomly selected archived logs – analyzes randomly selected logs and determines whether they are complete, correct, and useful to ensure adequate monitoring of system security

a) Yes b) No c) Don’t Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

Common Feature: A. **Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

Common Feature: B. **Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

***Common Feature: A.* Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

***Common Feature: B.* Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

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.

Goal

- 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.

- **Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.**

Example Work Products

- agreements between security engineering and other disciplines – definition of how security engineering will provide input to other disciplines (e.g., documents, memoranda, training, consulting)
- descriptions of input needed – standard definitions for each of the mechanisms for providing security input

a) Yes b) No c) Don't Know

- **Determine the security constraints and considerations needed to make informed engineering choices.**

Example Work Products

- security design criteria – security constraints and considerations that are needed to make decisions regarding overall system or product design
- security implementation rules – security constraints and considerations that apply to the implementation of a system or product (e.g., use of specific mechanisms, coding standards)
- documentation requirements – identification of specific documentation needed to support security requirements (e.g., administrators manual, users manual, specific design documentation)

a) Yes b) No c) Don't Know

- **Identify alternative solutions to security related engineering problems.**

Example Work Products

- security views of system architecture – describe at an abstract level relationships between key elements of the system architecture in a way that satisfies the security requirements

- security design documentation – includes details of assets and information flow in the system and a description of the functions of the system that will enforce security or that relate to security
- security models – a formal presentation of the security policy enforced by the system; it must identify the set of rules and practices that regulate how a system manages, protects, and distributes information; the rules are sometimes expressed in precise mathematical terms [NCSC88]
- security architecture – focuses on the security aspects of a systems architecture, describing the principles, fundamental concepts, functions, and services as they relate to the security of the system
- reliance analysis (safeguard relationships and dependencies) – a description of how the security services and mechanisms interrelate and depend upon one another to produce effective security for the whole system; identifies areas where additional safeguards may be needed

a) Yes b) No c) Don't Know

- **Analyze and prioritize engineering alternatives using security constraints and considerations.**

Example Work Products

- trade-off study results and recommendations – includes analysis of all engineering alternatives considering security constraints and considerations as provided in BP09.02
- end-to-end trade-off study results – results of various decisions throughout the life cycle of a product, system, or process, focusing on areas where security requirements may have been reduced in order to meet other objectives (e.g., cost, functionality)

a) Yes b) No c) Don't Know

- **Provide security related guidance to the other engineering groups.**

Example Work Products

- architecture recommendations – includes principles or constraints that will support the development of a system architecture that satisfies the security requirements
- design recommendations – includes principles or constraints that guide the design of the system
- implementation recommendations – includes principles or constraints that guide the implementation of the system

- security architecture recommendations – includes principles or constraints that define the security features of the system
- philosophy of protection – high-level description of how security is enforced, including automated, physical, personnel, and administrative mechanisms
- design standards, philosophies, principles – constraints on how the system is designed (e.g., least privilege, isolation of security controls)
- coding standards – constraints on how the system is implemented

a) Yes b) No c) Don't Know

- **Provide security related guidance to operational system users and administrators.**

Example Work Products

- administrators manual – description of system administrator functions and privileges for installing, configuring, operating, and decommissioning the system in a secure manner
- users manual – description of the security mechanisms provided by the system and guidelines for their use
- security profile – security environment (threats, organizational policy); security objectives (e.g., threats to be countered); security functional and assurance requirements; rationale that system developed to these requirements will meet the objectives
- system configuration instructions – instructions for configuration of the system to ensure its operation will meet the security objectives

a) Yes b) No c) Don't Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

***Common Feature: A.* Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

***Common Feature: B.* Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

***Common Feature: A.* Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

***Common Feature: B.* Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

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.

Goal

- 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.

- **Gain an understanding of the customer's security needs.**

Example Work Products

- customer security needs statement – high-level description of security required by the customer

a) Yes b) No c) Don't Know

- **Identify the laws, policies, standards, external influences and constraints that govern the system.**

Example Work Products

- security constraints – laws, policies, regulations, and other constraints that influence the security of a system
- security profile – security environment (threats, organizational policy); security objectives (e.g., threats to be countered); security functional and assurance requirements; rationale that system developed to these requirements will meet the objectives.

a) Yes b) No c) Don't Know

- **Identify the purpose of the system in order to determine the security context.**

Example Work Products

- expected threat environment – any known or presumed threats to the system assets against which protection is needed; include threat agent (expertise, available resources, motivation), the attack (method, vulnerabilities exploited, opportunity), the asset
- target of evaluation – description of the system or product whose security features are to be evaluated (type, intended application, general features, limitations of use)

a) Yes b) No c) Don't Know

- **Capture a high-level security oriented view of the system operation.**

Example Work Products

- security concept of operations – high-level security oriented view of the system (roles, responsibilities, assets, information flow, procedures)
- conceptual security architecture – a conceptual view of the security architecture; see BP09.03 security architecture

a) Yes b) No c) Don't Know

- **Capture high-level goals that define the security of the system.**

Example Work Products

- operational/environmental security policy – rules, directives, and practices that govern how assets are managed, protected, and distributed within and external to an organization
- system security policy – rules, directives, and practices that govern how assets are managed, protected, and distributed by a system or product

a) Yes b) No c) Don't Know

- **Define a consistent set of statements which define the protection to be implemented in the system.**

Example Work Products

- security related requirements – requirements which have a direct effect on the secure operation of a system or enforce conformance to a specified security policy
- traceability matrix – mapping of security needs to requirements to solutions (e.g., architecture, design, implementation) to tests and test results.

a) Yes b) No c) Don't Know

- **Obtain agreement that the specified security requirements match the customer's needs.**

Example Work Products

- approved security objectives – stated intent to counter identified threats and/or comply with identified security policies (as approved by the customer).
- security related requirements baseline – the minimum set of security related requirements as agreed to by all applicable parties (specifically the customer) at specified milestones**.**

a) Yes b) No c) Don’t Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- -

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- -

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- -

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

- -

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- -

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- -

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

Common Feature: A. **Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

Common Feature: B. **Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

Common Feature: A. **Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

Common Feature: B. **Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know

PA11 Verify and Validate Security

Process area summary:

The purpose of Verify and Validate Security is to ensure that solutions 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.

Goal

- 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.

- **Identify the solution to be verified and validated.**

Example Work Products

- verification and validation plans – definition of the verification and validation effort (includes resources, schedule, work products to be verified and validated)

a) Yes b) No c) Don't Know

- **Define the approach and level of rigor for verifying and validating each solution.**

Example Work Products

- test, analysis, demonstration, and observation plans – definition of the verification and validation methods to be used (e.g., testing, analysis) and the level of rigor (e.g., informal or formal methods)
- test procedures – definition of the steps to be taken in the testing of each solution
- traceability approach – description of how verification and validation results will be traced to customer's security needs and requirements

a) Yes b) No c) Don't Know

- **Verify that the solution implements the requirements associated with the previous level of abstraction.**

Example Work Products

- raw data from test, analysis, demonstration, and observation – results from any approaches used in verifying that the solution meets the requirements
- problem reports – inconsistencies discovered in verifying that a solution meets the requirements

a) Yes b) No c) 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.**

Example Work Products

- problem reports – inconsistencies discovered in validating that a solution meets the security need
- inconsistencies – areas where the solution does not meet the security needs
- ineffective solutions – solutions that do not meet the customer's security needs

a) Yes b) No c) Don't Know

- **Capture the verification and validation results for the other engineering groups.**

Example Work Products

- test results – documentation of outcome of testing
- traceability matrix – mapping of security needs to requirements to solutions (e.g., architecture, design, implementation) to tests and test results

a) Yes b) No c) Don't Know

---

2. Planned & Tracked

Do those involved in performing the base practices of the current process area also perform any of the following functions?

***Common Feature: A.* Planning Performance**

- Allocate adequate resources (including people) for performing the process area?

a) Yes b) No c) Don't Know

- -

- Assign responsibilities for developing the work products and/or providing the services of the process area?

a) Yes b) No c) Don't Know

- -

- Document the approach to performing the process area in policies, standards and/or procedures, including measurements to be taken?

a) Yes b) No c) Don't Know

- -

- Provide appropriate tools to support performance of the process area?

a) Yes b) No c) Don't Know

- -

- Ensure that the individuals performing the process are appropriately trained in how to perform the process?

a) Yes b) No c) Don't Know

- -

- Plan the performance of the process?

a) Yes b) No c) Don't Know

- -

***Common Feature: B.* Disciplined Performance**

- Follow documented plans and policies, standards, and/or procedures

a) Yes b) No c) Don't Know

- -

- Place work products under version control or configuration management, as appropriate?

a) Yes b) No c) Don't Know

Common Feature: C. **Verifying Performance**

- Verify compliance of the process with applicable policies, standards and/or procedures?

a) Yes b) No c) Don't Know

- Verify compliance of work products with the applicable standards and/or requirements?

a) Yes b) No c) Don't Know

Common Feature: D. **Tracking Performance**

- Track the status of the process against the plan using measurement?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when progress varies significantly from that planned?

a) Yes b) No c) Don't Know

---

3. Well Defined

Do those involved in managing processes based on the base practices of the current process area perform any of the following functions?

***Common Feature: A.* Defining a Standard Process**

- how to implement the base practices of the process area?

a) Yes b) No c) Don't Know

- Tailor the organizational standard process definition to meet the needs of a specific use?

a) Yes b) No c) Don't Know

***Common Feature: B.* Perform the Defined Process**

- Follow the tailored version of the organizational standard process definition?

a) Yes b) No c) Don't Know

- Perform defect reviews of appropriate work products?

a) Yes b) No c) Don't Know

- Use data on performing the defined process to manage the defined process?

a) Yes b) No c) Don't Know

***Common Feature: C.* Coordinate Practices**

- Coordinate communication within the security engineering group?

a) Yes b) No c) Don't Know

- Coordinate communication among the various groups within your project/organization?

a) Yes b) No c) Don't Know

- Coordinate communication with external groups?

a) Yes b) No c) Don’t Know

---

4. Quantitatively Controlled

Are the following visible and available to those using the organization's processes?

***Common Feature: A.* Establishing Measurable Quality Goals**

- Establishing measurable quality goals for the work products of the organization's standard process family?

a) Yes b) No c) Don't Know

***Common Feature: B.* Objectively Managing Performance**

- Determine the process capability of the defined process quantitatively?

a) Yes b) No c) Don't Know

- Take corrective action as appropriate when the defined process is not performing within its process capability?

a) Yes b) No c) Don't Know

---

5. Continuously Improving

Are the following characteristics visible in the organization's processes?

Common Feature: A. **Improving Organizational Capability**

- 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?

a) Yes b) No c) Don't Know

Common Feature: B. **Improving Process Effectiveness**

- Perform causal analysis of defects?

a) Yes b) No c) Don't Know

- Eliminate the causes of defects in the defined process selectively?

a) Yes b) No c) Don't Know

- Continuously improve performance of the defined process, incorporating all changes in its process definition?

a) Yes b) No c) Don't Know

- Continuously improving the process area by changing the organization's standard process definition to increase its effectiveness?

a) Yes b) No c) Don't Know
