Assurance for CMMI – Draft Training

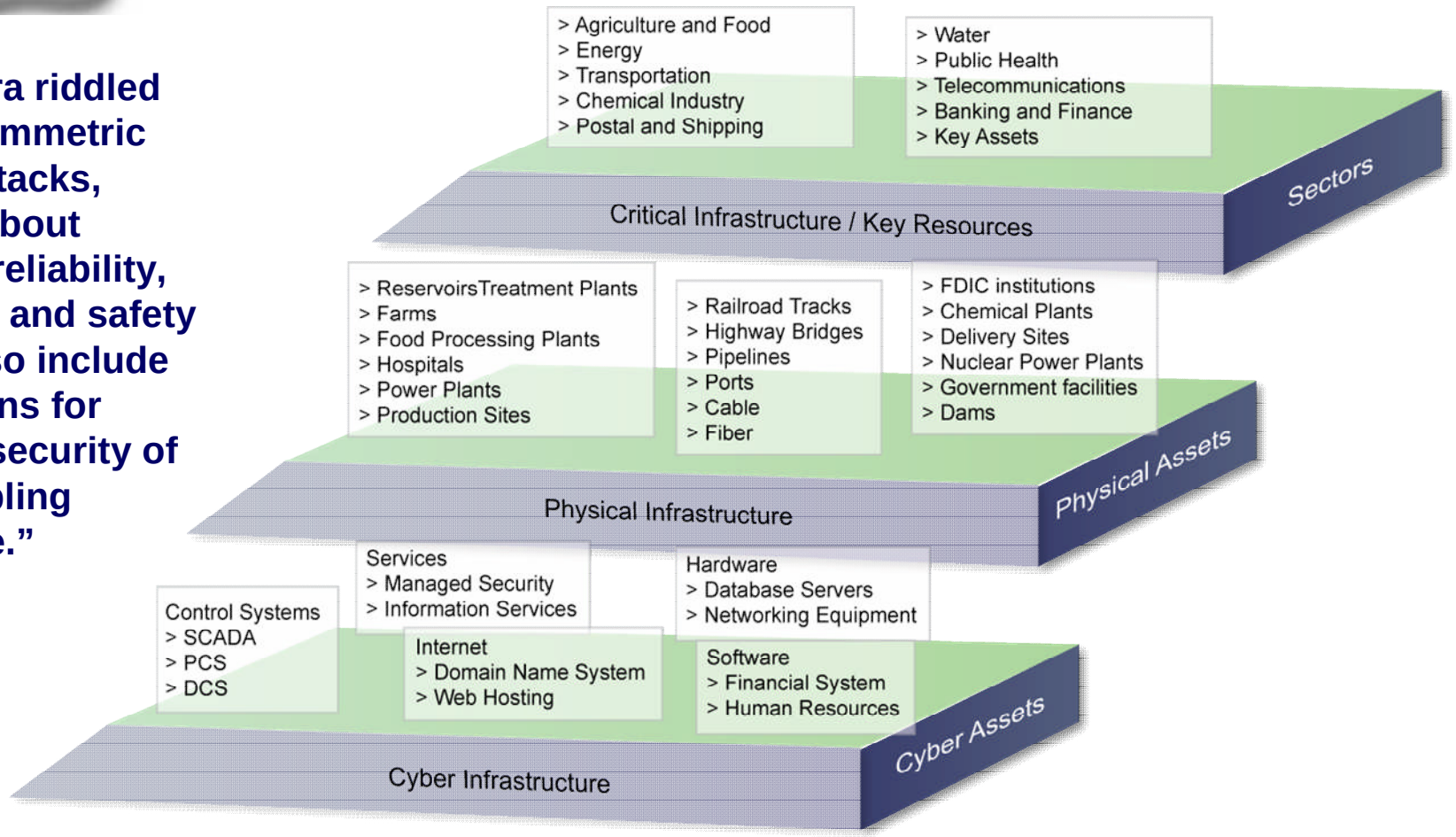
Homeland Security

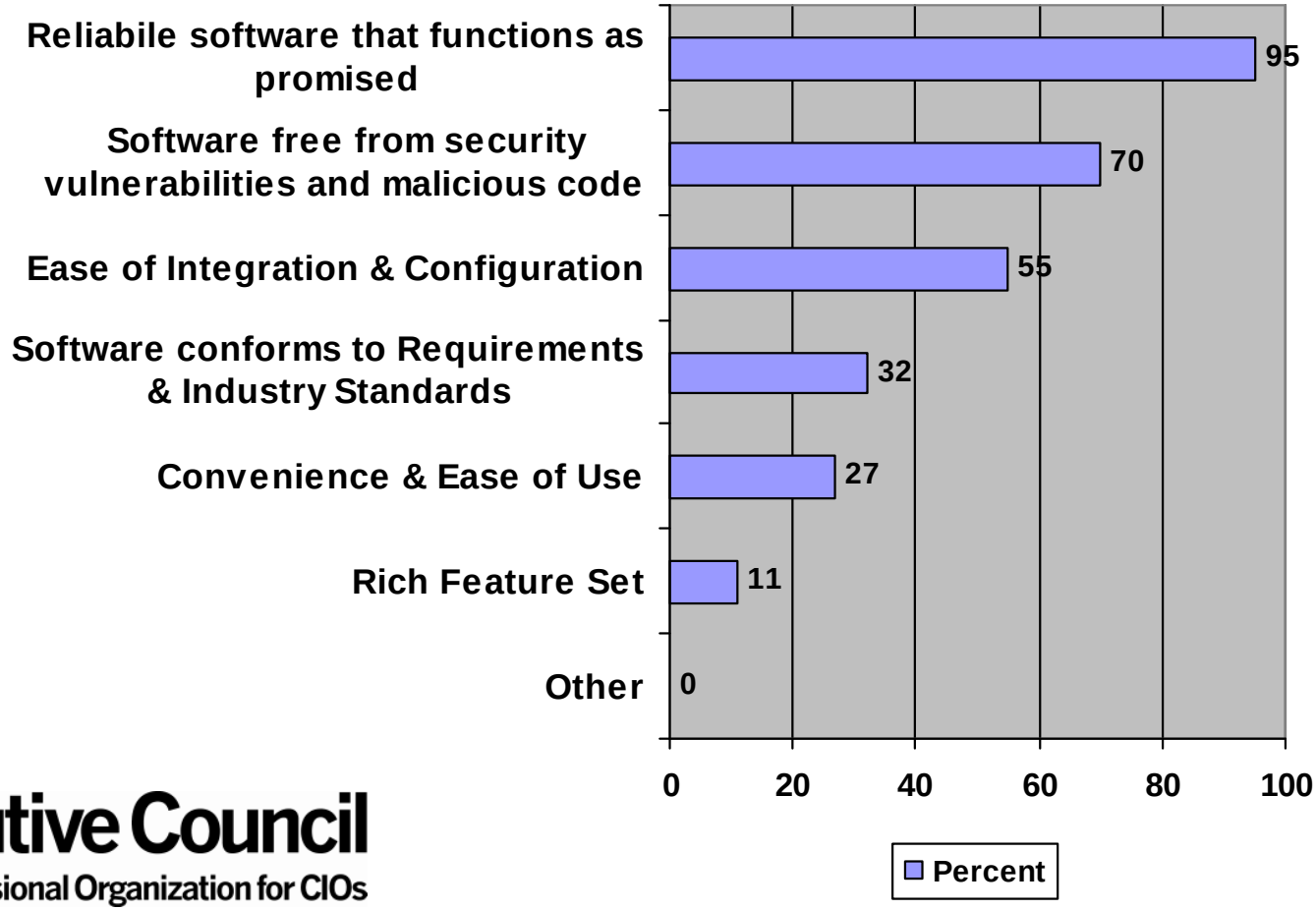
- Assurance 101 – why, what, where, how
- What does supply chain have to do with it?
- Understanding Process Capabilities
- Using measurement for decision making
- Conclusion

- **Assurance** – Grounds for confidence that an entity meets its security objectives [ISO/IEC 15408-1: 2005-10-01]
- **Software Assurance** – The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its life cycle, and the software functions in the intended manner [CNSSI 4009]

Assurance is a property of software or system that makes us more comfortable with relying on that system.

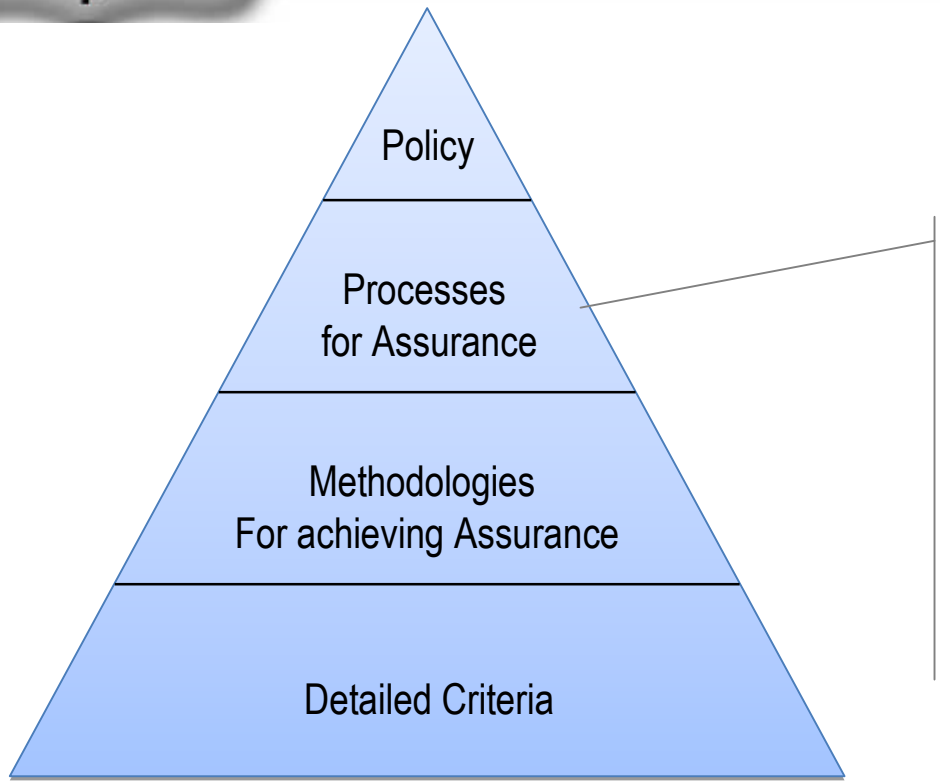
"In an era riddled with asymmetric cyber attacks, claims about system reliability, integrity and safety must also include provisions for built-in security of the enabling software."





CIO Executive Council
The Professional Organization for CIOs

https://www.cioexecutivecouncil.com October 11, 2006 Press Release



Project leadership and team members need to know where and how to contribute

Focus Topic: Assurance for CMMI ® defines the Assurance Thread for Implementation and Improvement of Assurance Practices

https://buildsecurityin.us-cert.gov/swa/procresrc.html

® Capability Maturity Model, Capability Maturity Modeling, and CMM are registered in the U.S. Patent & Trademark Office.

- March 2007: SEPG Birds of a Feather
- August 7, 2007: Industry Assurance for CMMI ® Meeting
- September 2007: Motorola, Lockheed Martin and Booz Allen form Assurance Working Group
- October 2007 – present: Assurance Harmonization Working Group
- January 2008 – present: Assurance Focus Topic Working Group
- July 16, 2008: Gained CMMI ® Steering Group approval to create Focus Topic for Assurance
- February 27, 2009: Submitted Change Requests for consideration in CMMI v 1.3
- Today
  - Completing draft documentation of the assurance thread through the CMMI ®
  - Refining practices and mapping to CMMI ® as necessary
  - Updating PRM practices with refined practices and revised CMMI mapping
  - Collecting feedback on use of draft materials

Requested Change

- Expand the current informative material in CMMI - DEV v1.2 to more specifically address assurance activities that enable predictable execution and trustworthiness of products and services Assurance practices have been harmonized and are articulated in a format compatible with the CMMI The latest work products from this effort are available at https://buildsecurityin.us-cert.gov/swa/procwg.html

Rationale

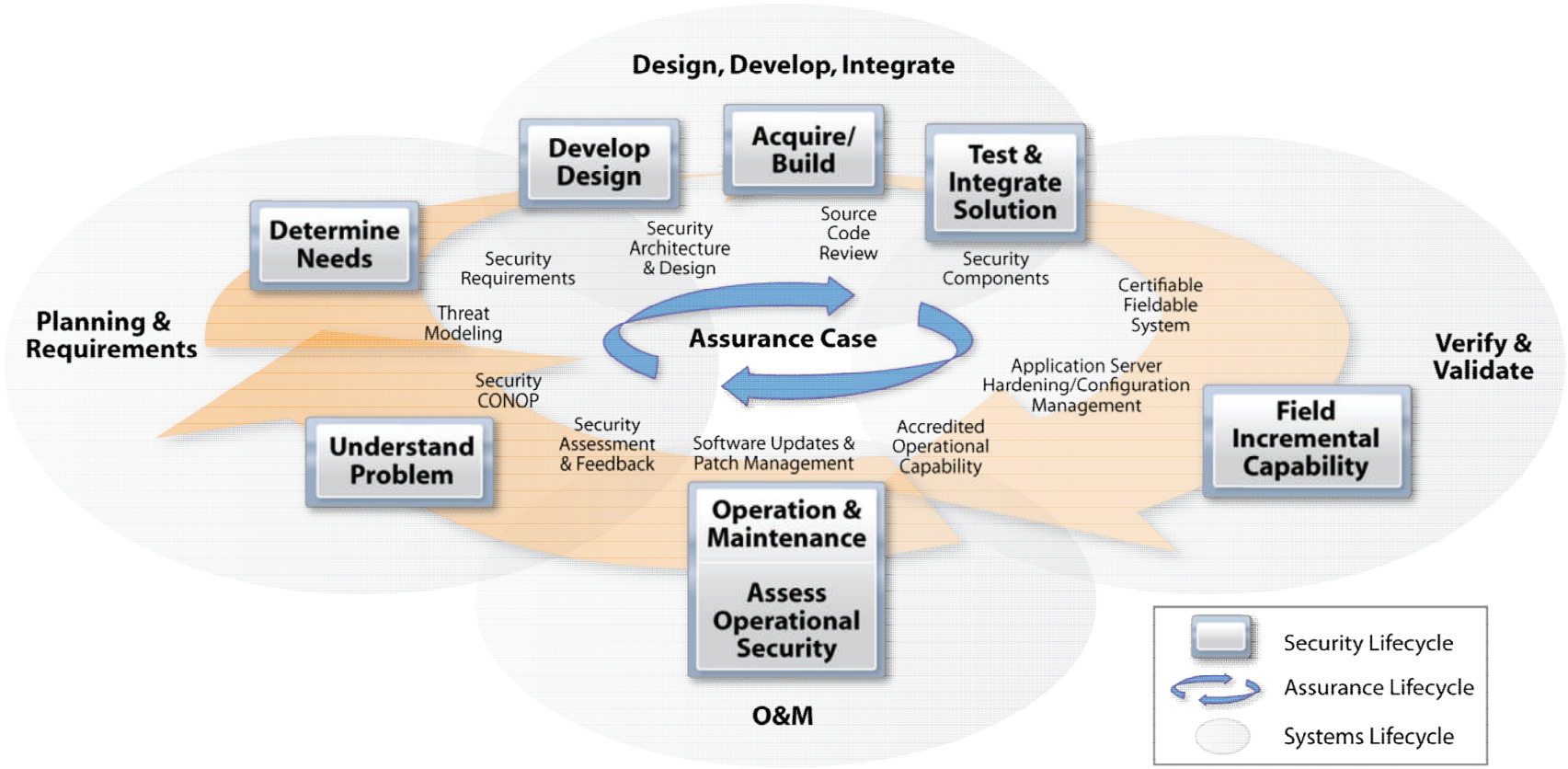
- Growing considerations related to globalization, systems of systems, system survivability, and cyber issues have resulted in an increasing number of organizations evolving the approach to address software and systems assurance in their products and services. Many of these organizations are formulating and implementing best practices and standards covering security, safety and reliability in the context of CMMI-DEV practices. Incorporating informative information in select CMMI-DEV practices will enable more streamlined planning, implementation, evaluation, and improvement of practices used to create and maintain products and services

Requested Change

- Establish a mechanism to enable use of the CMMI constellations and SCAMPI method with other frameworks and models deployed by organizations. Examples of other frameworks would include ISO 9000 and the Focus Topic for Assurance. The mechanism established should facilitate integration of the other frameworks/models with CMMI for both process improvement and appraisal. When other frameworks/models are used in conjunction with SCAMPI, they should be documented in the ADS. Given the challenges associated with integrating CMMI with other frameworks and models, consideration should be given to initially integrating those that more easily align architecturally with CMMI (e.g, CMMI Focus Topics) and those for which there is high user interest/need for alignment (e.g, in the assurance arena)

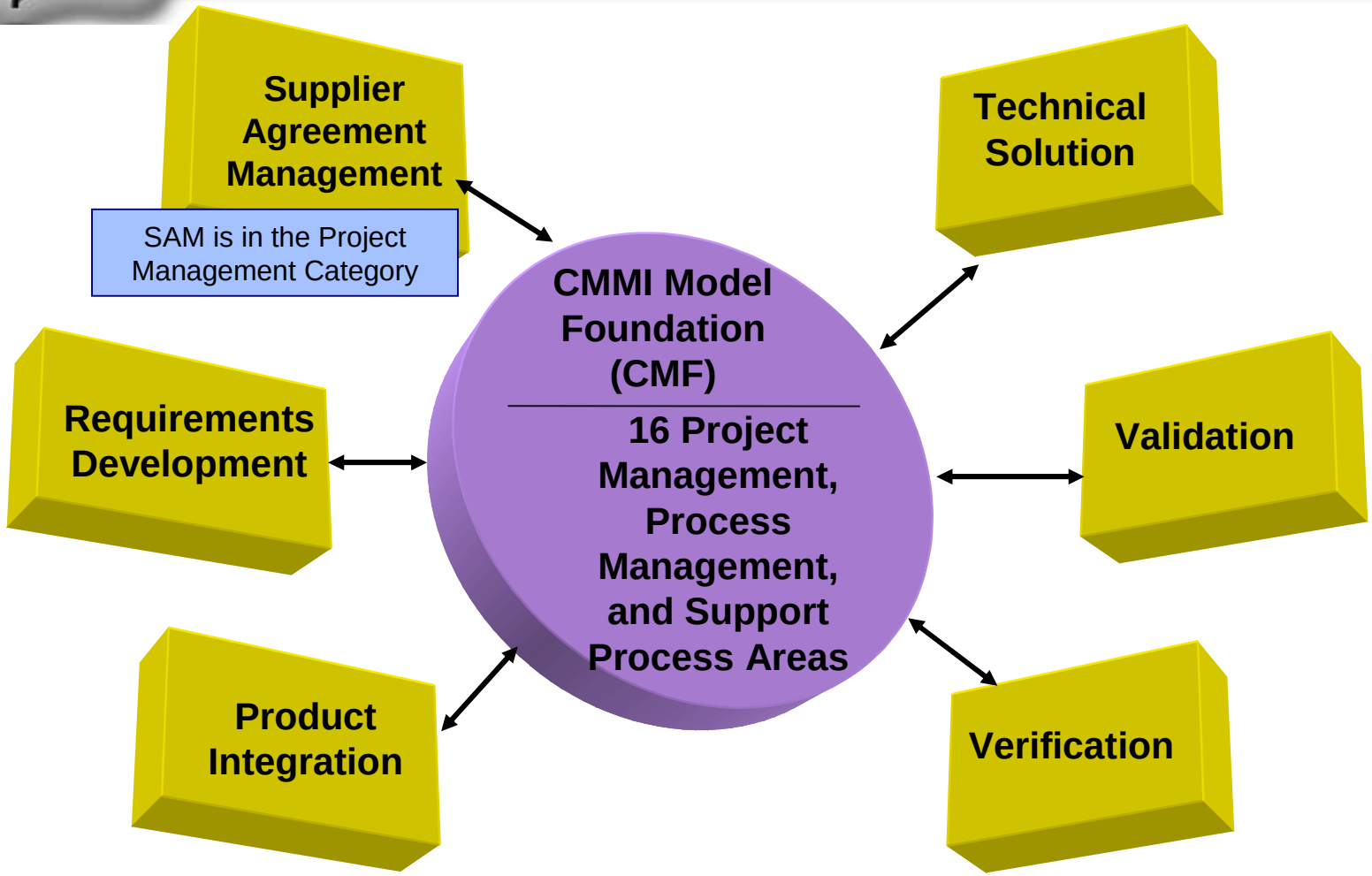
Rationale

- Organizations typically employ a number of frameworks and models to achieve their business and process improvement objectives. An integrated view of these frameworks/models with CMMI would enable more efficient and effective process improvement. In addition, appraisal could be conducted across multiple models/frameworks to reduce cost and disruption to program and organizational personnel

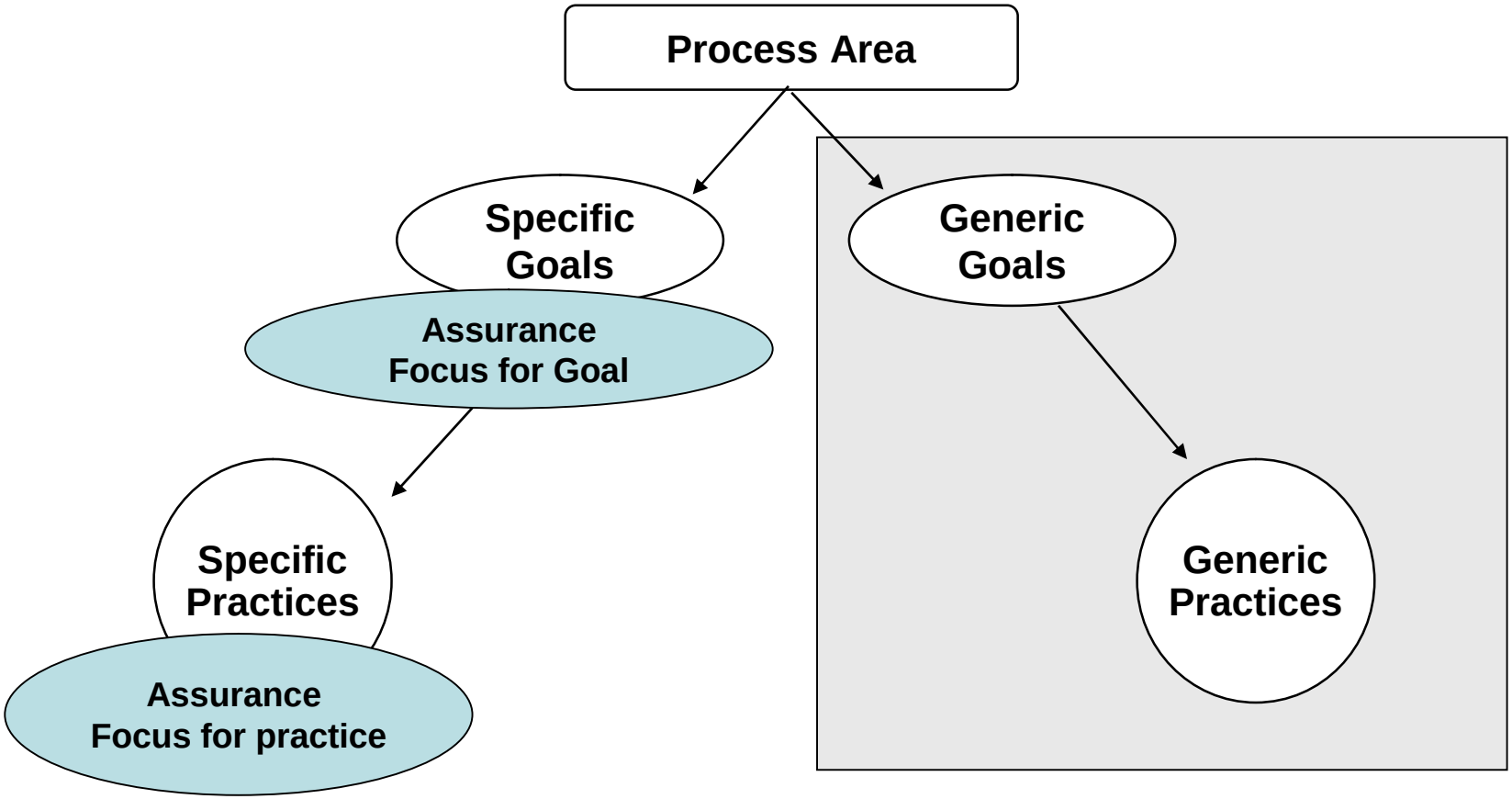


To be effective assurance must be integrated into the SDLC


SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN
CMMI-DEV v1.2


Supplier Agreement Management
SAM is in the Project Management Category
Technical Solution
CMMI Model Foundation (CMF)
16 Project Management, Process Management, and Support Process Areas
Requirements Development
Validation
Product Integration
Verification


SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN
Assurance For CMMI Identifies
The Assurance Thread for CMMI-DEV


Process Area
Specific Goals
Assurance Focus for Goal
Specific Practices
Assurance Focus for practice
Generic Goals
Generic Practices

The purpose of Organizational Training (OT) is to develop the skills and knowledge of people so they can perform their roles effectively and efficiently. [1, p. 275]

Addressing an organization's assurance training needs increases the likelihood that qualified and appropriately trained resources are performing the necessary integrated assurance activities on the project.

The use of the Focus Topic as described throughout this document creates a natural inclusion of assurance activities for the following practices within the OT process area: SP1.2, SP1.4, SP2.1, SP2.2, and SP2.3.

SG 1. A training capability, which supports the organization's management and technical roles, is established and maintained.

SP 1.1 Establish and maintain the strategic training needs of the organization.

Understanding the capabilities needed to achieve the strategic business objectives of an organization provides the foundation for planning and executing the necessary assurance skills within the organization.

AF 1.1.1 Establish and maintain the assurance training needs of the organization [2, SP1,3,3]

Specialized skills are necessary to achieve project and organizational assurance objectives. Assurance objectives included in the organization's strategic business objectives and process improvement plan contribute to the identification of potential future training needs.

Examples of categories of training needs for assurance include (but are not limited to) the following:

- Assurance (general awareness, organizational considerations, stakeholder considerations, legal implications, missions needs, abuse/misuse analysis, secure coding, testing, etc)
- Workforce credentials and certification maintenance requirements (i.e. Project Management Professional (PMP), Certified Information Systems Security Professional (CISSP))

Typical Work Products:

- Assurance Training Needs
- Assurance Assessment Analysis

Context of Assurance for the PA

Assurance practice aligned with existing CMMI® specific practice

Supporting examples, sub practices, etc that clarify the Assurance practice

Typical Work Products

CMMI Process Areas

- Organizational Process Focus
- Organizational Process Definition +IPPD
- Organizational Training
- Organizational Process Performance
- Organizational Innovation and Deployment

The purpose of Organizational Process Focus (OPF) is to plan, implement, and deploy organizational process improvements based on a thorough understanding of the current strengths and weaknesses of the organization's processes and process assets.

SG 1 Determine Process Improvement Opportunities

Strengths, weaknesses, and improvement opportunities for the organization's processes are identified periodically and as needed.

SP 1.1 Establish and maintain the description of the process needs and objectives for the organization.

In order to identify the assurance related process needs for the organization, it is necessary to understand the business objectives pertaining to assurance.

SP 1.2 Appraise the organization's processes periodically and as needed to maintain an understanding of their strengths and weaknesses.

SP 1.3 Identify improvements to the organization's processes and process assets

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for OPF SP 1.1

OPF SP 1.1

AF 1.1.1 Establish and maintain the description of the assurance context and objectives for the organization.

Description

The combination of these activities contribute to the identification and satisfaction of assurance needs for the organization and contribute to understanding the assurance context and objectives for the organization in the context of the business objectives

- Ensure assurance needs are reflected in organizational policy
- Establish and maintain budget allocation for the establishment, execution, and enhancement of assurance practices within the organization.
- Establish and maintain collaborations with external organizations promoting assurance.
- Review assurance related industry trends and available resources with higher level management
- Evolve assurance needs in line with the strategic plans and direction of the organization

Typical Work Products:

- Organization's assurance related process needs and objectives

SG 2 Plan and Implement Process Improvements

Process actions that address improvements to the organization's processes and process assets are planned and implemented.

SP 2.1 Establish and maintain process action plans to address improvements to the organization's processes and process assets.

SP 2.2 Implement process action plans.

SG 3 Deploy Organizational Process Assets and Incorporate Lessons Learned

The organizational process assets are deployed across the organization and process-related experiences are incorporated into the organizational process assets.

SP 3.1 Deploy organizational process assets across the organization.

SP 3.2 Deploy the organization's set of standard processes to projects at their startup and deploy changes to them as appropriate throughout the life of each project.

SP 3.3 Monitor the implementation of the organization's set of standard processes and use of process assets on all projects.

SP 3.4 Incorporate process-related work products, measures, and improvement information derived from planning and performing the process into the organizational process assets

The purpose of Organizational Process Definition (OPD) is to establish and maintain a usable set of organizational process assets and work environment standards.

SG 1 A set of organizational process assets is established and maintained.

SP 1.1 Establish and maintain the organization's set of standard processes.

Incorporating appropriate assurance considerations in the standard processes helps an organization achieve its business objectives. Assurance builds on the foundation established by the product life cycle processes of the organization. Assurance can be achieved most effectively by integrating into existing processes.

SP 1.2 Establish and maintain descriptions of the lifecycle models approved for use in the organization.

SP 1.3 Establish and maintain the tailoring criteria and guidelines for the organization's set of standard processes.

As there are legal ramifications for some of the components of assurance, e.g. security and safety, it is important that the organization defines clear tailoring guidelines associated with the assurance aspects of the standard processes. These guidelines are used by the organization to ensure that the assurance practices are not eliminated from the project activities.

SP 1.4 Establish and maintain the organization’s measurement repository.

SP 1.5 Establish and maintain the organization's process asset library.

SP 1.6 Establish and maintain work environment standards.

Assurance objectives require changes and additions to the organization’s work environment.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for OPD SP 1.1

OPD SP 1.1

AF 1.1.1 Establish and maintain organizational processes to achieve the assurance business objectives.

Description

A product cannot be completely protected from attack or hazard so business objectives must specify the level of assurance to be achieved for the product. The processes for the organization guide the team in the proper development of the product to achieve the assurance business objectives.

The process assets addressing assurance are incorporated with the other process assets of the organization and sustained accordingly. This ensures that assurance, like quality, is not a separate attachment to the system and software development activities but rather integral throughout each phase of the development.

Typical Work Products:

- Processes to ensure that assurance business objectives are achieved.
- Mechanisms to ensure that the organization's processes align to the organizational assurance policy.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for OPD SP 1.3

OPD SP 1.3

AF 1.3.1 Establish and maintain the tailoring criteria and guidelines for assurance in the organization's set of standard processes

Description

The tailoring criteria and guidelines should specify the latitude and constraints afforded to project teams when tailoring organizational processes with integrated assurance considerations. This ensures that the key business objectives pertaining to assurance are preserved.

Typical Work Products:

- Assurance considerations for tailoring the organization's set of standard processes

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for OPD SP 1.6

OPD SP 1.6

AF 1.6.1 Establish and maintain assurance of the organization's work environment based on the organization's work environment standards.

Description

The infrastructure to support assurance considerations requires the use of assurance tools that are properly maintained and improved based on lessons learned from the projects, organization and industry.

Typical Work Products:

- Work Environment Standards updated for assurance objectives

SG 2 (IPPD Addition) Organizational rules and guidelines, which govern the operation of integrated teams, are provided.

SP 2.1 Establish and maintain empowerment mechanisms to enable timely decision making.

SP 2.2 Establish and maintain organizational rules and guidelines for structuring and forming integrated teams.

SP 2.3 Establish and maintain organizational guidelines to help team members balance their team and home organization responsibilities

Addressing an organization's assurance training needs increases the likelihood that qualified and appropriately trained resources are performing the necessary integrated assurance activities on the project.

SG 1 A training capability, which supports the organization's management and technical roles, is established and maintained.

SP 1.1 Establish and maintain the strategic training needs of the organization.

Understanding the capabilities needed to achieve the strategic business objectives of an organization provides the foundation for building the necessary assurance skills within the organization.

SP 1.2 Determine which training needs are the responsibility of the organization and which will be left to the individual project or support group.

SP 1.3 Establish and maintain an organizational training tactical plan

SP 1.4 Establish and maintain training capability to address organizational training needs.

SG 2 Training necessary for individuals to perform their roles effectively is provided.

SP 2.1 Deliver the training following the organizational training tactical plan.

SP 2.2 Establish and maintain records of the organizational training.

SP 2.3 Assess the effectiveness of the organization's training program.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for OT SP 1.1

OT SP 1.1

AF 1.1.1 *Establish and maintain the strategic assurance training needs of the organization*

Description

Specialized skills are necessary to achieve project and organizational assurance objectives. Assurance objectives included in the organization's strategic business objectives and process improvement plan contribute to the identification of potential future training needs.

Once the training needs have been assessed, it is the responsibility of the organization to execute on providing the appropriate type and level of training to the various roles throughout the organization. The appropriateness of the training is defined by the organizational assurance objectives.

Typical Work Products:

- Assurance Training Needs
- Assurance Assessment

The purpose of Organizational Process Performance (OPP) is to establish and maintain a quantitative understanding of the performance of the organization's set of standard processes in support of quality and process-performance objectives, and to provide the process-performance data, baselines, and models to quantitatively manage the organization's projects.

SG 1 Establish Performance Baselines and Models

Baselines and models, which characterize the expected process performance of the organization's set of standard processes, are established and maintained.

SP 1.1 Select the processes or sub-processes in the organization's set of standard processes that are to be included in the organization's process-performance analyses.

SP 1.2 Establish and maintain definitions of the measures that are to be included in the organization's process-performance analyses.

SP 1.3 Establish and maintain quantitative objectives for quality and process performance for the organization.

SP 1.4 Establish and maintain the organization's process-performance baselines.

SP 1.5 Establish and maintain the process-performance models for the organization's set of standard processes.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

The purpose of Organizational Innovation and Deployment (OID) is to select and deploy incremental and innovative improvements that measurably improve the organization's processes and technologies. The improvements support the organization's quality and process-performance objectives as derived from the organization's business objectives.

SG 1 Select Improvements

Process and technology improvements, which contribute to meeting quality and process-performance objectives, are selected.

SP 1.1 Collect and analyze process- and technology-improvement proposals.

SP 1.2 Identify and analyze innovative improvements that could increase the organization's quality and process performance.

SP 1.3 Pilot process and technology improvements to select which ones to implement.

SP 1.4 Select process and technology improvements for deployment across the organization.

SG 2 Deploy Improvements

Measurable improvements to the organization's processes and technologies are continually and systematically deployed.

SP 2.1 Establish and maintain the plans for deploying the selected process and technology improvements.

SP 2.2 Manage the deployment of the selected process and technology improvements.

SP 2.3 Measure the effects of the deployed process and technology improvements.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

CMMI Process Areas

- Project Planning
- Project Monitoring and Control
- Supplier Agreement Management
- Integrated Project Management +IPPD
- Risk Management
- Quantitative Project Management

The purpose of Project Planning (PP) is to establish and maintain plans that define project activities.

SG 1 Establish Estimates

Estimates of project planning parameters are established and maintained.

SP 1.1 Establish a top-level work breakdown structure (WBS) to estimate the scope of the project.

Assurance objectives clarify the scope of the project

SP 1.2 Establish and maintain estimates of the attributes of the work products and tasks.

SP 1.3 Define the project lifecycle phases on which to scope the planning effort.

SP 1.4 Estimate the project effort and cost for the work products and tasks based on estimation rationale.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for PP SP 1.1 (1 of 2)

PP SP 1.1

AF 1.1.1 *Define project objectives for assurance*

Description

Project and stakeholder assurance objectives are applied to the project definition and customer requirements for the project to create assurance objectives for the project.

Typical Work Products:

Project objectives for assurance

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for PP SP 1.1 (2 of 2)

PP SP 1.1

AF 1.1.2 *Define the scope of assurance for the product or service*

Description

Devoting all of the project resources to assurance will not produce a completely resilient product or service. As a result, the scope of assurance for the project must be identified from the objectives for assurance along with the key requirements for the project. Due to the scope limitations, there are corresponding assurance activities and risks introduced to the project which need to be managed.

Typical Work Products:

- Task descriptions for assurance
- Assurance work package descriptions
- WBS with assurance

SG 2 Develop a Project Plan

A project plan is established and maintained as the basis for managing the project.

SP 2.1 Establish and maintain the project's budget and schedule.

SP 2.2 Identify and analyze project risks.

The complexity of systems, software, and hardware, the nature of the functions performed, and their interfaces require proactive steps to ensure that software is more resistant to attack or accidents, has fewer vulnerabilities, and minimizes mission risks. In this environment, project success is increasingly dependant on collaboration and mitigation of risks beyond traditional project boundaries.

SP 2.3 Plan for the management of project data.

SP 2.4 Plan for necessary resources to perform the project.

Resources for assurance may be integrated in team capabilities or specialized resources during critical points in the project. For example, successful peer reviews include considerations of unknown influences (i.e. intentional or unintentional behavior that causes additional harm to the product or service).

SP 2.5 Plan for knowledge and skills needed to perform the project.

SP 2.6 Plan the involvement of identified stakeholders.

SP 2.7 Establish and maintain the overall project plan content.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for PP SP 2.2

PP SP 2.2

AF 2.2.1 *Identify and analyze assurance related project risks.*

Description

The spectrum of project assurance risks can range from a project being technically infeasible to provide sufficient assurance to meet the project assurance objectives to compromising assurance objectives to meet mission needs.

Typical Work Products:

- Assurance risk impacts and probability of occurrence
- Assurance risk/mitigation associations and evaluations
- Assurance stakeholder involvement plan

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for PP SP 2.4

PP SP 2.4

AF 2.4.1 *Ensure that adequate resources to execute the assurance plans are provided*.

Description

Executing the assurance plans required to meet the project assurance objectives may require additional expertise or tools beyond the resources required to complete the project without assurance. As a result, it is necessary to plan for the provision of these additional resources.

Typical Work Products:

- Staffing requirements for assurance based on project size and scope
- Critical assurance facilities/equipment list
- Assurance process/workflow definitions and diagrams

The purpose of Project Planning (PP) is to establish and maintain plans that define project activities.

SG 3 Obtain Commitment to the Plan

Commitments to the project plan are established and maintained.

SP 3.1 Review all plans that affect the project to understand project commitments.

SP 3.2 Reconcile the project plan to reflect available and estimated resources.

SP 3.3 Obtain commitment from relevant stakeholders responsible for performing and supporting plan execution.

The purpose of Project Monitoring and Control (PMC) is to provide an understanding of the project's progress so that appropriate corrective actions can be taken when the project's performance deviates significantly from the plan.

SG 1 Monitor Project Against Plan

Actual performance and progress of the project are monitored against the project plan.

SP 1.1 Monitor the actual values of the project planning parameters against the project plan.

SP 1.2 Monitor commitments against those identified in the project plan.

SP 1.3 Monitor risks against those identified in the project plan.

Considering a combination of risks or inadequate resolution of a risk provides a more accurate understanding of a project's risk exposure. Periodic monitoring of assurance risks includes consideration of unknown influences (intentional or unintentional behavior that causes additional harm) as well as known and/or controllable influences. Additional risks or changes in risk status may occur as a result of periodic monitoring of assurance risks.

SP 1.4 Monitor the management of project data against the project plan.

SP 1.5 Monitor stakeholder involvement against the project plan.

SP 1.6 Periodically review the project's progress, performance, and issues.

SP 1.7 Review the accomplishments and results of the project at selected project milestones.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for PMC SP 1.3

PMC SP 1.3

AF 1.3.1 *Monitor Assurance Risk*

Description

Review of risks in the context of the project's current status and circumstances will identify when changes in the risks require action. Periodically and at key milestones of the project, it is important to monitor and manage the assurance risks because the probability and impact components of risk are dynamic for a given risk with time. Refer to the Assurance Focus Topic comments in Project Planning for more information about identifying assurance risks. Refer to the Assurance Focus Topic comments in Risk Management for more information about assurance risk management activities

Typical Work Products:

Records of assurance risk monitoring

SG 2 Manage Corrective Action to Closure

Corrective actions are managed to closure when the project's performance or results deviate significantly from the plan.

SP 2.1 Collect and analyze the issues and determine the corrective actions necessary to address the issues.

SP 2.2 Take corrective action on identified issues.

SP 2.3 Manage corrective actions to closure.

The purpose of Supplier Agreement Management (SAM) is to manage the acquisition of products from suppliers.

SG 1 Establish Supplier Agreements

Agreements with the suppliers are established and maintained.

SP 1.1 Determine the type of acquisition for each product or product component to be acquired.

SP 1.2 Select suppliers based on an evaluation of their ability to meet the specified requirements and established criteria.

The assurance activities address the identification of assurance capabilities of suppliers and of assurance risks introduced as a result of using a supplier.

SP 1.3 Establish and maintain formal agreements with the supplier.

There are legal considerations associated with assurance that may not appear in the usual supplier agreements.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for SAM SP1.2

SAM SP 1.2

AF 1.2.1 *Select suppliers based on an evaluation of their ability to meet specified assurance requirements and established criteria*

Description

These combined activities contribute to selecting suppliers for assurance.

- Establish assurance selection criteria.
- Establish strategy for risk management of suppliers.
- Incorporate assurance into the overall selection criteria
- Identify potential suppliers satisfying assurance selection criteria.
- Evaluate potential suppliers satisfying assurance selection criteria.

Typical Work Products:

- Assurance based market studies
- List of preferred assurance suppliers
- Solicitation materials incorporate assurance objectives
- Tradeoff analysis of selection criteria
- Analysis of ability of potential suppliers to meet assurance selection criteria and associated risks

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for SAM SP 1.3

SAM SP 1.3

AF 1.3.1 *Document supplier agreements for assurance.*

Description

The legal agreements associated with the supplier identify who carries the responsibilities and liabilities for correction of vulnerabilities identified in the product or service provided. Where agreements already exist, the agreements may need to be revised to address such issues. In cases of open source, it may not be possible to modify the agreement.

Typical Work Products:

- Contracts, Memoranda of Agreement, or License Agreements with assurance provisions
- Acceptance criteria for work products

SG 2 Satisfy Supplier Agreements

Agreements with the suppliers are satisfied by both the project and the supplier.

SP 2.1 Perform activities with the supplier as specified in the supplier agreement.

SP 2.2 Select, monitor, and analyze processes used by the supplier.

SP 2.3 Select and evaluate work products from the supplier of custom-made products.

SP 2.4 Ensure that the supplier agreement is satisfied before accepting the acquired product.

Before accepting the product from a supplier, the project team evaluates the assurance requirements of that product. It is as important to evaluate the unintentional vulnerabilities of the work product as well as its intended capabilities.

SP 2.5 Transition the acquired products from the supplier to the project.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for SAM SP 2.4

SAM SP 2.4

AF 2.4.1 *Evaluate supplier deliverables against assurance acceptance criteria.*

Description

The products are evaluated against expected and unexpected functionality/behavior, and behavior under unknown influences (i.e. intentional or unintentional behavior that causes additional harm). Static or dynamic analysis tools may be used.

Typical Work Products:

- Assurance acceptance test reports
- Risk Analysis of failed acceptance tests

The purpose of Integrated Project Management (IPM) is to establish and manage the project and the involvement of the relevant stakeholders according to an integrated and defined process that is tailored from the organization's set of standard processes.

SG 1 Use the Project's Defined Process

The project is conducted using a defined process that is tailored from the organization's set of standard processes.

SP 1.1 Establish and maintain the project's defined process from project startup through the life of the project.

SP 1.2 Use the organizational process assets and measurement repository for estimating and planning the project's activities.

SP 1.3 Establish and maintain the project's work environment based on the organization's work environment standards.

Assurance requirements require changes to the project's work environment.

SP 1.4 Integrate the project plan and the other plans that affect the project to describe the project's defined process.

SP 1.5 Manage the project using the project plan, the other plans that affect the project, and the project's defined process.

SP 1.6 Contribute work products, measures, and documented experiences to the organizational process assets.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for IPM SP 1.3

IPM SP 1.3

AF 1.3.1 *Establish and maintain assurance of the project's work environment based on the organization's work environment standards.*

Description

The infrastructure to support assurance considerations requires the use of assurance tools that are properly maintained and improved based on lessons learned from the project, organization and industry.

Typical Work Products:

- Assurance integrated processes requiring use of specific tools
- Tool outputs with associated corrective action
- Comprehensive tool evaluations with related mitigation strategies
- Documented and controlled access to the project environment
- Disaster Recovery and Contingency plans
- Assurance incident reports with corrective actions tracked and closed

SG 2 Coordinate and Collaborate with Relevant Stakeholders

Coordination and collaboration of the project with relevant stakeholders is conducted.

SP 2..1 Manage the involvement of the relevant stakeholders in the project.

SP 2..2 Participate with relevant stakeholders to identify, negotiate, and track critical dependencies.

SP 2.3 Resolve issues with relevant stakeholders.

SG 3 Apply IPPD Principles (IPPD Addition)

The project is managed using IPPD principles.

SP 3.1 Establish and maintain a shared vision for the project.

SP 3.2 Establish and maintain the integrated team structure for the project.

SP 3.3 Allocate requirements, responsibilities, tasks, and interfaces to teams in the integrated team structure.

SP 3.4 Establish and maintain integrated teams in the structure.

SP 3.5 Ensure collaboration among interfacing teams.

The purpose of Risk Management (RSKM) is to identify potential problems before they occur so that risk-handling activities can be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives.

SG 1 Prepare for Risk Management

Preparation for risk management is conducted.

SP 1.1 Determine risk sources and categories.

SP 1.2 Define the parameters used to analyze and categorize risks, and the parameters used to control the risk management effort.

SP 1.3 Establish and maintain the strategy to be used for risk management.

The risk management strategy is extended to address assurance related product weaknesses throughout development and as well as during operation and maintenance phases of the product life-cycle. Since assurance risks may involve low likelihoods and cover the product's life cycle, parameters, including likelihood, consequence, and thresholds for taking action on identified risks, should be reexamined for assurance risks. The strategy allows such risks to be managed appropriately. The project must consider strategies to address product assurance risks.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for RSKM SP 1.3

RSMK SP 1.3

AF 1.3.1 *Define and select the strategy for management of risk due to vulnerabilities and safety hazards.*

Description

The risk management strategy depends on both the product and the stakeholders. Consideration must be given to attacks and hazards with respect to product assurance.

Typical Work Products:

- Product risk management strategy
- Assurance risk management strategy

SG 2 Identify and Analyze Risks

Risks are identified and analyzed to determine their relative importance.

SP 2.1 Identify and document the risks.

Assurance considerations are included with cost, schedule, and performance in risk identification from project initiation through product operation.

SP 2.2 Evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority.

SG 3 Mitigate Risks

Risks are handled and mitigated, where appropriate, to reduce adverse impacts on achieving objectives.

SP 3.1 Develop a risk mitigation plan for the most important risks to the project as defined by the risk management strategy.

SP 3.2 Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for RSKM SP 2.1

RSMK SP 2.1

AF 2.1.1 *Identify and document risks associated with the identified threats, vulnerabilities and hazards.*

Description

Project and product risks related to known and unknown influences (i.e. intentional or unintentional behavior that causes additional harm to the product or service) are part of a harmonized risk analysis and prioritization. Vulnerabilities and hazards associated with other products in the public space must be part of the ongoing identification and documentation activities. Such information can be obtained from websites and other sources that provide ongoing analysis as a general service to the community.

Typical Work Products:

List of identified assurance risks including the context, conditions, and consequences of risk occurrence.

The purpose of Quantitative Project Management (QPM) is to quantitatively manage the project's defined process to achieve the project's established quality and process-performance objectives.

SG 1 Quantitatively Manage the Project

The project is quantitatively managed using quality and process-performance objectives.

SP 1.1 Establish and maintain the project's quality and process-performance objectives.

SP 1.2 Select the sub-processes that compose the project's defined process based on historical stability and capability data.

SP 1.3 Select the sub-processes of the project's defined process that will be statistically managed.

SP 1.4 Monitor the project to determine whether the project's objectives for quality and process performance will be satisfied, and identify corrective action as appropriate.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

SG 2 Statistically Manage Sub-process Performance

The performance of selected sub-processes within the project's defined process is statistically managed.

SP 2.1 Select the measures and analytic techniques to be used in statistically managing the selected sub-processes.

SP 2.2 Establish and maintain an understanding of the variation of the selected sub-processes using the selected measures and analytic techniques.

SP 2.3 Monitor the performance of the selected sub-processes to determine their capability to satisfy their quality and process-performance objectives, and identify corrective action as necessary.

SP 2.4 Record statistical and quality management data in the organization’s measurement repository.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

CMMI Process Areas

- Requirements Management
- Requirements Development
- Technical Solution
- Product Integration
- Verification
- Validation

The purpose of Requirements Management (REQM) is to manage the requirements of the project's products and product components and to identify inconsistencies between those requirements and the project's plans and work products.

SG 1 Manage Requirements

Requirements are managed and inconsistencies with project plans and work products are identified.

- SP 1.1 Develop an understanding with the requirements providers on the meaning of the requirements.
- SP 1.2 Obtain commitment to the requirements from the project participants.
- SP 1.3 Manage changes to the requirements as they evolve during the project.
- SP 1.4 Maintain bidirectional traceability among the requirements and work products.
- SP 1.5 Identify inconsistencies between the project plans and work products and the requirements.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

The purpose of Requirements Development (RD) is to produce and analyze customer, product, and product component requirements.

SG 1 Develop Customer Requirements

Stakeholder needs, expectations, constraints, and interfaces are collected and translated into customer requirements.

SP 1.1 Elicit stakeholder needs, expectations, constraints, and interfaces for all phases of the product lifecycle.

Ensuring that stakeholder assurance needs are understood and documented, provides the foundation for developing products that satisfy the customer, product, and product component assurance related requirements.

SP 1.2 Transform stakeholder needs, expectations, constraints, and interfaces into customer requirements.

Development of customer requirements demonstrates an understanding of expectations and constraints associated with the system under development. The stakeholder needs, expectations, constraints, and interfaces for assurance are reflected in the customer requirements.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for RD SP 1.1

RD SP 1.1

AF 1.1.1 *Understand the operating environment and define the operating constraints for assurance within the environments of system deployment*.

Description

Understanding the operating environment for the program under development will lead to a better understanding of assurance needs for that environment. Assurance of a product depends on its operating environment. The following activities contribute to the proper understanding of the product's operating environment.

Typical Work Products:

- Assurance related needs
- Assurance related expectations, constraints, and external interfaces associated with operating the system within the defined environment
- Constraints associated with the conduct of requirements verification and validation such as interface dependencies, and system boundaries

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for RD SP 1.2

RD SP 1.2

AF 1.2.1 *Develop Customer Assurance Requirements*

Description

Customer assurance needs may require some additional dialog to the usual requirements elicitation. Customers may not voice assurance requirements explicitly. It is useful to identify the key assets for customers and end users along with confidentiality, integrity, availability, and non-repudiation requirements for those assets. Furthermore, it is necessary to have a discussion of the tradeoffs associated with potential conflicts between these functional and nonfunctional requirements.

Typical Work Products:

Customer approved assurance requirements

SG 2 Develop Product Requirements

Customer requirements are refined and elaborated to develop product and product component requirements.

SP 2.1 Establish and maintain product and product component requirements, which are based on the customer requirements.

Incorporating product component requirements that address assurance and the potential impacts of component integration and interfaces creates a system for which the operational assurance needs of the system have been captured.

SP 2.2 Allocate the requirements for each product component.

SP 2.3 Identify interface requirements.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for RD SP 2.1

RD SP 2.1

AF 2.1.1 *Define product and product component assurance requirements.*

Description

Translate functional and nonfunctional customer assurance requirements into technical requirements that can be used to design the product and its components. Specific assurance requirements are derived by considering the higher level requirements, concept of operations, as well as the results of the specific analyses associated with assurance (e.g. threat analysis, abuse/misuse, and/or safety hazard analysis).

Typical Work Products:

- Derived assurance requirements
- Product assurance requirements
- Product component assurance requirements

SG 3 Analyze and Validate Requirements

The requirements are analyzed and validated, and a definition of required functionality is developed.

SP 3.1 Establish and maintain operational concepts and associated scenarios.

Assurance use cases including security, safety, and dependability requirements, allow for a more accurate understanding of what requirements are needed as well as establishing proper allocations of those requirements. For assurance, additional focus is given to define how the system is not to behave or how it behaves under unknown influences (i.e. intentional or unintentional behavior that causes additional harm).

SP 3.2 Establish and maintain a definition of required functionality.

SP 3.3 Analyze requirements to ensure that they are necessary and sufficient.

Requirements are analyzed to ensure assurance has been appropriately incorporated.

SP 3.4 Analyze requirements to balance stakeholder needs and constraints.

Given the defined operating environment and the assurance context for the product, risks to assurance are introduced into the product or service under development. The mitigation of these risks introduces additional assurance needs that must be balanced against mission, cost and schedule constraints.

SP 3.5 Validate requirements to ensure the resulting product will perform as intended in the user's environment.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for RD SP 3.1

RD SP 3.1

AF 3.1.1 *Identify operational concepts and associated scenarios for assurance.*

Description

Understanding assurance in the context of how the product is expected to operate in each intended environment includes an assurance view of roles, assets, flow of information, utilized resources, and protections. This context provides the foundation for creating assurance use cases and abuse cases. Assurance use cases may address, for example, authentication, the constraints of the environment (hostile, public, non-public), physical versus software access, and error handling. In the same context as use case development, abuse and failure case creation may highlight the need for additional functional requirements (or more specific derived requirements) to mitigate risks that are identified in the abuse or failure use cases.

Typical Work Products:

- Operational Concepts addressing assurance
- Use cases for assurance
- Abuse cases

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for RD SP 3.3

RD SP 3.3

AF 3.3.1 *Analyze assurance requirements.*

Description

Analysis of the assurance requirements involves using operational concepts and scenarios addressing assurance and ensuring the customer's assurance expectations and needs are met. For assurance, the requirements may need to be more specific. For example, instead of requiring a password, the requirement might be a password with at least “n’ characters and at least one numeric character. A nonfunctional requirement associated with this same example could be the specification that the username and password must differ by at least “m” characters.

Typical Work Products:

- Assurance performance measures
- Proposed requirements changes to resolve vulnerabilities recognized as a result of assurance considerations
- Proposed requirements changes to meet assurance objectives

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for RD SP 3.4

RD SP 3.4

AF 3.4.1. *Balance assurance needs against cost benefits.*

Description

The development of the systems meeting all assurance needs may be cost prohibitive. Analysis is performed to determine the balance between having an acceptable level of assurance and the cost to include that level of assurance in the product. Stakeholders need to agree upon what aspects of assurance are sufficient.

Typical Work Products:

- Results of the analysis to balance assurance needs and costs

The purpose of Technical Solution (TS) is to design, develop, and implement solutions to requirements. Solutions, designs, and implementations encompass products, components, and product-related lifecycle processes either singly or in combination as appropriate.

SG 1 Select Product Component Solutions

Product or product component solutions are selected from alternative solutions.

SP 1.1 Develop alternative solutions and selection criteria.

Understanding known vulnerabilities and limitations of design alternatives supports selection of the appropriate technical architecture.

SP 1.2 Select the product component solutions that best satisfy the criteria established.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for TS SP 1.1

TS SP 1.1

AF 1.1.1 Develop alternative solutions and selection criteria for assurance.

Description

Ensuring trustworthy operation in support of mission/business objectives begins with consideration of assurance in the development and selection of alternative solutions.

Typical Work Products:

- Alternative solution assurance screening criteria
- Evaluation reports of assurance of new technologies
- Alternative assurance solutions
- Assurance evaluation reports of COTS products

SG 2 Develop the Design

Product or product component designs are developed

SP 2.1 Develop a design for the product or product component.

Activities critical to addressing assurance considerations in design include understanding assurance risks related to architecture and design activities and using the knowledge to make decisions.

SP 2.2 Establish and maintain a technical data package.

SP 2.3 Design product component interfaces using established criteria.

SP 2.4 Evaluate whether the product components should be developed, purchased, or reused based on established criteria.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for TS 2.1 (1 of 2)

TS SP 2.1

AF 2.1.1 Architect for assurance.

Description

Architecting for assurance requires consideration of aspects that reduce the risk that the product or product component will be compromised intentionally or unintentionally via a threat agent or accidentally via a safety hazard. The design must consider how the system is intended to be used, the impact of misuse, and what might happen to the system when it is used for other purposes. Understanding how the system operates in all conditions and making design and implementation decisions based on that knowledge and the criticality of related risks contributes to the assurance of the product.

Typical Work Products:

- Product architecture incorporating provisions for assurance such as:
  - Documentation of product resources and trust boundaries
  - Minimizing damage and ensuring recovery from intentional or unintentional behaviors that cause harm to the product or service
- Threat model of the product
- Cost benefit analysis of assurance impacts related to each operating environment of the product

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for TS 2.1 (2 of 2)

TS SP 2.1

AF 2.1.2 Design for assurance.

Description

Designing for assurance requires correct understanding of the architecture and making implementation decisions based on the knowledge and criticality of related operational risks including assurance risk contributions.

Typical Work Products:

- Documented design with assurance provisions including:
  - Selection criteria for identifying the best design decision for the assurance of the product
  - Documentation of assurance analysis in selecting the final design solution.
  - Documented assurance analysis of potential designs.
  - Assurance analysis
  - Assurance design patterns

3 Implement the Product Design

Product components, and associated support documentation, are implemented from their designs.

SP 3.1 Implement the designs of the product components.

Vulnerabilities related to product configuration and coding errors are commonly introduced during design implementation.

SP 3.2 Develop and maintain the end-use documentation.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for TS SP 3.1 (1 of 2)

TS SP 3.1

AF 3.1.1 Implement the assurance designs of the product components.

Description

Introducing vulnerabilities during design implementation can be minimized by using assurance design patterns.

Typical Work Products:

- Implemented design for assurance

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for TS SP 3.1 (2 of 2)

TS SP 3.1

AF 3.1.2. Identify deviations from assurance coding standards. Implement appropriate mitigation to meet defined assurance objectives.

Description

In order to compensate for the inherent inadequacies contained within many implementation languages, coding standards for assurance can guide developers to compensate for those inadequacies. Static analysis tools and/or peer reviews can be used to identify potential vulnerabilities and recommend the appropriate level of mitigation.

Typical Work Products:

- List of vulnerabilities introduced during implementation and the corresponding mitigation applied.

The purpose of Product Integration (PI) is to assemble the product from the product components, ensure that the product, as integrated, functions properly, and deliver the product.

SG 1 Prepare for Product Integration

Preparation for product integration is conducted.

SP 1.1 Determine the product component integration sequence.

SP 1.2 Establish and maintain the environment needed to support the integration of the product components.

SP 1.3 Establish and maintain procedures and criteria for integration of the product components.

SG 2 Ensure Interface Compatibility

The product component interfaces, both internal and external, are compatible.

SP 2.1 Review interface descriptions for coverage and completeness.

SP 2.2 Manage internal and external interface definitions, designs, and changes for products and product components.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

SG 3 Assemble Product Components and Deliver the Product

Verified product components are assembled and the integrated, verified, and validated product is delivered.

SP 3.1 Confirm, prior to assembly, that each product component required to assemble the product has been properly identified, functions according to its description, and that the product component interfaces comply with the interface descriptions.

SP 3.2 Assemble product components according to the product integration sequence and available procedures.

SP 3.3 Evaluate assembled product components for interface compatibility.

SP 3.4 Package the assembled product or product component and deliver it to the appropriate customer.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

The purpose of Validation (VAL) is to demonstrate that a product or product component fulfills its intended use when placed in its intended environment.

SG 1 Prepare for Validation

Preparation for validation is conducted.

SP 1.1 Select products and product components to be validated and the validation methods that will be used for each.

SP 1.2 Establish and maintain the environment needed to support validation.

SP 1.3 Establish and maintain procedures and criteria for validation.

Validation includes ensuring that the product or service is predictable in its intended environment and does not fulfill any unintended uses that can negatively impact the intended uses

.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for VAL SP 1.3

VAL SP 1.3

AF 1.3.1 *Establish and maintain validation procedures and criteria for the assurance of selected work products.*

Description

Examples of validation procedures that contribute to determining trustworthiness and predictability of a product or service include:

- Validation of assurance criteria and measurements
- Validation of the resiliency of the product
- Assurance related capabilities of the system under development should be validated against resiliency criteria during appropriate validation activities
- Validation of the product through the results of threat modeling in addition to the usual validation practices of inspection, test, demonstration, and analysis. focus

Typical Work Products:

- Assurance validation procedures
- Assurance validation criteria
- Assurance validation/test and evaluation procedures for maintenance, training, and support

SG 2 Validate Product or Product Components

The product or product components are validated to ensure that they are suitable for use in their intended operating environment.

SP 2.1 Perform validation on the selected products and product components.

SP 2.2 Analyze the results of the validation activities.

Analysis of the validation results provides the information that can be used to determine adequacy of a product or service from an assurance perspective.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for VAL SP 2.2

VAL SP 2.2

AF 2.2.1 *Analyze the results of assurance validation activities.*

Description

Identify, characterize, and resolve issues resulting from validation activities to gain an understanding of the validity of assurance claims related to the predictability and trustworthiness of the product or service. The information learned about the system from validation activities contributes to a set of arguments that justify a claim about the assurance of a system. The claim, arguments, and quantifiable information are called an assurance case. Stakeholders can make decisions on the assurance of the product/service based on the justification provided. Resolution depends on the risk assessment and the assurance goals.

Typical Work Products:

Assurance based validation issues

The purpose of Verification (VER) is to ensure that selected work products meet their specified requirements.

SG 1 Prepare for Verification

Preparation for verification is conducted.

SP 1.1 Select the work products to be verified and the verification methods that will be used for each.

SP 1.2 Establish and maintain the environment needed to support verification.

SP 1.3 Establish and maintain verification procedures and criteria for the selected work products.

The assurance focus includes verifying that implemented requirements do not introduce unnecessary risks to the operation of the product. One assurance objective is to verify that unintended functionality is not available.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for VER SP 1.3

VER SP 1.3

AF 1.3.1 *Establish and maintain verification procedures and criteria for the assurance of selected work products.*

Description

The combination of these activities contribute to verification of assurance. Examples of verification procedures that contribute determining trustworthiness and predictability of a product or service include:

- Identify verification of measurement criteria used to establish the assurance case
- Verification of the product for assurance requirements
- Verification of the resiliency of the product
- Verification of the product when tested from an attacker perspective
- Verification of the product through the results of threat modeling in addition to the usual verification practices of inspection, test, demonstration, and analysis

Typical Work Products:

- Assurance verification procedures
- Assurance criteria
- Assurance scenarios
- Event/error handling verification procedures

SG 2 Perform Peer Reviews

Peer reviews are performed on selected work products.

SP 2.1 Prepare for peer reviews of selected work products.

SP 2.2 Conduct peer reviews on selected work products and identify issues resulting from the peer review.

SP 2.3 Analyze data about preparation, conduct, and results of the peer reviews.

SG 3 Verify Selected Work Products

Selected work products are verified against their specified requirements.

SP 3.1 Perform verification on the selected work products.

SP 3.2 Analyze the results of all verification activities.

Analysis of the verification results provides the information that can be used to determine adequacy of a product or service from an assurance perspective.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for VER SP 3.2

VER SP 3.2

AF 3.2.1 *Analyze the results of assurance verification activities.*

Description

Identify, characterize, and resolve issues resulting from verification activities to gain an understanding of the validity of assurance claims related to the predictability and trustworthiness of the product or service. The information learned about the system from verification activities contributes to a set of arguments that justify a claim about the assurance of a system. The claim, arguments, and quantifiable information are called an assurance case. Stakeholders can make decisions on the assurance of the product/service based on the justification provided. Resolution depends on the risk assessment and the assurance goals.

Typical Work Products:

- Assurance analysis reports
- Assurance trouble reports
- Change requests for assurance verification methods, criteria, and environment

CMMI Process Areas

- Configuration Management
- Process and Product Quality Assurance
- Measurement and Analysis
- Decision Analysis and Resolution
- Causal Analysis and Resolution

The purpose of Configuration Management (CM) is to establish and maintain the integrity of work products using configuration identification, configuration control, configuration status accounting, and configuration audits.

SG 1 Establish Baselines

Baselines of identified work products are established.

SP 1.1 Identify the configuration items, components, and related work products that will be placed under configuration management.

SP 1.2 Establish and maintain a configuration management and change management system for controlling work products.

SP 1.3 Create or release baselines for internal use and for delivery to the customer.

SG 2 Track and Control Changes

Changes to the work products under configuration management are tracked and controlled.

SP 2.1 Track change requests for the configuration items.

SP 2.2 Control changes to the configuration items.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices 2

SG 3 Establish Integrity

Integrity of baselines is established and maintained.

SP 3.1 Establish and maintain records describing configuration items.

SP 3.2 Perform configuration audits to maintain integrity of the configuration baselines.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

The purpose of Process and Product Quality Assurance (PPQA) is to provide staff and management with objective insight into processes and associated work products.

SG 1 Objectively Evaluate Processes and Work Products

Adherence of the performed process and associated work products and services to applicable process descriptions, standards, and procedures is objectively evaluated.

SP 1.1 Objectively evaluate the designated performed processes against the applicable process descriptions, standards, and procedures.

SP 1.2 Objectively evaluate the designated work product and services against the applicable process description, standards, and procedures.

SG 2 Provide Objective Insight

Noncompliance issues are objectively tracked and communicated, and resolution is ensured.

SP 2.1 Communicate quality issues and ensure resolution of noncompliance issues with the staff and managers.

SP 2.2 Establish and maintain records of the quality assurance activities.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

The purpose of Measurement and Analysis (MA) is to develop and sustain a measurement capability that is used to support management information needs.

SG 1 Align Measurement and Analysis Activities

Measurement objectives and activities are aligned with identified information needs and objectives.

SP 1.1 Establish and maintain measurement objectives that are derived from identified information needs and objectives.

SP 1.2 Specify measures to address the measurement objectives.

In order to support a project's assurance activities, creation of measures related to the assurance of a product or service may be required for internal and external stakeholders.

SP 1.3 Specify how measurement data will be obtained and stored.

SP 1.4 Specify how measurement data will be analyzed and reported.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for MA SP 1.2

MA SP 1.2

AF 1.2.1 *Define and improve project assurance measures.*

Description

Stakeholder organizations interested in assurance have identified information assurance needs and objectives. Based upon these assurance objectives, measures are defined to monitor and track the success the project team has in meeting those objectives. It is expected that the measures collected will evolve over time from advances in the assurance capabilities as well as changes in organizational and product assurance objectives. A subset of these measures may become a formal part of the product or service that provides updates on the assurance of the product or service over time.

Typical Work Products:

- Specification of base and derived assurance measures
- Updated sets of assurance measures

SG 2 Provide Measurement Results

Measurement results, which address identified information needs and objectives, are provided.

SP 2.1 Obtain specified measurement data.

SP 2.2 Analyze and interpret measurement data.

SP 2.3 Manage and store measurement data, measurement specifications, and analysis results.

Data related to the assurance of the product contains information about potentially exploitable weaknesses in a product or service. In the form of an assurance case, this data becomes part of the product or service. Improper access or use of the data may cause potential harm. Proper management and storage of this information is important to maintain the controlled access and ensure that the information is not lost or damaged.

SP 2.4 Report results of measurement and analysis activities to all relevant stakeholders

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance Focus for MA SP 2.3

MA SP 2.3

AF 2.3.1 *Store assurance measures appropriately.*

Description

Due to the sensitivity of the data, additional care must be given to identify the appropriate audiences for the various assurance measures. For audiences such as the project team, more detailed views may be desired and needed for effective use of the data. Conversely, executives or other stakeholders may only need a summary that can be used for justification of assurance practices or decision making based on a summary view of the data. The assurance data that is part of the assurance case becomes an important artifact and part of the product or service.

Typical Work Products:

- Stored assurance measurement data inventory.
- Assurance data protection mechanisms
- Assurance case

The purpose of Decision Analysis and Resolution (DAR) is to analyze possible decisions using a formal evaluation process that evaluates identified alternatives against established criteria.

SG 1 Evaluate Alternatives

Decisions are based on an evaluation of alternatives using established criteria.

SP 1.1 Establish and maintain guidelines to determine which issues are subject to a formal evaluation process.

SP 1.2 Establish and maintain the criteria for evaluating alternatives, and the relative ranking of these criteria.

SP 1.3 Identify alternative solutions to address issues.

SP 1.4 Select the evaluation methods.

SP 1.5 Evaluate alternative solutions using the established criteria and methods.

SP 1.6 Select solutions from the alternatives based on the evaluation criteria.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

The purpose of Causal Analysis and Resolution (CAR) is to identify causes of defects and other problems and take action to prevent them from occurring in the future.

SG 1 Determine Causes or Defects

Root causes of defects and other problems are systematically determined.

SP 1.1 Select the defects and other problems for analysis.

SP 1.2 Perform causal analysis of selected defects and other problems and propose actions to address them.

SG 2 Address Causes of Defects

Root causes of defects and other problems are systematically addressed to prevent their future occurrence.

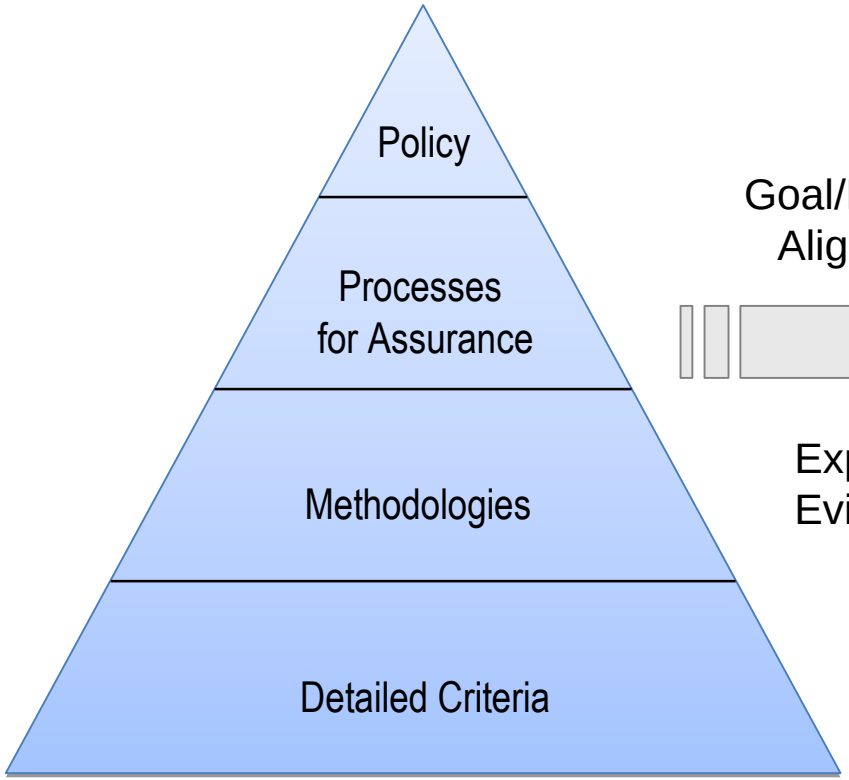
SP 2.1 Implement the selected action proposals that were developed in causal analysis.

SP 2.2 Evaluate the effect of changes on process performance.

SP 2.3 Record causal analysis and resolution data for use across the project and organization.

There is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices

Governance Framework



Goal/Process Alignment

Expected Evidence

Process Capability Assessment Results

Process Gap Analysis

Or

CMMI® SCAMPI℠

Plan and Prepare for Appraisal

Conduct Appraisal

Report Results

SM SCAMPI is a service mark of Carnegie Mellon University.

CMMI Model								
PA	Goal	Description of Goal	Practice	Description of Practice	Project / Organization	Possible Direct Artifact	Possible Indirect Artifact	Indirect Ar
RD	RD SG 1	Stakeholder needs, expectations, constraints, and interfaces are colleced and translated into customer requirements	SP 1.1	Elicit stakeholder needs, expectations, constraints, and interfaces for all phases of the product life cycle	Project	Documentation of stakeholder needs, expectations, and constraints. Examples include, prototypes, JAD session results, SOW, requirements interview results, survey results, ECPs/Change requests for maintenance projects. These are not meeting minutes, they are documented requirements and constraints.	Meeting documentation including discussion of DAs, emails, review documentation, or other documentation showing customer involvement in requirements development.	
RD	RD SG 1	Stakeholder needs, expectations, constraints, and interfaces are colleced and translated into customer requirements	AF 1.1.1	Understand the operating environment and define the operating constraints for assurance within the environments of system deployment	Project	Documentation of assurance related needs, expectations, constraints, and external interfaces associated with operating the system within the defined environment. Also documentation of constraints associated with the conduct of requirements verification and validation, such as interface dependencies, and system boundaries.	Meeting documentation including discussion of DAs, emails, review documentation, or other documentation showing customer involvement in requirements development.	

- Leverage existing resources to get started
- Watch for updates https://buildsecurityin.us-cert.gov/swa/procresrc.html
- Share your lessons learned (swawg-process@cert.org)
- Attend the summer Working Group sessions and contribute to discussions on using available resources