References: [4] [30] [61] [71] [98] [99] [117]

Related Publications: [100]

AR-4 MANAGE THE RESULTS OF SYSTEM ARCHITECTURE DEFINITION

AR-4.1 Obtain agreement on the security aspects of the architecture.

AR-4.2 Record key security-relevant system architecture decisions and the rationale.

AR-4.3 Maintain the traceability of the security aspects of the system architecture.

AR-4.4 Provide the security-relevant artifacts that have been selected for baselines.

AR-4.5 Provide support to organizational architecture governance and architecture management efforts.

References: [4] [30] [61] [71] [98] [99] [100] [117]

H.5. Design Definition

The purpose of the *Design Definition* process is to provide sufficient data and information about the system and its elements to realize the solution in accordance with the system requirements and architecture.

H.5.1. Security Purpose

- Provide sufficient detailed data and information about the security aspects of the system and its elements to realize a trustworthy secure solution in accordance with the system requirements and architecture.

H.5.2. Security Outcomes

- Security aspects of design alternatives for system elements are assessed.
- System requirements are allocated to address their security aspects.
- Security interfaces and security aspects of interfaces between system elements composing the system are defined.
- Security design characteristics of each system element are defined.
- Enabling systems or services for the security aspects of design definition are available.
- Traceability of security design characteristics is established.

H.5.3. Security Activities and Tasks

DE-1 PREPARE FOR DESIGN DEFINITION

DE-1.1 Establish the trustworthy secure aspects of the design definition strategy.

DE-1.2 Determine the security technologies required for each system element composing the system.

DE-1.3 Identify the security concerns associated with each technology required for each system element.

Note 1: This includes the security concerns due to known and potential vulnerability within or enabled by the supply chains involved with the acquisition of technologies.

Note 2: The concerns may have associated risks to record and track.

DE-1.4 Determine the necessary security and trustworthiness categories of system characteristics represented in the design.

DE-1.5 Define the precepts for trustworthy secure evolution of the system design.

DE-1.6 Identify the security aspects for enabling systems or services needed to support design definition.

DE-1.7 Identify and plan for enabling systems or services needed to support the security aspects of design definition.

DE-1.8 Obtain or acquire access to the security aspects of enabling systems or services to be used in design definition.

References: [4] [30] [61] [98] [99] [100]

DE-2 CREATE THE SYSTEM DESIGN

DE-2.1 Allocate security requirements to system elements.

DE-2.2 Transform security-relevant architectural entities and relationships into design elements.

DE-2.3 Transform security-relevant architectural characteristics into trustworthy secure design characteristics.

Note: The characteristics include or reflect the expected level of assurance.

DE-2.4 Define the necessary trustworthy secure design enablers.

DE-2.5 Examine trustworthy secure design alternatives.

DE-2.6 Refine or define the security aspects of interfaces between system elements and with external entities.

Note: The details of the defined interfaces are refined to include the security aspects. These include security and security-driven constraints applied to interfaces, interactions, and behavior between components and with external entities, such as interfacing systems (Section 2.1.2), peripheral devices, and humans interacting with the system.

DE-2.7 Develop the security aspects of design artifacts.

Note 1: Design artifacts include general and security-specific specifications, data sheets, databases, and documents.

Note 2: Design artifacts include configuration and procedures to ensure security mechanism behavior specified by system-level policy and enforced by configuration and procedures (Appendix C.3).

DE-2.8 Capture the security aspects of the design.

References: [4] [30] [61] [86] [98] [99] [100] [106] [107] [108] [109]

DE-3 EVALUTE THE SYSTEM DESIGN

DE-3.1 Analyze each system design alternative against criteria developed from expected trustworthy secure design properties and characteristics.

DE-3.2 Assess each system design alternative for how well it meets stakeholder protection needs and the security aspects of the system requirements.

Note: Assessment includes assessing configuration and procedures to ensure security mechanism behavior specified by system-level policy and enforced by configuration and procedures (Appendix C.3).

DE-3.3 Combine the security analyses and assessments in the overall evaluation to select a preferred design solution.

References: [4] [30] [61] [86] [98] [99] [100] [109]

DE-4 MANAGE THE RESULTS OF DESIGN DEFINITION

DE-4.1 Obtain agreement on the security aspects of the design.

DE-4.2 Map the trustworthy secure design characteristics to the system elements.

DE-4.3 Record the trustworthy secure design decisions and the rationale.

DE-4.4 Maintain traceability of the security aspects of the system design.

Note: Traceability is maintained between the trustworthy secure design characteristics and the security architectural entities, system element requirements, interface definitions, analysis results, and verification and validation methods or techniques.

DE-4.5 Provide the security-relevant artifacts that have been selected for baselines.

References: [4] [100] [106] [107] [108]

H.6. System Analysis

The purpose of the *System Analysis* process is to provide a rigorous basis of information and data for technical understanding to aid decision-making and technical assessments across the life cycle.

H.6.1. Security Purpose

- Produce a rigorous basis of data and information for the technical understanding of security aspects to aid decision-making and technical assessments across the life cycle.

H.6.2. Security Outcomes

- Security aspects of system analysis needs are identified.

- Security aspects of system analysis assumptions and results are validated.
- System analysis results provided for all decisions or technical assessment needs include security aspects.
- Enabling systems or services for the security aspects of system analysis are available.
- Traceability of the security aspects of the system analysis results is established.

H.6.3. Security Activities and Tasks

SA-1 PREPARE FOR SYSTEM ANALYSIS

SA-1.1 Define the security aspects of the system analysis strategy.

SA-1.2 Identify the security aspects of the problem or question that require system analysis.

Note: The problem or question may not be driven by or have obvious security considerations or aspects.

SA-1.3 Identify the security-relevant stakeholders of the system analysis.

SA-1.4 Define the scope, objectives, level of fidelity, level of rigor, and level of assurance for the security aspects of system analysis.

SA-1.5 Select the methods to address the security aspects of system analysis.

SA-1.6 Identify the security aspects for enabling systems or services needed to support system analysis.

SA-1.7 Identify and plan for enabling systems or services needed to support the security aspects of system analysis.

SA-1.8 Obtain or acquire access to the security aspects of enabling systems or services to be used in system analysis.

SA-1.9 Identify and validate security-relevant assumptions.

Note 1: This includes assumptions derived from the limits of certainty: what is known, what is insufficiently known, and what is unknown.

Note 2: Assumptions that cannot be validated represent uncertainty and potential risk.

SA-1.10 Plan for and collect the data and inputs needed for the security aspects of the analysis.

References: [4] [30] [61] [98] [99] [100]

SA-2 PERFORM SYSTEM ANALYSIS

SA-2.1 Apply the selected analysis methods to perform the required security-relevant aspects of system analysis.

SA-2.2 Review analysis results for security-relevant quality and validity.

Note: The results are coordinated with associated and previously completed security-relevant analyses. Trustworthiness of the results is determined with the review.

SA-2.3 Establish conclusions and recommendations for the security aspects of the system analysis.

Note: Subject-matter experts are consulted and participate in the formulation of conclusions and recommendations.

SA-2.4 Record the results of the security aspects of the system analysis.

References: [4] [86] [100] [106] [107] [108] [109]

SA-3 MANAGE SYSTEM ANALYSIS

SA-3.1 Maintain traceability of the security aspects of the system analysis results.

Note: Bidirectional traceability captures the relationship between the security aspects of the system analysis results, the methods employed, the data used for the analysis, the assumptions, and the context that defines the problem or question addressed.

SA-3.2 Provide the security-relevant artifacts that have been selected for baselines.

Note: This includes general artifacts and security-specific artifacts.

References: [4] [100] [106] [107] [108]

H.7. Implementation

The purpose of the *Implementation* process is to realize a specified system element.

H.7.1. Security Purpose

- Transform system security requirements, architecture, and design (including interfaces) into actions that create a trustworthy secure system element according to the practices of the selected implementation technology using appropriate security and non-security technical specialties or disciplines.

H.7.2. Security Outcomes

- Security-relevant implementation constraints that influence the requirements, architecture, or design are identified.
- A trustworthy secure system element is realized.
- System elements are securely packaged and stored.
- Enabling systems or services for the security aspects of implementation are available.
- Traceability of the security aspects of the implemented system elements is established.

H.7.3. Security Activities and Tasks

IP-1 PREPARE FOR IMPLEMENTATION

IP-1.1 Define the trustworthy secure aspects of the implementation strategy.

Note 1: These aspects apply to all system elements that are acquired new, built new, or reused (with or without modification). If the strategy is reuse, the project determines the extent,

source, suitability, and trustworthiness of the reused system elements for the new purpose. The implementation strategy includes procedures, fabrication processes, tools and equipment, tolerances, and verification uncertainties, which may introduce weaknesses and vulnerabilities. In the case of repeated system element implementation (e.g., mass production, replacement system elements), the procedures and fabrication processes are defined to achieve consistent and repeatable trustworthy producibility.

Note 2: The security aspects are informed by the targeted level of assurance, security verification uncertainties, and security concerns associated with implementation-related logistics, supply, and distribution of components.

IP-1.2 Identify security-relevant constraints and objectives from implementation in the system security requirements, architecture and design characteristics, or implementation techniques.

IP-1.3 Identify the security aspects for enabling systems, services, and materials needed to support implementation.

IP-1.4 Identify and plan for enabling systems, services, and materials needed to support the security aspects of implementation.

IP-1.5 Obtain or acquire access to the security aspects of enabling systems, services, and materials to be used in implementation.

References: [4] [30] [61] [98] [99] [111] [112] [113]

IP-2 PERFORM IMPLEMENTATION

IP-2.1 Realize or adapt system elements in accordance with the security aspects of the implementation strategy and implementation procedures, as well as security-relevant constraints.

Note: System elements can include:

- *Hardware and Software:* Hardware and software elements are either acquired or fabricated.

  Custom hardware fabrication and software development enable insight into the details of design and implementation. These insights often translate to increased assurance.

  Acquired hardware and software elements may not provide the opportunity to achieve the same insight into design and implementation and may offer more functionality and capability than required. The limits of what can be known about the internals of the elements translate to a level of uncertainty about vulnerability and the maximum assurance that can be achieved.
- *Firmware:* Firmware exhibits properties of hardware and software. Firmware elements may be acquired or developed to realize the software aspects and then fabricated to realize the physical form of the hardware aspects. Firmware elements, therefore, adhere to the security implementation considerations of both hardware and software elements.
- *Services:* System elements implemented by obtaining or leasing services are subject to the same criteria used to acquire hardware, firmware, and software but must also address the security considerations associated with utilization and support resources.
- *Utilization and Support Resources:* The security considerations of acquired or leased services account for the specific roles and responsibilities of individuals of the service/lease provider

and their ability to account for all of the security requirements and constraints associated with the delivery, utilization, and sustainment of the service or capability being leased.

IP-2.2 Place the system element in a secure state for future use, as needed.

Note: This includes protection of the element while stored and in transit, as well as the packaging and labeling of the element.

IP-2.3 Record objective evidence that system elements meet the system security requirements.

References: [4] [30] [61] [86] [98] [99] [109] [111] [112] [113]

IP-3 MANAGE RESULTS OF IMPLEMENTATION

IP-3.1 Record the security aspects of implementation results and any anomalies encountered.

IP-3.2 Maintain traceability of the security aspects of implemented system elements.

Note: Bidirectional traceability of the security aspects of the implemented system elements to the system security requirements, the security views of the architecture, the security design, and the security interface requirements is maintained.

IP-3.3 Provide the security-relevant artifacts that have been selected for baselines.

References: [4] [30] [61] [98] [99]

H.8. Integration

The purpose of the *Integration* process is to synthesize a set of system elements into a realized system that satisfies the system requirements.

H.8.1. Security Purpose

- Synthesize a set of system elements into a realized trustworthy secure system that satisfies the system requirements.

H.8.2. Security Outcomes

- Security-relevant integration constraints that influence requirements, architecture, design, or interfaces and interactions are identified.
- Approaches and checkpoints for the correct secure activation of the identified interfaces and system functions to an initial or established secure state are developed.
- Enabling systems or services for the security aspects of integration are available.
- A trustworthy secure system composed of implemented system elements is integrated.
- Security aspects of system external interfaces (system to external environment) and system internal interfaces (between implemented system elements) are checked.
- Security aspects of integration results and anomalies are identified.

- Traceability of the security aspects of the integrated system elements is established.

H.8.3. Security Activities and Tasks

IN-1 PREPARE FOR INTEGRATION

IN-1.1 Identify and define checkpoints for the correct secure activation and integrity of the interfaces and the selected system functions as the system elements are synthesized.

IN-1.2 Define the security aspects of the integration strategy.

Note: Integration is performed to achieve trustworthy secure results using aspects such as secure assembly sequences and checkpoints for the system elements based on established priorities while minimizing integration time and cost and providing appropriate risk treatments.

IN-1.3 Identify the security-relevant constraints and objectives from integration to be incorporated into the system requirements, architecture, or design.

IN-1.4 Identify the security aspects for enabling systems, services, and materials needed to support integration.

IN-1.5 Identify and plan for enabling systems, services, and materials needed to support the security aspects of integration.

IN-1.6 Obtain or acquire access to the security aspects of enabling systems, services, and materials to be used in integration.

References: [4] [30] [61] [81] [98] [99] [100] [111] [112] [113]

IN-2 PERFORM INTEGRATION

IN-2.1 Check interface availability and conformance of the interfaces in accordance with the security aspects of interface definitions and integration schedules.

IN-2.2 Perform actions to address any security-relevant conformance or availability issues.

IN-2.3 Securely combine the implemented system elements in accordance with planned sequences.

IN-2.4 Securely integrate system element configurations until the complete system is securely synthesized.

IN-2.5 Check for the expected results of interfaces, interconnections, selected functions, and security characteristics.

References: [4] [86] [100] [109] [111] [112] [113]

IN-3 MANAGE RESULTS OF INTEGRATION

IN-3.1 Record the security aspects of integration results and any anomalies encountered.

Note: Anomaly analyses determine corrective actions that may affect the protection capability of the system and the level of assurance that can be obtained.

IN-3.2 Maintain traceability of the security aspects of integrated system elements.

Note: Bidirectional traceability of the security aspects of the integrated system elements to the system security requirements, security views of the architecture, security design, and security

interface requirements is maintained. Traceability provides evidence that supports assurance and trustworthiness claims.

IN-3.3 Provide the security-relevant artifacts that have been selected for baselines.

References: [4] [30] [61] [98] [99] [100]

H.9. Verification

The purpose of the *Verification* process is to provide objective evidence that a system, system element, or artifact fulfills its specified requirements and characteristics.

H.9.1. Security Purpose

- Provide objective evidence that a system, system element, or artifact (e.g., system requirements, architecture description, or design description) fulfills its specified security requirements and characteristics.
- Identify security-relevant anomalies[98] in any artifact, implemented system elements, or life cycle processes, and provide the necessary information to determine the resolution of such anomalies.

H.9.2. Security Outcomes

- Security-relevant verification constraints that influence requirements, architecture, or design are identified.
- Enabling systems or services for the security aspects of verification are available.
- Security aspects of the system, system element, or artifact are verified.
- Security-relevant data that provides information for corrective actions is reported.
- Objective evidence that the realized system fulfills the security requirements and security aspects of the architecture and design is provided.
- Security aspects of verification results and anomalies are identified.
- Traceability of the security aspects of the verified system elements is established.

H.9.3. Security Activities and Tasks

VE-1 PREPARE FOR VERIFICATION

VE-1.1 Identify the security aspects within the verification scope and corresponding security verification actions.

Note: Scope includes the system, system elements, information items, or artifacts that will be verified against applicable requirements, security characteristics, or other security properties. Each verification action description includes what will be verified (e.g., actual system, model,

[98] Anomalies include behaviors and outcomes that are observed but not specified.

mock-up, prototype, procedure, plan, or other information item), the verification method (including any adversity emulation), and the expected result as defined by the success criteria. The security criteria may reflect considerations of strength of function/mechanism, resistance to tamper, misuse or abuse, penetration resistance, level of assurance, absence of flaws, weaknesses, and the absence of unspecified behavior and outcomes.

VE-1.2 Identify the constraints that can potentially limit the feasibility of the security-focused verification actions.

Note: Constraints include technical feasibility; the availability of qualified personnel and verification enablers; the availability of sufficient, relevant, and credible threat data; technology employed (including adversity emulation); the size and complexity of the system element or artifact; and the cost and time allotted for the verification.

VE-1.3 Select appropriate security verification methods and the associated success criteria for each security verification action.

Note: The methods and techniques are selected to provide the evidence required to achieve the expected results with the desired level of assurance.

VE-1.4 Define the security aspects of the verification strategy.

Note: This includes the approach used to incorporate security considerations into all verification actions while considering the trade-offs between scope, depth, and rigor needed for the desired level of assurance and the given constraints.

VE-1.5 Identify the security-relevant constraints and objectives that result from the security aspects of the verification strategy to be incorporated into the system requirements, architecture, and design.

VE-1.6 Identify the security aspects for enabling systems or services needed to support verification.

VE-1.7 Identify and plan for enabling systems or services needed to support the security aspects of verification.

VE-1.8 Obtain or acquire access to the security aspects of enabling systems or services to be used in verification.

References: [4] [30] [31] [61] [86] [[97] [98] [99] [100] [119] [120] [121] [122]

VE-2 PERFORM VERIFICATION

VE-2.1 Define the security aspects of the verification procedures, each supporting one or a set of verification actions.

Note: The procedures identify the security purpose of verification, the success criteria (expected results), the verification method to be applied, the necessary enabling systems (e.g., facilities, equipment), and the environmental conditions to perform each verification procedure (e.g., resources, qualified personnel, adversity emulations).

VE-2.2 Perform security verification procedures.

References: [4] [86] [97] [100] [109]

VE-3 MANAGE RESULTS OF VERIFICATION

VE-3.1 Record the security aspects of verification results and any anomalies encountered.

VE-3.2 Obtain agreement from the approval authority that the system, system element, or artifact meets the specified system security requirements.

Note: There may be multiple approval authorities with security-relevant responsibilities.

VE-3.3 Maintain traceability of the security aspects of verification.

Note: Bidirectional traceability is maintained between the verified security aspects of system elements and the system security requirements, architecture, design, and interface requirements. This traceability includes verification results or evidence, such as security-relevant anomalies, deviations, or requirement satisfaction.

VE-3.4 Provide the security-relevant artifacts that have been selected for baselines.

References: [4] [30] [61] [98] [99] [100] [109]

H.10. Transition

The purpose of the *Transition* process is to establish a capability for a system to provide services specified by stakeholder requirements in the operational environment.

H.10.1. Security Purpose

- Preserve the system's verified security characteristics during the orderly and planned transition of the system to be operable in the intended environment, which may be a new or changed environment.

H.10.2. Security Outcomes

- Security-relevant transition constraints that influence system requirements, architecture, or design are identified.
- Enabling systems or services for the security aspects of transition are available.
- The prepared site satisfies security criteria.
- The system is installed in its operational environment and can deliver its specified functions in a trustworthy secure manner.
- Operators, users, and other stakeholders necessary to the system utilization and support are trained in the system's security capabilities, mechanisms, and features.
- Security-relevant transition results and anomalies are identified.
- The installed system is activated and ready for trustworthy secure operation.
- Traceability of the security aspects of the transitioned elements is established.

H.10.3. Security Activities and Tasks

TR-1 PREPARE FOR TRANSITION

TR-1.1 Define the security aspects of the transition strategy.

Note: The transition strategy includes all security-relevant activities, from site delivery and installation through the deployment and commissioning of the system, as well as all security-relevant stakeholders, including human operators. The strategy also includes security roles and responsibilities, facility security considerations, secure shipping and receiving, contingency back out plans, security training, security aspects of installation acceptance demonstration tasks, secure operational readiness reviews, secure operations commencement, transition security success criteria, rights of secure access, data rights, and integration with other plans. System commissioning is considered along with the secure decommissioning of the old system when one exists. In this case, the Transition and Disposal processes are used concurrently.

TR-1.2 Identify and define any security-relevant facility or site changes needed.

TR-1.3 Identify the security-relevant constraints and objectives from the security aspects of transition to be incorporated into the system requirements, architecture, and design.

TR-1.4 Identify and arrange the security training of operators, users, and other stakeholders necessary to the system utilization and support.

TR-1.5 Identify the security aspects for enabling systems or services needed to support transition.

TR-1.6 Identify and plan for enabling systems or services needed to support the security aspects of transition.

TR-1.7 Obtain or acquire access to the security aspects of enabling systems or services to be used in transition.

TR-1.8 Identify security aspects, and arrange for the secure shipping and receiving of system elements and enabling systems.

References: [4] [30] [61] [98] [99]

TR-2 PERFORM TRANSITION

TR-2.1 Prepare the site of operation in accordance with secure installation requirements.

TR-2.2 Securely deliver the system for installation at the correct location and time.

Note: Secure delivery considers the various forms, means, and methods that accomplish the end-to-end transport of system elements to ensure that they are not tampered with during transport. Items and packages are delivered only to the intended recipient, which may mean shipping with more lead time to account for additional security.

TR-2.3 Install the system in its operational environment in accordance with the secure installation strategy, and establish secure interconnections to its environment.

TR-2.4 Demonstrate trustworthy secure system installation.

Note: The installation and connection procedures are to be properly verified to provide confidence that the intended system configuration across all system modes and states is

achieved. This includes completing acceptance tests defined in agreements. These tests include security aspects associated with physical connections between the system and the environment.

TR-2.5 Provide security training for the operators, users, and other stakeholders necessary for system utilization and support.

TR-2.6 Perform security activation and checkout of the system.

Note: Security activation and checkout shows that the system can initialize to its initial secure operational state for all defined modes of operation and accounts for all interconnections to other systems across physical, virtual, and wireless interfaces.

TR-2.7 Demonstrate that the installed system can deliver its required functions in a trustworthy secure manner.

TR-2.8 Demonstrate that the security functions provided by the system and the effects of the security functions are sustainable by enabling systems.

TR-2.9 Review the security trustworthiness of the system for operational readiness.

Note: The results of installation, operational, and enabling system checkouts are reviewed to determine whether the security performance and effectiveness are sufficient to justify operational use.

TR-2.10 Commission the system for secure operation.

Note: This includes providing security support to users and operators at the time of the system commissioning.

References: [4] [86]

TR-3 MANAGE RESULTS OF TRANSITION

TR-3.1 Record the security aspects of transition results and any anomalies encountered.

TR-3.2 Record the security aspects of operational incidents and problems, and track their resolution.

TR-3.3 Maintain traceability of the security aspects of transitioned system elements.

Note: Bidirectional traceability is maintained between all identified security aspects and the supporting data associated with the transition strategy and the system requirements, system architecture, and system design.

TR-3.4 Provide the security-relevant artifacts that have been selected for baselines.

References: [4]

H.11. Validation

The purpose of the *Validation* process is to provide objective evidence that the system, when in use, fulfills its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment.

H.11.1. Security Purpose

Provide objective evidence that the system, when in use, fulfills the protection needs associated with its business or mission objectives and the stakeholder requirements, thereby achieving its intended use in its intended operational environment in a trustworthy secure manner.

H.11.2. Security Outcomes

- Security validation criteria are defined.
- The availability of security services required by stakeholders is confirmed.
- Security-relevant validation constraints that influence system requirements, architecture, or design are identified.
- Security aspects of the system, system element, or artifact are validated.
- Enabling systems or services for the security aspects of validation are available.
- Security-focused validation results and anomalies are identified.
- Objective evidence of the successful validation of security aspects is provided.
- Traceability of the validated security aspects of the system, system elements, and artifacts is established.

H.11.3. Security Activities and Tasks

VA-1 PREPARE FOR VALIDATION

VA-1.1 Identify the security aspects within the validation scope and corresponding security validation actions.

Note: The security aspects of validation focus on the stakeholders' protection needs, concerns, and associated security requirements. The scope includes system elements, the entire system, or any artifact that impacts the stakeholder's confidence in the system and the decision to accept the system as being trustworthy for its intended use.

VA-1.2 Identify the constraints that can potentially limit the feasibility of the security validation actions.

Note: Constraints may include the level of assurance and the availability of business or mission stakeholders to support validation activities; the availability of sufficient, relevant, and credible threat data; the limits on conducting validation activities in actual operational conditions across all business and mission modes and associated system states and modes; the technology employed; the size and complexity of the system element or artifact; and the cost and time allotted for validation activities.

VA-1.3 Select appropriate security validation methods and the associated success criteria for each security validation action.

Note: Adversity emulation, including penetration testing and emulating abuse and misuse, is included.

VA-1.4 Develop the security aspects of the validation strategy.

Note: The security aspects of the validation strategy address the approach to incorporate security considerations into all validation actions, while considering the trade-offs between scope, depth, and rigor needed for the desired level of assurance and the given constraints.

VA-1.5 Identify the security-relevant system constraints that result from the security aspects of the validation strategy to be incorporated in the stakeholder protection needs and the requirements transformed from those needs.

Note: These constraints are associated with the clarity and accuracy of the expression of needs and requirements to achieve the desired level of assurance with certainty and repeatability.

VA-1.6 Identify the security aspects for enabling systems or services needed to support validation.

VA-1.7 Identify and plan for enabling systems or services to support the security aspects of validation.

VA-1.8 Obtain or acquire access to the security aspects of enabling systems or services to be used to support validation.

References: [4] [30] [61] [86] [97] [98] [99] [100] [118]

VA-2 PERFORM VALIDATION

VA-2.1 Define the security aspects of the validation procedures, each supporting one or a set of validation actions.

Note: This includes identification of the validation methods or techniques to be employed, the qualifications of the individuals conducting the validation, and any specialized equipment that may be needed, such as what may be required to emulate environmental adversities.

VA-2.2 Perform security validation procedures.

Note 1: Security-focused validation actions from the execution of validation procedures contribute to demonstrating that the system is sufficiently trustworthy.

Note 2: The performance of a security-focused validation action consists of capturing a result from the execution of the procedure, comparing the obtained result with the expected result, deducing the degree of compliance of the element, and deciding about the acceptability of compliance if uncertainty remains.

References: [4] [86] [97] [100] [118]

VA-3 MANAGE RESULTS OF VALIDATION

VA-3.1 Record the security aspects of validation results and any anomalies encountered.

Note: The recorded validation results include nonconformance issues, anomalies, or problems that are potentially security related. These results inform the analyses to determine causes and enable corrective or improvement actions. Corrective actions may affect the security aspects of the system architecture definition, design definition, system security requirements and associated constraints, the level of assurance that can be obtained, and/or the implementation strategy, including its security aspects.

VA-3.2 Record the security characteristics of operational incidents and problems, and track their resolution.

Note: Incidents that occur in the operational environment of the system are recorded and subsequently correlated to validation activities and results. This is an important feedback loop for continuous improvement in the engineering of trustworthy secure systems.

VA-3.3 Obtain agreement that the security validation criteria have been met.

VA-3.4 Maintain traceability of the security aspects of validation.

Note: Bidirectional traceability of the security aspects of validated system elements to stakeholder protection needs, security concerns, and security requirements is maintained. Traceability demonstrates completeness of the validation process and provides evidence that supports assurance and trustworthiness claims.

VA-3.5 Provide the security-relevant artifacts that have been selected for baselines.

References: [4] [30] [61] [98] [99] [100]

H.12. Operation

The purpose of the *Operation* process is to use the system to deliver its services.

H.12.1. Security Purpose

- Inform the security aspects of the requirements and constraints to securely operate the system and monitor the security aspects of products, services, and operator-system performance.
- Identify and analyze security-relevant operational anomalies.

H.12.2. Security Outcomes

- Security aspects of operation constraints that influence system requirements, architecture, or design are identified.
- Enabling systems, services, and material for the security aspects of operation are available.
- Trained and qualified personnel who can securely operate the system are available.
- System products or services that meet stakeholder security requirements are delivered.
- Security aspects of system performance during operation are monitored.
- Security support is provided to stakeholders.

H.12.3. Security Activities and Tasks

OP-1 PREPARE FOR OPERATION

OP-1.1 Define the security aspects of the operation strategy.

Note 1: This includes the approach to enable the continuous secure operation and use of the system and its security services, as well as the provision of support to operations elements to address anomalies identified during the operation and use of the system. It also includes:

- The capacity, availability, schedule considerations, and security of products or services as they are introduced, routinely operated, and disposed (including contingency operations)
- The human resources strategy and security qualification requirements for personnel, including all associated security-relevant training and personnel compliance requirements
- The security aspects of release and re-acceptance criteria and schedules of the system to permit modifications that sustain the security aspects of existing or enhanced products or services
- The approach to implement operational modes in the System Operational Concept, including normal and contingency operations
- The secure approaches for contingency, degraded, alternative, training, and other modes of operation, as well as the transition within and between modes while considering resilience in the face of adversity
- Measures for operation that will provide security insights into performance levels
- The approach to achieving situational awareness to determine security-relevant consequences

Note 2: This includes planning for securely starting the system, halting the system, shutting the system down, operating the system in a training mode, the secure implementation of work-around procedures to restore operations, performing back-out and restore operations, operating in any degraded mode, or alternative modes for special conditions. If needed, the operator performs the necessary steps to enter into contingency operations and possibly power down the system. Contingency operations are performed in accordance with the pre-established procedures for such an event.

Note 3: There may be a need to plan for certain modes of operation for which security functions and services are reduced or eliminated to achieve more critical system functions and services or to carry out certain maintenance or periodic testing. Predetermined procedures for entering and exiting such modes would be followed.

OP-1.2 Identify the constraints and objectives that result from the security aspects of operation to be incorporated into the system requirements, architecture, and design.

OP-1.3 Identify the security aspects for enabling systems and services needed to support operation.

OP-1.4 Identify and plan for enabling systems or services needed to support the security aspects of operation.

OP-1.5 Obtain or acquire access to the security aspects of enabling systems or services to be used in operation.

OP-1.6 Identify or define security training and qualification requirements to sustain the workforce needed for secure system operation.

Note: Security qualification and training includes role and function-oriented competency, proficiency, certification, and other criteria to securely operate and use the system in all of its defined modes or states.

OP-1.7 Assign the trained and qualified personnel needed for secure system operation.

References: [4] [86] [100] [111] [112] [113] [114]

OP-2 PERFORM OPERATION

OP-2.1 Securely use the system in its intended operational environment.

OP-2.2 Apply materials and other resources as required to securely operate the system and sustain its product and service capabilities.

Note 1: Materials and resources are provided by logistical actions. Logistics is discussed as part of the maintenance process.

Note 2: Operational personnel may perform system modification and support activities, such as software updates.

OP-2.3 Monitor system operations for deviations from intended behavior and outcomes.

Note: This includes (1) managing adherence to the operation strategy and operational procedures (the operations conducted by personnel), (2) monitoring that the system is operated in a secure manner and compliant with regulations, procedures, and directives, and (3) monitoring for anomalies that may not be directly observable as system behavior and may or may not be obviously security relevant.

OP-2.4 Use the measures defined in the strategy and analyze them to confirm that system security performance is within acceptable parameters.

Note: System monitoring includes reviewing whether the performance is within established security-relevant thresholds (loss margins), periodic instrument readings are acceptable, and service and response times are acceptable. Operator feedback and suggestions are useful input for improving the security aspects of system operational performance.

OP-2.5 Identify and record when system security or service performance is not within acceptable parameters.

References: [4] [30] [61] [86] [98] [99] [100]

OP-3 MANAGE RESULTS OF OPERATION

OP-3.1 Record the results of secure operations and any anomalies encountered.

Note: Anomalies include those associated with the operation strategy, the operation of enabling systems, the execution of the operation, and incorrect system definition, all of which may be due to security issues or may result in security issues.

OP-3.2 Record the security aspects of operational incidents and problems, and track their resolution.

OP-3.3 Maintain traceability of the security aspects of the operation elements.

OP-3.4 Provide the security-relevant artifacts that have been selected for baselines.

References: [4] [30] [61] [98] [99] [100]

OP-4 SUPPORT STAKEHOLDERS

OP-4.1 Provide security assistance and consultation to stakeholders as requested.

Note: Assistance and consultation includes the provision or recommendation of sources for security-relevant training, security aspects of documentation, vulnerability resolution, security reporting, and other security-relevant support services that enable the effective and secure use of the product or service.

OP-4.2 Record and monitor requests and subsequent actions for security support.

OP-4.3 Determine the degree to which the security aspects of delivered products and services satisfy the needs of stakeholders.

References: [4] [86] [100]

H.13. Maintenance

The purpose of the *Maintenance* process is to sustain the capability of the system to provide a product or service.

H.13.1. Security Purpose

- Establish the security aspects of requirements and constraints to securely sustain the capability of the system to provide a product or service.

  Note: Secure sustainment includes all maintenance and logistics activities for the packaging, handling, storage, and transportation of replacement system elements.

H.13.2. Security Outcomes

- Security aspects of maintenance and logistics constraints that influence system requirements, architecture, or design are identified.
- Enabling systems or services needed for the security aspects of system maintenance and logistics are available.
- Replacement, repaired, or modified system elements are securely made available.
- The need for required security-relevant maintenance and logistics actions is reported.
- Security-relevant failures and life cycle data, including associated costs, are determined.

H.13.3. Security Activities and Tasks

MA-1 PREPARE FOR MAINTENANCE AND LOGISTICS

MA-1.1 Define the security aspects of the maintenance strategy.

Note: The maintenance strategy seeks to preserve the secure capability and performance of the delivered system. The security aspects of the maintenance strategy generally include:

- The secure transition of the system and system elements into a secure maintenance mode or state, as well as the secure transition back to operation

- An approach to ensure that sourced materials and system elements that do not meet specified quality, origin, and functionality (e.g., counterfeit) are not introduced into the system
- The skill and personnel levels required to effect repairs, replacements, and restoration while accounting for maintenance staff requirements and any relevant legislation regarding health, safety, security, and the environment
- Maintenance measures that provide insight into the security aspects of performance levels, effectiveness, and efficiency

MA-1.2 Define the security aspects of the logistics strategy.

Note: The logistics strategy defines the specific security considerations required to perform logistics throughout the life cycle. This generally includes:

- Acquisition logistics to help ensure that security implications are considered early during the development stage
- Operations logistics to help ensure that the necessary material and resources are securely made available in the right quantity and quality and at the right place and time; considerations for securely making material and resources available include identification and marking, packaging, distribution, handling, and provisioning
- The security criteria for storage locations and conditions, as well as the number and type of replacement system security-specific elements, their anticipated replacement rate, and their storage life and renewal frequency

MA-1.3 Identify the security-relevant constraints and objectives that result from the security aspects of maintenance and logistics to be incorporated into the system requirements, architecture, and design.

MA-1.4 Identify trade-offs such that the security aspects of the system and associated maintenance and logistics actions result in a solution that is trustworthy, secure, affordable, operable, supportable, and sustainable.

Note: The cost of secure maintenance and logistics should be considered within the lifetime cost of the system.

MA-1.5 Identify the security aspects for enabling systems, products, and services needed to support maintenance and logistics.

MA-1.6 Identify and plan for enabling systems, products, and services needed to support the security aspects of maintenance and logistics.

MA-1.7 Obtain or acquire access to the security aspects of enabling systems, products, and services to be used in maintenance and logistics.

References: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113] [114] [115]

MA-2 PERFORM MAINTENANCE

Note: The need to perform maintenance may be driven by the need to address explicit security issues, incidents, or failures. All maintenance actions must be accomplished in a secure manner with the understanding that some actions may have a direct effect on the security posture of the system.

MA-2.1 Monitor and review stakeholder requirements and incident and problem reports to identify security-relevant corrective, preventive, adaptive, additive, or perfective maintenance needs.

Note: Security-relevant maintenance needs include those needs that are direct (e.g., an identified security incident) or indirect (e.g., considerations to securely address a maintenance need).

MA-2.2 Record the security aspects of maintenance incidents and problems, and track their secure resolution.

MA-2.3 Analyze the impact of the changes introduced by maintenance actions on the security aspects of the system and system elements.

MA-2.4 Upon encountering faults that cause a system failure, securely restore the system to secure operational status.

Note: Secure restoration means that the maintenance action itself does not worsen the secure state or condition of the system.

MA-2.5 Securely correct anomalies (e.g., defects, errors, and faults), and replace or upgrade system elements.

MA-2.6 Perform preventive maintenance by securely replacing or servicing system elements prior to failure.

MA-2.7 Securely perform adaptive, additive, or perfective maintenance as required.

References: [4] [30] [61] [86] [98] [99] [100] [114] [115]

MA-3 PERFORM LOGISTICS SUPPORT

MA-3.1 Perform the security aspects of acquisition logistics.

MA-3.2 Perform the security aspects of operational logistics.

MA-3.3 Implement mechanisms for the secure logistics needed during the life cycle.

Note 1: These mechanisms enable secure packaging, handling, storage, and transportation.

Note 2: These mechanisms aid in the prevention and detection of counterfeits, tampering, substitution, and redirection.

MA-3.4 Confirm that the security aspects of logistics actions are implemented.

Note: The security aspects of logistics actions satisfy both logistics protection concerns and the need to meet repair rates, replenishment levels, and planned schedules.

References: [4] [30] [61] [98] [99] [100] [111] [112] [113] [114] [115]

MA-4 MANAGE RESULTS OF MAINTENANCE AND LOGISTICS

MA-4.1 Record the security aspects of maintenance and logistics results and any anomalies encountered.

MA-4.2 Record maintenance and logistics security incidents and problems, and track their secure resolution.

MA-4.3 Identify and record the security-relevant trends of incidents, problems, and maintenance and logistics actions.

MA-4.4 Maintain traceability of the security aspects of maintenance and logistics.

MA-4.5 Provide security-relevant artifacts that have been selected for baselines.

MA-4.6 Monitor customer satisfaction with the security aspects of the system, maintenance, and logistics.

References: [4] [30] [61] [98] [99] [100] [114] [115] [116]

H.14. Disposal

The purpose of the *Disposal* process is to end the existence of a system element or system for a specified intended use, appropriately handle replaced or retired elements and any waste products, and properly attend to identified critical disposal needs (e.g., per an agreement, per organizational policy, or for environmental, legal, safety, or security aspects).

H.14.1. Security Purpose

- Provide the aspects needed to securely end the existence of a system element or system for a specified use, and securely preserve or destroy the associated data and information.

H.14.2. Security Outcomes

- Secure disposal constraints that influence system requirements, architecture, design, and implementation are identified.
- Enabling systems or services for the security aspects of disposal are available.
- System elements are destroyed, stored, reclaimed, or recycled in accordance with safety and security requirements.
- The environment is securely returned to its original secure or an agreed-upon secure state.
- Records of the security aspects of disposal actions and analysis are available.

H.14.3. Security Activities and Tasks

DS-1 PREPARE FOR DISPOSAL

DS-1.1 Define the security aspects of the disposal strategy.

Note: The security aspects address securely terminating system functions and services, transforming the system and environment into an acceptable secure state, addressing security concerns, and transitioning the system and system elements for future use. The disposal strategy determines approaches, schedules, resources, specific considerations of secure disposal, and the effectiveness and completeness of secure disposal and disposition actions.

- *Permanent termination of system functions and delivery of services:* The security aspects address the removal, decommissioning, or destruction of the associated system elements while preserving the security posture of any remaining functions and services.
- *Transform the system and environment into an acceptable state:* The security aspects address any alterations made to the system, its operation, and the environment to ensure that stakeholder protection needs and concerns are addressed by the remaining portions of the system and the functions and services it provides. When the entire system is removed, the security aspects address alterations to the environment to return it to its original or agreed-upon secure state.
- *Address security concerns for material, data, and information:* The security aspects address protections for sensitive components, technology, data, and information removed from service, dismantled, stored, prepared for reuse, or destroyed. The aspects may include the duration of protection level/state, downgrades, releasability, and criteria that define authorized access and use during the storage period. The protection needs for disposal are defined by stakeholders and agreements and may be subject to regulatory requirements, expectations, and constraints.
- *Transition the system and system elements for future use:* The security aspects address the transition of the system or system elements for future use in a modified or adapted form, including legacy migration and return to service. The security aspects may include constraints, limitations, or other criteria to enable recovery of the systems' functions and services within a specified time or to ensure security-oriented interoperability with future enabling systems and other systems. These aspects may also include periodic inspections to account for the security posture and return-to-service readiness of stored system elements, associated data and information, and all supporting operations and sustainment support materials. The security aspects apply to all system functions and services and are not limited to only security protection-oriented functions and services of the system.

DS-1.2 Identify the security-relevant constraints and objectives of disposal on the system requirements, architecture and design characteristics, and implementation techniques.

DS-1.3 Identify the security aspects for enabling systems or services needed to support disposal.

DS-1.4 Identify and plan for enabling systems or services needed to support the security aspects of disposal.

DS-1.5 Obtain or acquire access to the security aspects of enabling systems or services to be used in disposal.

DS-1.6 Specify security criteria for containment facilities, storage locations, inspection, and storage periods (if the system is to be stored).

DS-1.7 Define the security aspects of preventive methods to preclude disposed elements and materials that should not be repurposed, reclaimed, or reused from re-entering the supply chain.

References: [4] [86] [100]

DS-2 PERFORM DISPOSAL

DS-2.1 Securely deactivate the system or system element to prepare it for secure removal from operation.

Note: Deactivation is accomplished to preserve the security posture of the system.

DS-2.2 Securely remove the system, system element, or waste material from use or production for appropriate secure disposition and action.

DS-2.3 Securely withdraw impacted operating staff from the system or system element, and record relevant secure operation knowledge.

DS-2.4 Securely disassemble the system or system element into manageable elements to facilitate its secure removal for reuse, recycling, reconditioning, overhaul, archiving, or destruction.

Note: Secure disassembly preserves the security characteristics of the system elements that are not removed.

DS-2.5 Securely handle system elements and their parts that are not intended for reuse in a manner that will help ensure that they do not get back into the supply chain.

DS-2.6 Conduct secure sanitization and destruction of the system elements and life cycle artifacts.

Note 1: Governing agreements, laws, and regulations determine the appropriate means to sanitize and destroy data, information, and system elements that contain data and information, as well as retention periods before sanitization and destruction can occur.

Note 2: Sanitization and destruction techniques include clearing, purging, cryptographic erase, physical modification, and physical destruction.

Note 3: Sanitization and destruction techniques and methods may be specific to data, information, and system element type.

References: [4] [86] [100]

DS-3 FINALIZE THE DISPOSAL

DS-3.1 Confirm that no detrimental security factors exist following disposal.

DS-3.2 Return the environment to its original secure state or to a secure state specified by agreement.

DS-3.3 Securely archive data and information gathered through the lifetime of the system to permit audits and reviews in the event of long-term hazards to health, safety, security, and the environment and to permit future system creators and users to securely build a knowledge base from past experiences.

DS-3.4 Provide security-relevant artifacts that have been selected for baselines.

References: [4] [100]

Appendix I. Technical Management Processes

This appendix contains the *Technical Management Processes* from [4] with security-relevant considerations and contributions for the purpose, outcomes, activities, and tasks.

I.1. Project Planning

The purpose of the *Project Planning* process is to produce and coordinate effective and workable plans.

I.1.1. Security Purpose

- Determine and coordinate the security aspects of effective and workable plans.

I.1.2. Security Outcomes

- Security objectives, security-specific plans, and security aspects of other plans are defined.
- Security-relevant roles, responsibilities, accountabilities, and authorities within the project are defined.
- Security aspects of performance and achievement criteria are defined.
- The resources and services necessary to achieve the security objectives are committed.
- Plans for the execution of the security aspects of the project are activated.

I.1.3. Security Activities and Tasks

PL-1 DEFINE THE PROJECT

PL-1.1 Identify the security aspects of project objectives and constraints.

Note: Objectives and constraints include strategic security, assurance, and trustworthiness goals, as well as loss thresholds and regulatory concerns. Each security-relevant objective is identified with a level of detail that permits selecting, tailoring, and implementing the appropriate processes and activities.

PL-1.2 Define the security aspects of the project scope as established in agreements.

Note: This includes the relevant activities required to satisfy the security aspects of decision criteria and complete the project successfully.

PL-1.3 Define and maintain the security views of the project life cycle model that are comprised of stages using the defined life cycle models of the organization.

PL-1.4 Establish appropriate security aspects of the work breakdown structure.

Note: Each security-relevant element of the work breakdown structure is described with a level of detail that is consistent with identified security risks and required visibility.

PL-1.5 Define and maintain the security aspects of processes that will be applied to the project.

Note: Entry criteria, inputs, process sequence constraints, and Measures of Effectiveness and/or Measures of Performance attributes may all have security aspects.

References: [4][30] [61] [86] [96] [98] [99] [100] [111] [112] [113] [123]

PL-2 PLAN PROJECT AND TECHNICAL MANAGEMENT

PL-2.1 Define and maintain the security aspects of a project schedule based on management and technical objectives, and work estimates.

Note: This includes security aspects that impact the definition of the duration, relationship, dependencies, and sequence of activities; achievement milestones; resources employed; reviews (including security subject matter expertise employed); and schedule reserves for security risk management necessary to achieve timely completion of the project.

PL-2.2 Define the security aspects of achievement criteria for the life cycle decision gates, delivery dates, and major dependencies on external inputs and outputs.

Note: This includes the criteria defined by regulatory, certification, evaluation, and other approval authorities.

PL-2.3 Define the security aspects of project performance criteria.

PL-2.4 Define the security-relevant project costs, and plan the budget.

PL-2.5 Define the security-relevant roles, responsibilities, accountabilities, and authorities.

Note: This includes defining the project organization, staff acquisitions, and development of staff security-relevant skills. Authorities include legally responsible roles and individuals, as appropriate. These security-relevant authorities include security design authorization, security test and operation authorization, and the award of certification, accreditation, or authorization.

PL-2.6 Define the security aspects of the infrastructure and services required.

Note: This includes defining the capacity needed for security infrastructure and services, its availability, and its allocation to project tasks. Security infrastructure includes facilities (e.g., Sensitive Compartmented Information Facilities [SCIFs] and isolated networks), specific strength of mechanism mediated access, cross-domain solutions, tools, communication, and information technology assets.

PL-2.7 Plan the security aspects of acquiring materials and enabling system services supplied from outside of the project.

PL-2.8 Generate and communicate a plan for the security aspects of project and technical management and execution, including security reviews that address security considerations.

Note: Security considerations and the planning to address those considerations are captured in a Systems Engineering Management Plan, Software Engineering Management Plans, and similar plans.

References: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

PL-3 ACTIVATE THE PROJECT

PL-3.1 Obtain authorization for the security aspects of the project.

PL-3.2 Submit requests and obtain commitments for the necessary resources to perform the security aspects of the project.

PL-3.3 Implement the security aspects of project plans.

References: [4] [86] [100]

I.2. Project Assessment and Control

The purpose of the *Project Assessment and Control* process is to assess if the plans are aligned and feasible; determine the status of the project, technical, and process performance; and direct execution to help ensure that the performance is within projected budgets according to plans and schedules to satisfy technical objectives.

I.2.1. Security Purpose

- Assess whether the security aspects of plans and security plans are aligned and feasible.
- Determine the state of the project, technical, and process security performance.
- Direct execution to help ensure that the security performance is within projected budgets according to plans and schedules to satisfy security and other technical objectives.

I.2.2. Security Outcomes

- Security aspects of performance measures or assessment results are available.
- Security-relevant roles, responsibilities, accountabilities, authorities, and resources are assessed for adequacy.
- Security aspects of technical progress reviews are performed.
- Deviations in the security aspects of project performance from plans are analyzed.
- Affected stakeholders are informed of the security aspects of the project's status.
- Corrective action is directed when project performance or achievement does not meet security-relevant targets.
- Security aspects of project replanning are initiated, as necessary.
- Security aspects of project action to progress (or not) from one scheduled milestone or event to the next are authorized.

I.2.3. Security Activities and Tasks

PA-1 PLAN FOR PROJECT ASSESSMENT AND CONTROL

PA-1.1 Define the security aspects of the project assessment and control strategy.

Note 1: This includes the planned security assessment methods and time frames, as well as necessary security management and technical reviews.

Note 2: Expectations of regulatory, certification, and authorization entities inform the security aspects of the project assessment and control strategy.

References: [4] [30] [61] [98] [99] [100]

PA-2 ASSESS THE PROJECT

PA-2.1 Assess the alignment of the security aspects of project objectives and plans with the project context.

PA-2.2 Assess the security aspects of the management and technical plans against objectives to determine adequacy and feasibility.

PA-2.3 Assess the security aspects of the project and technical status against appropriate plans to determine actual and projected cost, schedule, and performance variances.

PA-2.4 Assess the adequacy of the security-relevant roles, responsibilities, accountabilities, and authorities.

Note: This includes assessment of the adequacy of personnel competencies to perform project roles and accomplish project tasks.

PA-2.5 Assess the security aspects of resource adequacy and availability.

PA-2.6 Assess progress using measured security achievement and the security aspects of milestone completion.

Note: This includes collecting and evaluating security-relevant data for labor, materials, service costs, and technical performance, as well as other technical data about security objectives. These are compared against security-relevant measures of achievement, including conducting effectiveness assessments to determine the adequacy of the evolving system to fulfill security requirements.

PA-2.7 Conduct required management and technical reviews, audits, and inspections relevant to the security aspects of the project.

Note: The reviews, audits, and inspections are formal or informal and are conducted to determine the security-relevant readiness to proceed to the next stage or milestone, to help ensure that project and technical security objectives are being meet, or to solicit feedback from stakeholders with security concerns.

PA-2.8 Monitor the security aspects of critical processes and new technologies.

Note: This includes identifying and evaluating technology maturity from a security perspective, as well as the feasibility of technology insertion for satisfying security objectives.

PA-2.9 Make recommendations based on security measurement results and other security-relevant project information.

Note: Measurement results are analyzed to identify security-relevant deviations, variations, or undesirable trends from planned values and to make security-relevant recommendations for corrective, preventive, adaptive, additive, or perfective actions.

PA-2.10 Record and provide security status and security findings from the assessment tasks.

PA-2.11 Monitor the security aspects of process execution within the project.

Note: This includes an analysis of process security measures and a review of security-relevant trends with respect to project objectives.

References: [4] [30] [61] [86] [98] [99] [100]

PA-3 CONTROL THE PROJECT

PA-3.1 Initiate the actions needed to address identified security issues.

PA-3.2 Initiate the necessary security aspects of project replanning.

Note: Replanning is initiated when the security aspects of project objectives or constraints have changed or when security-relevant planning assumptions are shown to be invalid.

PA-3.3 Initiate necessary change actions when there is a contractual change to cost, time, or quality due to the security impact of an acquirer or supplier request.

Note: The security impact is not necessarily obvious when the request is not security-driven or security-oriented.

PA-3.4 Recommend that the project proceed toward the next milestone or event, if justified, based on the achievement of security-relevant milestones or event criteria.

References: [4] [86] [100] [111] [112] [113]

I.3. Decision Management

The purpose of the *Decision Management* process is to provide a structured, analytical framework for objectively identifying, characterizing, and evaluating a set of alternatives for a decision at any point in the life cycle and select the most beneficial course of action.

I.3.1. Security Purpose

- Identify, analyze, characterize, and evaluate the security aspects of alternatives for a decision.
- Recommend the most beneficial course of security-informed action.

I.3.2. Security Outcomes

- Security aspects of decisions requiring alternative analysis are identified.
- Security aspects of alternative courses of action are identified and evaluated.
- A preferred security-informed course of action is selected.
- Security aspects of a resolution, the decision rationale, and the assumptions are identified.

I.3.3. Security Activities and Tasks

DM-1 PREPARE FOR DECISIONS

DM-1.1 Define the security aspects of the decision management strategy.

Note: A decision management strategy includes the identification of security-relevant roles, responsibilities, accountabilities, and authorities. It also includes the identification of security-specific decision categories and a prioritization scheme. Security-relevant decisions often arise because of a security effectiveness assessment, a technical trade-off, a security-relevant problem that needs to be solved, a response to a security risk that exceeds the acceptable threshold, or a new opportunity.

DM-1.2 Identify the security aspects of the circumstances and the need for a decision.

DM-1.3 Identify stakeholders with relevant security expertise to support decision-making efforts.

References: [4] [86] [100]

DM-2 ANALYZE THE DECISION INFORMATION

DM-2.1 Select and declare the security aspects of the decision management strategy for each decision.

Note: This includes the security-relevant level of rigor and the data and system analysis needed.

DM-2.2 Determine the desired security outcomes and the measurable security attributes of selection criteria.

Note: The desired value for all quantifiable security criteria and the threshold value(s) beyond which the attribute will be unsatisfactory are determined.

DM-2.3 Identify the security aspects of the trade space and alternatives.

Note: If many alternatives exist, security aspects are to qualitatively screen to reduce alternatives to a manageable number for further detailed system analysis.

DM-2.4 Evaluate each alternative against the security criteria.

References: [4] [86] [100]

DM-3 MAKE AND MANAGE DECISIONS

DM-3.1 Determine the preferred alternative for each security-informed and security-based decision.

DM-3.2 Record the security-informed or security-based resolution, decision rationale, and assumptions.

DM-3.3 Record, track, evaluate, and report the security aspects of security-informed and security-based decisions.

Note: Security aspects of problems or opportunities and the alternative courses of action that will resolve their outcomes – including those with security impacts – are recorded, categorized, and reported.

References: [4] [86] [100]

I.4. Risk Management

The purpose of the *Risk Management* process is to identify, analyze, treat, and monitor the risks continually.

I.4.1. Security Purpose

- Continually identify, analyze, treat, and monitor the risks associated with the uncertainty of achieving security objectives and the effects of security protection efforts on achieving system objectives.

I.4.2. Security Outcomes

- Security-relevant risks are identified.
- Security-relevant risks are analyzed.
- Security-relevant risk treatments are selected.
- Security-relevant risk treatments are implemented.
- Security-relevant risks are evaluated on an ongoing basis to assess changes in status and progress in treatment.
- Security-relevant risks are recorded and maintained in the risk profile.

I.4.3. Security Activities and Tasks

RM-1 PLAN RISK MANAGEMENT

RM-1.1 Define the security aspects of the risk management strategy.

Note 1: The nature of security risk includes intentional and unintentional casual events, considerations of the intended behaviors and outcomes, functions (security and other functions), and the potential effects of security risk realization. Casual events may be combinations of events in the operational environment and events in the system environment.

Note 2: The security aspects scope of the risk management process, risk management approach, risk criteria, measures, parameters, rating scale, and treatment alternatives are defined. This includes security aspects of the risk management process at all levels of the supply chain (e.g., suppliers, subcontractors) and how they are incorporated into the project risk management process.

Note 3: The strategy can include those security-relevant issues (i.e., risks with a likelihood of occurrence of 1) and opportunities (i.e., risks with positive outcomes) within scope and approach. Opportunity aspects include opportunity criteria, measures, parameters, rating scale, and treatment alternatives.

RM-1.2 Define and record the security context of the risk management process.

Note 1: This includes the identification of security-relevant stakeholders and descriptions of their perspectives, risk categories, and technical and managerial objectives, assumptions, and constraints.

Note 2: Security opportunities provide potential benefits for the system or project. Security contexts consider the security impact of not pursuing an opportunity and the security risk of not achieving the effects provided by the opportunity.

References: [4] [30] [61] [86] [98] [99] [100] [124] [125]

RM-2 MANAGE THE RISK PROFILE

RM-2.1 Define and record the security risk thresholds and conditions.

Note: The security risk thresholds define the levels at which the appropriate treatment strategies are considered.

RM-2.2 Establish and maintain the security aspects of the risk profile.

Note: The risk profile records each security risk and opportunity, including a description of the security risk or opportunity, a record of the risk or opportunity parameters, the priority based on the risk or opportunity criteria, and the risk or opportunity's current state, treatment, and contingency strategy. The risk profile is updated when an individual security risk or opportunity state changes.

RM-2.3 Provide the security aspects of the relevant risk profile to stakeholders.

Note: Project planning determines the frequency of communicating the risk profile and its security aspects.

References: [4] [86] [100] [124] [125]

RM-3 ANALYZE RISK

RM-3.1 Identify security risks in the categories described in the risk management context.

Note: Security risks are commonly identified through various security and other analyses (e.g., safety, assurance, producibility, and performance analyses); technology, architecture, integration, and readiness assessments; measurement reports; and trade-off studies. Additionally, security risks are often identified through the analysis of measures associated with system security goals (e.g., security-relevant Measures of Effectiveness or Measures of Performance).

RM-3.2 Measure each identified security risk.

RM-3.3 Evaluate each security risk against its risk thresholds.

RM-3.4 Define and record recommended treatment strategies and measures for each security-relevant risk that exceeds its risk threshold.

References: [4] [30] [61] [86] [98] [99] [100] [124] [125]

RM-4 TREAT RISKS THAT EXCEED THEIR RISK THRESHOLD

RM-4.1 Identify recommended alternatives for security risk treatment.

RM-4.2 Define measures for determining the effectiveness of security risk treatments.

RM-4.3 Implement selected security risk treatments.

Note: The implemented alternative should be the one for which the security-relevant stakeholders determine that the actions taken will make a security-relevant risk acceptable.

RM-4.4 Coordinate management action for selected security risk treatments.

References: [4] [86] [100] [124] [125]

RM-5 MONITOR RISK

RM-5.1 Continually monitor all security-relevant risks and the security risk management context.

Note: Changes with security-relevant risks and their treatments may prompt reevaluation. The initial treatment plans for a security-relevant risk may include preplanned additional actions when risk increases or insufficiently decreases despite treatment.

RM-5.2 Implement and monitor measures to evaluate the effectiveness of security-relevant risk treatments.

RM-5.3 Continually monitor for the emergence of new security-relevant risks and sources of risk throughout the life cycle.

Note: This includes monitoring known changes in adversities.

References: [4] [30] [61] [86] [98] [99] [100] [124] [125]

I.5. Configuration Management

The purpose of the *Configuration Management* process is to manage system and system elements and configurations over the life cycle.

I.5.1. Security Purpose

- Incorporate security considerations to securely manage system and system elements and configurations over the life cycle.

I.5.2. Security Outcomes

- System element configurations are securely managed.
- Security aspects of configuration baselines are established.
- Changes to items under configuration management are securely controlled.
- Security aspects of configuration status information are available.
- Security aspects of required configuration audits are completed.
- Security aspects of system releases are approved.

I.5.3. Security Activities and Tasks

CM-1 PREPARE FOR CONFIGURATION MANAGEMENT

CM-1.1 Define a secure configuration management strategy.

Note: These include:

- Security-relevant roles, responsibilities, accountabilities, and authorities

- Criteria for the secure management of changes to items under configuration management, including dispositions, access, release, and control
- Security considerations, criteria, and constraints for the locations, conditions, and environment of storage
- Criteria or events for commencing secure configuration control and securely maintaining the baselines of evolving configurations
- Security aspects of the audit strategy and the responsibilities for assessing the continual integrity and security of the configuration definition information
- Criteria and constraints for secure change management, planned configuration control boards and security configuration control boards, regulatory and emergency change requests, and procedures for secure change management
- Secure coordination among stakeholders, acquirers, suppliers, supply chain, and other interacting organizations

CM-1.2 Define the secure archive and retrieval approach for configuration items, configuration management artifacts, and data.

Note: This includes rules that govern secure retention, access, and use.

References: [4] [74] [86] [100] [126] [127]

CM-2 PERFORM CONFIGURATION IDENTIFICATION

CM-2.1 Identify the security aspects of system elements and artifacts that need to be under configuration management.

CM-2.2 Identify the security aspects of the configuration data to be managed.

CM-2.3 Establish the security aspects of identifiers for items under configuration management.

CM-2.4 Define the security aspects of baselines throughout the life cycle.

CM-2.5 Obtain applicable stakeholder agreement on the security aspects to establish a baseline.

CM-2.6 Approve and track the security aspects of system or system element releases.

Note 1: The security aspects of a release are security-relevant considerations of authorization of the use of a system or system element for a specific purpose with or without security-relevant restrictions. Examples are releases for tests or operational use.

Note 2: Releases generally include a set of changes made through the Technical Processes. Release approval generally includes acceptance of the verified and validated changes and any impacts to security of the changes.

References: [4] [86] [100] [111] [112] [113]

CM-3 PERFORM CONFIGURATION CHANGE MANAGEMENT

CM-3.1 Identify and record the security aspects of requests for change and requests for variance.

Note 1: This includes requests for deviation, waiver, or concession.

Note 2: Change or variance can be based on reasons other than security or without an obvious relevance to security.

CM-3.2 Determine the security aspects of action to coordinate, evaluate, and disposition requests for change or requests for variance.

Note: The security aspects identified are coordinated and evaluated across all impacted performance and effectiveness evaluation criteria, as well as the criteria of project plans, cost, benefits, risks, quality, and schedule.

CM-3.3 Submit requests for security review and approval.

Note: Control boards may or may not be security focused. For a non-security control board activity, security should be reviewed to verify that a request has no security aspects.

CM-3.4 Track and manage the security aspects of approved changes to the baseline, requests for change, and requests for variance.

References: [4] [86] [100]

CM-4 PERFORM CONFIGURATION STATUS ACCOUNTING

CM-4.1 Develop and maintain security-relevant configuration management status information for system elements, baselines, approved changes, and releases.

Note: The information includes security certification, accreditation, authorization, or approval decisions for a system, system element, baseline, or release.

CM-4.2 Capture, store, and report security-relevant configuration management data.

References: [4] [86] [100]

CM-5 PERFORM CONFIGURATION EVALUATION

CM-5.1 Identify the need for secure configuration and configuration management verification activities and audits.

CM-5.2 Verify that the product or service configuration meets the security-relevant configuration requirements.

Note: This is performed by comparing security requirements, constraints, and waivers (variances) with the results of formal verification activities.

CM-5.3 Monitor the secure incorporation of approved configuration changes.

CM-5.4 Perform configuration and configuration management security verification activities and audits to establish the security aspects of product baselines.

Note: This includes the security aspects of the functional configuration audit (FCA) that are focused on functional and performance capabilities and of the physical configuration audit (PCA) that are focused on system conformance to operational and configuration information items.

CM-5.5 Record the security aspects of the configuration management audit and other configuration evaluation results and disposition action items.

References: [4] [86] [100]