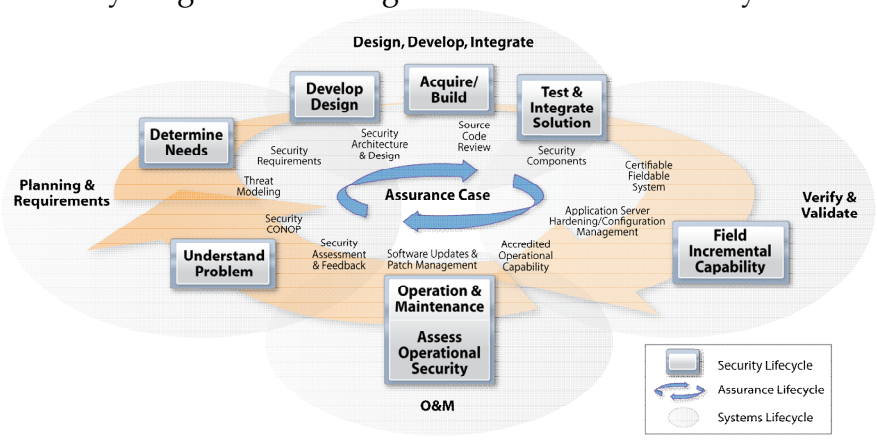
Summary of Assurance for CMMI® Efforts

System and Software Assurance is defined as

- The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner. *CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006*
- Grounds for confidence that an entity meets its relevant needs, goals or objectives for safety, security and dependability or other characteristics deemed to be critical, and possesses the related required properties. *ISO/IEC CD 15026, 2007, Systems and Software Assurance*

Current problems in achieving System and Software Assurance include:

- Assurance-related risks have dramatically increased due to the simultaneous growth in software vulnerabilities and threats
- Commonly used risk management processes inadequately address these threats and risks
- Government and industry are being confronted by risks presented by suppliers of software products and services
- Current development and acquisition processes inadequately address System and Software Assurance
- There is a fundamental lack of both the scientific understanding of software risks, and the capabilities to effectively diagnose and mitigate them in the in a timely manner



To solve this problem a blend of process (CMMI, ISO 9000) and product (Certification and Accreditation, Common Criteria, static code analysis) solutions is required. To address the process portion, the Assurance Working Group has created two work products

1. A draft set of assurance goals and practices that harmonize and enhance existing Security Capability Maturity Models (MSSDM, SSE-CMM)
2. A mapping of the draft set of assurance goals and practices to the CMMI-DEV v1.2

® CMMI is a registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

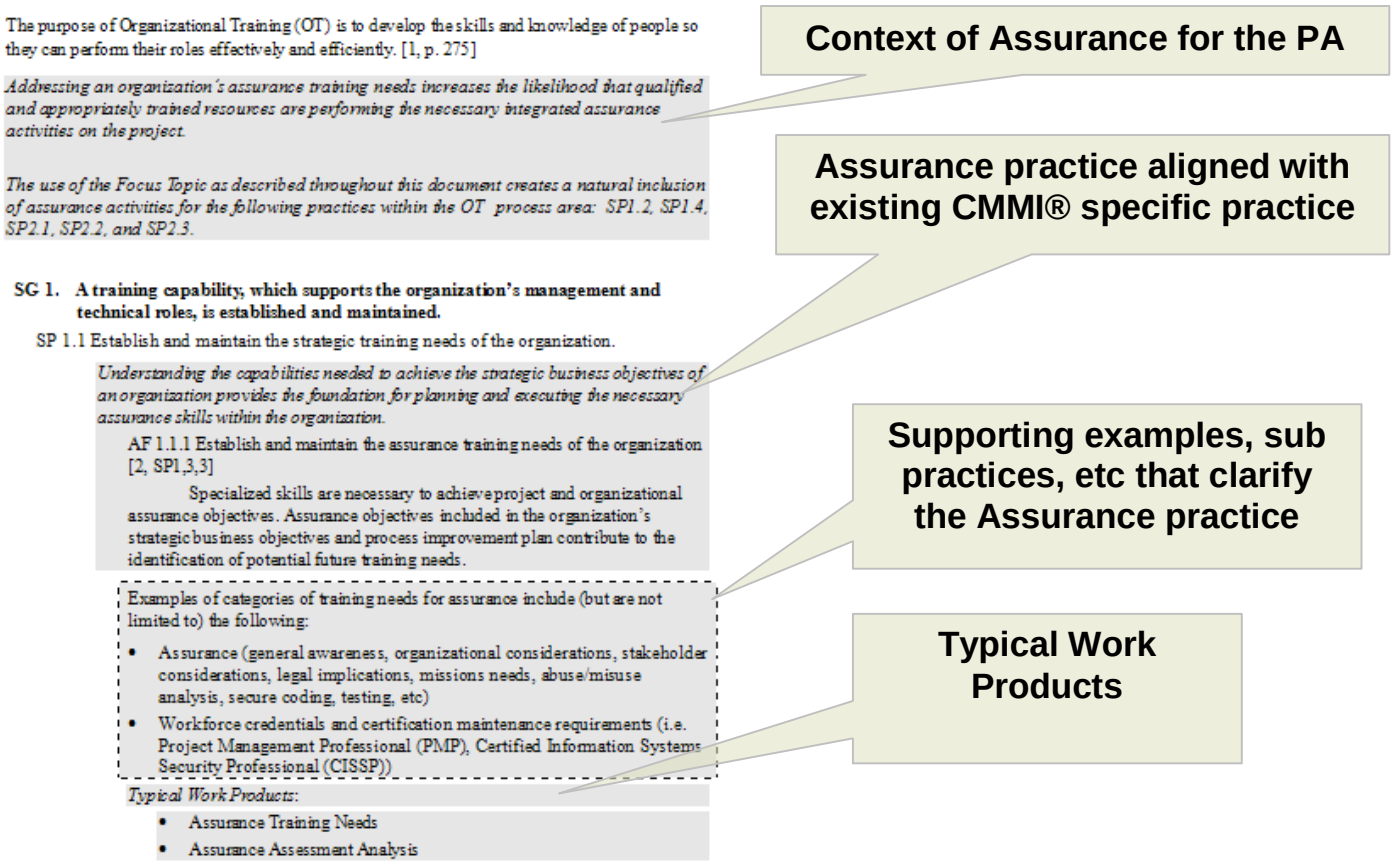
Material adapted from "Leveraging CMMs and Standards for Assurance" Paul Croll and Michele Moss SSTC 2008, Track 6, Wednesday, April 30

"Leveraging the CMMI® To Address Assurance – Benchmarking Assurance Practices and Managing Assurance Risks" Paul Croll and Michele Moss NDIA CMMI Technology Conference, November 19, 2008

"Update on the Assurance for CMMI Practices", Michele Moss and Margaret Nadworny, DHS SwA Working Group, December 4, 2008

The mapping of the practices to CMMI-DEV v1.2 is providing the basis for creating an Assurance Focus Topic as a third work product. The Focus Topic will document the assurance thread within the CMMI.

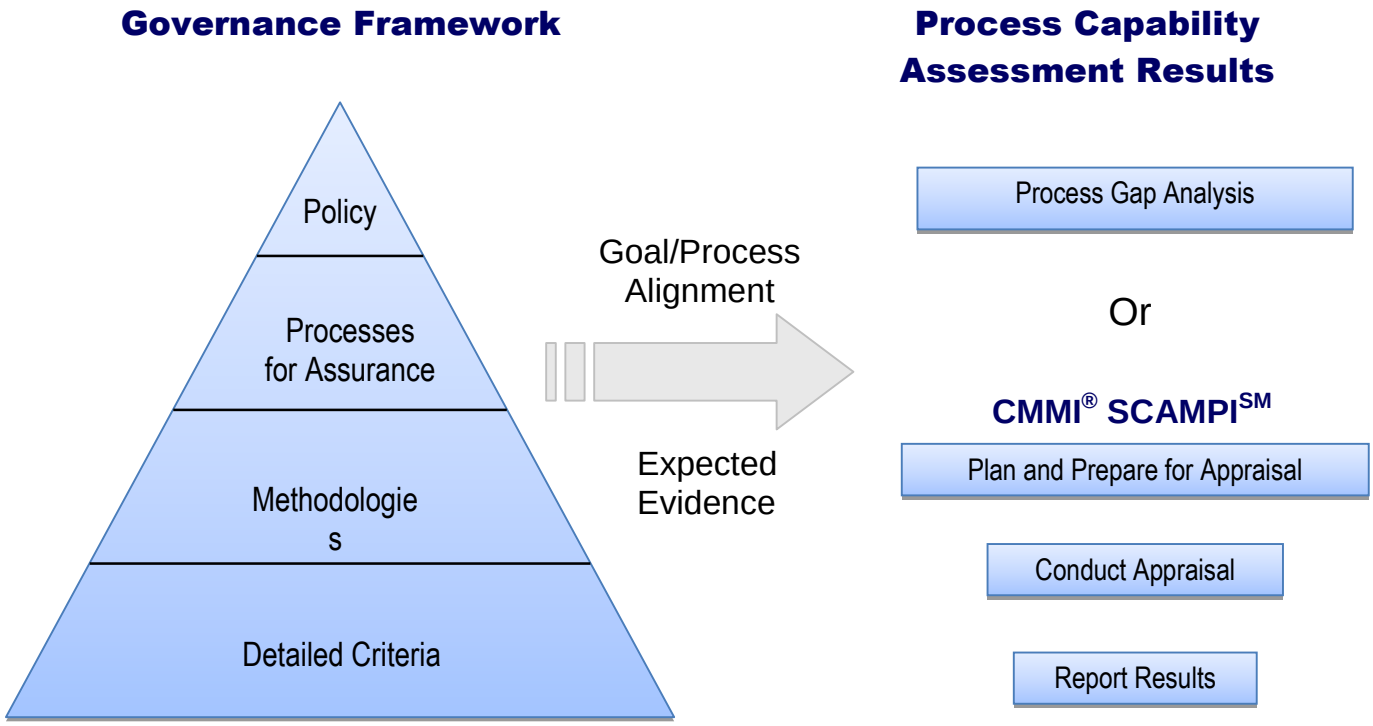
Annotated view of Organizational Training



® *CMMI is a registered in the U.S. Patent and Trademark Office by Carnegie Mellon University*

Material adapted from "Leveraging CMMs and Standards for Assurance" Paul Croll and Michele Moss SSTC 2008, Track 6, Wednesday, April 30
"Leveraging the CMMI® To Address Assurance – Benchmarking Assurance Practices and Managing Assurance Risks" Paul Croll and Michele Moss NDIA CMMI Technology Conference, November 19, 2008
"Update on the Assurance for CMMI Practices", Michele Moss and Margaret Nadworny, DHS SwA Working Group, December 4, 2008

The assurance thread can be used to assist organizations with making progress in the integration of systems and software assurance as part of their continuous process improvement efforts.



® CMMI is a registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

Material adapted from "Leveraging CMMs and Standards for Assurance" Paul Croll and Michele Moss SSTC 2008, Track 6, Wednesday, April 30

"Leveraging the CMMI® To Address Assurance – Benchmarking Assurance Practices and Managing Assurance Risks" Paul Croll and Michele Moss NDIA CMMI Technology Conference, November 19, 2008

"Update on the Assurance for CMMI Practices", Michele Moss and Margaret Nadworny, DHS SwA Working Group, December 4, 2008

Process Area Status

The PAs were into 2 groups to manage the workload and provide organizations interested in piloting the Assurance Focus earlier access to the draft material

	Group 1	***Group 2***
Process Areas	• Organizational Training (OT) • Project Planning (PP) • Project Monitoring and Control (PMC) • Measurement and Analysis (MA) • Requirements Development (RD)	• Supplier Agreement Management (SAM) • Integrate Project Management (IPM) • Verification (VER) • Validation (VAL) • Organizational Process Focus (OPF) • Organizational Process Definition (OPD) • Technical Solution (TS)
Estimated Draft	Completed	Completed

Note: Generic Practices have been put on hold due to the potential revision/streamlining of the CMMI Generic Practices in CMMI v1.3

Practices for Process and Product Quality Assurance (PPQA), Requirements Management (REQM), CM (Configuration Management), Product Integration (PI), Decision Analysis and Resolution (DAR), Organizational Process Performance (OPP), Quantitative Project Management (QPM), Organizational innovation and Deployment (OID), or Causal Analysis and Resolution (CAR) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

Updates to the Process Reference Model for Assurance are planned after completion of the draft Assurance Focus for CMMI PAs.

Material adapted from "Leveraging CMMs and Standards for Assurance" Paul Croll and Michele Moss SSTC 2008, Track 6, Wednesday, April 30
"Leveraging the CMMI® To Address Assurance – Benchmarking Assurance Practices and Managing Assurance Risks" Paul Croll and Michele Moss NDIA CMMI Technology Conference, November 19, 2008
"Update on the Assurance for CMMI Practices", Michele Moss and Margaret Nadworny, DHS SwA Working Group, December 4, 2008

Practice List

PROCESS MANAGEMENT

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

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

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

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

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

OPF SP 2.2 Implement process action plans.

OPF SP 3.1 Deploy organizational process assets across the organization.

OPF 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.

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

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

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

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

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

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

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

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

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

OPD SP 1.6 Establish and maintain work environment standards.

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

OPD SP 2.1	Establish and maintain empowerment mechanisms to enable timely decision making.
OPD SP 2.2	Establish and maintain organizational rules and guidelines for structuring and forming integrated teams.
OPD SP 2.3	Establish and maintain organizational guidelines to help team members balance their team and home organization responsibilities

OT SP 1.1	Establish and maintain the strategic training needs of the organization.
	OT AF 1.1.1 Establish and maintain the strategic assurance training needs of the organization
OT 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.
OT SP 1.3	Establish and maintain an organizational training tactical plan
OT SP 1.4	Establish and maintain training capability to address organizational training needs.
OT SP 2.1	Deliver the training following the organizational training tactical plan.
OT SP 2.2	Establish and maintain records of the organizational training.
OT SP 2.3	Assess the effectiveness of the organization’s training program.

OPP 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.
OPP SP 1.2	Establish and maintain definitions of the measures that are to be included in the organization’s process-performance analyses.
OPP SP 1.3	Establish and maintain quantitative objectives for quality and process performance for the organization.
OPP SP 1.4	Establish and maintain the organization's process-performance baselines.
OPP SP 1.5	Establish and maintain the process-performance models for the organization’s set of standard processes.

OID SP 1.1	Collect and analyze process- and technology-improvement proposals.
OID SP 1.2	Identify and analyze innovative improvements that could increase the organization’s quality and process performance.
OID SP 1.3	Pilot process and technology improvements to select which ones to implement.
OID SP 1.4	Select process and technology improvements for deployment across the organization.

OID SP 2.1	Establish and maintain the plans for deploying the selected process and technology improvements.
OID SP 2.2	Manage the deployment of the selected process and technology improvements.
OID SP 2.3	Measure the effects of the deployed process and technology improvements.

PROJECT MANAGEMENT

PP SP 1.1	Establish a top-level work breakdown structure (WBS) to estimate the scope of the project.
PP AF 1.1.1	*Define project objectives for assurance*
PP AF 1.1.2	*Define the scope of assurance for the product or service*
PP SP 1.2	Establish and maintain estimates of the attributes of the work products and tasks.
PP SP 1.3	Define the project lifecycle phases on which to scope the planning effort.
PP SP 1.4	Estimate the project effort and cost for the work products and tasks based on estimation rationale.
PP SP 2.1	Establish and maintain the project's budget and schedule.
PP SP 2.2	Identify and analyze project risks.
PP AF 2.2.1	*Identify and analyze assurance related project risks.*
PP SP 2.3	Plan for the management of project data.
PP SP 2.4	Plan for necessary resources to perform the project.
PP AF 2.4.1	*Ensure that adequate resources to execute the assurance plans are provided.*
PP SP 2.5	Plan for knowledge and skills needed to perform the project.
PP SP 2.6	Plan the involvement of identified stakeholders.
PP SP 2.7	Establish and maintain the overall project plan content.
PP SP 3.1	Review all plans that affect the project to understand project commitments.
PP SP 3.2	Reconcile the project plan to reflect available and estimated resources.
PP SP 3.3	Obtain commitment from relevant stakeholders responsible for performing and supporting plan execution.

PMC SP 1.1	Monitor the actual values of the project planning parameters against the project plan.
PMC SP 1.2	Monitor commitments against those identified in the project plan.
PMC SP 1.3	Monitor risks against those identified in the project plan.
PMC AF 1.3.1	*Monitor Assurance Risk*
PMC SP 1.4	Monitor the management of project data against the project plan.

PMC SP 1.5 Monitor stakeholder involvement against the project plan.

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

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

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

PMC SP 2.2 Take corrective action on identified issues.

PMC SP 2.3 Manage corrective actions to closure.

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

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

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

SAM SP 1.3 Establish and maintain formal agreements with the supplier.

SAM AF 1.3.1 Document supplier agreements for assurance.

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

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

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

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

SAM AF 2.4.1 Evaluate supplier deliverables against assurance acceptance criteria.

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

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

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

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

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

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

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

IPM SP 1.6	Contribute work products, measures, and documented experiences to the organizational process assets.
IPM SP 2..1	Manage the involvement of the relevant stakeholders in the project.
IPM SP 2..2	Participate with relevant stakeholders to identify, negotiate, and track critical dependencies.
IPM SP 2.3	Resolve issues with relevant stakeholders.
IPM SP 3.1	Establish and maintain a shared vision for the project.
IPM SP 3.2	Establish and maintain the integrated team structure for the project.
IPM SP 3.3	Allocate requirements, responsibilities, tasks, and interfaces to teams in the integrated team structure.
IPM SP 3.4	Establish and maintain integrated teams in the structure.
IPM SP 3.5	Ensure collaboration among interfacing teams.
RSKM SP 1.1	Determine risk sources and categories.
RSKM SP 1.2	Define the parameters used to analyze and categorize risks, and the parameters used to control the risk management effort.
RSKM SP 1.3	Establish and maintain the strategy to be used for risk management.
	RSKM AF 1.3.1 Define and select the strategy for management of risk due to vulnerabilities and safety hazards.
RSKM SP 2.1	Identify and document the risks.
RSKM AF 2.1.1	Identify and document risks associated with the identified threats, vulnerabilities and hazards.
RSKM SP 2.2	Evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority.
RSKM SP 3.1	Develop a risk mitigation plan for the most important risks to the project as defined by the risk management strategy.
RSKM SP 3.2	Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.
QPM SP 1.1	Establish and maintain the project’s quality and process-performance objectives.
QPM SP 1.2	Select the sub-processes that compose the project’s defined process based on historical stability and capability data.
QPM SP 1.3	Select the sub-processes of the project's defined process that will be statistically managed.

QPM 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.

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

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

QPM 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.

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

ENGINEERING

REQM SP 1.1 Develop an understanding with the requirements providers on the meaning of the requirements.

REQM SP 1.2 Obtain commitment to the requirements from the project participants.

REQM SP 1.3 Manage changes to the requirements as they evolve during the project.

REQM SP 1.4 Maintain bidirectional traceability among the requirements and work products.

REQM SP 1.5 Identify inconsistencies between the project plans and work products and the requirements.

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

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

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

RD AF 1.2.1 Develop Customer Assurance Requirements

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

RD AF 2.1.1 Define product and product component assurance requirements.

RD SP 2.2 Allocate the requirements for each product component.

RD SP 2.3 Identify interface requirements.

RD SP 3.1 Establish and maintain operational concepts and associated scenarios.

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

RD SP 3.2 Establish and maintain a definition of required functionality.

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

RD AF 3.3.1 Analyze assurance requirements.

RD SP 3.4 Analyze requirements to balance stakeholder needs and constraints.

RD AF 3.4.1. Balance assurance needs against cost benefits.

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

TS SP 1.1 Develop alternative solutions and selection criteria.

RD AF 1.1.1 Develop alternative solutions and selection criteria for assurance.

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

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

RD AF 2.1.1 Architect for assurance.

RD AF 2.1.2 Design for assurance.

TS SP 2.2 Establish and maintain a technical data package.

TS SP 2.3 Design product component interfaces using established criteria.

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

TS SP 3.1 Implement the designs of the product components.

TS AF 3.1.1 Implement the assurance designs of the product components.

TS AF 3.1.2 Identify deviations from assurance coding standards.

TS SP 3.2 Develop and maintain the end-use documentation.

PI SP 1.1 Determine the product component integration sequence.

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

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

PI SP 2.1 Review interface descriptions for coverage and completeness.

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

PI 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.

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

PI SP 3.3 Evaluate assembled product components for interface compatibility.

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

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

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

VAL SP 1.3 Establish and maintain procedures and criteria for validation.

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

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

VAL SP 2.2 Analyze the results of the validation activities.

VAL AF 2.2.1 Analyze the results of assurance validation activities.

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

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

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

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

VER SP 2.1 Prepare for peer reviews of selected work products.

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

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

VER SP 3.1 Perform verification on the selected work products.

VER SP 3.2 Analyze the results of all verification activities.

VER AF 3.2.1 Analyze the results of assurance verification activities.

SUPPORT

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

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

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

CM SP 2.1 Track change requests for the configuration items.

CM SP 2.2 Control changes to the configuration items.

CM SP 3.1	Establish and maintain records describing configuration items.
CM SP 3.2	Perform configuration audits to maintain integrity of the configuration baselines
PPQA SP 1.1	Objectively evaluate the designated performed processes against the applicable process descriptions, standards, and procedures.
PPQA SP 1.2	Objectively evaluate the designated work product and services against the applicable process description, standards, and procedures.
PPQA SP 2.1	Communicate quality issues and ensure resolution of noncompliance issues with the staff and managers.
PPQA SP 2.2	Establish and maintain records of the quality assurance activities.
MA SP 1.1	Establish and maintain measurement objectives that are derived from identified information needs and objectives.
MA SP 1.2	Specify measures to address the measurement objectives.
	MA AF 1.2.1 Define and improve project assurance measures.
MA SP 1.3	Specify how measurement data will be obtained and stored.
MA SP 1.4	Specify how measurement data will be analyzed and reported.
MA SP 2.1	Obtain specified measurement data.
MA SP 2.2	Analyze and interpret measurement data.
MA SP 2.3	Manage and store measurement data, measurement specifications, and analysis results.
	MA AF 2.3.1 Store assurance measures appropriately.
MA SP 2.4	Report results of measurement and analysis activities to all relevant stakeholders
DAR SP 1.1	Establish and maintain guidelines to determine which issues are subject to a formal evaluation process.
DAR SP 1.2	Establish and maintain the criteria for evaluating alternatives, and the relative ranking of these criteria.
DAR SP 1.3	Identify alternative solutions to address issues.
DAR SP 1.4	Select the evaluation methods.
DAR SP 1.5	Evaluate alternative solutions using the established criteria and methods.
DAR SP 1.6	Select solutions from the alternatives based on the evaluation criteria.
CAR SP 1.1	Select the defects and other problems for analysis.

CAR SP 1.2	Perform causal analysis of selected defects and other problems and propose actions to address them.
CAR SP 2.1	Implement the selected action proposals that were developed in causal analysis.
CAR SP 2.2	Evaluate the effect of changes on process performance.
CAR SP 2.3	Record causal analysis and resolution data for use across the project and organization.

Organizational Project Focus

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. [1, p. 241]

The key aspect of assurance in OPF is integrating assurance considerations, including those evolving from globalization, systems of systems, system survivability, and cyber issues, into the planning, implementation, and deployment of organizational process improvements.

OPF Practices without assurance focus informative material (SP 1.2, SP 1.3 and all of the SG 2 and SG 3 practices) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

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

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 [2, SP1.1.1]

- Ensure assurance needs are reflected in organizational policy [2. SP 1.2.2]
- Establish and maintain budget allocation for the establishment, execution, and enhancement of assurance practices within the organization. [2, PS 1.3.1]
- Establish and maintain collaborations with external organizations promoting assurance. [2, SP1.2.4]
- Review assurance related industry trends and available resources with higher level management[New]
- Evolve assurance needs in line with the strategic plans and direction of the organization[1.3.4]

Typical Work Products:

- *Organization's assurance related process needs and objectives*

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.

SG 2. 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. The organizational process assets are deployed across the organization and process related experience 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 derives from planning and performing the process into the organizational process assets.

Organizational Process Definition +IPPD

The purpose of Organizational Process Definition (OPD) is to establish and maintain a usable set of organizational process assets and work environment standards. For IPPD, OPD +IPPD also covers the establishment of organizational rules and guidelines that enable conducting work using integrated teams. [1, p. 219]

OPD is essential for the establishment and ongoing maintenance of organizational process assets that integrate assurance through people, process, policy, and technology to support the development and delivery of appropriately secure products and services. The IPPD portion provides the framework for the coordination of the assurance work for integrated teams.

OPD Practices without assurance focus informative material (SP 1.2, SP 1.4, SP 1.5, SP 2.1, SP 2.2, SP 2.3) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

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.

AF 1.1.1 Establish and maintain organizational processes to achieve the assurance business objectives. [2, SP1.1.2]

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.

Examples of process elements that contribute to establishment and maintenance of processes that support assurance objectives include the following:

- Mechanisms to record information concerning product vulnerabilities.
- Measures for vulnerabilities, incidents and their reporting mechanisms.
- Methodology for use of static analysis tools and peer reviews
- Inclusion of assurance roles, standards, tools, measures, etc. in the critical attributes of process elements.
- Inclusion of assurance in identifying the relationships of process elements.
- Guidelines for reporting organizational goals for assurance
- Mechanisms for monitoring the results of peer reviews conducted on the processes which have been enhanced for assurance.
- Mechanisms to update the processes as necessary based upon newly identified vulnerabilities or as required for customer compliance.

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.

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.

AF 1.3.1 Establish and maintain the tailoring criteria and guidelines for assurance in the organization's set of standard processes [2, SP1.1.3]

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

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.

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

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.

The combination of these activities contribute to both the assurance of the organization's work environment and the ability of the work environment to support assurance needs of the organization.

- Identify assurance tools. [2, SP2.1.1.5]
  Assurance tools include: threat modeling tools, static analysis tools, dynamic analysis tools, fuzzing tools, compliance tools, audit logging tools
- Maintain effective tools by ensuring any identified assurance weaknesses in the tools are fixed or mitigated. [2, SP2.1.2.5]
- Properly configure and control the work environment in accordance with the appropriate assurance controls. [2, SP4.3.1]
- Plan and test for appropriate levels of availability and recovery of the organization's environment. [2, SP4.3.5, SP4.3.5.1]
- Detect, track, and record both internal and external assurance related events. [2, SP4.3.2]
- Respond to incidents according to organizational policy. [2, SP4.3.3]
- Monitor internal and external environments for all factors that might have an impact on the assurance of the work environment and ensure they are addressed in accordance with the assurance objectives. [2,SP4.3.4]

Typical Work Products:

- Work Environment Standards updated for assurance objectives

SG 2. 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.

Organizational Training

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.

OT Practices without assurance focus informative material (SP1.2, SP1.3, SP 1.4, and all of the SG2 practices) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices..

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.

AF 1.1.1 Establish and maintain the strategic 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.

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.

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

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

Typical Work Products:

- Assurance Training Needs
- Assurance Assessment Analysis

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.

Organizational Process Performance

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. [1, p. 261]

OPP Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Establish Performance Baselines and Models

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.

Organizational Innovation and Deployment

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. [1, p. 198]

OID Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Select Improvements

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

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.

Project Planning

The purpose of Project Planning (PP) is to establish and maintain plans that define project activities. [1, p. 327]

Incorporating assurance in PP is essential for ensuring the definition of project activities encompasses assurance related aspects needed to perform and control the project. A project may not be able to meet commitments without considering assurance while estimating the attributes of the work products and tasks, determining the resources needed, negotiating commitments, producing a schedule, and identifying and analyzing project risks.

PP Practices without assurance focus informative material (SP1.2, SP1.3, SP1.4, SP2.1, SP2.3, SP2.5, SP2.6, SP2.7, and all of SG3) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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

AF 1.1.1 Define project objectives for assurance [2, SP2.1.1.1]

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

AF 1.1.2 Define the scope of assurance for the product or service. [2, SP2.1.1.4]

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

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.

SG 2. 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

AF 2.2.1 Identify and analyze assurance related project risks. [2, SP 2.1.1.8]

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.

These combined activities contribute to the proper identification and analysis of assurance related project risks.

- Consider the magnitude and technical feasibility of the project.

The magnitude and technical feasibility of the project along with the assurance objectives impact the level of risk associated with the project.

- Recognize potential assurance risks for the project.

The assurance risks depend on the assurance scope identified for the project as well as the assets impacted by the project.

- Identify mitigation alternatives for achieving product objectives

Once the risks have been identified, it is possible to consider alternatives for mitigation of the identified risk which fall within the magnitude and technical feasibility of the project.

- Prioritize the risks to be tracked as project risks.
- Plan for stakeholder involvement throughout the project [2, SP 2.1.1.3]

The appropriate stakeholders require early input to requirements and design decisions that affect them. As assurance vulnerabilities are identified throughout the life cycle of the project, decisions are made associated with the risk level associated with the vulnerabilities. Stakeholders expect to be informed of the risks to assurance and provide inputs to the acceptable levels of risk delivered at project's end.

Typical Work Products:

- Assurance Risk Impacts and Probability of Occurrence
- Assurance Risk/Mitigation associations and evaluations
- Assurance Stakeholder involvement plan

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).

AF 2.4.1 Ensure that adequate resources to execute the assurance plans are provided. [2, SP2.1.1.7]

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

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.

SG 3. 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.

Project Monitoring and Control

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. [1, p. 313]

Understanding a project's progress towards assurance objectives, enables timely corrective action to be taken when performance deviates significantly from the plan.

PMC Practices without assurance focus informative material, (SP1.1, SP1.2, SP1.4, SP1.5, SP 1.7, SP2.1, SP2.2, and SP2.3), do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

AF 1.3.1 Monitor Assurance Risk [2, SP 3.4.7]

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

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.

SG 2. 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.

Supplier Agreement Management

The purpose of Supplier Agreement Management (SAM) is to manage the acquisition of products from suppliers. [1, p. 438]

When using supplier provided hardware, software, systems, products or services, it can not be assumed that project assurance requirements will be met. The potential impact of intentional and unintentional assurance vulnerabilities from third parties must be acknowledged, identified and managed. Furthermore, the legal and business liabilities associated with poor assurance by suppliers increases the project's risks.

SAM Practices without assurance focus informative material (SP1.1, SP2.1, SP 2.2, SP2.4, SP2.5) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

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

These combined activities contribute to selecting suppliers for assurance. (2, SP2.3.1.1-SP2.3.2.2

- Establish assurance selection criteria.

  Understanding the resources created and utilized by the product provides a sound basis for identifying threats against the product. This understanding is enhanced through the deliberate specification of the level of trust required by any user of the system to access the resources provided by the product.
- Establish strategy for risk management of suppliers.

  The information collected by the previous activity is used to define the mechanisms required to manage the risk introduced by any supplier.
- Incorporate assurance into the overall selection criteria

  The general selection criteria may be impacted by the identified assurance criteria to cause a modification in either the general selection criteria or the associated risk of the item to be selected. Trade-offs of capabilities are expected and require careful consideration by the project team.
- Identify potential suppliers satisfying assurance selection criteria.

  Based upon the overall selection criteria combining general and assurance objectives along with the market research resulting from previous activities, potential suppliers are identified.
- Evaluate potential suppliers satisfying assurance selection criteria.

  The potential suppliers identified in the previous activity are evaluated according to the assurance selection criteria for understanding of the risks introduced by each supplier.

Examples of factors impacting assurance selection criteria:

- Publicly and privately identified vulnerabilities of supplier's similar products
- Evaluation of supplier's assurance capabilities
- Supplier responsiveness to resolving identified assurance issues
- Processes used to produce the product or service
- Processes used to acquire a product or service

Examples of general selection criteria impacted by assurance criteria:

- Performance
- Functionality
- Cost

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

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.

AF 1.3.1 Document supplier agreements for assurance. [2, SP2.3.3]

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. 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.

AF 2.4.1 Evaluate supplier deliverables against assurance acceptance criteria. [2, SP 2.3.5]

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

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

Integrated Project Management + IPPD

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. [1, p. 145]

Stakeholder expectations of the assurance for the project environment are key aspects to Integrated Project Management..

IPM Practices without assurance focus informative material, (SP 1.1, SP1.2, SP1.4, SP 1.5, SP1.6, SP2, and SP3), do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

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

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.

The combination of these activities contribute to both the assurance of the project's work environment and the ability of the work environment to support assurance needs of the product and service.

- Identify assurance tools. [2, SP2.1.1.5]

  Assurance tools include: threat modeling tools, static analysis tools, dynamic analysis tools, fuzzing tools, compliance tools, audit logging tools
- Maintain effective tools by ensuring any identified assurance weaknesses in the tools are fixed or mitigated. [2, SP2.1.2.5]
- Properly configure and control the work environment in accordance with the appropriate assurance controls. [2, SP4.3.1]
- Plan and test for appropriate levels of availability and recovery of project environment. [2, SP4.3.5, SP4.3.5.1]
- Detect, track, and record both internal and external assurance related events. [2, SP4.3.2]
- Respond to incidents according to organizational policy. [2, SP4.3.3]
- Monitor internal and external environments for all factors that might have an impact on the assurance of the work environment and ensure they are addressed in accordance with the assurance objectives. [2,SP4.3.4]

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.

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.

SG 2. 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. 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.

Risk Management

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 [1, p. 419]

The concept of risk is expanded to include the scope of assurance risks. The risks associated with failure to meet the project plan schedule, quality, and costs must be harmonized with specialized assurance risks such as unintentional and intentional vulnerabilities in the product and threats against the product, safety hazards, and reliability impacts. This will ensure that all stakeholders are included in risk management activities.

RSKM practices without assurance focus informative material, (SP1.1, SP1.2, SP2.2, SP3.1 and SP3.2), do not require unique activities to incorporate assurance. However, there is an assumption that assurance is incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

AF 1.3.1 Define and select the strategy for management of risk due to vulnerabilities and safety hazards. [2, SP3.4.1]

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. 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.

AF 2.1.1 Identify and document risks associated with the identified threats, vulnerabilities and hazards. [2, SP3.4.3]

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.

Examples of risks associated with identified threats, vulnerabilities, and hazards

- For web applications, there is a threat of the cross site scripting attack which can result in the assets of the application being compromised
- For mechanical applications, the boundary conditions of safe operations have the risk of users taking the product outside of the safety zones.
- For some software applications, it is common for the system administrator to be asked to change a password that is now recognized as a risk of an attacker escalating the privilege for that application during operation.
- Architects may decide that encryption is required to ensure confidentiality of data but the developers attempt to code their own algorithm rather than using well established algorithms implemented by cryptography experts. This results in a very high risk that the data being protected is compromised.

Typical Work Products:

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

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

SG 3. 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 the risk management strategy.

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

Quantitative Project Management

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. [1, p. 364]

QPM Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Quantitatively Manage the Project

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.

.

Requirements Management

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. [1, p. 408]

REQM Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Manage Requirements

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.

Requirements Development

The purpose of Requirements Development (RD) is to produce and analyze customer, product, and product component requirements. [1, p. 387]

As a part of Requirements Development, it is necessary to include requirements for assurance. Assurance requirements are derived from relevant regulations, laws, standards, and policy that define levels of assurance for the customer, product, and product components. Assurance requirements need to be developed, allocated, traced, verified and validated as part of the systems development lifecycle. Assurance requirements, like other requirements, need to be decomposed into lower level components.

RD Practices without assurance focus informative material (SP2.2, SP2.3, SP3.2, and SP.) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

AF 1.1.1 Understand the operating environment and define the operating constraints for assurance within the environments of system deployment. [2, SP 3.1.1]

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.

These combined activities contribute to the proper understanding of the operating environment (SP3.1.1.1 – SP 3.1.1.3)

- Identify the system assurance context.

The context of the system includes the rationale for the existence of the product. The assurance implications of the primary functional, operational and performance requirements for the product are evaluated.

- Identify the system vulnerabilities with each operating environment defined for the system.

Each operating environment may be known to have vulnerabilities associated with specific security threats and safety hazards. These vulnerabilities need to be understood in association with the product under development. The system and human interfaces are an element of the system assurance context and related vulnerabilities should be examined in the context of mission critical threads.

- 3. Identify applicable assurance laws, policies, and constraints.

Understanding how relevant assurance laws, policies, and constraints impact the product within the prescribed operating environment is critical to ensure appropriate and effective compliance with these governing requirements.

Examples of assurance related issues associated with the operating environment:

- A product operating on a closed network would have fewer assurance implications than a product operating in an environment with multiple interfaces such as an intranet or the Internet.
- There are well known threats and vulnerabilities associated with Linux, Windows, Web Applications, etc.

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.

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.

AF 1.2.1 Develop Customer Assurance Requirements[2, SP 3.1.2.1]

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. 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.

AF 2.1.1 Define product and product component assurance requirements. [2, SP 3.1.2.4]

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.

SP 2.2 Allocate the requirements for each product component.

SP 2.3 Identify interface requirements.

SG 3. 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).

AF 3.1.1 Identify operational concepts and associated scenarios for assurance. [2, SP 3.1.2.2 and SP 3.1.2.3]]

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
- Any assurance related assumptions or external dependencies for operating environments

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.

AF 3.3.1 Analyze assurance requirements. [2, SP 3.1.1.3, SP 3.1.3.1 and SP 3.1.3.2, and SP 3.1.3.3]

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.

Activities that contribute to a comprehensive analysis of requirements for assurance include:

- Requirements at all component levels are analyzed to ensure the proper allocation of assurance requirements. Part of this analysis requires that the architecture behaves as expected. For example, if there is an error within the system, the error handling function addresses the error appropriately.
- Analysis of the requirements against the assurance objectives ensures that the requirements match the assurance needs of the project. This analysis may result in the need for additional requirements or modifications of requirements.

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.

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.

AF 3.4.1. Balance assurance needs against cost benefits. [2, SP 3.1.3.3]

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

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

Technical Solution

The purpose of Technical Solution (TS) is to design, develop, and implement solutions to requirements. Solutions, designs, and implementations encompass products, product components, and product-related lifecycle processes either singly or in combination as appropriate. [1, p. 455]

The assurance focus in technical solution is on the implementation of requirements in the context of ensuring trustworthy operation in support of mission/business objectives. These considerations contribute to the quality of the product.

TS practices without assurance focus informative material, (SP1.2, SP2.2, SP2.3, SP2.4, and SP 3.2), do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

AF 1.1.1 Develop alternative solutions and selection criteria for assurance. [2, SP3.4.2]

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

The following activities enhance the understanding of assurance considerations when developing and selecting alternative solutions.

- Identify assurance defects and effectiveness of corrective actions in relevant products/systems/operations and apply lessons learned to alternative solutions
- Understand the assurance capabilities of other products similar to the one under development that have been developed internally, by partners, and by competitors
- Use current events regarding intentional and unintentional threat agents and their potential direction to identify alternative solutions.
- Use assurance resources (i.e. Object Management Group, SANS, domain specific resources, etc) to understand the issues, vulnerabilities, threats, and risks to the current product under development.
- Use resolutions from previous events to provide useful information in the effectiveness of alternative solutions.
- Use security, safety, reliability and resiliency issues to identify and prioritize mitigation of assurance concerns in the selection criteria.

Typical Work Products:

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

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

SG 2. 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.

AF 2.1.1 Architect for assurance. [2, SP3.2.1]

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.

These combined activities contribute to an architecture for assurance. [2, SP3.2.1]

- Ensure the assurance of the product from the end-user's perspective
- Ensure the customer's assurance responsibilities are specified
- Identify resources and trust boundaries.
  Understanding the resources created and utilized by the product provides a sound basis for identifying threats against the product. This understanding is enhanced through the deliberate specification of the level of trust required by any user of the system to access the resources provided by the product.
- Architect the error handling and failure modes to support resiliency, continuity of operations, containment, and disaster recovery.
- Identify and characterize threats to the assurance of the system.
- Identify and characterize risks to the operation of the system.
- Confirm that identified counter-measures sufficiently address threats to mitigate the risks.
- Evolve architectures based upon a cost-benefit analysis and assurance requirements in each of the operational environments for the system.
  Operational environments can vary from a single user on an isolated network to any user on the internet. The protections for operational environments differ depending on the product requirements. The different protections will naturally have different costs and constraints associated with them. The product architects are expected to consider the best options for the product based upon the individual operating environments while meeting the overall requirements.
  This is especially important when components are reused or acquired from third parties. The original architecture includes assumptions about the operating environment for the components. The exercise of specifying the proper operating environments will result in fewer surprised exploits for the current product and applications of reuse for current components used in future applications.

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

AF 2.1.2 Design for assurance. [2, SP3.2.2]

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.

These combined activities contribute to a design for assurance. (2, SP3.2.2.1-SP3.2.2.4)

- Understand threat related design issues for design alternatives

  Emphasize potential design issues related to threat models or risk scenarios when considering design solutions to optimize the design for assurance.
- Evolve operational concepts and scenarios for assurance.

  For each design, the operational environments specified by the architecture and the various threat models are applied to identify potential vulnerabilities.
- Select solution for assurance.

  Based upon the designs, the corresponding operational risk analyses, and the selection criteria, the design meeting the criteria for assurance for the
  product is selected.
- Employ appropriate assurance design patterns and anti-patterns.

  Numerous design patterns for assurance exist in the literature and are used by the design team to address common countermeasures to established attacks or failures. These are already reviewed and tested in the wider engineering community enabling designers to maintain focus on the functional requirements of the product.

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

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.

SG 3. 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.

AF 3.1.1 Implement the assurance designs of the product components. [2, SP 3.2.3]

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

Examples of assurance design patterns include:

- Ensuring protection against commonly exploited vulnerabilities
- Ensuring proper configuration of components

Typical Work Products:

- Implemented design for assurance

AF 3.1.2. Identify deviations from assurance coding standards. Implement appropriate mitigation to meet defined assurance objectives. [2, SP 3.2.3.1]

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.

SP 3.2 Develop and maintain the end-use documentation.

Product Integration

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. [1, p. 293]

PI Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Prepare for Product Integration

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

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.

SG 3. Assemble Product Components and Deliver the Product

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.

.

Validation

The purpose of Validation (VAL) is to demonstrate that a product or product component fulfills its intended use when placed in its intended environment. [1, p. 482]

The Assurance emphasis in validation is on the trustworthiness or predictability of a product or service in its intended environment. Critical to this step is demonstrating that a product or product component does not fulfill any unintended uses in any of the intended environments which can negatively impact the intended uses. The results of the validation efforts contribute to quantifying assurance as a common platform for communicating information about the assurance of a product or service.

VAL Practices without assurance focus informative material (SP1.1, SP1.2, and SP2.1) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

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

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

- Validation of assurance criteria and measurements. [2, SP3.4.3.1]

The assurance validation and measurement criteria define the expected behavior of a product or service in its intended environment. Criteria to be evaluated include unintended functionality, unintended use, malicious attacks, and out of sequence events (e.g. sequence/timing attacks, race conditions, etc.).

- 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. Resiliency includes operational design, error handling capability, containment, continuity of operations, and disaster recovery.

- Validation of the product through the results of threat modeling in addition to the usual validation practices of inspection, test, demonstration, and analysis. [2, SP 3.4.3.2]

Threat and vulnerability awareness in conjunction with threat modeling, should be part of the overall validation activities with regard to the assurance focus.

Typical Work Products:

- Assurance Validation Procedures
- Assurance Validation Criteria
- Assurance Validation/Test and evaluation procedures for maintenance, training, and support

SG 2. 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.

AF 2.2.1 Analyze the results of assurance validation activities. [2, SP3.3.3.4]

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

Verification

The purpose of Verification (VER) is to ensure that selected work products meet their specified requirements. [1, p. 495]

For assurance, verification includes employing the appropriate rigor in checking that requirements were implemented correctly to achieve confidence in the trustworthiness and predictability of a product or service. If requirements are not implemented correctly potential exploitation from unintended functionality may exist in the product or service.

Verification practices without assurance focus informative material, (SP1.1, SP1.2, SP2.1, SP 2.2, SP2.3, and SP 3.1) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

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

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

The combination of these activities contribute to verification of assurance

- Identify verification of measurement criteria used to establish the assurance case. [2, SP3.3.2.1]

The assurance verification and measurement criteria define a list of cases that check against the implementation of requirements. Criteria evaluated include unintended functionality, scenarios not defined as part of requirements (out of scope), and out of sequence events (e.g. sequence/timing attacks, race conditions, etc.).

- Verification of the product for assurance requirements.[2, SP 3.3.2.3]

Perform the verification of assurance requirements in such a way as to objectively evaluate that products and services fulfill their intended use.

- Verification of the resiliency of the product. [2, SP 3.1.2.3.1]

Assurance related capabilities of the system under development should be verified against resiliency criteria during appropriate verification activities (i.e. during integration testing). Resiliency includes operational design, error handling capability, containment, continuity of operations, and disaster recovery.

- Verification of the product when tested from an attacker perspective [2, SP 3.3.2.4]

Assurance verification conducted throughout the system life cycle should be performed in a manner that exercises the security and safety aspects of the requirements. Verification in this regard is a positive response to mitigate the effects imposed on the system by malicious attackers.

- Verification of the product through the results of threat modeling in addition to the usual verification practices of inspection, test, demonstration, and analysis. [2, SP 3.3.2.4.1]

Threat and vulnerability awareness in conjunction with threat modeling, should be part of the overall verification activities with regard to the assurance focus.

Typical Work Products:

- Assurance Verification procedures
- Assurance criteria
- Assurance scenarios
- Event/ Error handling verification procedures

SG 2. 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. 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.

AF 3.2.1 Analyze the results of assurance verification activities. [2, SP3.3.3.4]

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.

Configuration Management

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.[1, p. 114]

CM Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Establish Baselines

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

SP 2.1 Track change requests for the configuration items.

SP 2.2 Control changes to the configuration items.

SG 3. Establish Integrity

SP 3.1 Establish and maintain records describing configuration items.

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

Process and Product Quality Assurance

The purpose of Process and Product Quality Assurance (PPQA) is to provide staff and management with objective insight into processes and associated work products. [1, p. 353]

PPQA Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Objectively Evaluate Processes and Work Products

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

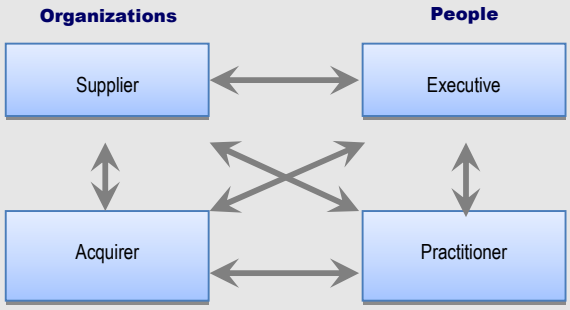
SP 2.1 Communicate quality issues and ensure resolution of noncompliance issues with the staff and managers.

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

Measurement and Analysis

The purpose of Measurement and Analysis (MA) is to develop and sustain a measurement capability that is used to support management information needs. [1, p. 178]

Quantifying assurance through the use of measurement and analysis provides a common platform for communicating information about the assurance of a product or service. The quantifiable information about the system is assembled to support a set of arguments that justify a claim about the assurance of a system. The claim, arguments, and quantifiable information is called an assurance case. Stakeholders can make decisions on the assurance of the product/service based on the justification provided.



MA Practices without assurance focus informative material (SP1.1, SP1.3, SP1.4, SP 2.1, SP2.3 and SP 2.4) do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. 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.

AF 1.1.1 Define and improve project assurance measures. [2, SP2.2.4.1]

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.

Examples of project assurance measures.

- Estimates and actual effort of assurance activities
- Reduction in vulnerabilities between peer reviews
- Assurance measures (e.g., number of vulnerabilities by severity.)
- Estimates and actual number of assurance threats not identified

Typical Work Products:

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

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

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

SG 2. Measurement results, which address identified information needs and objectives, are provided.

SP 2.1 Obtain specified measurement data.

SP 2.2 Analyze and interpret the 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.

AF 2.3.1 Store assurance measures appropriately. [2, SP 2.2.4.3]

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

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

Decision Analysis and Resolution

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.[1, p. 131]

DAR Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Evaluate Alternatives

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.

Causal Analysis and Resolution

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. [1, p. 101]

CAR Practices do not require unique activities to incorporate assurance. However, there is an assumption that assurance incorporated in related activities and work products are considered in the execution of these practices.

SG 1. Determine Causes or Defects

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

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.