INFOSEC Assessment Capability Maturity Model

(IA-CMM)

Version 2.1

February 2002

TABLE OF CONTENTS

Introduction

The National Information Infrastructure (NII) is comprised of thousands of organizations that own and operate automated information systems. Marketing research in 1998 identified nearly 22,000 organizations listed under 48 standard industrial category (SIC) codes related to the eight critical sectors in Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection. Many of these critical NII organizations need outside assistance in assessing the security posture of their information systems in order to make fundamental, cost-effective security improvements.

In the last few years, U.S. Government Agencies and Departments have seen an increase in requests for INFOSEC assessments due to the proliferation of automated information systems and the emphasis on critical infrastructure protection generated by PDD-63.

The number of government organizations and private companies who offer security assessment services has also grown over the last few years. However, without any standardization, these organizations have implemented varying interpretations of the INFOSEC assessment service. Today the terminology, scope and cost of security assessment services offered by industry differ widely. The lack of definition and standardization within the industry is confusing and, at times, unnecessarily costly for consumers.

INFOSEC Assessment Training and Rating Program (IATRP)

NSA operates the IATRP on the assumption that there are a significant number of NII organizations (**Customers**) who own and operate systems that store, process, and transmit information with national security implications that need assistance in vulnerability discovery and risk management decisions. These Customers face a myriad of organizations with INFOSEC assessment service providers (**Providers**) that offer an array of service. Customers are often confused about what needs to be done during an INFOSEC Assessment and how to compare both assessors (individuals) and provider organizations. The IATRP provides a standardized set of baseline activities that are required for an INFOSEC Assessment, trains and certifies assessors in the standard, and rates provider organizations against a standardized metric to determine the provider's organizational capability to perform INFOSEC assessments. The IATRP standardized rating system provides consumers with the appropriate information required to be better informed when negotiating with INFOSEC assessment providers to properly meet their INFOSEC concerns.

NSA Vulnerability Discovery Services Triad

The INFOSEC Assessment Methodology (IAM) is the foundation for NSA's Vulnerability Discovery Services Triad. The Triad consists of INFOSEC Assessment, Evaluations, and Red Team Exercises.

INFOSEC Assessments are a high level overview of the INFOSEC posture of an operational system concentrating on information criticality, INFOSEC policy, documented and undocumented procedures, and control of information flow. The primary focus is on information assurance through INFOSEC but can also incorporate other Information Assurance disciplines (e.g., Operations Security). Assessments usually consume the least resources and are the least time consuming of the three services. This is mainly due to the fact that they are performed without hands-on testing. A major advantage of the Assessment service is that it not only provides potential vulnerabilities and countermeasures, but its analysis can be used to focus the efforts of the other two Triad services. The INFOSEC Assessment information flow analysis can assist in focusing testing of the critical security components.

The Evaluation Service builds on the assessment by providing the framework to perform hands-on testing. Although more resource intense, evaluations provide a higher level of assurance that security components and the system are operating in a desired manner. The hands-on tools used by the Evaluation Service include diagnostics that are performed with the cooperation of system administrators. The output of these activities is a mapping of the organization's information flows, and the protections and potential vulnerability to these flows.

The Red Team Exercise is the most resource intense of the Triad services. However, it also provides the most realistic analysis of the INFOSEC posture. The Red Team will estimate an identified adversary capabilities and perform a "no notice" attack on the system. Red Team exercises can be performed at various intensities according to predetermined "rules of engagement".

INFOSEC Assessment Methodology (IAM)

The IAM consists of a standardized set of activities required to perform an INFOSEC assessment. In other words, the methodology explains the depth and breadth of the assessment activities that must be performed to be acceptable within the IATRP. The IAM “sets the bar” for what needs to be done for an activity to be considered a complete INFOSEC Assessment. Providers who advertise an INFOSEC assessment capability and consumers seeking assistance in performing INFOSEC Assessments should use the IAM as the baseline for their discussions. Because the IAM is a baseline, providers can expand upon it to further meet the needs of the customers. However any "expansion" must not reduce or interfere with the original intent of any IAM activity.

The IAM baseline activities include:

On-site customer coordination

- Information criticality analysis
- Identifying customer concerns

Documented INFOSEC Assessment Plan

On-site information gathering of the IAM minimal information categories (18)

- Interviews
- Documentation review
- System demonstrations

Documented final report of findings and recommendations

The IAM is taught in a two-day training class. Although the class material is the same, the IAM is taught in two formats. There are IAM Certification classes and Government Sponsorship classes.

The certification class is open to anyone meeting the requirements (government, contractor, or private individual). To qualify for the certification class, individuals must have five years of demonstrated experience in the field of INFOSEC, communications security, or computer security, with two of the five years of experience directly involved in analyzing/evaluating/assessing computer system/network vulnerabilities and security risks. To further qualify for certification, students must demonstrate an understanding of the IAM through participating in all of the two-day training, group presentations to the class, and a passing grade on the IAM final exam. Each student who meets all these requirements will receive an IAM certificate stating that they have been trained and demonstrated an understanding of the IAM. The IAM certification provides no assurance as to the INFOSEC analysis ability of the individuals beyond that of the qualifications. Organizations can bring together a cadre of IAM certified individuals to provide an INFOSEC Assessment capability to market for the U.S. government.

The Government sponsorship class is a non-certification class that is open to individuals (government or private) who have sponsorship from a U.S. Government organization. This class is geared for the consumers of the IAM service. Individuals with INFOSEC responsibilities for U.S. Government systems can learn the IAM in order to help them identify and retain an appropriate IAM provider to meet their needs. These providers can be contracted for a single assessment or be permanent staff members.

INFOSEC Assessment – Capability Maturity Model (IA-CMM)

The INFOSEC Assessment – Capability Maturity Model (IA-CMM) is based on the System Security Engineering Capability Maturity Model (SSE-CMM) and modified to address the INFOSEC Assessment Process. For a deeper understanding of the SSE-CMM and its associated Appraisal Method please refer to the current drafts of the documents on the website: www.sse-cmm.org.

Whereas IAM training focuses on an individual's ability to conduct an INFOSEC assessment within the guidelines of the IATRP, the IA-CMM appraisal focuses on a provider organization's capability to support its assessors in the conduct of their mission objectives (i.e. to provide quality INFOSEC assessments). The IA-CMM focuses on the processes (specific functions) that produce products (e.g., identified vulnerabilities, countermeasures, and threats). Capability maturity is a measurement of the level of assurance that an organization can perform a process consistently (i.e., providing a consistent product from the process).

The IA-CMM identifies nine process areas related to performing an INFOSEC assessment. For each of the nine process areas, the IA-CMM defines six levels of process maturity from Level 0 to Level 5. The higher the maturity levels, the more likely the process will be performed consistently. From this consistency, quality can be implied but not guarantied. The Process Areas in the IA-CMM are developed for INFOSEC Assessments. However, they have relevance when performing all of the Triad services. Future CMM efforts will incorporate additional process areas that will encompass all of the Triad services.

In CMM processes, it is conceivable that a well-defined process that consistently produces a poor product can receive a fairly high maturity rating. The IA-CMM counters this by focusing on the process areas as they relate to the IAM. The search for the use of standardized IAM products adds additional assurance of quality (i.e., the right products are being produced.)

At the conclusion of an IA-CMM appraisal, the organization will be assigned an IA-CMM Ratings Profile. This is a list of nine numbers from 0 to 5 (one for each process area.) When a customer is deciding on a provider organization, they can use the IA-CMM rating profile along with the experience of the INFOSEC assessors to determine what is required to meet their needs. The lower the process area rating, the more dependence the customer should put on the experience of the individual assessors.

.

Acknowledgments

Sponsoring Organizations

The INFOSEC Assessment – Capability Maturity Model (IA-CMM) was sponsored, written, and developed by the National Security Agency.

Author Group Members

The following individuals are primarily responsible for applying the principles of the System Security Engineering Capability Maturity Model to develop the IA-CMM:

W. Hildebrand	National Security Agency
R. Canfield	National Security Agency
Charles Menk	InterAct Solutions Group, Incorporated (ISG)

Points of Contact

The following are points of contact if require further information:

NSA, IA-CMM, 410-854-7827
NSA, IATRP Program Manager, 410-854-7827
NSA, IAM Training Coordinator, 410-854-7827

Process Area Format

The general format of the process areas is shown in Figure 1-1. The summary description contains a brief overview of the purpose of the PA. Each PA is decomposed into a set of base practices (BPs). The BPs are considered mandatory items (i.e., they must be successfully implemented to accomplish the purpose of the process area they support). Each base practice is described in detail following the PA summary. Goals identify the desired end result of implementing the PA.

Figure 1-1 provides the general format of the process areas and describes the content of each part.

IA-PA 01 – Process Area Title (in verb-noun form)

Summary Description – An overview of the process area.

Goals – A list indicating the desired results of implementing this process area.

Process Area Notes – Any other notes about this process area.

Base Practices List – A list showing the number and name of each base practice.

IA-BP 01.01 – Base Practice Title (in verb-noun form)

Descriptive Name – A sentence describing the base practice.

Description – An overview of this base practice.

Example Work Products – A list of examples illustrating some possible output.

Notes – Any other notes about this base practice.

IA-BP 01.02...

Figure 1-1. Process Area Format

IA-PA01: Provide Ongoing Skills and Knowledge to Support the IAM

Summary Description

The purpose of Provide Ongoing Skills and Knowledge is to ensure that INFOSEC assessors have the necessary knowledge and skills to achieve project and organizational objectives. To ensure the effective application of these critical resources that are predominantly available only from people, the knowledge and skill requirements within the organization need to be identified, as well as the specific site needs.

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

If the organization does not have in-house assessors, and therefore is not directly responsible for conducting training, the organization may receive a '1' in all of PA01. In this case, it may be argued that the IAM could be adequately performed through the use of subject matter experts (SME) external to the organization. These subject matter experts would be responsible for ensuring their own training for maintaining proficiency to address each assessment need. Proficiency in the IA-CMM technical process areas helps support this argument. That being said the organization is still responsible for providing evidence that the SMEs meet the minimum criteria for training (i.e. the organization can defend it's understanding of the requirements identified by the BPs and that the SME meets them.) If the organization does not have in-house assessors and wishes to receive a rating higher than ‘1’, they will need to provide the training evidence for the assessor resources (i.e., obtain the evidence from the sub organization that provides the subject matter experts).

Goal

?? Ensure that INFOSEC assessors are trained in the skills and knowledge to appropriately support and execute the IAM.

Process Area Notes

INFOSEC assessors require skills and knowledge to properly perform their functions. These include the IAM, INFOSEC analysis, and technical and non-technical INFOSEC information.

The choice of providing internal training or relying upon external sources for the needed skills and knowledge is often determined by the availability of training expertise, the project's schedule, budget, and business goals. Successful training programs result from an organization's commitment to continuing education agendas. In addition, they are administered in a manner that optimizes the learning process, is repeatable, assessable, and easily modifiable to meet the ever-changing education needs of the organization. Training is not limited to "classroom" events: it includes many vehicles that support the enhancement of skills and the building of knowledge. When training is not a viable approach due to compressed schedules or lack of availability of training resources, external sources of the needed skills and knowledge may need to be pursued.

Base Practices List

The following list contains the base practices that are essential elements to provide training in the INFOSEC processes that support the IAM:

IA-BP01.01	Identify training needs.
IA-BP01.02	Select method of INFOSEC knowledge or skills training.
IA-BP01.03	Ensure availability of INFOSEC skills and knowledge training.
IA-BP01.04	Train personnel.
IA-BP01.05	Assess training effectiveness.

IA-BP01.01 – Identify Training Needs

Identify needed skills and knowledge throughout the organization using project requirements, organizational strategic plans, and employee skills and deficiencies as guidance.

Description

This Base Practice is the ability of the organization to identify the needed INFOSEC skills and knowledge. The needs are determined using inputs from projects (e.g. a particular INFOSEC assessment), organizational plans, and a compilation of employee skills and deficiencies. Project inputs help to identify existing deficiencies that may be remedied through training or acquisition of skills and knowledge by other means. Organizational strategic plans can be used to help identify training needs that address emerging technologies.

Example Work Products

?? List of INFOSEC training needs

Notes

None

IA-BP01.02 – Select Method of INFOSEC Knowledge or Skills Training

Select the appropriate method (mode and provider) for INFOSEC knowledge or skills training.

Description

The purpose of this Base Practice is to ensure an appropriate mode for providing INFOSEC skills and knowledge training is selected (e.g. Computer Based Training, hands-on lab, formal instruction). Project and organizational needs are analyzed, and training solutions are selected from alternatives such as consultants, subcontracts, and knowledge acquired from subject matter experts, and/or internal or external training.

Example Evidence

?? Description of process for selecting training methods.

Notes

Evidence must show an established chain of command responsible for selecting the method of training.

IA-BP01.03 – Ensure Availability of Skills and Knowledge Training

Ensure that appropriate skills and knowledge training are available to support an organization's IAM capability.

Description

This Base Practice relies upon deliberate analysis and preparation that develops and executes plans that ensure the proper availability of INFOSEC knowledge and skills training (e.g. threat, impact, vulnerability, and risk analysis; other functional INFOSEC; computer systems; applications; interpersonal, multidisciplinary, and process-related skills).

Example Evidence

?? Description of process for ensuring availability of training to support IAM capability.

Notes

Training plans/schedules, assessment of skill types needed by skill category, project knowledge, acquisition plan, training plan, list of identified and available subject matter experts are examples of supporting evidence which can demonstrate that a process for ensuring training is in place.

An important factor for ensuring reasonable availability of training is a prioritization process that matches needs (IA-BP01.01) with resources (e.g. funding/travel restrictions).

IA-BP01.04 – Train Personnel

Train personnel to have the skills and knowledge needed to support their assigned IAM roles.

Description

This Base Practice is designed to verify that training is currently being properly conducted to support the IAM, in accordance IA-BP01.03 (Ensure Availability of Skills and Knowledge Training).

To ensure proper training, materials for each class need to be developed, acquired or identified. This activity can be accomplished with internal resources or obtained from external sources (e.g. commercial training organization, academia, contracted subject matter experts. A copy of all course materials generated should be maintained for future use by employees, and for maintaining traceability in changes to course materials.

Individual records need to be maintained to track the training that each employee has received and the employee's skills and capabilities. These records are fundamental for IA-BP01.01 (Identify Training Needs) and provide the foundation for allocating properly trained resources for performing IAM tasks.

Example Evidence

?? Verification that training is conducted
?? Description of the process for obtaining materials to support IAM training needs.
?? Description of how training and experience records are created and maintained
?? Description of how training materials are maintained

Notes

While an organization can meet immediate technical needs by hiring/contracting subject matter experts, continuing education is an integral part of maintaining technical proficiency Course curricula, descriptions, texts, and handouts are examples of supporting evidence that can be used to demonstrate that a process for obtaining training materials is in place. A repository of baseline training materials and revisions to training materials are examples of supporting evidence that can demonstrate that a process for maintaining course materials is in place.

Training records, personnel profiles, and personnel capability statements are examples of supporting evidence that can demonstrate that a process for maintaining training records is in place. Records should be kept for all students who successfully complete each training course or other approved training activity. Also, records of successfully completed training are made available for consideration in the assignment of the staff and managers.

If the organization relies solely on the expertise of contractors it is still incumbent on them to verify that the contractor personnel are maintaining their proficiencies. While it is not likely or practical for the organization to maintain the training records of every contractor, there should be provisions for reviewing said records at any time. If training is provided to contractors by the organization, a local copy of the training shall be maintained and copies provided to the contractor for inclusion in personnel files.

IA-BP01.05 – Assess Training Effectiveness

Assess the effectiveness of the training to meet the identified training needs (IA-BP01.01).

Description

This Base Practice focuses on the ability of the organization to determine the effectiveness of its training process. A process should exist to determine the skill level of the employee after receiving the training to determine the success of the training. This could be accomplished via formal testing, on-the-job skill demonstration, or assessment mechanisms embedded in the courseware.

Example Evidence

?? Description of the process used to analyze training effectiveness

Notes

Changes to the training curricula due to this analysis is an example of supporting evidence which can demonstrate that a process for determining the effectiveness of training is in place. Student feedback forms can also be examples of supporting evidence. All personnel shall be held accountable to this BP (both internal, SMEs and contractors alike.)

IA-PA02: Coordinate with Customer Organization

Summary Description

The purpose of this PA is to ensure that INFOSEC assessment providers perform coordination activities with the customer organizations in accordance with the IAM. Various mechanisms may be used to communicate the INFOSEC assessment coordination decisions with customer organizations (e.g. memoranda, documents, e-mail, meetings, and working groups).

Goals

?? All participating members of the assessment organization are aware of IAM coordination activities to the extent necessary to perform their functions.

?? Coordination methods to communicate IAM decisions to the customer organization are agreed upon.

?? Assessment decisions are effectively communicated to the customer organization.

Process Area Notes

The Assessment Plan is the primary mechanism for documenting IAM coordination activities. IAM coordination activities occur continuously throughout the assessment process.

Base Practices List

IA-BP02.01	Ensure assessor awareness of IAM coordination activities and mechanisms.
IA-BP02.02	Facilitate IAM assessment coordination.

IA-BP02.01 – Ensure assessor awareness of IAM coordination activities and mechanisms.

Ensure assessors are aware of the IAM coordination activities with the customer and the mechanisms used to perform them.

Description

This BP addresses the need for INFOSEC assessors to be aware of and involved with IAM coordination activities. Relationships and commitments with the customer need to be established and accepted. The objective for assessor awareness ensures that they are conducting coordination activities in accordance with the IAM. Successful relationships take many forms, but must be acknowledged by all the involved parties.

Example Work Products

?? Documented procedures and processes for IAM coordination activities

?? Identification of coordination mechanisms for information sharing.

Notes

Defining IAM coordination should begin as early as possible in the assessment project to ensure that objectives, relationships and mechanisms are well established.

IA-BP02.02 – Facilitate IAM assessment coordination.

Facilitate IAM assessment coordination with customer.

Description

This BP addresses the need for continual use of communication mechanisms providing IAM related decisions to the customer. Successful relationships are based on good facilitation. Communication between the assessment provider and the customer may result in conflicts. This base practice ensures that IAM decisions (e.g. schedule, scope, methods of communication, and conflict resolution procedures) are coordinated appropriately.

Example Work Products

?? INFOSEC Assessment Plans:

Examples of facilitating IAM coordination activities.

?? IAM coordination mechanisms:

Describe how the mechanisms were used to facilitate IAM coordination activities.

?? Documented decisions:
Provide evidence that IAM related decisions are communicated to the customer (e.g. meeting reports, memoranda, working group minutes, e-mail, security guidance, or bulletin boards).

?? Conflict resolution:

Describe the procedure for efficiently resolving conflicts between assessment provider and customer.

Notes

Accountability and responsibilities must be established to ensure effective facilitation.

IA-PA03: Specify Initial INFOSEC Needs

Summary Description

The purpose of this IA-PA is to determine an assessor’s ability to identify the INFOSEC requirements of the system being assessed. This includes identifying organizational information criticality and regulatory documents, along with customer concerns and constraints. This information is analyzed to identify organizational high-level INFOSEC goals. These goals are then translated into initial security requirements for each system being assessed and become the basis for the INFOSEC assessment analysis.

Goal

?? A common understanding of initial INFOSEC needs is required to properly perform the INFOSEC assessment analysis.

Process Area Notes

This process area addresses how the customers' information is obtained and refined into a coherent baseline of initial INFOSEC requirements to be used in the vulnerability analysis of the customers' systems. The information gained and produced by this process area is collected, further refined, used, and updated throughout an INFOSEC assessment activity (particularly in Assess Vulnerability (IA-PA07) and Provide Security Input (IA-PA09), in order to ensure site needs are being addressed.

Base Practices List

IA-BP03.01	Understand criticality of customer’s mission(s), information, and systems.
IA-BP03.02	Identify applicable policies, regulations, standards, procedures and laws.
IA-BP03.03	Identify customer's concerns and constraints
IA-BP03.04	Capture organizational high-level goals.
IA-BP03.05	Capture initial system security requirements.

IA-BP03.01 – Understand criticality of customer’s mission(s), information, and systems

Verify assessor's ability to gain an understanding of the site’s mission(s), critical information, and identify the systems that are used.

Description

The purpose of this base practice is to collect all information necessary for a comprehensive understanding of the site’s critical mission functions, information needed to perform these functions, and the systems that store, process, or transmit this information.

Example Work Products

?? Assessment Plans

Notes

The Assessment Plan should contain the site mission description as well as the organizational and system information criticality analysis. In the IAM top-down approach, this is the initial process that will provide the baseline information that will be used for the assessment.

IA-BP03.02 – Identify applicable policies, regulations, standards, procedures and laws

Verify assessor's ability to identify policies, standards, procedures, laws, and other regulatory influences that are applicable to the INFOSEC posture of the organization.

Description

The purpose of this base practice is to identify all regulatory influences that affect the INFOSEC of the organization. The determination of applicability should identify the laws, regulations, policies and commercial standards that govern the organization. A determination of precedence between global and local policies should be performed. Requirements for INFOSEC placed on the organization must be identified and the INFOSEC implications extracted

Example Work Products

?? Repository of INFOSEC policies, regulations, standards, procedures, and laws.

?? Mechanism for identifying applicable policies, regulations, standards, procedures, and laws from the repository.

?? Mechanism for identifying applicable policies, regulations, standards, procedures, and laws which are not in the repository.

Notes

Central to this activity is the understanding of the operational environment. Particular consideration is required when multiple domains are involved. Conflict may occur between laws and regulations that are applicable in different countries and different types of business. As part of the identification process, conflicts should at a minimum, be identified and resolved if possible.

IA-BP03.03 – Identify customer's concerns and constraints

Verify an assessor's ability to identify the specific concerns and constraints of the customer.

Description

The purpose of this base practice is to determine the assessors' ability to understand the customer's concerns and constraints. The assessor will use this set of concerns as input to focus the activities of the INFOSEC analysis. The customer-generated constraints will also assist in determining the scope of the INFOSEC assessment.

Example Work Products

?? Assessment Plans

Notes

The Assessment Plan should contain a section on the customer's concerns and constraints.

Customer satisfaction will depend on an assessor's ability to adequately address the customer's concerns and constraints. Customer concerns (e.g. known vulnerabilities, confirmed incidents, threat agents, upcoming certifications) need to be addressed throughout the remaining INFOSEC assessment activities (e.g. Outbrief, Final Report). Customer constraints may influence the results of the INFOSEC assessment. If the customer imposes constraints that have a major impact on the outcome of the assessment, this should be noted in the assessment plan and in the final report.

Additional factors influence the INFOSEC concerns and constraints of the organization. These factors include the political orientation and changes in political focus, technology developments, economic influences, global events, and Information Warfare activities. As none of these factors are static they require monitoring and periodic assessment of the potential impact of change.

IA-BP03.04 – Capture organizational high-level goals

Verify assessor's ability to capture a high-level view of the organization's INFOSEC goals.

Description

The purpose of the base practice is to analyze the information from IA-BP03.01(Understand criticality of customer's mission(s), information, and systems), IA-BP03.02 (Identify applicable policies, regulations, standards, procedures and laws), IA-BP03.03 (Identify customer's concerns and constraints), and determine (at a high-level) the INFOSEC goals of the organization. These goals represent the overall information protection philosophy and are the basis for analyzing vulnerabilities and developing recommendations IA-PA08 (Provide IAM Analysis and Results).

Example Work Products

?? Assessment Plans

Notes

While there is no specific section in the Assessment Plan that lists these high-level goals, the goals should be addressed throughout the Plan.

The most likely source of the organizations overall protection philosophy is the INFOSEC Policy document. At a minimum, confidentiality, integrity, and availability of critical information need to be considered when determining organizational goals.

IA-BP03.05 – Capture initial system security requirements

Verify assessor's ability to determine initial INFOSEC requirements for the organizational systems.

Description

The purpose of this base practice is to apply the high level goals to the identified systems and determine the proper INFOSEC posture. To attain this proper INFOSEC posture, the system will need to meet a certain set of requirements. Failing to meet any of these requirements will most likely cause potential vulnerabilities. These requirements will be the basis for IA-PA05 (Assess Vulnerability)

Example Work Products

?? Assessment Plan
  ?? INFOSEC requirements
?? Final Report.

Notes

While there is no specific section in the final report that specifically lists system security requirements, the requirements should be addressed throughout the plan and final report.

The understanding of the system(s) environment is critical in determining INFOSEC requirements. The INFOSEC requirements of the system are not restricted to the internal system(s). For example, INFOSEC requirements may be addressed by the facility in which the system resides and the personnel operating the system. This enables physical measures to be considered as part of the INFOSEC requirements analysis.

IA-PA04: Assess Threat

Summary Description

The purpose of the Assess Threat Process Area is to verify an assessor's ability to identify applicable security threats.

Goals

?? Threats to the organization's mission with respect to INFOSEC are identified and characterized.

Process Area Notes

This Process Area addresses the assessor's ability to determine applicable potential and known threats to the organization. Many approaches can be used to perform threat analysis. An important consideration for determining which approach to use is how it will interface with other IAM activities.

While the activities involved with gathering threat, vulnerability, and impact are unique and have been grouped into separate Process Areas, they are interdependent when performing risk analysis. Therefore, threat analysis should be focused, to a certain extent, by the existence of potential corresponding vulnerabilities and impacts.

This process area focuses on the analysis required to identify the applicable threats. The analysis required for proper use of the identified threats will be addressed in IA-PA07 (Assess Risk).

Since threats are constantly changing, this Process Area must incorporate periodic up-dates of threat sources to ensure the validity of the threat analysis.

Base Practices List

IA-BP04.01 Identify applicable threats arising from a natural source.

IA-BP04.02 Identify applicable threats arising from man-made sources, either accidental or deliberate.

IA-BP04.01 – Identify applicable threats arising from a natural source

Verify assessor's ability to identify threats arising from a natural source that have the capability to impact the site operations.

Description

The purpose of this base practice is to develop a list of natural threats that are applicable to a particular location. A critical aspect of identifying threat applicability is the analysis of site-specific impacts to organizational operation for a particular threat.

Example Work Products

?? List of applicable natural threats

Notes

Threats arising from natural causes include earthquakes, tsunami, tornadoes, and floods. Not all threats can occur in all locations. For example it is not possible for a tsunami to occur in the center of a large continent. Thus it is important to identify which natural threats can occur in a specific location.

Much of the information required for INFOSEC assessments can be obtained from actuarial lists and natural phenomena occurrence databases. While this information is valuable, it should be used with caution as it may be highly generalized and therefore may need to be interpreted to address the specific environment in terms of actual potential impact

IA-BP04.02 – Identify applicable threats arising from man-made sources

Verify assessor's ability to identify threats arising from man-made sources, either accidental or deliberate, which have the potential to impact the site operations.

Description

The purpose of this base practice is to analyze man-made threats that are applicable to a particular organization. A critical aspect of identifying threat applicability is the analysis of site-specific impacts to organizational operation for a particular threat.

Example Work Products

?? List of applicable man-made threats

Notes

The IAM focuses on the capabilities of potential adversaries. Thus, it is important to remain current with known, as well as postulated tools and techniques that could potentially be used by an adversary.

The IAM addresses two types of man-made threats: those that are inadvertent, and those that result from a deliberate act. To understand the applicability of man-made threats, it may be helpful to develop scenarios describing how the threat might potentially impact site operations. Use of generic man-made threat sources should be reviewed for completeness and relevancy.

The probability of a successful attack depends upon the ability of the threat agent, motivation, and the resources that the threat agent has at their disposal. Motivation for performing the act may be affected by the agent's assessment of the attractiveness of the target. A threat agent may use multiple attacks in sequence or concurrently to achieve the desired goal. The effect of multiple attacks occurring in sequence or concurrently needs to be considered. The development of scenarios can assist in performing this task.

IA-PA05: Assess Vulnerability

Summary Description

The purpose of Assess Vulnerability is to determine the assessor's ability to identify and characterize INFOSEC vulnerabilities. This process area includes analyzing current INFOSEC posture against system security requirements IA-BP03.05 (Capture Initial System Security Requirements). In the IAM, "vulnerability" refers to a weakness of the system (mechanism or procedure) that can potentially be exploited in some way that is detrimental to the organization's capability to perform its mission.

Goals

?? To identify and understand organizational INFOSEC vulnerabilities.

Process Area Notes

While the activities involved with gathering threat, vulnerability, and impact information have been grouped into separate Process Areas, they are interdependent when performing risk analysis. Therefore, the search for vulnerabilities should be guided to a certain extent, by the existence of corresponding threats and impacts.

Since new vulnerabilities are constantly arising, this Process Area must incorporate periodic up-dates of vulnerability sources and analysis techniques.

Base Practices List

IA-BP05.01	Identify applicable INFOSEC vulnerabilities
IA-BP05.02	Define vulnerability characteristics
IA-BP05.03	Determine overall vulnerability

IA-BP05.01 – Identify Applicable INFOSEC Vulnerabilities

Verify assessor's ability to identify applicable INFOSEC vulnerabilities for a specified operational system.

Description

The purpose of this base practice is to determine an assessor's ability to identify applicable INFOSEC vulnerabilities for a specified operational system. These INFOSEC vulnerabilities apply to any combination of system mechanisms, assurances, and/or procedures that fall within the scope of the INFOSEC assessment as outlined in the INFOSEC Assessment Report

Example Work Products

?? Final INFOSEC Assessment Report

Notes

The final INFOSEC Assessment Report can be used as evidence that vulnerabilities were identified.

For completeness purposes, procedures should be in place that guide assessors in determining that all applicable INFOSEC vulnerabilities (to include, at a minimum, the IAM baseline categories) were investigated and determined to potentially exist or not.

The applicability of INFOSEC vulnerabilities must encompass a systems approach. INFOSEC functions are sometimes supported by non-INFOSEC mechanisms that may have exploitable vulnerabilities that could adversely impact the INFOSEC posture as such, the search for potential vulnerabilities should not be strictly limited to INFOSEC functions and mechanisms.

IA-BP05.02 – Define Vulnerability Characteristics

Verify assessor's ability to analyze the characteristics of identified INFOSEC vulnerabilities.

Description

The purpose of this base practice is to define vulnerabilities in the context of the operational environment. Assessors need to understand the underlying characteristics of the vulnerabilities. Both why they are vulnerabilities as well as their dependency to an impacts are important in order to provide appropriate recommendations for the elimination or mitigation of the vulnerabilities.

Example Work Products

?? Final INFOSEC Assessment Report

Notes

The Final INFOSEC Assessment Report can be used as evidence that vulnerability characteristics were analyzed. The discussion portion of the vulnerability analysis should provide information concerning the characteristics of the identified vulnerabilities.

INFOSEC mechanisms and functions are susceptible to varying levels of attack depending upon their implementation. An example is the implementation of passwords. There are varying characteristics of passwords (e.g. length, format, expiration), each of which lends itself to varying degrees of exploitation and can have varying effects on impacts.

IA-BP05.03 – Determine Aggregate Vulnerability

Verify assessor's ability to analyze combinations of specific vulnerabilities in order to determine aggregate system vulnerabilities.

Description

The purpose of this base practice is to measure and assessor's ability to identify vulnerabilities that result from interdependencies of INFOSEC mechanisms and procedures, and/or the aggregate effects/concerns of identified vulnerabilities.

Example Work Products

?? Final Assessment Report.

Notes

The assessor needs to be able to analyze the interdependencies of the identified vulnerabilities. These interdependencies can promulgate additional vulnerabilities or increase the likelihood of exploitation of known vulnerabilities. In addition, the assessors need to identify vulnerabilities from the aggregate of dependent INFOSEC mechanisms and procedures which individually do not contain vulnerabilities. The aggregate effect of putting certain sets of non-INFOSEC mechanisms and procedures together can adversely affect the INFOSEC vulnerability posture of a site. These combinations should be identified and reported whenever possible within the scope of an INFOSEC appraisal.

IA-PA06: Assess Impact

Summary Description

The purpose of Assess Impact is to determine an assessor’s ability to identify the severity and type of impact to organizational capabilities caused by the exploitation of vulnerabilities to information assets. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.

Goals

?? To identify and characterize potential impacts to the organization’s capability.

Process Area Notes

The organizational capabilities are impacted as a consequence of the exploitation of vulnerabilities, either deliberate or accidental. The types of impacts the IAM addresses are, at a minimum, confidentiality, integrity, and availability.

The severity of impacts assists in determining the balance between the results of an unwanted incident and the cost (financial and/or operational) of the safeguards to protect against the unwanted incident.

While the activities involved with gathering threat, vulnerability, and impact information have been grouped into separate Process Areas, they are interdependent when performing risk analysis. The identification of impacts is influenced by the convergence of potential threats and vulnerabilities.

Base Practices List

IA-BP06.01 Analyze organizational missions and capabilities.

IA-BP06.02 Identify information assets required to support organizational missions.

IA-BP06.03 Identify system assets required to support organizational missions.

IA-BP06.04 Identify and characterize impacts.

IA-BP06.01 – Analyze Organizational Missions and Capabilities

Verify assessor’s ability to identify organizational missions and analyze the capabilities required to perform those missions.

Description

The purpose of this base practice is to determine an assessor's ability to understand operational missions. Additionally, the capabilities needed to perform these missions must be identified and analyzed. The understanding of organizational capabilities is crucial to the identification and analysis of critical information assets.

Example Work Products

?? INFOSEC Assessment Plan

Notes

The INFOSEC Assessment Plan should identify the organizational missions and capabilities.

The analyses of impact, threat, vulnerability, risk, and the recommendation of countermeasures are all dependent upon a clear understanding of the organizational missions.

IA-BP06.02 – Identify Information Assets Required to Support Organizational Missions

Verify assessor's ability to identify organizational information assets that are required to support critical missions.

Description

The purpose of this base practice is to determine an assessor's ability to identify information assets that support the organization's mission(s).

Example Work Products

?? The INFOSEC Assessment Plan

Notes

The INFOSEC Assessment Plan should identify information assets.

The IAM focuses on information assets. It is recognized that organizational assets also include the people, environment, technology, and infrastructure. In the context of the IAM, these other assets are only examined with respect to information assets.

IA-BP06.03 - Identify system assets required to support organizational mission

Verify the assessor’s ability to identify system assets that store, transmit, and/or process critical information.

Description

The purpose of this base practice is to determine and assessor's ability to identify the systems that are/could be handling critical information in the performance of organizational missions.

Example Work Products

?? INFOSEC Assessment Plan

Notes

The Assessment Plan should contain system(s) description identifying all relevant systems assets required for critical mission capability.

All potential critical systems should be examined to properly scope the assessment effort. Assessors and customers should use a prioritized list of systems (with their system criticality matrices), along with time constraints, size of the systems, and other consideration to assist in the planning of the assessment effort.

IA-BP06.04 – Identify and Characterize Impacts

Verify the assessor's ability to identify and characterize impacts to the organizational missions.

Description

The purpose of this base practice is to determine the assessor's ability to describe the type and severity of impacts in terms of their effect on organizational capabilities.

Example Work Products

?? INFOSEC Assessment Plan

Notes

The assessment plan should contain analysis of impacts, to include criticality matrices along with impact definitions and assignments.

The types of impacts the IAM addresses are, at a minimum, confidentiality, integrity, and availability. The severity of impacts assists in determining the balance between the results of an unwanted incident and the cost (financial and/or operational) of the safeguards to protect against the unwanted incident.

Characterization helps in determining the significance of an impact based on its effect on the organization's ability to carry out its mission. In most cases there will be some subjectivity associated with specifying impact within a specified environment.

IA-PA07: Assess INFOSEC Risk

Summary Description

The purpose of Assess INFOSEC Risk is to determine an assessor’s ability to identify and analyze INFOSEC risks to a specified system in a specified environment. The assessor should be able to compare risk factors for “exploitations” of information assets. “Exploitation” refers to manifestation of an event due to the combination of threats, vulnerabilities, and impacts that influence an organization's missions. For the IA-CMM purposes, risk can be thought of as violations of INFOSEC requirements.

This process area focuses on ascertaining 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 exploitations.

Goals

?? Identifying the interdependencies of threats, vulnerabilities, and impacts

?? An analysis that allows an organization to compare and contrast exploitation scenarios as relating to the implementation of countermeasures.

?? An understanding of the security risk associated with operating the system within a defined environment is achieved.

Process Area Notes

INFOSEC risk is the likelihood and the impact of an unwanted incident. While related to program risks that apply to cost and schedule, INFOSEC risk deals specifically with protection of organizational missions from exploitations of information assets.

The first part of Assess INFOSEC Risk is the identification of the interdependence of input from threat, vulnerability, and impact process areas in order to form exploitation scenarios. The second part of Assess INFOSEC Risk is to analyze exploitations with respect to proposed countermeasures.

Risk estimates always include a factor of uncertainty, which will vary dependent upon a particular situation. This means that the likelihood can only be predicted within certain limits. In addition, impact assessed for a particular risk also has associated uncertainty, as the unwanted incident may not turn out as expected. Thus the majority of factors have a certain amount of uncertainty thereby reducing the accuracy of the predictions associated with them. In some cases these uncertainties may be large. This makes planning and the justification of security countermeasures very difficult.

Anything that can reduce the uncertainty associated with a particular situation is of considerable importance. For this reason, assurance is important as it indirectly reduces the risk of the system. This assurance is a factor of the assessor's ability and the infrastructure supporting the assessor (i.e. the organizational processes that ensure assessor capabilities).

The risk information produced by this PA depends on the threat information gathered from activities associated with IA-PA04 (Assess Threat), IA-PA05 (Assess Vulnerability), and IA-PA06 (Assess Impact). While activities involved with gathering threat, vulnerability, and impact information, are grouped into separate PAs, they are interdependent. This information forms the basis for the results provided in IA-PA08 (Provide IAM Analysis and Results).

Since risk environments are subject to change, they must be periodically monitored to ensure that the understanding of risk generated by this PA is maintained at all times.

Base Practices List

IA-BP07.01 Verify assessor's ability to identify threat/vulnerability/impact triples.

IA-BP07.02 Verify assessor's ability to assess risk associated with exploitations.

IA-BP07.03 Verify assessor's ability to identify potential countermeasures to risk

IA-BP07.01 – Identify threat/vulnerability/impact triples

Verify assessor's ability to identify threat/vulnerability/impact triples (exploitations).

Description

The purpose of this process area is to determine an assessor’s ability to identify exploitations by recognizing the interdependencies between threats, vulnerabilities, and impacts of exploitations.

These exploitations will be inputs to the analysis and selection of recommended countermeasures for the specified system.

Example Work Products

?? Final Assessment Report

Notes

IA-PA04 (Assess Threat), IA-PA05 (Assess Vulnerability) and IA-PA06 (Assess Impact) have identified and analyzed the components of risk independently. This PA determines the assessor's ability to bring them together and analyze them for interdependencies.

The accuracy of the products (information) from the previous PAs will have a great effect on the accuracy of the risk analysis.

IA-BP07.02 – Assess Risk Associated with Exploitations

Verify assessor's ability to identify and analyze risk.

Description

Determine the assessor’s ability to identify risks associated with identified exploitations.

Example Work Products

?? List of exploitations

Notes

The likelihood of exploitation is the combination of the likelihood of the threat and the likelihood of the vulnerability. In many cases the likelihood of a specific or generalized magnitude or severity of impact must also be factored in. In all cases there will be uncertainty associated with metrics. It is more effective to keep the factors of uncertainty separate so that when actions are taken to refine the working data it can be seen whether the refinement a result of the data or the uncertainty associated with the data. This can often impact the strategies adopted to address the risks. Once the exploitation scenarios are identified, risk factors must be assigned (quantitative and/or qualitative) in order to assist in risk management..

IA-BP07.03 – Identify Potential Countermeasures

Verify assessor's ability to determine potential countermeasures (solutions) to identified risks.

Description

Once risks are identified and analyzed, the assessor knows the current INFOSEC posture. This posture needs to be compared with the INFOSEC requirements identified in IA-PA03 (Specify Initial INFOSEC Needs) to determine the shortfalls. The assessors then must identify countermeasures that the customer can implement to mitigate or eliminate the possibility of exploitation.

Example Work Products

?? Final Assessment Report

Notes

The final assessment report should contain recommended countermeasures for each identified vulnerability. The assessor's analysis should provide alternate countermeasures (when applicable) so the customer can analyze them along with other factors (e.g., cost) when determining proper actions.

Although risk can be reduced by solutions for threat, vulnerability, or impact, the majority of solutions will pertain to the elimination or mitigation of vulnerabilities.

IA-PA08: Provide IAM Analysis and Results

Summary Description

The purpose of Provide IAM Analysis and Results is to determine an assessor’s ability to accurately report the findings and recommendations of an INFOSEC assessment activity to the site and interested third parties. This information includes the analysis performed in IA-PA04 (Assess Threat), IA-PA05 (Assess Vulnerability), IA-PA06 (Assess Threat) and IA-PA07 (Assess Risk) .

Goals

?? Provide the customer IAM analysis and results so they can make informed decisions concerning the enhancement of their INFOSEC posture.

?? Assure that any constraints or special emphasis requested by the customer are incorporated (when possible) into the results.

Process Area Notes

This process area provides security input to support the INFOSEC assessor organization’s ability to report results and analysis in accordance with the IAM.

Base Practices List

IA-BP08.01 Verify assessor's ability to properly convey the assessment analysis and results to the customer.

IA-BP08.02 Verify assessor's ability to ensure concerns and constraints are incorporated in the IAM analysis and results.

IA-BP08.01 – Convey Assessment Analysis and Results to the Customer

Verify assessor's ability to provide complete and proper information to the customer.

Description

The customer must be provided the results of the INFOSEC Assessment in order to meet the goals of making informed risk management decisions. The IAM has specified minimal guidelines in order to assure this occurs.

Example Work Products

?? Final Assessment report

?? Assessment out-brief materials

Notes

While the IAM specifies the minimal set of products to meet IARTP requirements, a complete INFOSEC assessment activity should also include additional materials to address specific customer needs.

IA-BP08.02 – Ensure Concerns and Constraints are Incorporated in Analysis and Results

Verify assessor's ability to Analyze and prioritize alternatives using INFOSEC constraints and considerations.

Description

The purpose of this base practice is to identify the ability of the assessor to provide the customer the INFOSEC analysis with all constraints and considerations taken into account. The INFOSEC analysis can incorporate constraints and considerations on the requirements, design, implementation, configuration, and documentation.

Example Work Products

?? INFOSEC Assessment Plan and Final report

Notes

The assessment plan should identify concerns and constraints. The final report can be used to demonstrate that the concerns and constraints were incorporated in the assessment analysis.

IA-PA09: Manage INFOSEC Assessment Processes

Summary description

The purpose of Manage INFOSEC Assessment Processes is to maintain data on and manage the status of the IAM processes. This includes the overall IAM management structure as well as the management of individual INFOSEC Assessments and to analyze and control changes to the process and its corresponding process management units.

In addition, this process area is applicable to all work products that are generated throughout the IAM activities. An example set of work products that may be placed under process management could include the INFOSEC Assessment Methodology, Assessment reports, Assessments Plans, Assessment schedule, and any Assessor tools.

Process Area Notes

The process management function supports the traceability of management decisions by allowing the process to be traced back through the occurrence of management events.

Proper INFOSEC Assessment management processes will allow for the optimization of IAM resources with respect to customer priorities.

Base Practices List

The following list contains the base practices that are essential elements of good systems engineering:

IA-BP09.01	Identify IAM process management structure.
IA-BP09.02	Manage Program and Project risk
IA-BP09.03	Maintain a repository of work product baselines.

IA-BP09.01 – Identify IAM Process Management Structure

Verify the proper management structure is in place to manage the IAM processes.

Description

The purpose of this Process Area is to provide assurance that the proper decisions are being made by the organization providing management resources. Analyzing the organizational chain of command and lines of authority is one way to help make this determination.

Typical Work Products

?? Identified organizational management structure

Notes

An example of the presence of a mature Management structure would be a set of processes that outline the review and release process for Final INFOSEC Assessment Reports.

IA-BP09.02 – Manage Program and Project Risk

Identify process that manages risk to successful completion of the IAM processes.

Description

The purpose of the Base Practice is to identify, assess, monitor, and mitigate risks to the success of both the overall IAM organization and individual INFOSEC Assessments.

Typical Work Products

?? Program risk management plan

Notes

This BP provides a level of assurance that the provider organizations are mature enough to determine potential pitfalls within their own ability to perform quality INFOSEC assessments.

IA-BP09.03 – Maintain a Repository of Work Product Baselines

Maintain a repository of work product baselines.

Description

This Base Practice involves establishing and maintaining a repository of information about the work products. Typically, this repository provides the configuration and examples of all work products that support the IAM. The repository can be used to maintain standardization for the different work products. This could also include an established procedure for additions, deletions, and modifications to the baseline, as well as procedures for tracking/ monitoring, auditing, and the accounting of configuration data.

Typical Work Products

?? Baseline configuration repository

Notes

Optimally, configuration data can be maintained in electronic format to facilitate updates and changes to supporting documentation.

If the proper baseline work products are in the repository, they can be used to measure the level of assurance that the organization is in compliance with the IAM program objective.

Generic Practices

This chapter contains the generic practices, that is, the practices that apply to all processes. The generic practices (GPs) are used in a process appraisal to determine the capability level of a specific Process Area (PA). The generic practices are grouped according to common feature and capability level.

The generic practices are divided into the following capability levels, each of which has several common features:

- ?? Capability Level 0 - Not Performed
- ?? Capability Level 1 - Performed Informally
- ?? Capability Level 2 - Planned and Tracked
- ?? Capability Level 3 - Well Defined
- ?? Capability Level 4 - Quantitatively Controlled
- ?? Capability Level 5 - Continuously Improving

Capability Level 1 – Performed Informally

Summary Description

Base practices of the process area are generally performed. The performance of these base practices may not be rigorously planned and tracked. Performance depends on individual knowledge and effort. Work products of the process area testify to their performance. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for the process.

Common Features List

This capability level comprises the following common features:

?? Common Feature 1.1 – Base Practices Are Performed

Common Feature 1.1 – Base Practices Are Performed

Summary Description

The Generic Practices of this Common Feature simply ensure that the Base Practices of the Process Area are being performed in some manner. However, the consistency or performance and the quality of the work products produced are likely to be highly variable due to the ad hoc nature of the controls that are in place.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 1.1.1 – Perform the Process

GP 1.1.1 – Perform the Process

Description

Perform a process that implements the base practices of the process area to provide work products and/or services to a customer.

Notes

This process may be termed the “informal process.” The customer(s) of the process area may be internal or external to the organization.

Capability Level 2 – Planned and Tracked

Summary Description

Performance of the base practices in the process area is planned and tracked. Performance according to specified procedures is verified. Work products conform to specified standards and requirements. Measurement is used to track process area performance, thus enabling the organization to manage its activities based on actual performance. The primary distinction from the Performed Informally level is that the performance of the process is planned and managed via a documented process.

Common Features List

This capability level comprises the following common features:

?? Common Feature 2.1 – Planning Performance

?? Common Feature 2.2 – Disciplined Performance

?? Common Feature 2.3 – Verifying Performance

?? Common Feature 2.4 – Tracking Performance

Common Feature 2.1 – Planning Performance

Summary Description

This generic practice introduces the first level of measurable maturity (i.e. a plan). The purpose is to establish a baseline capability that is used within a provider organization. The plans do not have to be standardized process across the organization, but are applicable to specific group of individuals (i.e. Assessment team, Network team, Threat analysis team).

Generic Practices List

This common feature comprises the following generic practices:

?? GP 2.1.1 – Allocate Resources

?? GP 2.1.2 – Assign Responsibilities

?? GP 2.1.3 – Document the Process

?? GP 2.1.4 – Provide Tools

?? GP 2.1.5 – Ensure Training

?? GP 2.1.6 – Plan the Process

GP 2.1.1 – Allocate Resources

Description

Allocate adequate resources (including time, tools, and people) for performing the process area.

Notes

In order to allocate resources effectively, an organization should have, at a minimum, an individual responsible for allocation functions (e.g. needs identification, levels of effort, qualifications). At this level, the responsible entity may be defined on a project-by-project basis, but as the organization matures, one would expect to see a centralized allocation method/authority.

Relationships

The INFOSEC assessment plan can provide evidence that critical resources have been identified for a particular activity. In order to achieve level two, evidence must be provided that managerial controls exist at the project level to support the activity.

GP 2.1.2 – Assign Responsibilities

Description

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

Notes

This activity is generally assigned to the local operational authority responsible for the execution of a specific task. It is not until higher levels of maturity that clear lines of responsibility and authority originate and are enforced from the top down.

Relationships

This practice is focuses on an organization's ability to adequately staff an individual INFOSEC assessment activity to ensure that the final products (e.g. Assessment report) address the customer needs.

GP 2.1.3 – Document the Process

Description

Document the approach to performing the process area in standards and/or procedures (i.e. INFOSEC Assessment Methodology)

Notes

Participation of the people who perform a process (its owners) is essential for creating a usable process description. Processes in an organization or on a project need not map one to one with the process areas in the IA-CMM. Therefore, processes addressing a process area may be described in more than one way (e.g., policies, standards, and/or procedures), to cover a process area, and process descriptions may span more than one process area.

Relationships

Relationship to other generic practices: This is the “level 2” process description.

Standards and procedures that describe the process at this level are likely to include measurements, so that the performance can be tracked in GP 2.4 (Tracking Performance).

GP 2.1.4 – Provide Tools

Description

Provide appropriate tools to support performance of the process area.

Notes

Tools can range from formal special purpose process tracking tools developed in house to COTS scheduling software, e-mail, databases, best-practice matrices or status meetings.

Relationships

Tool changes made at this level may adversely impact the organization’s ability to achieve higher levels of maturity. Therefore organizations should evaluate and select tools that support their level of maturity objectives.

GP 2.1.5 – Ensure Training

Description

Ensure that the individuals performing the process area are appropriately trained in how to perform the process.

Notes

Training, and how it is delivered, must flex with process capability due to changes in how the process is performed and managed. The Provide Ongoing Skills and Knowledge PA measures whether a training program exists; this GP determines whether the specific training for a given PA is adequate to support the activities defined within the PA. It is possible to have a level 5 training program (e.g. IA-PA01 = Level 5) and still not train in the proper areas.

Relationships

Training and training management is described in IA-PA01 (Provide Ongoing Skills and Knowledge).

GP 2.1.6 – Plan the Process

Description

Plan the performance of the process area.

Notes

Plans for process areas in the engineering and project categories may be in the form of a project plan, whereas plans for the organization category may be at the organizational level.

Relationships

This GP leverages off GP 2.1.3 (Document the Process). Without a documented process, there is little assurance that effective planning can be developed.

Common Feature 2.2 – Disciplined Performance

Summary Description

Once a baseline set of documents is established, the organization must provide evidence that they are being implemented appropriately within the individual assessment activity to achieve level 2.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 2.2.1 – Use Plans, Standards, and Procedures

?? GP 2.2.2 – Do Process management

GP 2.2.1 – Use Plans, Standards, and Procedures

Description

Use documented plans, standards, guidelines, and/or procedures in implementing the process area.

Notes

A process performed according to its descriptions is termed a "described process." Process measures should be defined in the standards, procedures, and plans. The IAM shall be a fundamental part of establishing a documented process for conducting INFOSEC assessments.

Relationships

The standards and procedures used here were documented in 2.1.3 (Document the Process), and the plans used were documented in 2.1.6 (Plan the Process). This practice is an evolution of 1.1.1 (Perform the Process) and evolves to 3.2.1 (Use a Well-Defined Process).

GP 2.2.2 – Do Process Management

Description

This generic practice requires that the work products of the process area are placed under version control and appropriately managed

Notes

The appropriate management of the work products implies that various documents and procedures are appropriately maintained and disseminated throughout the organization to facilitate knowledge transfer from lessons as learned.

Relationships

Where process area IA-PA09 (Manage INFOSEC Assessment Processes) focuses on the general practices of the IAM process. This generic practice is focused on the management (e.g. version control) of the various work products within a specific process area.

Common Feature 2.3 – Verifying Performance

Summary Description

This Generic Practice is the verification and validation of the level 2 activities.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 2.3.1 – Verify Process Compliance

?? GP 2.3.2 – Audit Work Products

GP 2.3.1 – Verify Process Compliance

Description

Verify compliance of the process with applicable standards and/or procedures.

Notes

This generic process focuses on the management's ability to ensure that the procedures are followed as documented.

Relationships

Relationship to other generic practices: The applicable standards and procedures were documented in 2.1.3 (Document the Process) and used in 2.2.1 (Use Plans Standards and Procedures).

GP 2.3.2 – Audit Work Products

Description

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

Notes

Work products are those documents that support the activities of the IAM and are the resultant output of an assessment (i.e. The INFOSEC assessment report).

Relationships

?? Relationship to other generic practices: The applicable standards and procedures were documented in 2.1.3 (Document the Process) and used in 2.2.1 (Use Plans Standards and Procedures).

Common Feature 2.4 – Tracking Performance

Summary Description

This Generic Practice is designed to gather process related measurements as the foundation for building a standardized process capability. Corrective action is used to refine the current processes to ensure the most efficient standard is created.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 2.4.1 – Track with Measurement

?? GP 2.4.2 – Take Corrective Action

GP 2.4.1 – Track with Measurement

Description

Track the status of the process area against the plan using measurement.

Notes

Building a history of measures is a foundation for managing by data, and is begun here. Measurements of interest are process oriented. For example, if during an assessment a problem is encountered that results in a significant divergence from the assessment plan, the cause of the problem should be identified and documented for future reference. The purpose of measurement is to identify potential process weaknesses encountered during an assessment. The potential weaknesses identified here will be used as a foundation for refining processes at the higher levels of maturity.

Relationships

Relationship to other generic practices: The use of measurement implies that the measures have been defined and selected in 2.1.3 (Document the Process) and 2.1.6 (Plan the Process), and data have been collected in 2.2.1 (Use Plans Standards and Procedures).

GP 2.4.2 – Take Corrective Action

Description

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

Notes

Progress may vary from documented or past performance because estimates were inaccurate, performance was affected by external factors, or the requirements, on which the plan was based, have changed. Corrective action may involve changing the process, changing the plan, or both. The corrective action is the result of an unexpected occurrence during an assessment activity that the team was not prepared to address. These actions are documented and reported for use in refining future assessment activities.

Relationships

Relationship to other generic practices: The use of measurement implies that the measures have been defined and selected in 2.1.3 (Document the Process) and 2.1.6 (Plan the Process), and data have been collected in 2.2.1 (Use Plans, Standards and Procedures).

Capability Level 3 – Well-Defined

Summary Description

Base practices are performed according to a well-defined process using approved, tailored versions of a standard, documented process. The primary distinction from the Planned and Tracked level is that the process is planned and managed using an organization-wide standard process as opposed to an individual assessment activity

Common Features List

This capability level comprises the following common features:

?? Common Feature 3.1 – Defining a Standard Process

?? Common Feature 3.2 – Perform the Defined Process

?? Common Feature 3.3 – Coordinate Practices

Common Feature 3.1 – Defining a Standard Process

Summary Description

The Generic Practices of this Common Feature focus on the institutionalization of a standard process for the organization. The origin or basis of the institutionalized process may be one or more similar processes used successfully on specific projects. An organization standard process is likely to need tailoring to specific situational usage so the development of tailoring needs is also considered. Thus documentation of a standard process for the organization, and tailoring of the standard process to specific uses are addressed. These Generic Processes form an essential foundation to the performance of defined processes.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 3.1.1 – Standardize the Process

?? GP 3.1.2 – Tailor the Standard Process

GP 3.1.1 – Standardize the Process

Description

Document a standard process or family of processes for the organization that describes how to implement the base practices of the process area.

Notes

The critical distinction between the Level 2 Generic Practices and Level 3 Generic Practices is the scope of application of the policies, standards, and procedures. At Level 2, the standards and procedures may be in use in only an individual assessment activity. At Level 3, policies, standards, and procedures are being established at an organizational level for common use.

More than one standard process description may be defined to cover a process area, as the processes in an organization need not correspond one to one with the process areas in this capability maturity model. Also, a defined process may span multiple process areas. The IA-CMM does not dictate the organization or structure of process descriptions. Therefore, more than one standard process may be defined to address the differences among application domains, customer constraints, etc. These are termed a “standard process family.”

Relationships

The Level 2 process description was provided in GP 2.1.3 (Document the Process). The Level 3 process description is tailored in 3.1.2 (Tailor the Standard Process).

GP 3.1.2 – Tailor the Standard Process

Description

Tailor the organization's standard process to create a defined process that addresses the particular needs of a specific use.

Notes

Tailoring the organization’s standard process creates the Level 3 process definition. For defined processes at the project level, the tailoring addresses the particular needs of an individual assessment activity.

Relationships

The organization's standard process is documented in 3.1.1 (Standardize the Process). The tailored process definition is used in 3.2.1 (Use a Well-Defined Process).

Common Feature 3.2 – Perform the Defined Process

Summary Description

The Generic Practices of this Common Feature focus on the repeatable performance of a well-defined process. Thus the use of the institutionalized process, the review of the results of the process, work products, for defects, and use of data on the performance and results of the process are addressed. These Generic Practices form an important foundation for the coordination of the various assessment activities.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 3.2.1 – Use a Well-Defined Process

?? GP 3.2.2 – Perform Defect Reviews

?? GP 3.2.3 – Use Well-Defined Data

GP 3.2.1 – Use a Well-Defined Process

Description

Use a well-defined process in implementing the process area.

Notes

A "defined process" will typically be tailored from the organization's standard process definition. A well-defined process is one with policies, standards, inputs, entry criteria, activities, procedures, specified roles, measurements, validation, templates, outputs, and exit criteria that are documented, consistent, and complete.

Relationships

Relationship to other generic practices: The organization's standard process definition is described in 3.1.1 (Standardize the Process). The defined process is established through tailoring in 3.1.2 (Tailor the Standardized Process).

GP 3.2.2 – Perform Defect Reviews

Description

Perform defect reviews of appropriate work products of the process area.

Notes

This Generic Practice requires that the organization have a central point of control for the review and release of critical information (e.g. Assessment Reports).

Relationships

Defects (i.e. errors or failures in quality) identified in the various work products should be used to refine the data in future reports.

GP 3.2.3 – Use Well-Defined Data

Description

Use data on performing the defined process to manage it.

Notes

The measurement activity-based data was first collected at level 2. At Level 3 this data is analyzed to generate information that can be used to manage the process and lay the foundation for process-based metrics. Data at Level 3 can be qualitative or quantitative in nature as long is it is defined and applied across the entire organization. In order to transition to Level 4 all data must be quantitative.

This GP lays the foundation for quantitative management that will be used at the Level 4.

Relationships

This is an evolution of 2.4.2 (Take Corrective Action) and 3.2.2 (Perform Defect Reviews). Corrective action taken here is based on GP 3.2.1 (Use a Well-Defined Process).

Common Feature 3.3 – Coordinate Practices

Summary Description

The Generic Practices of this Common Feature focus on the coordination of activities throughout the project and the organization. Various groups throughout the projects and organization perform significant activities. A lack of coordination can cause delays or incompatible results. Thus the coordination of intra-group, inter-group, and external activities must be appropriately addressed. These generic practices form an essential foundation to having the ability to quantitatively control processes.

A group is the set of people assigned to an individual assessment activity.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 3.3.1 – Perform Intra-Group Coordination

?? GP 3.3.2 – Perform Inter-Group Coordination

?? GP 3.3.3 – Perform External Coordination

GP 3.3.1 – Perform Intra-Group Coordination

Description

Coordinate communication within an individual assessment activity group.

Notes

This type of coordination addresses the need for the individuals within a specific area of expertise to relate their experiences with one another to mitigate potential future failures.

Relationships

Relationship to other generic practices: This GP is closely tied to GP 3.2.1 (Use a Well-Defined Process) in that processes need to be well defined in order to be effectively coordinated.

GP 3.3.2 – Perform Inter-Group Coordination

Description

Coordinate communication among the individual assessment activity groups within the organization.

Notes

Relationships between the individual assessment activity groups are established by management to ensure a common understanding of the commitments, expectations, and responsibilities of each activity within an organization. These activities and understandings are documented and agreed upon throughout the organization and address the interaction among various groups within the organization. Issues are tracked and resolved among all the affected groups within the organization.

Relationships

Relationship to other generic practices: This GP is closely tied to GP 3.2.1 (Use a Well-Defined Process) in that processes need to be well defined in order to be effectively coordinated.

Coordination objectives and approaches are addressed in IA-PA09 (Manage INFOSEC Assessment Processes)

GP 3.3.3 – Perform External Coordination

Description

Coordinate communication with external groups.

Notes

This type of coordination addresses the needs of external entities that request or require assessment results (e.g., customers, research organizations, sponsor organizations).

A relationship between external groups is established via a common understanding of the commitments, expectations, and responsibilities of each activity within an organization.

Relationships

Relationship to other generic practices: This GP is closely tied to GP 3.2.1 (Use a Well-Defined Process) in that processes need to be well-defined in order to be effectively coordinated.

Coordination objectives and approaches are addressed in IA-PA02 (Coordinate with Customer Organization)

Capability Level 4 – Quantitatively Controlled

Summary Description

Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed, and the quality of work products is quantitatively known. The primary distinction from the Well-Defined level is that the defined process is **quantitatively** understood and controlled.

Common Features List

This capability level comprises the following common features:

?? Common Feature 4.1 – Establishing Measurable Quality Goals

?? Common Feature 4.2 – Objectively Managing Performance

Common Feature 4.1 – Establishing Measurable Quality Goals

Summary Description

The Generic Practices of this common feature focus on the establishment of measurable targets for the work products developed by the organization's processes. Thus the establishment of quality goals is addressed. These generic practices form an essential foundation to objectively managing the performance of a process.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 4.1.1 – Establish Quality Goals

GP 4.1.1 – Establish Quality Goals

Description

Establish measurable quality goals for the work products of the organization's standard process family.

Notes

These quality goals can be tied to the strategic quality goals of the organization, the particular needs and priorities of the customer, or to the tactical needs of the project. The measures referred to here go beyond the traditional end-product measures. They are intended to imply sufficient understanding of the processes being used to enable intermediate goals for work product quality to be set and used.

Relationships

Data that is gathered in GP3.2.2 (Perform Defect Reviews) should be used as input for developing and measuring against a set of quality goals.

Common Feature 4.2 – Objectively Managing Performance

Summary Description

The Generic Practices of this common feature focus on determining a **quantitative** measure of process capability and making use of quantitative measures to manage the process. The determining the process capability quantitatively, and using the quantitative measures as a basis for corrective action are addressed. These generic practices form an essential foundation to having the ability to achieve continuous improvement.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 4.2.1 – Determine Process Capability

?? GP 4.2.2 – Use Process Capability

GP 4.2.1 – Determine Process Capability

Description

Determine the process capability of the defined process quantitatively.

Notes

This is a quantitative process capability based on a well-defined and measured process. Measurements are inherent in the process definition and are collected as the process is being performed. Quantitative metrics showing process capabilities are required at this level.

Relationships

The defined process is established through tailoring in 3.1.2 (Tailor the Standard Process) and performed in 3.2.1 (Use a Well-Defined Process). All data collected in GP 3.2.3 (Use Well-Defined Data) must be converted to quantitative data to be accepted at this level.

GP 4.2.2 – Use Process Capability

Description

Take corrective action as appropriate when the process is not performing within its process capability.

Notes

Special causes of variation, identified based on an understanding of process capability, are used to understand when and what kind of corrective action is appropriate. The corrective action being taken here is to future programs. The key here is that the organization has the ability to accurately capture the cause of a process failure within the current program and feed the information back to prevent future failures.

Relationships

Once GP 4.2.1 (Determine Process Capability) has been established, the organization can react to problems in the process set. This practice is an evolution of 3.2.3 (Use Well-Defined Data), with the addition of quantitative process capability to the defined process.

Capability Level 5 – Continuously Improving

Summary Description

Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization. Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies. The primary distinction from the quantitatively controlled level is that the defined process and the standard process undergo continuous refinement and improvement, based on a quantitative understanding of the impact of changes to these processes.

Common Features List

This capability level comprises the following common features:

?? Common Feature 5.1 – Improving Organizational Capability

?? Common Feature 5.2 – Improving Process Effectiveness

Common Feature 5.1 – Improving Organizational Capability

Summary Description

The Generic Practices of this common feature focus on comparing the use of the standard process throughout the organization and making comparisons between those different uses. As the process is used opportunities are sought for enhancing the standard process, and defects produced are analyzed to identify other potential enhancements to the standard process. Thus goals for process effectiveness are established, improvements to the standard process are identified, and are analyzed for potential changes to the standard process. These generic practices form an essential foundation to improving process effectiveness.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 5.1.1 – Establish Process Effectiveness Goals

?? GP 5.1.2 – Continuously Improve the Standard Process

GP 5.1.1 – Establish Process Effectiveness Goals

Description

Establish quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability.

GP 5.1.2 – Continuously Improve the Standard Process

Description

Continuously improve the process by changing the organization's standard process family to increase its effectiveness.

Notes

The information learned from managing individual projects is communicated back to the organization for analysis and deployment to other applicable areas. Changes to the organization's standard process family may come from innovations in technology or incremental improvements. Innovative improvements will usually be externally driven by new technologies. Incremental improvements will usually be internally driven by improvements made in tailoring for the defined process. Improving the standard process attacks common causes of variation.

Relationships

Special causes of variation are controlled in 4.2.2 (Use Process Capability).

Common Feature 5.2 – Improving Process Effectiveness

Summary Description

The generic practices of this common feature focus on making the standard process one that is in a continual state of controlled improvement.

Generic Practices List

This common feature comprises the following generic practices:

?? GP 5.2.1 – Perform Causal Analysis

?? GP 5.2.2 – Eliminate Defect Causes

?? GP 5.2.3 – Continuously Improve the Defined Process

GP 5.2.1 – Perform Causal Analysis

Description

Perform causal analysis of defects.

Notes

Those who perform the process are typically participants in this analysis. This is a pro-active causal analysis activity as well as re-active. Defects from prior projects of similar attributes can be used to target improvement areas for the new effort.

Relationships

Results of these analyses are used in 5.2.2 (Eliminate Defect Causes), and 5.2.3 (Continuously Improve the Defined Process).

GP 5.2.2 – Eliminate Defect Causes

Description

Eliminate the causes of defects in the defined process selectively.

Notes

Both common causes and special causes of variation are implied in this generic practice, and each type of defect may result in different action.

Relationships

Causes were identified in 5.2.1 (Perform Causal Analysis).

GP 5.2.3 – Continuously Improve the Defined Process

Description

Continuously improve process performance by changing the defined process to increase its effectiveness.

Notes

The improvements may be based on incremental improvement or innovative improvements such as new technologies (perhaps as part of pilot testing). Improvements will typically be driven by the goals established in 5.1.1 (Establish Process Effectiveness Goals). The key to this GP is that the corrections are made in "real time", not passed to the next program.

Relationships

Generic Practice 5.2.2 (Eliminate Defect Causes) may be one source of improvements. Goals were established in 5.1.1 (Establish Process Effectiveness Goals).