VDA | QMC

Qualitäts Management Center
im Verband der Automobilindustrie

Joint Quality Management in the Supply Chain

Automotive SPICE® for Cybersecurity

Part I: Process Reference and Assessment Model for Cybersecurity Engineering

Part II: Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering

1st edition, February 2021
Online download document

Joint Quality Management in the Supply Chain

Automotive SPICE® for Cybersecurity

Part I: Process Reference and Assessment Model for Cybersecurity Engineering

Part II: Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering

1st edition, February 2021
Verband der Automobilindustrie e. V. (VDA)

Non-Binding VDA Standard Recommendation

The Association of the German Automotive Industry (VDA) recommends its members apply the following standard for the implementation and maintenance of quality management systems.

Exclusion of Liability

VDA volumes are recommendations available for general use. Anyone applying them is responsible for ensuring they are used correctly in each case.

This VDA volume takes into account the state of knowledge and technology prevailing at the time of publication. Implementation of VDA recommendations does not absolve anyone of responsibility for their own actions. Every user is accountable for their own behavior. Liability on the part of the VDA and those involved in preparing VDA recommendations is excluded.

If during the use of VDA recommendations errors or the possibility of misinterpretation are found, it is requested that these be reported to the VDA immediately for correction (if required).

Copyright

Translations

This publication will also be issued in other languages. The current status must be requested from VDA QMC.

Copyright Notice

This document is a supplement to the Automotive SPICE Process Assessment Model 3.1. It has been developed by the Project Group 13 of the Quality Management Center (QMC) in the German Association of the Automotive Industry.

This document reproduces relevant material from:

- **ISO/IEC 33020:2015**
  Information technology – Process assessment – Process measurement framework for assessment of process capability

ISO/IEC 33020:2015 provides the following copyright release statement:

'Users of this International Standard may reproduce subclauses 5.2, 5.3, 5.4 and 5.6 as part of any process assessment model or maturity model so that it can be used for its intended purpose.'

Relevant material from this standard is incorporated under the copyright release notice.

Derivative Works

The detailed descriptions contained in this document may be incorporated as part of any tool or other material to support the performance of process assessments, so that this process assessment model can be used for its intended purpose, provided that any such material is not offered for sale.

All distribution of derivative works shall be made at no cost to the recipient.

Distribution

The enhancement for cybersecurity to the Automotive SPICE® Process Assessment Model and the enhancement to the Automotive SPICE guideline may only be obtained via download from the www.automotivespice.com website. Further distribution of the document by the recipient is prohibited.

Trademark

Automotive SPICE® is a registered trademark of the *Verband der Automobilindustrie e.V.* (VDA).

For further information about Automotive SPICE® visit www.vda-qmc.de.

Table of Contents

List of Figures

List of Tables

Introduction

Scope

The UNECE regulation R155 requires, among others, the vehicle manufacturer identification and management of cybersecurity risks in the supply chain. Automotive SPICE is an appropriate method to identify process-related product risks. To incorporate cybersecurity-related processes into the proven scope of Automotive SPICE, additional processes have been defined in a Process Reference and Assessment Model for Cybersecurity Engineering (Cybersecurity PAM).

Part I of this document supplements the Automotive SPICE PAM 3.1 and the Automotive SPICE Guideline (1st edition), enabling the evaluation of cybersecurity-relevant development processes.

Certain aspects of the ISO/IEC 21434 are not in the scope of this document, as they are not performed in a development project context but are part of the cybersecurity management system. These aspects, such as cybersecurity management, continuous cybersecurity activities, post-development phases and decommissioning are subject to a cybersecurity management system audit.

The performance of the Cybersecurity PAM requires a VDA scope assessment of Automotive SPICE 3.1. The Cybersecurity PAM can be used in a separate assessment or when the assessment scope is a combination of the VDA scope and Cybersecurity PAM.

With regard to this requirement, the repetition of indicators from SYS and SWE process groups is avoided. When assessing the entire process profile using an existing assessment, the processes from SUP process group need not to be re-evaluated. In cases when the assessment takes place in the context of a cyber-security-relevant development, all cybersecurity-specific aspects in the PRM and PAM must be considered.

In cases when a VDA scope assessment was not previously done, then a subsequent full VDA scope assessment – including the Cybersecurity PAM – has to contain ACQ.4 from the Cybersecurity PAM.

The SUP processes in the Automotive SPICE PAM do not address security aspects. However, a PA 2.2 rating of the security processes sufficiently covers security-specific SUP process features.

In cases of a combined assessment using the Automotive SPICE 3.1 PAM and the Cybersecurity PAM, it is recommended assessing two process instances for ACQ.4, that is, one following the Automotive SPICE PAM 3.1 ACQ.4 and the other using the Cybersecurity PAM ACQ.4 indicators.

Part II of this document is aimed at complementing the existing Automotive SPICE Guideline (1st edition). It contains interpretation and rating guidelines for the processes defined in Part I. Chapters 1 and 2 of the Automotive SPICE Guideline (1st edition) also apply to Part II and therefore are not repeated here.

Annex B only contains Work Product Characteristics that are relevant for cybersecurity processes.

Statement of Compliance

The Automotive SPICE process assessment and process reference models conform with ISO/IEC 33004, and can be used as the basis for conducting an assessment of process capability.

ISO/IEC 33020:2015 is used as an ISO/IEC 33003-compliant measurement framework.

A statement of compliance of the process assessment and process reference models with the requirements of ISO/IEC 33004 is provided in Annex A.

Part I Process Reference and Assessment Model for Cybersecurity Engineering

1 Process Capability Assessment

The concept of process capability assessment by using a process assessment model is based on a two-dimensional framework. The first dimension is provided by processes defined in a process reference model (process dimension). The second consists of capability levels that are further subdivided into process attributes (capability dimension). The process attributes provide the measurable characteristics of process capability.

The process assessment model selects processes from a process reference model and supplements it with indicators. These indicators support the collection of objective evidence that enable an assessor to assign ratings for processes according to the capability dimension.

The relationship is shown in Figure 1:

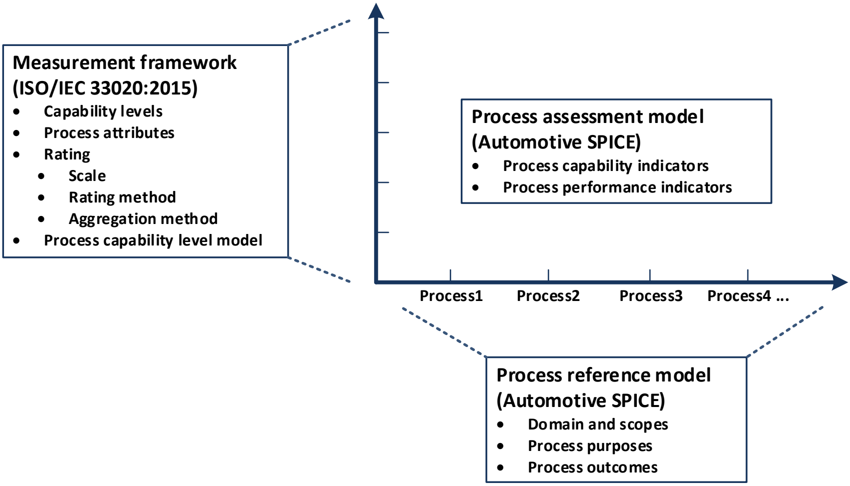

Measurement framework (ISO/IEC 33020:2015)
• Capability levels
• Process attributes
• Rating
• Scale
• Rating method
• Aggregation method
• Process capability level model
Process assessment model (Automotive SPICE)
• Process capability indicators
• Process performance indicators
Process1
Process2
Process3
Process4 ...
Process reference model (Automotive SPICE)
• Domain and scopes
• Process purposes
• Process outcomes

Figure 1 — Process Assessment Model Relationship

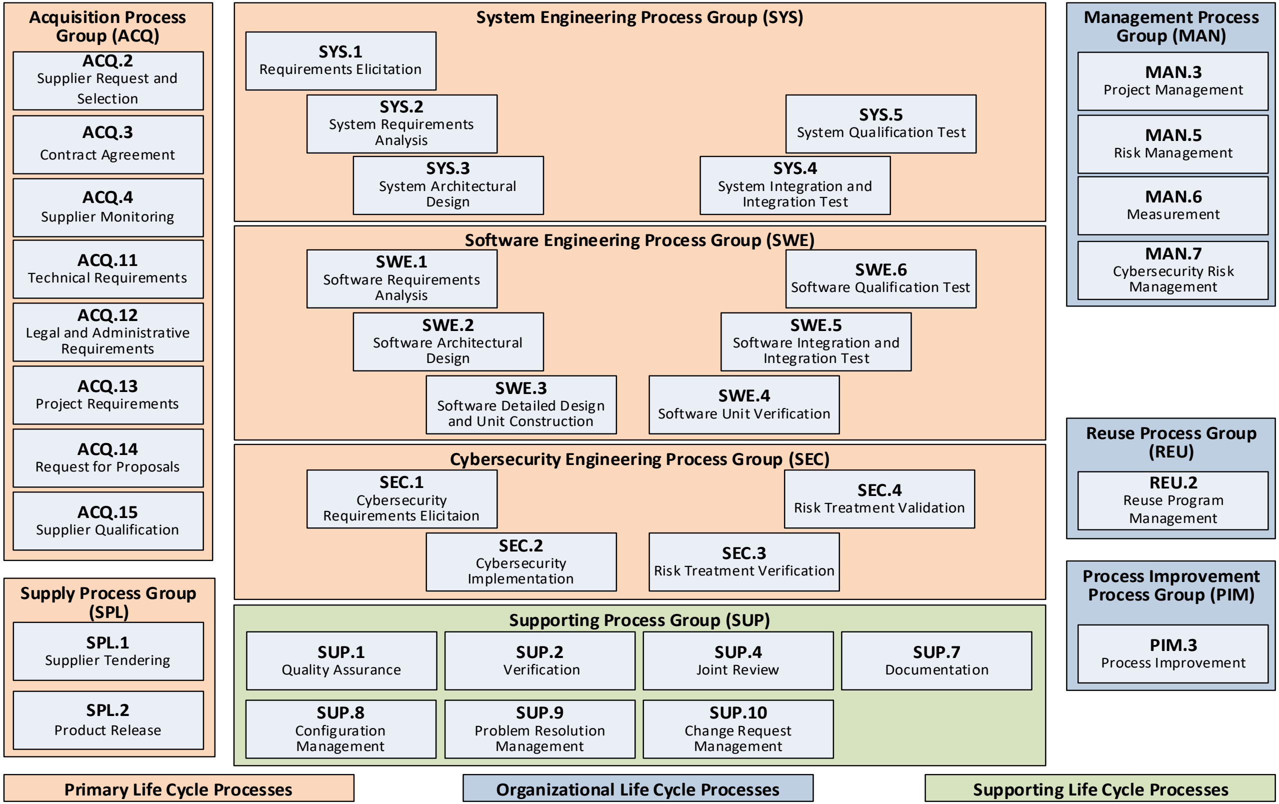
1.1 Process reference model

Processes are grouped by category and at a second level into groups according to the type of activity they address.

There are 3 process categories: primary lifecycle, organizational lifecycle, and supporting lifecycle processes.

Each process is described in terms of a purpose statement. The purpose statement contains the unique functional objectives of the process when performed in a particular environment. For each purpose statement, a list of specific outcomes is associated with a list of expected positive results from the process performance.

For the process dimension, the Automotive SPICE and Automotive SPICE for Cybersecurity process reference models provide the set of processes shown in Figure 2.



Acquisition Process Group (ACQ)
ACQ.2 Supplier Request and Selection
ACQ.3 Contract Agreement
ACQ.4 Supplier Monitoring
ACQ.11 Technical Requirements
ACQ.12 Legal and Administrative Requirements
ACQ.13 Project Requirements
ACQ.14 Request for Proposals
ACQ.15 Supplier Qualification
Supply Process Group (SPL)
SPL.1 Supplier Tendering
SPL.2 Product Release
System Engineering Process Group (SYS)
SYS.1 Requirements Elicitation
SYS.2 System Requirements Analysis
SYS.3 System Architectural Design
SYS.4 System Integration and Integration Test
SYS.5 System Qualification Test
Software Engineering Process Group (SWE)
SWE.1 Software Requirements Analysis
SWE.2 Software Architectural Design
SWE.3 Software Detailed Design and Unit Construction
SWE.4 Software Unit Verification
SWE.5 Software Integration and Integration Test
SWE.6 Software Qualification Test
Cybersecurity Engineering Process Group (SEC)
SEC.1 Cybersecurity Requirements Elicitaion
SEC.2 Cybersecurity Implementation
SEC.3 Risk Treatment Verification
SEC.4 Risk Treatment Validation
Supporting Process Group (SUP)
SUP.1 Quality Assurance
SUP.2 Verification
SUP.4 Joint Review
SUP.7 Documentation
SUP.8 Configuration Management
SUP.9 Problem Resolution Management
SUP.10 Change Request Management
Management Process Group (MAN)
MAN.3 Project Management
MAN.5 Risk Management
MAN.6 Measurement
MAN.7 Cybersecurity Risk Management
Reuse Process Group (REU)
REU.2 Reuse Program Management
Process Improvement Process Group (PIM)
PIM.3 Process Improvement
Primary Life Cycle Processes
Organizational Life Cycle Processes
Supporting Life Cycle Processes

Figure 2: Automotive SPICE and Automotive SPICE for Cybersecurity Process Reference model – Overview

1.1.1 Primary Lifecycle Processes category

The Primary Lifecycle Processes category consists of processes that may be used by the customer when acquiring products from a supplier, and by the supplier when responding and delivering products to the customer, including the engineering processes needed for specification, design, development, integration and testing.

The Primary Lifecycle Processes category consists of the following groups:

- the Acquisition Process Group
- the Supply Process Group
- the Security Engineering Process Group
- the System Engineering Process Group
- the Software Engineering Process Group

The Acquisition Process Group (ACQ) consists of processes that are performed by the customer, or the supplier when acting as a customer for its own suppliers, in order to acquire a product and/or service.

ACQ.2	Supplier Request and Selection
ACQ.3	Contract Agreement
ACQ.4	Supplier Monitoring
ACQ.11	Technical Requirements
ACQ.12	Legal and Administrative Requirements
ACQ.13	Project Requirements
ACQ.14	Request for Proposals
ACQ.15	Supplier Qualification

Table 1 — Primary Lifecycle Processes – ACQ

The Supply Process Group (SPL) consists of processes performed by the supplier in order to supply a product and/or a service.

SPL.1	Supplier Tendering
SPL.2	Product Release

Table 2 — Primary Lifecycle Processes – SPL

The Security Engineering Process Group (SEC) consists of processes performed in order to achieve cybersecurity goals.

SEC.1	Cybersecurity Requirements Elicitation
SEC.2	Cybersecurity Implementation
SEC.3	Risk Treatment Verification
SEC.4	Risk Treatment Validation

Table 3 — Primary Lifecycle Processes – SEC

The System Engineering Process Group (SYS) consists of processes addressing the elicitation and management of customer and internal requirements, definition of the system architecture and the integration and testing at the system level.

SYS.1	Requirements Elicitation
SYS.2	System Requirements Analysis
SYS.3	System Architectural Design
SYS.4	System Integration and Integration Test
SYS.5	System Qualification Test

Table 4 — Primary Lifecycle Processes – SYS

The Software Engineering Process Group (SWE) consists of processes addressing the management of software requirements derived from the system requirements, development of the corresponding software architecture, and design as well as the implementation, integration and testing of the software.

SWE.1	Software Requirements Analysis
SWE.2	Software Architectural Design
SWE.3	Software Detailed Design and Unit Construction
SWE.4	Software Unit Verification
SWE.5	Software Integration and Integration Test
SWE.6	Software Qualification Test

Table 5 — Primary Lifecycle Processes – SWE

1.1.2 Supporting Lifecycle Processes category

The Supporting Lifecycle Processes (SUP) category consists of processes that may be employed by any of the other processes at various points in the lifecycle.

SUP.1	Quality Assurance
SUP.2	Verification
SUP.4	Joint Review
SUP.7	Documentation
SUP.8	Configuration Management
SUP.9	Problem Resolution Management
SUP.10	Change Request Management

Table 6 — Supporting Lifecycle Processes – SUP

1.1.3 Organizational Lifecycle Processes category

The Organizational Lifecycle Processes category consists of processes that develop process, product and resource assets which, when used by projects in the organization, will help the organization achieve its business goals.

The organizational lifecycle processes category consists of the following groups:

- the Management Process Group
- the Process Improvement Process Group
- the Reuse Process Group

The Management Process Group (MAN) consists of processes that may be used by anyone who manages any type of project or process within the lifecycle.

MAN.3	Project Management
MAN.5	Risk Management
MAN.6	Measurement
MAN.7	Cybersecurity Risk Management

Table 7 — Organizational Lifecycle Processes – MAN

The Process Improvement Process Group (PIM) covers one process that contains practices to improve the processes performed in the organizational unit.

PIM.3	Process Improvement

Table 8 — Organizational Lifecycle Processes – PIM

The Reuse Process Group (REU) covers one process to systematically exploit opportunities in an organization’s reuse programs.

REU.2	Reuse Program Management

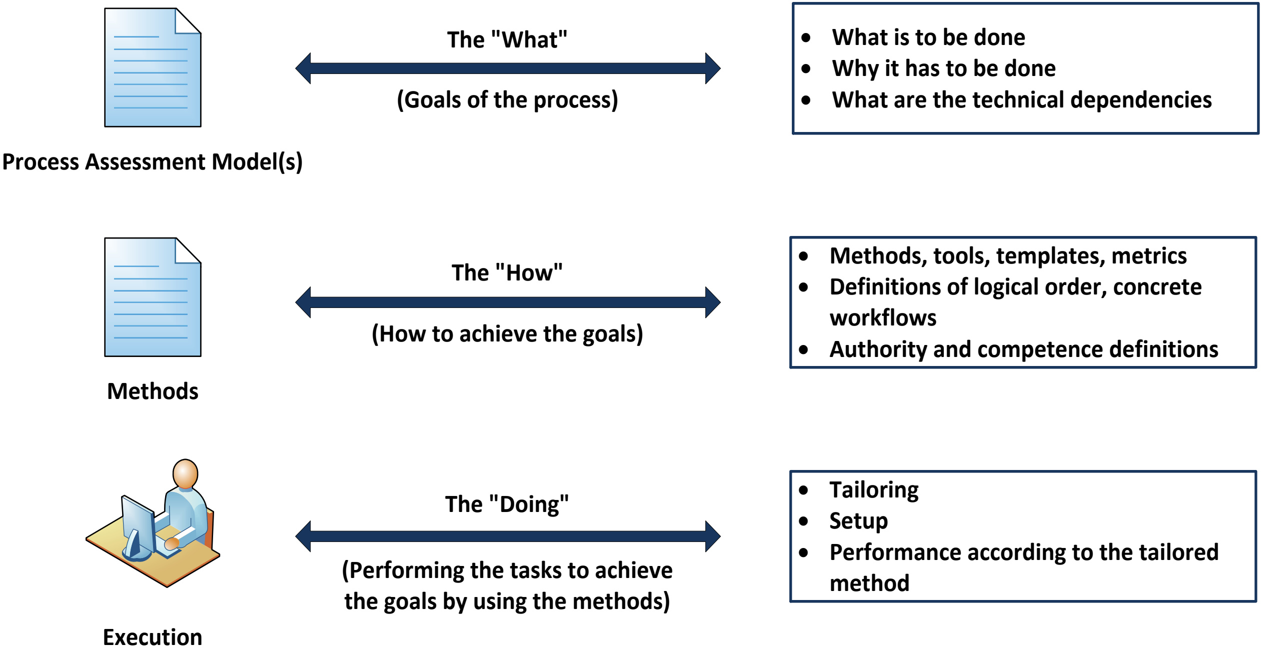
Table 9 — Organizational Lifecycle Processes – REU

1.2 Measurement framework

The process capability levels, process attributes, rating scale and capability level rating model are identical to those defined in ISO/IEC 33020:2015, clause 5.2. The detailed descriptions of the capability levels and corresponding process attributes can be found in PAM 3.1.

1.3 Understanding the level of abstraction of a PAM

The term "process" can be understood at three levels of abstraction. Note that these levels of abstraction are not meant to define a strict black-or-white split or provide a scientific classification schema. The message here is to understand that, in practice, when it comes to the term "process" there are different abstraction levels, and that a PAM resides at the highest.



Process Assessment Model(s)

The "What"

(Goals of the process)

- What is to be done
- Why it has to be done
- What are the technical dependencies

Methods

The "How"

(How to achieve the goals)

- Methods, tools, templates, metrics
- Definitions of logical order, concrete workflows
- Authority and competence definitions

Execution

The "Doing"

(Performing the tasks to achieve the goals by using the methods)

- Tailoring
- Setup
- Performance according to the tailored method

Figure 3 — Possible Levels of Abstraction for the Term "Process"

Capturing experience acquired during product development (i.e., at the DOING level) in order to share this experience with others means creating a HOW level. However, a HOW is always specific to a particular context such as a company, organizational unit or product line. For example, the HOW of a project, organizational unit, or company A is potentially not applicable as is to a project, organizational unit or company B. However, both might be expected to adhere the principles represented by PAM indicators for process outcomes and process attribute achievements. These indicators are at the WHAT level, while deciding on solutions for concrete templates, proceedings, tooling, etc. is left to the HOW level.

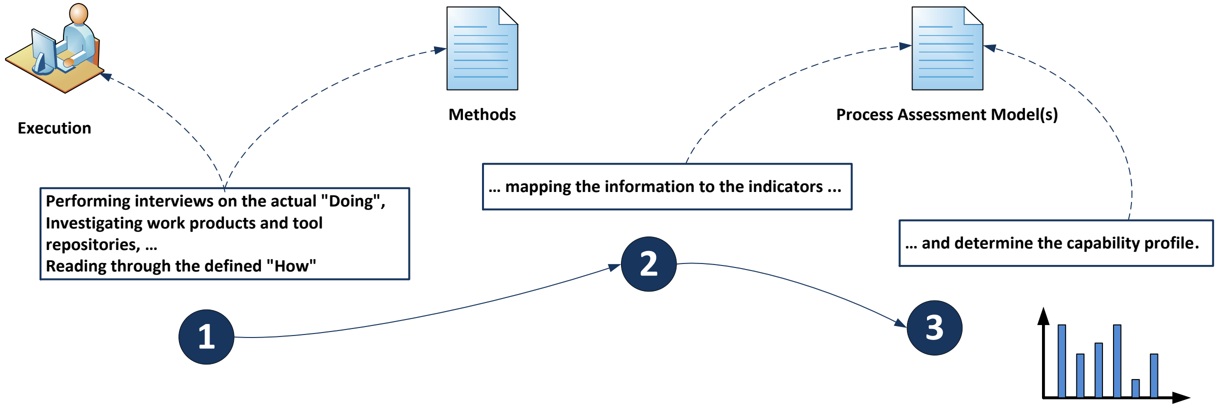

Execution
Methods
Process Assessment Model(s)
Performing interviews on the actual "Doing",
Investigating work products and tool
repositories, ...
Reading through the defined "How"
... mapping the information to the indicators ...
... and determine the capability profile.
1
2
3

Figure 4 — Performing a Process Assessment for Determining Process Capability

2 Process Reference Model and Performance Indicators (Level 1)

2.1 Acquisition Process Group (ACQ)

2.1.1 ACQ.2 Supplier request and selection

Process ID	ACQ.2
Process name	Supplier Request and Selection
Process purpose	The purpose of supplier request and selection process is to award a supplier a contract/agreement based on relevant criteria.
Process outcomes	As a result of successful implementation of this process 1) evaluation criteria are established for suppliers, 2) suppliers are evaluated against the defined criteria, 3) a request for quotation is issued to nominated suppliers, and 4) contract, action, and risk mitigation plans are agreed upon, the supplier is contracted based on the evaluation result.

Base practices	**ACQ.2.BP1: Establish supplier evaluation criteria.** Analyze relevant requirements to define evaluation criteria for supplier's capabilities. [OUTCOME 1] *NOTE 1: Criteria should consider:* • *Commercial and quality requirements* • *Technical evaluation regarding cybersecurity capabilities of the supplier, including cybersecurity concepts and methods (threat analysis and risk assessment, attack models, vulnerability analysis, etc.)* • *The organization's capability of the supplier concerning cybersecurity (e.g., cybersecurity best practices from the development, post-development, governance, quality, and information security)* • *Continuous operation, including cybersecurity* • *Supplier capability and performance evidence in terms of cybersecurity obtained by supplier monitoring in previous projects*

ACQ.2.BP2: Evaluate potential suppliers. Collect information about the supplier’s capabilities and evaluate it against the established evaluation criteria. Short-list the preferred suppliers and document the results. [OUTCOME 2]

NOTE 2: The evaluation of potential suppliers may be supported by:

- *Summaries of previous Automotive SPICE cybersecurity assessments*
- *evidence of the organizational cybersecurity management system (e.g., organizational audit results if available)*
- *evidence of an information security management system*
- *evidence of the organization's quality management system appropriate/capable of supporting cybersecurity engineering*

ACQ.2.BP3: Prepare and execute request for quotation (RFQ). Identify supplier candidates based on the evaluation. Prepare and issue a request for quotation including a corrective action plan for identified deviations. [OUTCOME 3, 4]

NOTE 3: The request for quotation should include:

- *A formal request to comply with all relevant and applicable standards*
- *The expectation of cybersecurity responsibilities taken by the supplier*
- *The scope of work regarding cybersecurity, including the cybersecurity goals or the set of relevant cybersecurity requirements and their attributes, depending on what the supplier is quoting for*
- *Action plan for identified deviations and risks*

ACQ.2.BP4: Negotiate and award the contract/agreement. Establish a contract based on the evaluation of the request for quotation results, covering the relevant requirements and the agreed corrective actions. [OUTCOME 4]

NOTE 4: The contract should consider requirements including cybersecurity and safety requirements, if applicable (e.g., as part of customer requirements).
NOTE 5: An initial interface agreement (e.g., for cybersecurity) may be set up and used for the detailed contract definition.

Output work products	02-00 Contract	[OUTCOME 4]
	02-01 Commitment/agreement	[OUTCOME 4]
	02-50 Interface agreement	[OUTCOME 4]
	08-20 Risk mitigation plan	[OUTCOME 4]
	12-01 Request for quotation	[OUTCOME 3]
	14-02 Corrective action register	[OUTCOME 3, 4]
	14-05 Preferred supplier register	[OUTCOME 2]
	15-21 Supplier evaluation report	[OUTCOME 2]
	18-50 Supplier evaluation criteria	[OUTCOME 1]

	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Base Practices				
ACQ.2.BP1	x			
ACQ.2.BP2		x		
ACQ.2.BP3			x	x
ACQ.2.BP4				x
Output Work Products				
02-00 Contract				x
02-01 Commitment/agreement				x
02-50 Interface agreement				x
08-20 Risk mitigation plan				x
12-01 Request for quotation			x	
14-02 Corrective action register			x	x
14-05 Preferred supplier register		x		
15-21 Supplier evaluation report		x		
18-50 Supplier evaluation criteria	x			

2.1.2 ACQ.4 Supplier Monitoring

Process ID	**ACQ.4**
Process name	**Supplier Monitoring**
Process purpose	The purpose of the Supplier Monitoring Process is to track and assess the performance of the supplier against agreed requirements and agreed corrective actions.
Process outcomes	As a result of successful implementation of this process 1) agreements have been concluded regarding joint processes, interfaces and exchange of information. Joint activities, as agreed between the customer and the supplier, are performed as needed, 2) all information, agreed upon for exchange, is communicated regularly between the supplier and customer, 3) performance of the supplier is monitored against the agreements, deliveries of the supplier are reviewed for acceptance by the customer, and 4) changes and risks to the agreement and risks, if needed, are exchanged and negotiated between the customer and the supplier and documented in the agreement.

Base practices	**ACQ.4.BP1: Agree on and maintain joint processes, joint interfaces, and information to be exchanged.** Establish and maintain an agreement on information to be exchanged and on joint processes and joint interfaces, responsibilities, type and frequency of joint activities, communications, meetings, status reports and reviews. [Outcome 1,4] *NOTE1: Cybersecurity requirements and responsibilities need to be aligned between customer and supplier.* *NOTE 2: Joint processes and interfaces usually include project management, risk management, requirements management, change management, configuration management, problem resolution, quality assurance, and customer acceptance. This includes incident response management and application of a cybersecurity-specific test provided by the customer.*

	NOTE 3: Joint activities to be performed should be mutually agreed upon between the customer and the supplier. *NOTE 4: The term customer in this process refers to the assessed party. The term supplier refers to the supplier of the assessed party.* *NOTE5: Distributed cybersecurity or safety activities should be specified within a cybersecurity or safety interface agreement by the start of these activities considering all relevant aspects (e.g., contacts, tailoring, responsibilities, information share, milestones, timing).* **ACQ.4.BP2: Exchange all agreed information.** Use the agreed joint interfaces between customer and supplier for the exchange of all agreed information. [OUTCOME 1,2] *NOTE 6: Agreed upon information should include all relevant work products as outlined in the interface agreement.* **ACQ.4.BP3: Review technical development with the supplier.** Review development with the supplier on the agreed regular basis, covering technical aspects, problems and risks. Identify and record open items and risks. [OUTCOME 1, 3, 4] *NOTE 7: The chosen methods for implementation of cybersecurity or safety requirements need to be reviewed by the customer.* *NOTE 8: The supplier should indicate any clarification needs with the customer.* **ACQ.4.BP4: Review progress of the supplier**. Review progress of the supplier regarding schedule, quality and cost on the agreed upon regular basis. Identify and record open items and risks. [OUTCOME 1,3,4] **ACQ.4.BP5: Track open items to closure.** Take action when agreed upon objectives are not achieved to correct deviations and prevent reoccurrence of identified problems. Negotiate changes to objectives and document them in the agreements. [OUTCOME 4]

	NOTE 9: Agreed objectives may include: • *Cybersecurity goals* • *Project milestones* • *Safety goals* • *Quality goals* *NOTE 10: While changing objectives and agreements, possible impacts of additional or new vulnerabilities or sufficient maintenance of additional/new vulnerabilities must be taken into account.* *NOTE 11: Review the effectiveness of the applied mitigation and the corrections/solution for the risks or problem.*
Output work products	02-01 Commitment/agreement [OUTCOME 4] 02-50 Interface agreement [OUTCOME 1] 08-20 Risk mitigation plan [OUTCOME 3, 4] 13-01 Acceptance record [OUTCOME 3] 13-04 Communication record [OUTCOME 1, 2] 13-14 Progress status record [OUTCOME 2, 3] 13-16 Change request [OUTCOME 4] 13-19 Review record [OUTCOME 3] 14-02 Corrective action register [OUTCOME 4] 15-01 Analysis report [OUTCOME 3]

	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Base Practices				
ACQ.4.BP1	x			x
ACQ.4.BP2	x	x		
ACQ.4.BP3	x		x	x
ACQ.4.BP4	x		x	x
ACQ.4.BP5				x
Output Work Products				
02-01 Commitment/agreement				x
02-50 Interface agreement	x			
08-20 Risk mitigation plan			x	x
13-01 Acceptance record			x	
13-04 Communication record	x	x		
13-14 Progress status record		x	x	
13-16 Change request				x
13-19 Review record			x	
14-02 Corrective action register				x
15-01 Analysis report			x	

2.2 Security Engineering Process Group (SEC)

2.2.1 SEC.1 Cybersecurity Requirements Elicitation

Process ID	SEC.1
Process name	**Cybersecurity Requirements Elicitation**
Process purpose	The purpose of the Cybersecurity Requirements Elicitation Process is to derive cybersecurity goals and requirements out of the risk treatment decision, which involve risk mitigation and maintaining consistency between the risk assessment, cybersecurity goals and cybersecurity requirements.
Process outcomes	As a result of successful implementation of this process 1) cybersecurity goals are defined, 2) cybersecurity requirements are derived from cybersecurity goals, 3) consistency and bidirectional traceability are maintained, and 4) the cybersecurity requirements are agreed and communicated to all affected parties.
Base practices	**SEC.1.BP1: Derive cybersecurity goals and cybersecurity requirements.** Derive cybersecurity goals for those threat scenarios, where the risk treatment decision requires risk reduction. Specify functional and non-functional cybersecurity requirements for the cybersecurity goals, including a rationale for the achievement of the cybersecurity goals. [OUTCOME 1, 2] *NOTE 1: This includes the refinement of requirements during iterations of this process.* *NOTE 2: This includes requirements for post-development phases.* *NOTE 3: Post-development phases may include production, operation, maintenance and decommissioning.* **SEC.1.BP2: Establish bidirectional traceability.** Establish bidirectional traceability between the cybersecurity requirements and the cybersecurity goals. Maintain bidirectional traceability between the cybersecurity goals and the threat scenarios. [Outcome 3]

	SEC.1.BP3: Ensure consistency. Ensure consistency between the cybersecurity requirements and the cybersecurity goals. Maintain consistency between the cybersecurity goals and the threat scenarios. [OUTCOME 3] **SEC.1.BP4: Communicate cybersecurity requirements**. Communicate cybersecurity goals and cybersecurity requirements to all relevant parties. [OUTCOME 4]
Output work products	17-51 Cybersecurity goals [OUTCOME 1] 15-01 Analysis report [OUTCOME 1, 2] 17-11 Software requirements specification [OUTCOME 1, 2] 17-12 System requirements specification [OUTCOME 1, 2] 13-22 Traceability record [OUTCOME 3] 13-19 Review record [OUTCOME 3] 13-04 Communication record [OUTCOME 4]

	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Base Practices				
SEC.1.BP1	x	x		
SEC.1.BP2			x	
SEC.1.BP3			x	
SEC.1.BP4				x
Output Work Products				
13-04 Communication record				x
13-19 Review record			x	
13-22 Traceability record			x	
15-01 Analysis report	x	x		
17-11 Software requirements specification	x	x		
17-12 System requirements specification	x	x		
17-51 Cybersecurity Goals	x			

2.2.2 SEC.2 Cybersecurity Implementation

Process ID	**SEC.2**
Process name	**Cybersecurity Implementation**
Process purpose	The purpose of the Cybersecurity Implementation Process is to implement the risk treatment actions that involve risk mitigation in order to reduce the residual risk to an acceptable level.
Process outcomes	As a result of successful implementation of this process 1) the architectural design is refined, 2) cybersecurity requirements are allocated to elements of the architectural design, 3) appropriate cybersecurity controls are selected, 4) vulnerabilities are analyzed, 5) the detailed design is refined, 6) software units are developed, 7) consistency and bidirectional traceability are maintained between architectural design and implementation of risk treatment, and 8) the cybersecurity risk treatment implementation is agreed upon and communicated to all affected parties.
Base practices	**SEC.2.BP1: Refine the details of the architectural design.** The architectural design is refined based on cybersecurity goals and cybersecurity requirements. [Outcome 1] *NOTE 1: Refinement could be on system or SW level architecture.* *NOTE 2: Refinement here means to add, adapt or rework elements of the architecture.* **SEC.2.BP2: Allocate cybersecurity requirements.** Allocate the cybersecurity requirements to one or more elements of the architectural design. [Outcome 2] *NOTE 3: Cybersecurity requirements include, e.g., system and software requirements.*

SEC.2.BP3: Select cybersecurity controls. Select appropriate cybersecurity controls to achieve or support the cybersecurity requirements. [OUTCOME 3]

NOTE 4: Cybersecurity controls are technical solutions to avoid, detect, counteract or minimize cybersecurity risks.

SEC.2.BP4: Define interfaces. Identify and describe interfaces between the elements of the architectural design and operating environment. [OUTCOME 1]

SEC.2.BP5: Analyze architectural design. Analyze the software architectural design to identify and evaluate vulnerabilities. [OUTCOME 4]

SEC.2.BP6: Refine the details of the detailed design. The detailed design is refined based on architectural design. [OUTCOME 5]

NOTE 5: Refinement means here, e.g., to add, adapt or rework components of the detailed design.

SEC.2.BP7: Develop software units. Implement the software using appropriate modeling or programming languages. [OUTCOME 6]

NOTE 6: Criteria for appropriate modeling and programming languages for cybersecurity can include the use of language subsets, enforcement of strong typing and/or the use of defensive implementation techniques.

NOTE 7: Example to cover the defined criteria could be the use of a coding guideline or an appropriate development environment.

SEC.2.BP8: Establish **bidirectional traceability**. Establish bidirectional traceability between the refined architectural design and the detailed design. [OUTCOME 2, 7]

SEC.2.BP9: Ensure consistency. Ensure consistency between the refined architectural design and the detailed design. [OUTCOME 7]

	SEC.2.BP10: Communicate results of cybersecurity implementation. Communicate results of the cybersecurity implementation to all relevant parties including stakeholders from post-development phases. [Outcome 8] *NOTE 8: The communicated contents may include both results of the cybersecurity implementation and vulnerabilities identified within the architectural design analysis.*	
Output work products	04-04 Software architectural design	[Outcome 1]
	04-05 Software detailed design	[Outcome 5]
	04-06 System architectural design	[Outcome 1]
	11-05 Software unit	[Outcome 6]
	13-04 Communication record	[Outcome 8]
	13-19 Review record	[Outcome 7]
	13-22 Traceability record	[Outcome 2, 7]
	15-50 Vulnerability analysis report	[Outcome 4]
	17-52 Cybersecurity controls	[Outcome 3]

	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5	Outcome 6	Outcome 7	Outcome 8
Base Practices								
SEC.2.BP1	x							
SEC.2.BP2		x						
SEC.2.BP3			x					
SEC.2.BP4	x							
SEC.2.BP5				x				
SEC.2.BP6					x			
SEC.2.BP7						x		
SEC.2.BP8							x	
SEC.2.BP9							x	
SEC.2.BP10								x
Output Work Products								
04-04 Software architectural design	x							
04-05 Software detailed design					x			
04-06 System architectural design	x							
11-05 Software unit						x		
13-04 Communication record								x
13-19 Review record							x	
13-22 Traceability record		x					x	
15-50 Vulnerability analysis report				x				
17-52 Cybersecurity controls			x					

2.2.3 SEC.3 Risk Treatment Verification

Process ID	**SEC.3**
Process name	**Risk Treatment Verification**
Process purpose	The purpose of the Risk Treatment Verification Process is to confirm that the implementation of the design and components integration comply with the cybersecurity requirements and the refined architectural and detailed design.
Process outcomes	As a result of successful implementation of this process 1) a risk treatment verification and integration strategy are developed, implemented and maintained. 2) A specification for risk treatment verification of the implementation according to the risk treatment verification strategy suitable to provide evidence of compliance in implementing cybersecurity requirements as well as the refined architectural and detailed design is developed. 3) Identified work products are verified according to the risk treatment verification strategy and the defined criteria for risk treatment verification. The implementation of the design and the integration of the components is tested using the defined test cases. Verification and test results are recorded. 4) Bidirectional traceability between the cybersecurity requirements and risk treatment verification specification (including test cases), and bidirectional traceability between the refined architectural (including detailed) design and the risk treatment verification specification (including test cases), and bidirectional traceability between risk treatment verification specification (including test cases) and test results is established. 5) Consistency between the cybersecurity requirements and risk treatment verification specification (including test cases) and consistency between the refined architectural (including detailed) design and the risk treatment verification specification (including test cases) is established. 6) Results of the verification are summarized and communicated to all affected parties.

Base practices	**SEC.3.BP1: Develop a risk treatment verification and integration strategy.** Develop and implement a verification and integration strategy, including a regression strategy. This contains activities with associated methods, techniques and tools; work product or processes under verification; degrees of independence for verification and a schedule for performing these activities and verification criteria. [Outcome 1] *NOTE 1: The verification and integration strategy is implemented by a plan.* *NOTE 2: Verification may provide objective evidence that the outputs of a particular phase of the system and software development lifecycle (e.g., requirements, design, implementation, testing) meet all of the specified requirements for that phase.* *NOTE 3: Verification strategy may include* • *requirements-based test and interface test on system and software level,* • *test for any unspecified functionalities,* • *resource usage evaluation,* • *control flow verification and data flow, and* • *static analysis; for software: static code analysis.* *NOTE 4: Verification methods and techniques may include* • *network tests simulating attacks (non-authorized commands, signals with wrong hash key, flooding the connection with messages, etc.), and* • *simulating brute force attacks.* *NOTE 5: Verification methods and techniques may also include inspections, peer reviews (see also SUP.4), audits, walkthroughs, analysis, code reviews, checks against coding standards and guidelines, and other techniques.* **SEC.3.BP2: Develop specification for risk treatment verification.** Develop the specification for risk treatment verification (including test cases) according to the risk treatment verification strategy. It shall be suitable to provide evidence of compliance of the implementation with the cybersecurity requirements and the refined architectural and detailed design. [Outcome 2]

NOTE 6: Methods of deriving test case may include

- *analysis of requirements,*
- *generation and analysis of equivalence classes,*
- *boundary values analysis, and/or*
- *error guessing based on knowledge or experience.*

SEC.3.BP3: Perform verification activities. Verify identified work products according to the specified strategy and developed criteria in order to confirm that the products meet their specified requirements.
Test the implementation of the design and component integration according to the risk treatment verification specification.

The results of verification activities are recorded. [OUTCOME 3]

SEC.3.BP4: Establish bidirectional traceability.
Establish bidirectional traceability between the cybersecurity requirements and risk treatment verification specification, including test cases comprised in the risk treatment verification specification.

Establish bidirectional traceability between the refined architectural and detailed design and the risk treatment specification.

Establish bidirectional traceability between the risk treatment verification specification, including test cases and verification results.
[OUTCOME 4]

NOTE 8: Bidirectional traceability supports coverage, consistency and impact analysis.

SEC.3.BP5: Ensure consistency.
Ensure consistency between the cybersecurity requirements and the risk treatment verification specification, including test cases.

Ensure consistency between the refined architectural and detailed design and the risk treatment verification specification.
[OUTCOME 4]

NOTE 9: Consistency is supported by bidirectional traceability and can be demonstrated by review records.

SEC.3.BP6: Summarize and communicate results. Summarize the verification results and communicate them to all affected parties.
[OUTCOME 5]

	NOTE 10: Providing all necessary information from the test case execution in a summary enables other parties to judge the consequences.

Output work products	08-50 Test specification 08-52 Test plan 13-04 Communication record 13-25 Verification results 13-19 Review record 13-22 Traceability record 13-50 Test result 19-10 Verification strategy	[OUTCOME 2] [OUTCOME 1] [OUTCOME 6] [OUTCOME 3] [OUTCOME 3, 5] [OUTCOME 4] [OUTCOME 3] [OUTCOME 1]

	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5	Outcome 6
Base Practices						
SEC.3 BP1	x					
SEC.3 BP2		x				
SEC.3 BP3			x			
SEC.3 BP4				x		
SEC.3 BP5					x	
SEC.3 BP6						x
Output Work Products						
08-50 Test specification		x				
08-52 Test plan	x					
13-04 Communication record						x
13-19 Review record			x		x	
13-22 Traceability record				x		
13-25 Verification results			x			
13-50 Test result			x			
19-10 Verification strategy	x					

2.2.4 SEC.4 Risk Treatment Validation

Process ID	SEC.4
Process name	Risk Treatment Validation
Process purpose	The purpose of the Risk Treatment Validation Process is to confirm that the integrated system achieves the cybersecurity goals.
Process outcomes	As a result of successful implementation of this process 1) a risk treatment validation strategy is developed, implemented and agreed upon with relevant stakeholders and maintained suitably to provide evidence that the implementation achieves the cybersecurity goals, 2) the implementation of the design and component integration is validated according to the defined risk treatment validation strategy, 3) validation activities are documented and the results recorded, 4) bidirectional traceability between the cybersecurity goals, risk treatment validation specification and validation results is established, 5) consistency between the cybersecurity goals and the risk treatment validation specification is established, and 6) results of the validation are summarized and communicated to all affected parties.
Base practices	**SEC.4.BP1: Develop a risk treatment validation strategy.** Develop and implement a validation strategy including specification for validation activities with associated methods, techniques and tools, work products or processes under validation, and a schedule for performing these activities. [OUTCOME 1] *NOTE 1: The validation strategy is implemented by a plan.* *NOTE 2: Validation methods and techniques typically include cybersecurity-relevant methods to detect unidentified vulnerabilities (e.g., penetration testing).* *NOTE 3: Validation examines whether the cybersecurity goals are adequate and achieved.*

	SEC.4.BP2: Perform and document activities. Validate the implementation of the design and the integration of the components according to the defined risk treatment validation strategy. The validation activities are documented, and the results are recorded. [OUTCOME 2] **SEC.4.BP3: Establish bidirectional traceability.** Establish bidirectional traceability between the cybersecurity goals and the documented validation specification. Establish bidirectional traceability between the documented validation specification and the validation results. [OUTCOME 3] *NOTE 4: Bidirectional traceability supports coverage, consistency and impact analysis.* **SEC.4.BP4: Ensure consistency.** Ensure consistency between the cybersecurity goals and the risk treatment validation specification. [OUTCOME 3] *NOTE 5: Consistency is supported by bidirectional traceability and can be demonstrated by review records.* **SEC.4.BP5: Summarize and communicate results.** Summarize the validation results and communicate them to all affected parties. [OUTCOME 4] *NOTE 6: Providing necessary information from the validation activities and highlighting important findings concerning additional vulnerabilities enables other parties to judge the consequences.*
Output work products	13-04 Communication record [OUTCOME 5] 13-19 Review record [OUTCOME 2, 4] 13-22 Traceability record [OUTCOME 3] 13-24 Validation results [OUTCOME 2] 19-11 Validation strategy [OUTCOME 1]

	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Base Practices					
SEC.3 BP1	x				
SEC.3 BP2		x			
SEC.3 BP3			x		
SEC.3 BP4				x	
SEC.3 BP5					x
Output Work Products					
13-04 Communication record					x
13-19 Review record		x		x	
13-22 Traceability record			x		
13-24 Validation results		x			
19-11 Validation strategy	x				

2.3 Management Process Group (MAN)

2.3.1 MAN.7 Cybersecurity Risk Management

Process ID	**MAN.7**
Process name	**Cybersecurity Risk Management**
Process purpose	The purpose of the Cybersecurity Risk Management Process is to identify, prioritize and analyze risks of damage to relevant stakeholders as well as monitor and control respective risk treatment options continuously.
Process outcomes	As a result of successful implementation of this process 1) the scope of the risk management to be performed is determined, 2) appropriate risk management practices are defined and implemented, 3) potential risks are identified as they evolve during the conduct of the project, 4) potential risks are prioritized for estimated damage and impact, 5) potential risks are analyzed and risks evaluated, 6) risk treatment options are determined, 7) risks are continuously monitored and identified for relevant changes, and 8) corrective actions are performed when expected progress is not achieved.
Base practices	**MAN.7.BP1: Determine cybersecurity risk management scope.** Determine the scope of the cybersecurity risk management to be performed including project and project assets with cybersecurity properties, damage scenarios, relevant stakeholders, impact categories and related product phases. Determine the scope in accordance with organizational risk management policies. [OUTCOME 1] *NOTE 1: Cybersecurity properties of assets include confidentiality, integrity and availability.* *NOTE 2: Typical impact categories are safety, financial, operational and privacy.*

MAN.7.BP2: Defined cybersecurity risk management practices.

Define appropriate practices to manage the cybersecurity risks according the defined scope including:

- Potential risk identification
- Risk analysis
- Risk evaluation
- Risk determination
- Risk treatment decision

[OUTCOME 2]

NOTE 3: Relevant risk assessment practices may be included from established standards covering practices such as FMEA, TARA, HARA, FTA.

MAN.7.BP3: Identify potential risks.

Identify potential risks within the project scope initially and during the conduct of the project, continuously looking for risk factors at any occurrence of technical or managerial decisions. [OUTCOME 3]

NOTE 4: The identification of potential risks shall include the determination of threat scenarios that impose a specific risk to initiate a damage scenario with impact on relevant stakeholders for all related properties and assets within the scope.

MAN.7.BP4: Prioritize potential risks initially for damage.

Prioritize potential risks with respect to damage and impact on the relevant category and stakeholder. [OUTCOME 4]

Note 5: The potential risks prioritization should be consistent with the scope of risk assessment.

MAN.7.BP5: Analyze potential risks and evaluate risks.

Analyze potential risks to determine the probability, consequence and severity of risks. [OUTCOME 5]

NOTE 6: Risks are analyzed based on identified attack paths that realize a threat scenario and the ease with which identified attack paths can be exploited.

NOTE 7: Different techniques for evaluation of metrics, rating and scoring scheme may be used to analyze a system, e.g., functional analysis, simulation, FMEA, FTA, etc.

	MAN.7.BP6: Define risk treatment option. For each risk (or set of risks) define the selected treatment option to keep, reduce, avoid or share (transfer) the risks. [OUTCOME 6] **MAN.7.BP7: Monitor risks.** For each risk (or set of risks) determine changes in the status of a risk and evaluate the progress of the treatment activities. [OUTCOME 7] *NOTE 8: Major risks may need to be communicated to and monitored by higher levels of management.* *NOTE 9: Risk treatment decisions may be revised for changed conditions, or arise from new and updated estimations and analysis results.* **MAN.7.BP8: Take corrective action.** When expected progress in risk treatment is not achieved, take appropriate corrective action. [OUTCOME 8] *NOTE 10: Corrective actions may involve developing and implementing new risk treatment practices or adjusting existing practices.*	
Output work products	07-07 Risk measure	[OUTCOME 5]
	08-14 Recovery plan	[OUTCOME 6, 7, 8]
	08-19 Risk management plan	[OUTCOME 1, 2, 4, 5, 6, 7, 8]
	13-20 Risk action request	[OUTCOME 5, 6, 7, 8]
	14-08 Tracking system	[OUTCOME 4, 5, 6, 7, 8]
	14-51 Cybersecurity scenario register	[OUTCOME 1, 3, 4, 5]
	14-52 Asset	[OUTCOME 1, 3, 4]
	15-09 Risk status report	[OUTCOME 6, 7, 8]

	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5	Outcome 6	Outcome 7	Outcome 8
Base Practices								
MAN.7.BP1	X							
MAN.7.BP2		X						
MAN.7.BP3			X					
MAN.7.BP4				X				
MAN.7.BP5					X			
MAN.7.BP6						X		
MAN.7.BP7							X	
MAN.7.BP8								X
Output Work Products								
07-07 Risk measure					x			
08-14 Recovery plan						x	x	x
08-19 Risk management plan	x	x		x	x	x	x	x
13-20 Risk action request					x	x	x	x
14-08 Tracking system				x	x	x	x	x
14-51 Cybersecurity scenario register	x		x	x	x			
14-52 Asset library	x		x	x				
15-08 Risk analysis report					x	x		
15-09 Risk status report						x	x	x

Part II Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering

3 ACQ.2 Supplier Request and Selection

The purpose of the Supplier Request and Selection Process is to award a supplier a contract/agreement based on relevant criteria.

The main requirement for distributed cybersecurity activities of ISO 21434 is to execute request for quotations for cybersecurity-relevant services and products. Request for quote processes is common and standardized in automotive industry's purchasing departments and covered in Automotive SPICE PAM 3.1 by three processes: ACQ.3 "Contract Agreement", ACQ.11 "Technical Requirements" and ACQ.15 "Supplier Qualification".

In order to keep Automotive Security SPICE lean for supplier management, the decision was made to create the new process "ACQ.2 Supplier Request and Selection" with elements out of the three processes ACQ.3, ACQ.11 and ACQ.15.

The customer in the supplier request and selection process identifies use cases of supplier involvements and the relationships with suppliers. Supplier evaluation and selection criteria are defined and need to be applied at least in the following use cases:

- Supplier develops a component on the basis of customer requirements (e.g., engineering service)
- Supplier delivers and maintains a component that is provided off-the-shelf to the customer (e.g., operating system, device drivers, system with hard- and software)
- Supplier delivers a component created based on the customer's requirements and contains off-the-shelf (sub-)components
- Excluded are suppliers that deliver products without any support (e.g., open-source software)

3.1 Rating recommendations

3.1.1 Evaluation criteria for cybersecurity

In cases of cybersecurity-relevant services and products, the evaluation criteria must include cybersecurity-relevant supplier criteria, such as a certified Cybersecurity Management System, capability profile of an Automotive Cybersecurity SPICE Assessment, cybersecurity best practices from previous projects, etc.

> **[ACQ.2.RC1]** If cybersecurity-relevant services and products are requested and cybersecurity capabilities are not covered in the evaluation criteria, the corresponding indicator BP1 should be downrated.

Related to:

- BP1: Establish supplier evaluation criteria
- Output WP 18-50: “Supplier evaluation criteria”

3.1.2 Missing evidence ACSMS and ASPICE

In cases of cybersecurity relevant services and products and no evidence are available regarding supplier’s certified Cybersecurity Management System, Automotive SPICE Assessment and Automotive Cybersecurity SPICE Assessment results, activities must be defined in the agreed upon action plan to obtain the missing evidence.

> **[ACQ.2.RC2]** If cybersecurity-relevant services and products are requested and cybersecurity evidence such as certification of Cybersecurity Management System, Automotive SPICE Assessment results and Automotive Cybersecurity SPICE Assessment are not available and not part of the agreed upon action plan, the corresponding indicator BP4 should be rated no higher than “P”.

Related to:

- BP4: “Negotiate and award the contract/agreement”
- Output WP 14-02: "Corrective action register"
- Output WP 02-00: "Contract"

- Output WP 02-01: "Commitment/agreement"
- Output WP 02-50: "Interface agreement"
- Output WP 08-20: "Risk mitigation plan"

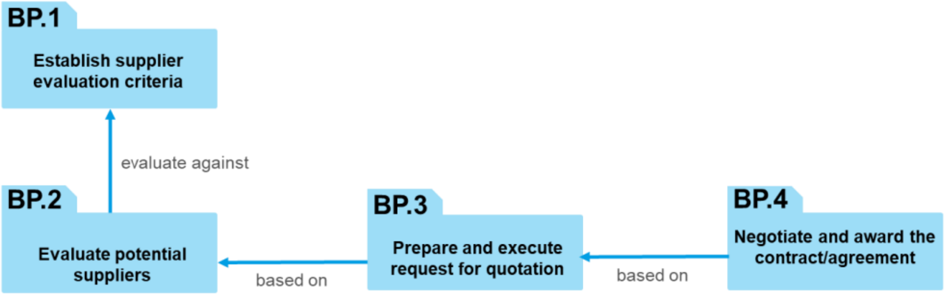
3.1.3 Missing cybersecurity concept

In cases of cybersecurity-relevant services and products, the basis for evaluation criteria and supplier agreements is the customer cybersecurity concept (of the assessed organization). Supplier-relevant aspects of the customer cybersecurity concept must be broken down and shared with the supplier as part of the quotation request.

> [ACQ.2.RC3] If cybersecurity-relevant services and products are requested and cybersecurity-relevant aspects of the customer cybersecurity concept are not broken down, the corresponding indicator PA1.1 should be downrated.

3.2 Rating consistency

The following figure shows the relationships between ACQ.2 base practices:


BP.1
Establish supplier evaluation criteria
evaluate against
BP.2
Evaluate potential suppliers
based on
BP.3
Prepare and execute request for quotation
based on
BP.4
Negotiate and award the contract/agreement

3.2.1 Rating consistency within ACQ.2

Within ACQ.2, the following base practices have relationships to each other.

BP2 Evaluate potential suppliers

[ACQ.2.RL1] If the indicator BP1 is downrated due to an inappropriate, insufficient or incomplete definition of the supplier evaluation criteria, the corresponding indicator BP2 shall be downrated.

BP3 Prepare and execute request for quotation (RFQ)

[ACQ.2.RL2] If the indicator BP2 is downrated due to an inappropriate, insufficient or incomplete evaluation of the potential suppliers, the corresponding indicator BP3 shall be downrated.

BP4 Negotiate and award the contract/agreement

[ACQ.2.RL3] If the indicator BP3 is downrated due to an inappropriate, insufficient or incomplete quotation request, the corresponding indicator BP4 shall be downrated.

4 ACQ.4 Supplier Monitoring

The purpose of the Supplier Monitoring Process is to track and assess the performance of the supplier against agreed upon requirements and corrective actions.

The customer has to introduce a supplier monitoring process for the following relationships with suppliers:

- Supplier develops a component on basis of the customer requirements
- Supplier delivers and maintains a component provided off-the-shelf to the customer (e.g., operating system, device drivers, system with hard- and software)
- Supplier delivers a component with off-the-shelf sub-components and development based on the customer's requirements
- Excluded are suppliers that deliver products without any support (e.g., open-source software)

Interfaces between supplier and customer have to be established for exchanging, monitoring and tracking all relevant information between both parties. Even for a small number of deliveries (e.g., commercial off the shelf component, interfaces have to be set up and maintained at the least for component deliveries, managing changes and problem reports.

4.1 Rating recommendations

4.1.1 Monitoring all suppliers

All project-relevant suppliers have to be tracked against the agreed upon requirements (including suppliers for engineering service, commercial off-the-shelf products, firmware, etc.). Excluded are suppliers that deliver products without any support (e.g., open-source software).

[ACQ.4.RL1] If not all suppliers – excluding suppliers without any support – involved in the project are monitored according to ACQ.4, PA 1.1 cannot be rated “F”.

4.1.2 Agreements with supplier

Agreements between the supplier and customer have to be established and maintained, which cover:

- Supplier’s project content and scope
- Interface agreement
- Exchanged information between customer and supplier
- Joint activities
- Joint processes and interfaces
- Responsibilities and stakeholders
- Joint project management
- Test specification and testing activities
- Joint problem and change management
- Joint reporting and reviews
- Escalation mechanism
- Cybersecurity requirements and responsibilities (if applicable)

Examples for such agreed documents are distributed interface agreements, work statements, license agreements, etc.

[ACQ.4.RL2] If agreements between the supplier and customer are incomplete with respect to all aspects above, the indicator BP1 shall be downrated.

Related to:

- BP1: “Agree on and maintain joint processes”
- Output WP 13-04: “Communication record”
- Output WP 02-50: “Interface agreement”

4.1.3 Consistency to main customer agreements

Agreements of the customer's client (e.g., OEM) have to be taken into consideration for establishing the agreements between the supplier (e.g., TIER 2) and customer (e.g., TIER 1). For example, quality requirements in the agreements between supplier and customer have to be in line with OEM quality agreements.

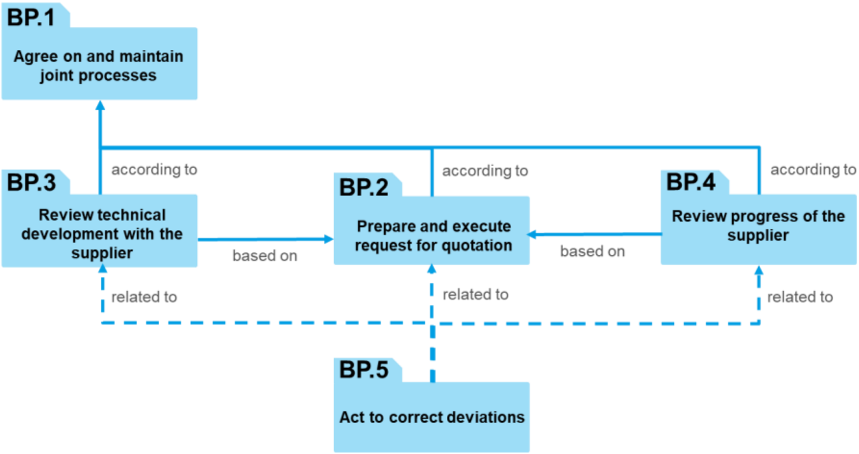
> **[ACQ.4.RC1]** If relevant agreed upon requirements of the customer's client (e.g., OEM), are not part of agreements between the supplier and customer, the indicator BP1 should be downrated.

Related to:

- BP1: "Agree on and maintain joint processes"
- Output WP 13-04: "Communication record"
- Output WP 02-50: "Interface agreement"

4.2 Rating consistency

The following figure shows the relationships between ACQ.4 base practices as well as with other processes:


BP.1
Agree on and maintain joint processes
according to
according to
according to
BP.3
Review technical development with the supplier
BP.2
Prepare and execute request for quotation
BP.4
Review progress of the supplier
based on
based on
related to
related to
related to
BP.5
Act to correct deviations

These relationships are used as the basis for the rating rules and recommendations defined in the following subchapters.

Generic aspects regarding communication (2.1.2) shall also be considered for rating.

4.2.1 Rating consistency within ACQ.4

Within ACQ.4, the following base practices have relationships to each other.

[ACQ.4.RL3] If the indicator BP1 is downrated due to incomplete agreements between the supplier and customer (see ACQ.4.RL2), the corresponding indicators (BP2, BP3, BP4) shall be downrated.

BP3 Review technical development with the supplier

[ACQ.4.RL4] If the indicator BP2 is downrated due to an incomplete exchange of all agreed upon information necessary for reviewing technical development, the indicator BP3 shall be downrated.

BP4 Review progress of the supplier

[ACQ.4.RL5] If the indicator BP2 is downrated due to incomplete exchange of all agreed information necessary for reviewing the progress of the supplier, the indicator BP4 shall be downrated.

BP5 Act to correct deviations

[ACQ.4.RC2] If the indicators BP2, BP3 or BP4 are downrated due to identified non-conformities not managed as corrective actions, the indicator BP5 should be downrated.

5 SEC.1 Cybersecurity Requirements Elicitation

The purpose of the Cybersecurity Requirements Elicitation Process is to specify cybersecurity goals and requirements out of the risk treatment decision involving risk mitigation, and to maintain consistency between the risk assessment, cybersecurity goals and cybersecurity requirements.

The Cybersecurity Requirements Elicitation Process uses the risks where risk treatment involves risk mitigation from the Risk Management Process (MAN.7) as an input. Such risks are related to a threat scenario. A cybersecurity goal is typically the achievement of a residual risk that is assumed acceptable. To achieve a cybersecurity goal, a set of functional and/or non-functional cybersecurity requirements that support the achievement of the cybersecurity goals will be specified.

Cybersecurity requirements shall be detailed in an iterative process that can be assigned to elements of the product architecture.

The rationale for the effectiveness of the selected risk treatment action is typically documented in the risk action request (WP 13-20).

Cybersecurity claims are, by nature, not subject to risk treatment. The related risk value has been evaluated as a residual risk that is acceptable. Cybersecurity claims maybe reevaluated when new vulnerabilities are identified, or an attack path feasibility increases.

Cybersecurity goals and stakeholder requirements can contradict each other, such as when a technical solution for a connected service imposes a high risk of a threat scenario. In these cases, cybersecurity requirements will be derived as a trade-off between said stakeholder requirements and cybersecurity goals in dialog with the customer.

The definition of cybersecurity goals is not limited to the development of a product. Where appropriate, they should be defined also for post-development phases, such as production and decommissioning.

Vulnerabilities that are discovered during implementation, verification and validation will change the risk value for particular threat scenarios and require an iteration of the Cybersecurity Requirements Elicitation Process.

5.1 Rating recommendations

5.1.1 Cybersecurity goals

Cybersecurity goals are high-level requirements that consistently address threat scenarios. Their achievement will be validated in the integrated system.

5.1.2 Cybersecurity requirements

Cybersecurity requirements are a particularly desired characteristics of a system and/or software. They are consistent with the cybersecurity goal they are derived from. Their implementation will be verified in the corresponding integration level.

Cybersecurity requirements may address, among others:

- Functions that are implemented in mechanics, hardware or software or cover a combination of these elements
- Processing of signals from other systems
- Non-functional requirements

Cybersecurity requirements have to be granular and understandable. Unclear or generic requirements have to be clarified with the individual stakeholders.

Non-functional requirements at a system level may be decomposed into functional requirements on a component level – for example, when cybersecurity of a system is a non-functional requirement. This non-functional requirement may be detailed into functional requirements for hardware and software components.

The existence of a set of cybersecurity requirements shall be demonstrated as a populated list or database that allows the structuring of the cybersecurity requirements.

Recommendations and rules:

[SEC.1.RC1] If unclear or inconsistent requirements are not clarified with the individual stakeholders, indicator BP1 will be downrated.

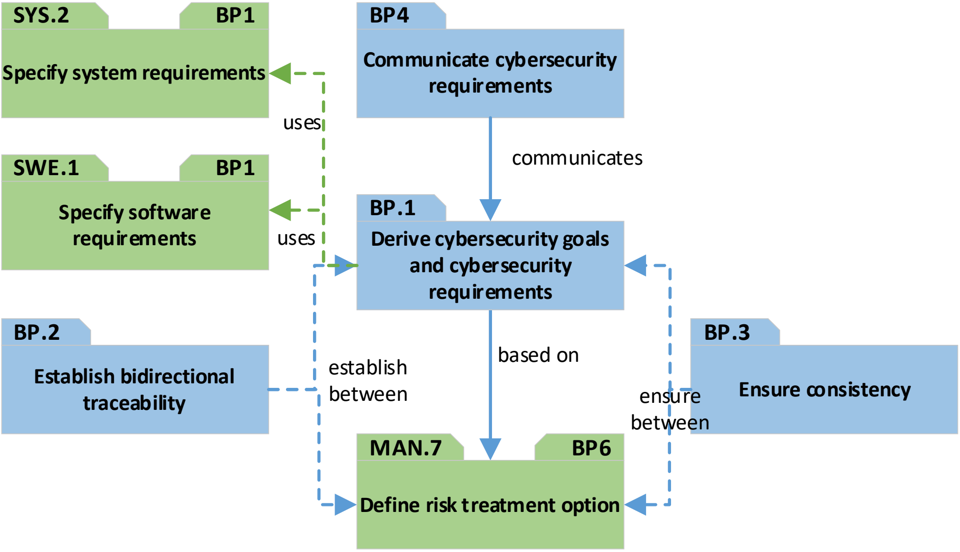
[SEC.1.RC2] If the cybersecurity requirements specification does not reflect the results of the risk assessment, BP1 cannot be rated higher than “L”.

Related to:

- BP1: “Derive cybersecurity goals and cybersecurity requirements”
- Output WP 17-51: “Cybersecurity goals”
- Output WP 17-11: “Software requirements specification”
- Output WP 17-12: “System requirements specification”
- Output WP 17-50: “Verification criteria”

5.2 Rating consistency

The following figure shows the relationships between SEC.1 base practices as well as their relationships to other processes:


SYS.2
BP1
Specify system requirements
SWE.1
BP1
Specify software requirements
BP.2
Establish bidirectional traceability
BP4
Communicate cybersecurity requirements
communicates
BP.1
Derive cybersecurity goals and cybersecurity requirements
uses
uses
establish between
based on
ensure between
BP.3
Ensure consistency
MAN.7
BP6
Define risk treatment option

These relationships are used as the basis for the rating rules and recommendations defined in the following subchapters.

Generic aspects regarding traceability and consistency, summaries and communication, and strategy and plan shall also be considered for rating. Please refer to the VDA Automotive SPICE guideline for further information.

5.2.1 Rating consistency within SEC.1

There are no rating rules defined for dependencies within SEC.1.

5.2.2 Rating consistency to other processes at Level 1

The following base practices of SEC.1 have relationships to other processes.

BP1: Derive cybersecurity goals and cybersecurity requirements

> **[SEC.1.RC3]** If PA 1.1 for MAN.7 is downrated, this should be in line with the rating of the BP1 indicator.
>
> **[SEC.1.RC4]** If BP1 for SYS.2 is downrated, this should be in line with the rating of the BP1 indicator.
>
> **[SEC.1.RC5]** If BP1 for SWE.1 is downrated, this should be in line with the rating of the indicator BP1.

6 SEC.2 Cybersecurity Implementation

The purpose of Cybersecurity Implementation Process is to implement the risk treatment actions involving risk mitigation to reduce the remaining risk to an acceptable level.

The Cybersecurity Implementation Process uses the initial product architecture to perform refinements to the architectural elements and their interfaces based on the cybersecurity goals and requirements. The PAM uses no specific term for an architecture that is related solely to cybersecurity.

Cybersecurity is a property of a product; therefore, the system and software architecture shall reflect the cybersecurity requirements. This can be achieved by additional elements of the architecture or adaptations to the interfaces between the elements.

The cybersecurity requirements are allocated to one or more elements of the product architecture.

Cybersecurity controls are used to achieve the cybersecurity goals and cybersecurity requirements. These controls may be complex software algorithms, electronic hardware solutions or even warnings in a manual for decommissioning. They should be appropriate to mitigate the risk of a threat scenario.

The selection of cybersecurity controls typically has an influence on the system, software, mechanical and hardware architecture.

Where changes to the elements of the product architecture are necessary the detailed design of such elements will be changed accordingly.

The development of software units as well as the establishing of traceability and consistency is similar to SWE.3.

Vulnerabilities that are discovered during implementation are communicated to those who are performing risk assessment to reconcile the determination of risk value for particular threat scenarios.

6.1 Rating recommendations

The architectural design is the highest level design description of a product or product component with different (high level) abstraction views reflecting concerns of different stakeholders. The term “stakeholder” is not limited to the customer. It also includes strategic planning, project management, development, testing, quality assurance, safety, etc. of the supplier or other entities, such as legal bodies.

These views are architecture visualizations that are required for communication, discussion, reviews, analysis, evaluation, planning, change request analysis, impact analysis, maintenance, etc. of the product or product component.

There is no common definition of which views are required and no criteria for the completeness of the sum of views. There are some approaches in the industry that specify the kind of information that is required for the view (“viewpoints” that are collections of patterns, templates, and conventions for constructing one type of view) and the integration of the views in a thoroughly architectural design description.

In most cases the architectural design is a graphical representation supplemented by textual explanations. The graphical representation consists at least of a static view providing an overview of the structure and a dynamic view describing the designated behavior of the product or product component. See SYS.3 and SWE.2 for details.

6.1.1 Cybersecurity controls

Cybersecurity controls are technical measures that are appropriate to mitigate or avoid a cybersecurity risk related to a threat scenario. Examples for such measures are:

- Robust software design
- Specific hardware
- User warning on potential attack
- Common state-of-the-art solutions
- Encryption

Recommendations and rules:

[SEC.2.RL1] If documentation for cybersecurity controls does not contain an explanation on how the related risk is mitigated, the indicator BP3 shall be downrated.

Related to:

- BP3: “Select cybersecurity controls”
- Output WP 17-52: “Cybersecurity controls”

6.1.2 Analyze software architectural design

The analysis of the software architectural design in this process is focused on detecting new vulnerabilities. These vulnerabilities are documented so they can be used in risk assessment for the determination of new or updated risk treatment decisions.

Recommendations and rules:

[SEC.2.RL2] If detected vulnerabilities are not documented, the indicator BP5 shall be downrated.

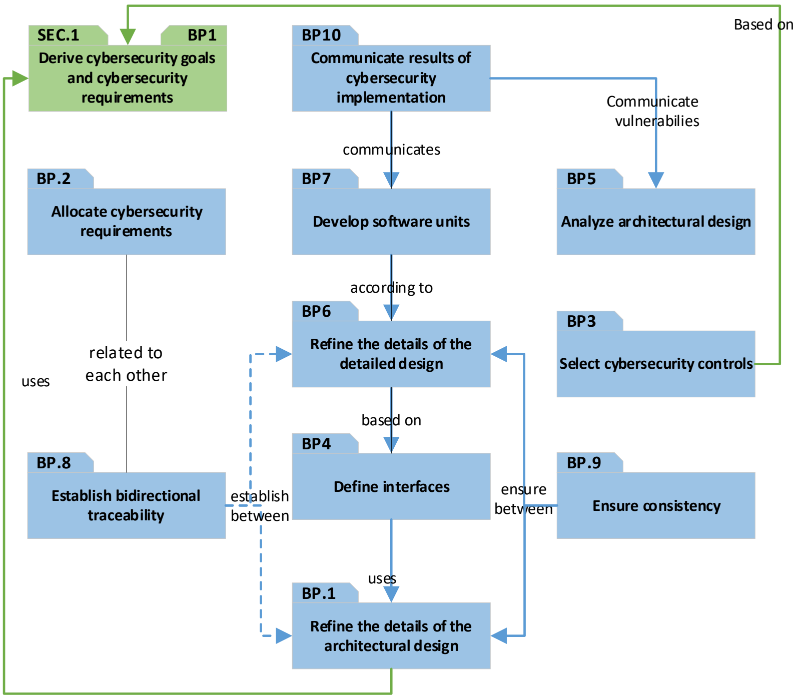
[SEC.2.RL3] If no vulnerabilities were found and the analysis is documented, the indicator BP1 must not be downrated.

Related to:

- BP5: “Analyze software architectural design”
- Output WP 15-50: “Vulnerability analysis report”

6.2 Rating consistency

The following figure shows the relationships between SEC.1 base practices:


SEC.1
BP1
Derive cybersecurity goals and cybersecurity requirements
BP10
Communicate results of cybersecurity implementation
Based on
Communicate vulnerabilies
communicates
BP.2
Allocate cybersecurity requirements
BP7
Develop software units
BP5
Analyze architectural design
according to
BP6
Refine the details of the detailed design
BP3
Select cybersecurity controls
related to each other
uses
based on
BP.8
Establish bidirectional traceability
establish between
BP4
Define interfaces
ensure between
BP.9
Ensure consistency
uses
BP.1
Refine the details of the architectural design

These relationships are used as the basis for the rating rules and recommendations defined in the following subchapters.

> **[SEC.2.RC1]** If SEC.1.BP1 is downrated, this should be in line with the rating of PA1.1.

> **[SEC.2.RC2]** If SEC.1.BP6 is downrated, this should be in line with the rating of BP7.

Generic aspects regarding traceability and consistency, summaries and communication, and strategy and plan shall also be considered for rating. Please refer to the VDA Automotive SPICE guideline for further information.

7 SEC.3 Risk Treatment Verification

The purpose of the Risk Treatment Verification Process is to confirm that the design implementation and components integration comply with the cybersecurity requirements and the architectural design.

The Risk Treatment Verification Process ensures the implementation of the cybersecurity controls according to the cybersecurity requirements and the corresponding architectural design.

Cybersecurity controls are in most cases specified by functional or non-functional requirements and a corresponding architectural design. They are identified solutions to achieve the cybersecurity requirements.

The objective of the Risk Treatment Verification Process is to prove that the implementation meets these requirements and the specified design. It provides evidence that measures are being done correctly.

In that sense, the verification process cannot measure whether the right measures have been specified and implemented. It cannot provide any evidence of the suitability of a corresponding cybersecurity goal to reduce an associated risk.

Verification results may serve as an input to the SEC.4 process, e.g., to define necessary validation activities.

The suitability of the cybersecurity goals and the effectiveness of associated solutions in terms of achieving the intended risk reduction is in scope of the risk treatment validation process SEC.4.

7.1 Rating recommendations

7.1.1 Risk treatment verification strategy

Cybersecurity requirements are particularly desired characteristics of a system and/or software. Their verification will be performed within different integration levels, such as software units, integrated software or a completely integrated system.

Cybersecurity verification may include among others:

- Static software analysis
- Software unit testing
- Software integration and acceptance testing
- System integration and acceptance testing

In general, all verification activities follow a documented risk treatment verification strategy.

The expectations for a verification strategy cover these aspects:

a) A definition of the scope of verification, including work product or processes under verification

b) A definition of how specific requirements regarding verification and testing (e.g., cybersecurity related stakeholder agreements, ISO 21434, Metrics, MISRA, test coverage) are covered

c) A definition of the methods and tools for verification and for reviews

d) A definition of the methods to identify unspecified functionality

e) A definition of the methods for test case and test data development (e.g., development of positive/negative tests, equivalence partitioning)

f) A definition of the regression strategy for verification activities

g) A definition of the verification/test environment regarding each verification method

h) A definition of entry/exit and pass/fail criteria for verification

i) An approach for the handling of failed tests and verification results
Note: Aspect i of the risk treatment verification strategy should refer to the Problem Resolution Management strategy (SUP.9)

Recommendations and rules:

[SEC.3.RL1] If the risk treatment verification strategy does not cover all aspects above, the indicator BP1 cannot be rated “F”.

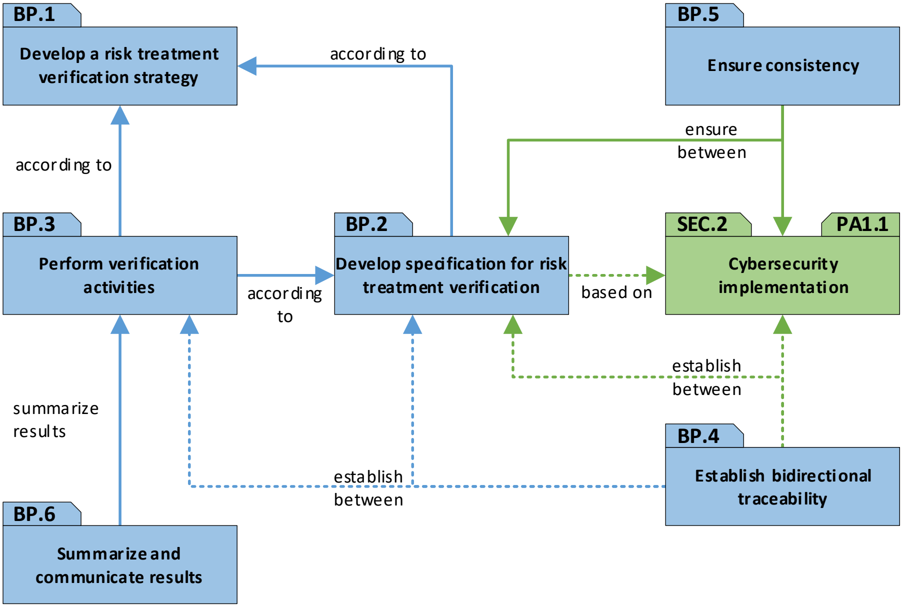
[SEC.3.RL2] If the test strategy does not cover aspects b, c, d or g, the indicator BP1 cannot be rated higher than “P”.

Related to:

- BP1: “Develop a risk treatment verification strategy”
- Output WP 08-52 “Test plan”
- Output WP 19-10 “Verification strategy”

7.2 Rating consistency

The following figure shows the relationships between SEC.3 base practices as well as to other processes:


BP.1
Develop a risk treatment verification strategy
according to
BP.5
Ensure consistency
ensure between
according to
BP.3
Perform verification activities
according to
BP.2
Develop specification for risk treatment verification
based on
SEC.2
PA1.1
Cybersecurity implementation
establish between
summarize results
establish between
BP.4
Establish bidirectional traceability
BP.6
Summarize and communicate results

These relationships are used as the basis for the rating rules and recommendations defined in the following subchapters.

Generic aspects regarding traceability and consistency, summaries and communication, and strategy and plan shall also be considered for rating. Please refer to the VDA Automotive SPICE guideline for further information.

7.2.1 Rating consistency within SEC.3

The following rating rule is related to the system qualification test strategy and thus covers several base practices of the process:

Within SEC.3, the following base practices have relationships to one another:

BP2: Develop specification for risk treatment verification

> **[SEC.3.RL3]** If the indicator for developing the verification strategy (BP1) is downrated due to missing or inadequate definitions of methods for test case and test data development, the indicator BP2 shall be downrated.

BP3: Perform verification activities

> **[SEC.3.RL4]** If the indicator for developing the verification specification (BP2) is downrated, the indicator BP3 cannot be rated higher.

7.2.2 Rating consistency to other processes at Level 1

The following base practices of SEC.3 have relationships to other processes.

BP2: Develop specification for risk treatment verification

> **[SEC.3.RC1]** If the PA 1.1 for SEC.1 or SEC.2 is downrated, this should be in line with the rating of the indicator BP2.

8 SEC.4 Risk Treatment Validation

The purpose of the Risk Treatment Validation Process is to confirm that the integrated system achieves the cybersecurity goals.

Cybersecurity goals are high-level requirements addressing an associated threat scenario. To achieve a cybersecurity goal, a set of functional and/or non-functional cybersecurity requirements and a corresponding design are specified. The verification of the implementation against these requirements and the design is in scope of the Risk Treatment Verification Process (SEC.3).

The scope of the Risk Treatment Validation Process is to provide evidence that the right measures have been specified. Thereby, the process SEC.4 probes and questions the defined cybersecurity goals and the associated proposed solutions themselves.

A typical way of validating cybersecurity goals and associated cybersecurity controls is to perform penetration tests that attempt to compromise the system.

Therefore, a validation strategy shall define validation activities including effective methods to detect vulnerabilities **not** identified by the TARA and thus have **not** been addressed by specific risk treatment actions.

Validation activities may include tests with specified test cases and/or also explorative test methods, given that the goal here is to identify unknown vulnerabilities and attack paths.

Vulnerabilities discovered during validation may affect the risk value for particular threat scenarios and require an iteration of the Risk Assessment Process (MAN.7) and Cybersecurity Elicitation Process (SEC.1); hence a specific handling of the validation results is necessary. This is typically addressed by the Problem Resolution Management Process (SUP.9).

8.1 Rating recommendations

8.1.1 Develop a risk treatment validation strategy

The validation of cybersecurity goals and associated controls includes activities to detect vulnerabilities and unidentified attack paths. In general, these activities follow a validation strategy.

Cybersecurity validation methods may include, among others:

- Vulnerability scanning
- Penetration testing
- Fuzz testing
- Interface testing

  Note: Details on the specific cybersecurity related test methods can be found in ISO 21434

Validation methods may also include inspections, including an analysis of applications and operating systems for security flaws. An inspection can also be done via code reviews.

The expectations for a validation strategy cover these aspects:

a) A definition of the scope of validation

b) A definition of how specific requirements regarding validation – such as cybersecurity-related stakeholder agreements or cybersecurity standards – are covered.

c) A definition of the methods and tools for validation and reviews

d) A definition of the methods for test case and test data development.

e) A definition of the regression strategy for validation activities.

f) A definition of the validation environment for the validation activities.

g) A definition of entry/exit and pass/fail criteria for validation.

h) An approach for the handling of validation results.

   Note: Aspect 'h' of the risk treatment validation strategy should refer to the Problem Resolution Management Process (SUP.9).

Recommendations and rules:

> **[SEC.4.RL1]** If the risk treatment verification strategy does not cover all aspects above, the indicator BP1 must not be rated “F”.
>
> **[SEC.4.RL2]** If the test strategy does not cover aspect b, c, g or h, the indicator BP1 cannot be rated higher than “P”.

Related to:

- BP1: “Develop a risk treatment validation strategy”
- Output WP 19-11: “Validation strategy”

8.1.2 Document and perform validation activities

In order to check the completeness and appropriateness of the validation activities with respect to the defined strategy, a documentation is essential. *Note: This should not be confused with the validation results which is made available after performing the tests.*

Recommendations and rules:

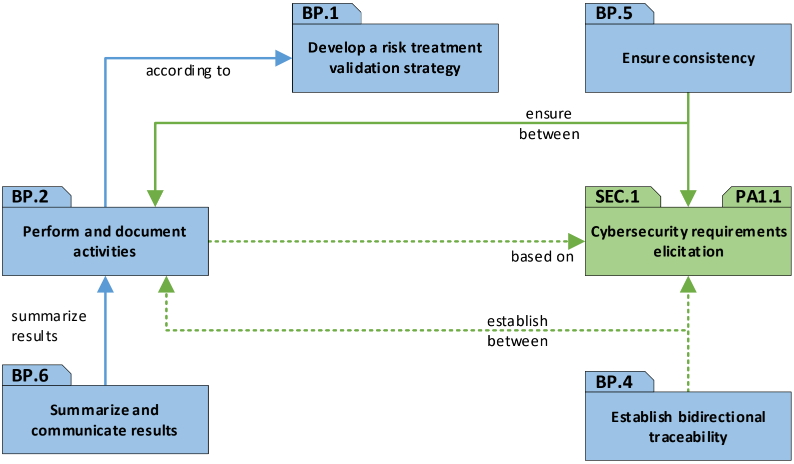
> **[SEC.4.RL3]** If documentation of the validation activities is missing or not suitable to evaluate the completeness of the activities according to the validation strategy, the indicator BP2 cannot be rated higher than “P”.

Related to:

- BP5: “Summarize and communicate results”
- Output WP 13-24: “Validation results”

8.2 Rating consistency

The following figure shows the relationships between SEC.4 base practices and to other processes:


BP.1
Develop a risk treatment validation strategy
BP.5
Ensure consistency
according to
ensure between
BP.2
Perform and document activities
SEC.1
PA1.1
Cybersecurity requirements elicitation
based on
summarize results
establish between
BP.6
Summarize and communicate results
BP.4
Establish bidirectional traceability

These relationships are used as the basis for the rating rules and recommendations defined in the following subchapters.

Generic aspects regarding traceability and consistency, summaries and communication, and strategy and plan shall also be considered for rating. Please refer to the VDA Automotive SPICE guideline for further information.

8.2.1 Rating consistency within SEC.4

There are no specific rules regarding the consistency within SEC.4.

8.2.2 Rating consistency to other processes at Level 1

The following base practices of SEC.4 have relationships to other processes.

> **[SEC.4.RC1]** If the PA 1.1 for SEC.1 is downrated, this should be in line with the rating of the indicator BP2.

9 MAN.7 Cybersecurity Risk Management

The purpose of the Cybersecurity Risk Management Process is to identify, prioritize and analyze risks of damage to relevant stakeholders, and to continuously monitor and control respective risk treatment options.

Risk management is a central part of projects and can be applied to all technical, organizational and commercial risk identification and analysis.

The Risk Management Process ensures a systematic identification of potential risks. **Potential risks** can be identified at all times before, during and after project development – even within production and post-production. They require systematic analysis and estimation. A distinction between potential risks and risks is made in accordance with technical standards like ISO 26262 and ISO 21434. Potential risks are called risks as soon as they are assigned to probability and severity.

Potential risks may become high in numbers during complex project developments. Before running through an intensive analysis phase, a first prioritization should be performed. The initial prioritization is based on the damage or potential harm potential risks may cause. The effort for risk analysis might be a bottleneck in the project, impacting the timeline; hence this initial prioritization should ensure that the most relevant potential risks are analyzed first.

Risk analysis includes the criteria for risk identification, exploitability and occurrence to estimate the feasibility of attacks as well as in case of error. The analysis can either be structural, numerical or a combination thereof. Established structural risk analysis are, for instance, fault tree analysis or Ishikawa. Structural analysis is commonly used in automotive engineering (for reference, see make-buy-reuse analysis used in BP6 of SWE.2). A numerical analysis may use cross-industry approaches and their respective established rating schemes, if applicable.

Risk management prepares the fundamental risk treatment options based on the determination of risk, damage and harm. Such risk treatment options can be avoidance, reduction, transfer or acceptance of risks. The risk management process does not include risk treatment actions or provide solutions. Corresponding risk treatment actions should be defined within related processes like project management, engineering or even acquisition.

Risk management is an essential process able to react upon unplanned and sudden changes, news, general lack of progress and gaps in stakeholder interfaces. Therefore, monitoring of related changes and the capability to take corrective actions is a prerequisite of Level 1 and Level 2.

9.1 Rating recommendations

9.1.1 Cybersecurity Risk Management scope

The risk management scope needs to define the boundaries to apply within the risk management process. The scope definition needs to include:

a) ***Assets:*** Products, their components and SW/HW elements are related to assets intended for protection from risks within the project.
b) ***Damage scenarios*** to be managed and controlled
c) *Risk related* ***properties*** are ***attributes*** of those assets. For example:
    1. Confidentiality
    2. Integrity
    3. Availability
d) ***Relevant stakeholders*** that could be affected by the adverse consequences of risks, including:
    1. Road user
    2. Customer
    3. Supplier
    4. Vehicle occupants

e) The ***impact categories are*** related to the adverse consequences they can cause to relevant stakeholders of each. Impact categories include, but are not limited to:

   1. Safety – e.g., for vehicle occupants
   2. Privacy – e.g., driver personal information
   3. Financial – e.g., customers service network
   4. Operational – e.g., impact on infrastructure within manufacturing of customer, etc.
   5. Quality – relevant to stakeholder expectation not specifically covered in other impact categories

f) ***Phases*** that are within scope to be managed for the asset:

   1. Innovation or demonstrator builds
   2. Pre-development
   3. Development
   4. Production and manufacturing
   5. Maintenance and servicing
   6. Decommissioning

The scope definition should represent a minimum definition, including initial damage scenarios. Later identified damage scenarios should not be considered as incomplete scope definition.

Risk-related *properties* can be overlapping and interpreted differently. For example, “authentication” could be interpreted as “confidentiality” or "availability”, depending on the stakeholder view.

Relevant *stakeholders* should be evaluated and aligned within the supply chain and distributed development. A sub-supplier may have had a different view for their initial risk management of an off-the-shelf part, for example. The scope must at least include the road user.

The phases in scope could be limited. This shall be justified if minimum requirements are not met.

Recommendations and rules:

[MAN.7.RL1]: If the risk management scope does not consider relevant assets (aspects a and c) that are significant for product-related quality risks, BP1 cannot be rated higher than "P".

[MAN.7.RC1]: If the scope does not consider cost- (financial) and schedule (organizational)-related risks (aspect e) but these are covered when estimating work packages in the project planning, this should not be used to downrate the indicator BP1.

[MAN7.RL2]: If the scope does not consider the road user as stakeholder (aspect d), BP1 cannot be rated higher than "P".

Related to:

- BP1: "Determine cybersecurity risk management scope"
- Output WP 08-19: "Risk management plan"
- Output WP 14-51: "Cybersecurity scenario register"
- Output WP 14-52: "Asset library"

9.1.2 Risk management practices

The practices used to establish Cybersecurity Risk Management result out of the strategy definition required within an automotive Cybersecurity Management System (ACSMS).

Risk management practices should include the methods, roles, tools, review, and release criteria of:

a) Potential risks identification: Repositories and practices for identification and documentation of threat scenarios and damage scenarios, e.g.:
    1. Assessment scheme to inspect thread mode effect analysis (TMEA) practices of spoofing, tempering, repudiation, information disclosure, denial of service and elevation of privileges (STRIDE)

   2. Fault tree analysis (Ishikawa)
   3. Brainstorming
- b) Risk analysis: Repositories and practices for attack path analysis and attack feasibility evaluation, e.g.:
   1. Inductive approach, for instance with reengineering of knowledge
   2. Deductive approach, for instance with an attack tree analysis
   3. Numerical analysis methods, for example common vulnerability scoring system
   4. Combination of a–c
- c) Weighting and rating practices:
   1. Scaling and rating methods
   2. Weighing criteria, e.g., selection of heatmap variants
   3. Usage of Cybersecurity Assurance Level (CAL).
- d) Risk breakdown within process:
   1. Expert boards
   2. Roles involved, RACI
   3. Unique identification and traceability of related items
- e) Related internal and external interfaces:
   1. Sources and practices for current and historical data evaluation
   2. Criteria for monitoring
   3. Verification of accepted risks
   4. Sub-supplier and contractor cooperation
- f) Corrective action management:
   1. Internal dependencies of the project
   2. External dependencies of the project

Appropriate documentation of practices can be established within textual descriptions, tools, diagrams, scripts, flow charts, and also training.

Recommendations and rules:

[MAN.7 RL3] If the practices do not include aspects a–d, the indicator BP2 cannot be rated “F”.

[MAN.7 RC2] If the use of practices is obvious by the implementation in a tool but not explicitly documented, this should not be used to downrate the indicator BP1 to “N” or “P”.

[MAN.7 RL4] If the practices do not address interfaces (aspects e and f) between multisite organizations or projects, subprojects, management systems and/or groups in cases of corresponding complex projects, the indicator BP2 cannot be rated higher than “P”.

Related to:

- BP2: “Defined cybersecurity risk management practices”
- Output WP 08-19: “Risk management plan”

9.1.3 Prioritization

Within complex projects including many assets and stakeholders, the potential risks identification can lead quickly to large numbers. The risk analysis and evaluation may therefore require a substantial amount of time and effort.

The work breakdown for cybersecurity risk analysis shall therefore be prioritized initially for the impact the related damage may cause. This initial prioritization (BP4) assures that risks related to the highest potential damage are analyzed first.

Further grouping, sorting, and categorizing is necessary in later stages of the CS Risk Management Process to support prioritization and may overwrite and contradict results from BP4. For example, a potential risk may cause a severe impact and initially be prioritized as high, but can easily be avoided with established workarounds and thereby become a low priority in a later evaluation phase.

Recommendations and rules:

[MAN.7.RC3] If initial risk prioritization for impact is not created before risk analysis – despite this being relevant to the project – BP4 should not be rated “F”.

[MAN.7.RC.4] If initial prioritization of potential risks is not in line with grouping, sorting, categorization in later process steps, the indicator BP4 should not be downrated.

Related to:

- MAN.7.BP4: “Prioritize potential risks initially for damage”
- Output WP 08-19: “Risk management plan”
- Output WP 14-08: “Tracking system”
- Output WP 14-51: “Cybersecurity scenario register”
- Output WP 14-52: “Asset library”

9.1.4 Potential risk analysis and risk determination

The analysis of risks is the basis for selecting a suitable treatment option and all subsequent actions. Cybersecurity risks are subject to change. This makes documentation of risk assumptions and constraints necessary. The analysis of a risk shall include the sequence of actions that can lead to the identification and its exploitation, and an evaluation of each action´s individual probability. This analysis for sequences of actions is called Attack Path Analysis for Cybersecurity Risk Management.

Attack path analysis can be performed in the form of:

a) **Attack potential analysis**:
   The expertise, item knowledge, window of opportunity, equipment and elapsed time are evaluated separately with a final feasibility level aggregation, or
b) **Attack vector analysis**:
   Describes four feasibility ratings depending on the logical and physical distance of exploits. Attack vector analysis may also be included for evaluation of a cybersecurity assurance level (CAL), or
c) **Numerical analysis:**
   Considers several aspects of a and b with defined, model-specific numbers and calculation algorithm.
d) **A tailored combination** of a–c.

The attack path analysis can be supported by research, experience, and historical data to **evaluate and verify the ease of exploitation.** Such intelligence data can come from:

a) **Cybersecurity Management System** (CSMS), e.g., the vulnerability data of former projects, disclosure programs and shared information.
b) External intelligence service providers, e.g., test centers
c) Information Sharing and Analysis Centers (ISACS)
d) Simulation

All attack paths that create a risk are to be considered. Within the risk analysis, further attack paths might be identified that could lead to other – even unidentified – threats and damage scenarios. The analysis shall ensure these risks are similarly considered, including reasonable prioritization if necessary.

The resulting cybersecurity risk of a threat scenario can be expressed by different levels and shall result from **cybersecurity risk determination** – the evaluation of the impact and the related attack feasibility within the context of the project.

Recommendations and rules:

[MAN.7.RL.5] If none of the described approaches (aspects a–d) for attack path analysis is observable in the assessed project, PA 1.1 shall be downrated.

[MAN.7.RC.5] If the cybersecurity risk analysis does not evaluate the ease of exploitation, the indicator BP5 shall be downrated.

Related to:

- MAN.7.BP5: "Analyze potential risks and evaluate risks"
- Output WP 07-07: "Risk measure"
- Output WP 13-20: "Risk action request"
- Output WP 14-08: "Tracking system"
- Output WP 14-51: "Cybersecurity scenario register"
- Output WP 14-52: "Asset library"

9.1.5 Define risk treatment option

For each risk or set of risks, an initial **treatment option** should be selected (risk treatment decision):

a) Avoidance of risk, for example the attack path is made impossible.
b) Reduction of risk, for example the feasibility of the attack path is decreased.
c) Transfer of risk, for example to assign resources with higher knowledge on avoidance or reduction of the risk.
d) Acceptance of risk, for example if the risk cannot be lowered any more, it is kept unmitigated.

The risk treatment options can be consecutive and overlapping, since a risk can have multiple attack paths in which each is treated individually through different phases of the project. The elements of one attack path can have different owners and interfaces that require individual treatment options.

Restrictions to the traceability of risk options shall be included to the risk treatment decision process.

Related to:

- BP6: “Define risk treatment option”
- Output WP 08-14: “Recovery plan”
- Output WP 08-19: “Risk management plan”
- Output WP 13-20: “Risk action request”
- Output WP 14-08: “Tracking system”
- Output WP 15-08: “Risk analysis report”
- Output WP 15-09: “Risk status report”

9.1.6 Monitoring and control of cybersecurity risks

Cybersecurity risks challenge management and control as they can face sudden and frequent changes. Therefore, cybersecurity risk management needs to identify changes and monitor them accordingly.

Monitoring of risks should include:

- Continuous monitoring for new threats and attack paths.
- Continuous monitoring for changed attack paths, e.g., by published attacks proving the feasibility has been increased since last risk analysis.
- Continuous monitoring of accepted risks, also to provide implicit verification of unmitigated risks.
- Identification of changes to assumptions and constraints considered for the analysis and evaluation of cybersecurity risks.
- Identification of risks that refer to obsolete techniques, values, items and assets.
- Changed conditions and results in project implementation, concept, verification and validation.
- Changed conditions and results of relevant interfaces, for example on transferred risks.

An active exchange with the cybersecurity management system, e.g., on intelligence data, as described in aspects e–h of subchapter 9.1.4, may provide further evidence for the effectiveness of monitoring.

Corrective actions shall be taken appropriately to keep cybersecurity risk evaluation and treatment valid and adapted for changed conditions at all times.

Monitoring or tracking systems can either support push (event driven) or pull (polling) principle. It is required to establish appropriate monitoring cycles for polling systems.

Recommendations and rules:

[MAN.7.RL6] If monitoring does not assess fulfillment of activities (i.e., risk action request), the indicator BP7 must not be rated higher than "L".

[MAN.7.RC6] If action items or corrective actions are not properly tracked, the corresponding indicators BP7 and BP8 should be downrated.

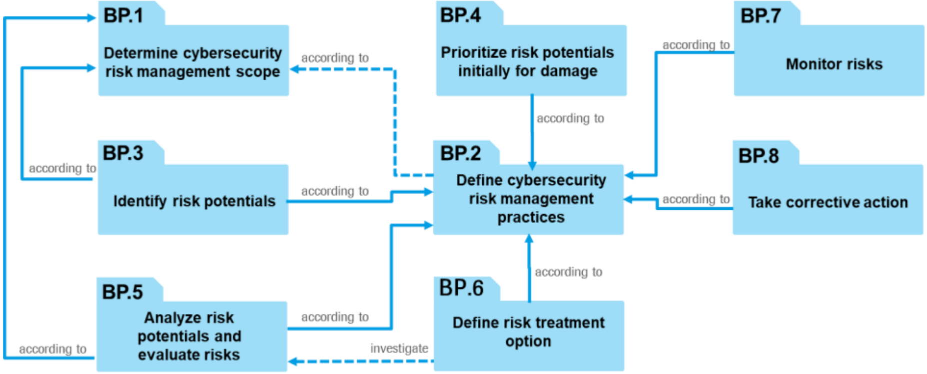
[MAN.7 RC7] If the confirmation of a successful implementation of a risk action request is not based on documented criteria, the indicator BP7 should be downrated.

Related to:

- BP7: "Monitor risks"
- BP8: "Take corrective action"
- Output WP 08-14: "Recovery plan"
- Output WP 08-19: "Risk management plan"
- Output WP 13-20: "Risk action request"
- Output WP 14-08: "Tracking system"
- Output WP 15-09: "Risk status report"

9.2 Rating consistency

The following figure shows the relationships between MAN.7 base practices:



These relationships are used as the basis for the rating rules and recommendations defined in the following subchapters.

9.2.1 Rating consistency within MAN.7

BP.1 Determine cybersecurity risk management scope

[MAN.7. RC8] If the determination of the cybersecurity risk management scope (BP1) is incomplete, then the indicator BP2 should be downrated.

[MAN.7.RL7] If the determination of the cybersecurity risk management scope (BP1) is downrated, then the indicator BP3 and BP5 shall be as well.

BP2 Defined cybersecurity risk management practices

[MAN.7.RL8] If the practice-related activities are not performed according to the defined practices (BP2), the indicators BP3, BP4, BP5, BP6, BP7 and BP8 shall be downrated, respectively.

BP5 Analyze potential risks and evaluate risks

[MAN.7.RC9] If the analysis of potential risks and evaluation of risks (BP5) is rated “P” or “N”, the indicator BP6 should be downrated.

Annex A Process Assessment and Reference Model Conformity

A.1 Introduction

The Automotive SPICE process assessment and reference model meet the requirements for conformity defined in ISO/IEC 33004. The process assessment model can be used in the performance of assessments that meet the requirements of ISO/IEC 33002.

This clause serves as the statement of conformity of the process assessment and reference models to the requirements defined in ISO/IEC 33004.

> *[ISO/IEC 33004, 5.5 and 6.4]*

Due to copyright reasons each requirement is only referred to by its number. The full text of the requirements can be drawn from ISO/IEC 33004.

A.2 Conformity to the requirements for process reference models

Clause 5.3, "Requirements for process reference models"

The following information is provided in Chapter 1 of this document:

- the declaration of the domain of this process reference model,
- the description of the relationship between this process reference model and its intended use, and
- the description of the relationship between the processes defined within this process reference model.

The descriptions of the processes within the scope of this process reference model that meet the requirements of ISO/IEC 33004 clause 5.4 are provided in Chapter 2 of this document.

> *[ISO/IEC 33004, 5.3.1]*

The relevant communities of interest and their mode of use and the consensus achieved for this process reference model are documented in the copyright notice and scope of this document.

> *[ISO/IEC 33004, 5.3.2]*

The process descriptions are unique. The identification is provided by unique names and by the identifier of each process of this document.

> *[ISO/IEC 33004, 5.3.3]*

Clause 5.4: Process descriptions

These requirements are met by the process descriptions in Chapter 2 of this document.

> *[ISO/IEC 33004, 5.4]*

A.3 Conformity to the requirements for process assessment models

Clause 6.1: "Introduction"

The purpose of this process assessment model is to support assessment of process capability within the automotive domain using the process measurement framework defined in ISO/IEC 33020:2015.

> *[ISO/IEC 33004, 6.1]*

Clause 6.2: "Process assessment model scope"

The process scope of this process assessment model is defined in the process reference model included in subchapter 3.1 of this document. The Automotive SPICE Process Reference Model satisfies the requirements of ISO/IEC 33004, clause 5 as described in Annex A.2.

The process capability scope of this process assessment model is defined in the process measurement framework specified in ISO/IEC 33020:2015, which defines a process measurement framework for process capability satisfying the requirements of ISO/IEC 33003.

> *[ISO/IEC 33004, 6.2]*

<u>**Clause 6.3: "Requirements for process assessment models"**</u>

The Automotive SPICE Process Assessment Model is related to process capability.

> *[ISO/IEC 33004, 6.3.1]*

This process assessment model incorporates the process measurement framework specified in ISO/IEC 33020:2015, which satisfies the requirements of ISO/IEC 33003.

> *[ISO/IEC 33004, 6.3.2]*

This process assessment model is based on the Automotive SPICE Reference Model included in this document.

This process assessment model is based on the measurement framework defined in ISO/IEC 33020:2015.

> *[ISO/IEC 33004, 6.3.3]*

The processes included in this process assessment model are identical to those specified in the process reference model.

> *[ISO/IEC 33004, 6.3.4]*

For all processes in this process assessment model all levels defined in the process measurement framework from ISO/IEC 33020:2015 are addressed.

> *[ISO/IEC 33004, 6.3.5]*

This process assessment model defines

- the selected process quality characteristic,
- the selected process measurement framework,
- the selected process reference model(s), and
- the selected processes from the process reference model(s)

in Chapter 3 of this document.

> *[ISO/IEC 33004, 6.3.5 a-d]*

In the capability dimension, this process assessment model addresses all of the process attributes and capability levels defined in the process measurement framework in ISO/IEC 33020:2015.

> *[ISO/IEC 33004, 6.3.5 e]*

Clause 6.3.1: "Assessment indicators"

NOTE: Due to an error in numbering in the published version of ISO/IEC 33004, the following reference numbers are redundant to those stated above. To refer to the correct clauses from ISO/IEC 33004, the text of the clause heading is additionally specified for the following three requirements.

The Automotive SPICE Process Assessment Model provides a two-dimensional view of process capability for the processes in the process reference model, through the inclusion of assessment indicators as defined in subchapter 3.3. The assessment indicators used are:

- Base practices and output work products

> *[ISO/IEC 33004, 6.3.1 a: "Assessment indicators"]*

- Generic practices and Generic resources

> *[ISO/IEC 33004, 6.3.1 b: "Assessment indicators"]*

Clause 6.3.2: "Mapping process assessment models to process reference models"

The mapping of the assessment indicators to the purpose and process outcomes of the processes in the process reference model is included in each description of the base practices in Chapter 4.

The mapping of the assessment indicators to the process attributes in the process measurement framework including all of the process attribute achievements is included in each description of the generic practices in Chapter 5.

Each mapping is indicated by a reference in square brackets.

> *[ISO/IEC 33004, 6.3.2: "Mapping process assessment models"]*

Clause 6.3.3: "Expression of assessment results"

The process attributes and the process attribute ratings in this process assessment model are identical to those defined in the measurement framework. As a consequence, results of assessments based upon this process assessment model are expressed directly as a set of process attribute ratings for each process within the scope of the assessment. No form of translation or conversion is required.

[ISO/IEC 33004, 6.3.3: "Expression of assessment results"]

Annex B Work Product Characteristics

Work product characteristics listing interface agreement should include definitions regarding:

a) Customer and supplier stakeholder and contacts
b) Tailoring agreements
c) Customer/supplier responsibilities (e.g., roles, RASIC chart) for distributive activities, including required actions in development and post-development
d) Share of information/work products in case of issues (e.g., vulnerabilities, findings, risks)
e) Agreed customer/supplier milestones

The duration of the supplier's support and maintenance in this annex can be used when reviewing potential outputs of process implementation. The characteristics are provided as guidance regarding the attributes that should be looked for in a particular sample work product in order to provide objective evidence supporting the assessment of a particular process.

A documented process and assessor judgment is needed to ensure that the process context (application domain, business purpose, development methodology, size of the organization, etc.) is considered when using this information.

Work products are defined using the schema in Table B.1. Work products and their characteristics should be considered as a starting point for considering whether, given the context, they are contributing to the intended purpose of the process and not as a checklist of what every organization must have.

Table B.1 — Structure of WPC Tables

Work product identifier	An identifier number for the work product used to reference the work product.
Work product name	Provides an example of a typical name associated with the work product characteristics. This name is furnished as an identifier of the type of work product the practice or process might produce. Organizations may call these work products by different names. The name of the work product in the organization is not significant. Similarly, organizations may have several equivalent work products that contain the characteristics defined in one work product type. The formats for the work products can vary. It is up to the assessor and the organizational unit coordinator to map the actual work products produced in their organization to the examples given here.
Work product characteristics	Provides examples of the potential characteristics associated with the work product types. The assessor may look for these in the samples supplied by the organizational unit.

Work products (with the ID NN-00) are sets of characteristics that would be expected to be evident in work products of generic types as a result of achievement of an attribute. The generic work products form the basis for the classification of specific work products defined as process performance indicators.

Specific work product types are typically created by process owners and applied by process deployers in order to satisfy an outcome of a particular process purpose.

*NOTE: The generic work products denoted with * are not used in the Automotive SPICE Process Assessment Model but are included for completeness.*

Table B.2 — Work Product Characteristics

[For the review this table contains only the relevant work product characteristics for the SEC-PAM]

WP ID	WP Name	WP Characteristics
02-00	Contract	• Defines what is to be purchased or delivered • Identifies time frame for delivery or contracted service dates • Identifies any statutory requirements • Identifies monetary considerations • Identifies any warranty information • Identifies any copyright and licensing information • Identifies any customer service requirements • Identifies service level requirements • References to any performance and quality expectations/constraints/monitoring • Standards and procedures to be used • Evidence of review and approval • As appropriate to the contract the following are considered: - references to any acceptance criteria - references to any special customer needs (i.e., confidentiality requirements, security, hardware, etc.) - references to any change management and problem resolution procedures - identification of any interfaces to independent agents and subcontractors - identification of customer's role in the development and maintenance process - identification of resources to be provided by the customer
02-01	Commitment/ agreement	• Signed off by all parties involved in the commitment/agreement • Establishes what the commitment is for

WP ID	WP Name	WP Characteristics
		• Establishes the resources required to fulfill the commitment, such as: - time - people - budget - equipment - facilities
02-50	Interface agreement	• Interface agreement should include definitions regarding - customer and supplier stakeholder and contacts - tailoring agreements - customer/supplier responsibilities (e.g., roles, RASIC chart) for distributive activities, including required actions in development and post-development - share of information/work products in case of issues (e.g., vulnerabilities, findings, risks) - agreed customer/supplier milestones - duration of supplier's support and maintenance
04-04	Software architectural design	• Describes the overall software structure • Describes the operative system including task structure • Identifies inter-task/inter-process communication • Identifies the required software elements • Identifies own developed and supplied code • Identifies the relationship and dependency between software elements • Identifies where the data (e.g., application parameters or variables) are stored and which measures (e.g., checksums, redundancy) are taken to prevent data corruption • Describes how variants for different model series or configurations are derived

WP ID	WP Name	WP Characteristics
		• Describes the dynamic behavior of the software (start-up, shutdown, software update, error handling and recovery, etc.) • Describes which data is persistent and under which conditions • Consideration is given to: - any required software performance characteristics - any required software interfaces - any required security characteristics required - any database design requirements
04-05	Software detailed design	• Provides detailed design (could be represented as a prototype, flow chart, entity relationship diagram, pseudo code, etc.) • Provides format of input/output data • Provides specification of CPU, ROM, RAM, EEPROM and Flash needs • Describes the interrupts with their priorities • Describes the tasks with cycle time and priority • Establishes required data naming conventions • Defines the format of required data structures • Defines the data fields and purpose of each required data element • Provides the specifications of the program structure
04-06	System architectural design	• Provides an overview of all system design • Describes the interrelationship between system elements • Describes the relationship between the system elements and the software • Specifies the design for each required system element, consideration is given to aspects such as: - memory/capacity requirements - hardware interface requirements

WP ID	WP Name	WP Characteristics
		- user interface requirements - external system interface requirements - performance requirements - command structures - security/data protection characteristics - settings for system parameters (such as application parameters or global variables) - manual operations - reusable components • Mapping of requirements to system elements • Description of the operation modes of the system components (startup, shutdown, sleep mode, diagnosis mode, etc.) • Description of the dependencies among the system components regarding the operation modes • Description of the dynamic behavior of the system and the system components
08-14	Recovery plan	• Identifies what is to be recovered: - procedures/methods to perform the recovery - schedule for recovery - time required for the recovery - critical dependencies - resources required for the recovery - list of backups maintained - staff responsible for recovery and roles assigned - special materials required - required work products - required equipment - required documentation - locations and storage of backups - contact information on who to notify about the recovery - verification procedures

WP ID	WP Name	WP Characteristics
		- cost estimation for recovery
08-20	Risk mitigation plan	• Planned risk treatment activities and tasks: - describes the specifics of the risk treatment selected for a risk or combination of risks found to be unacceptable - describes any difficulties that may be found in implementing the treatment • Treatment schedule • Treatment resources and their allocation • Responsibilities and authority: - describes who is responsible for ensuring that the treatment is being implemented and their authority • Treatment control measures: - defines the measures that will be used to evaluate the effectiveness of the risk treatment • Treatment cost • Interfaces among parties involved: - describes any coordination among stakeholders or with the project's master plan that must occur for the treatment to be properly implemented • Environment/infrastructure: - describes any environmental or infrastructure requirements or impacts (e.g., safety or security impacts that the treatment may have) • Risk treatment plan change procedures and history
08-50	Test specification	• Test Design Specification • Test Case Specification • Test Procedure Specification • Identification of test cases for regression testing

WP ID	WP Name	WP Characteristics
		• Additionally, for system integration: - identification of required system elements (hardware elements, wiring elements, settings for parameters (such as application parameters or global variables), databases, etc.) - necessary sequence or ordering identified for integrating the system elements
08-52	Test plan	• Test Plan according to ISO29119-3 • Context: - project/Test sub-process - test item(s) - test scope - assumptions and constraints - stakeholder - testing communication • Test strategy - identifies what needs are to be satisfied - establishes the options and approach for satisfying the needs (black-box and/or white-box testing, boundary class test determination, regression testing strategy, etc.) - establishes the evaluation criteria against which the strategic options are evaluated - identifies any constraints/risks and how these will be addressed - test design techniques - test completion criteria - test ending criteria - test start, abort and re-start criteria - metrics to be collected - test data requirements - retesting and regression testing - suspension and resumption criteria

WP ID	WP Name	WP Characteristics
		- deviations from the Organizational Test Strategy • Test data requirements • Test environment requirements • Test sub-processes • Test deliverables • Testing activities and estimates
11-05	Software unit	• Follows established coding standards (as appropriate to the language and application): - commented - structured or optimized - meaningful naming conventions - parameter information identified - error codes defined - error messages descriptive and meaningful - formatting – indented, levels • Follows data definition standards (as appropriate for the language and application): - variables defined - data types defined - classes and inheritance structures defined - objects defined • Entity relationships defined • Database layouts are defined • File structures and blocking are defined • Data structures are defined • Algorithms are defined • Functional interfaces defined
12-01	Request for quotation	• Reference to the requirements specifications • Identifies supplier selection criteria • Identifies desired characteristics, such as: - system architecture, configuration requirements or the requirements for service (consultants, maintenance, etc.)

WP ID	WP Name	WP Characteristics
		- quality criteria or requirements - project schedule requirements - expected delivery/service dates - cost/price expectations - regulatory standards/requirements • Identifies submission constraints: - date for resubmission of the response - requirements with regard to the format of response
13-01	Acceptance record	• Record of the receipt of the delivery • Identification of the date received • Identification of the delivered components • Records the verification of any customer acceptance criteria defined • Signed by receiving customer
13-04	Communication record	• All forms of interpersonal communication, including: - letters - faxes - emails - voice recordings - podcast - blog - videos - forum - live chat - wikis - photo protocol - meeting support record
13-14	Progress status record	• Record of the status of a plan(s) (actual against planned), e.g.: - status of actual tasks against planned tasks - status of actual results against established objectives/goals

WP ID	WP Name	WP Characteristics
		- status of actual resources allocation against planned resources - status of actual cost against budget estimates - status of actual time against planned schedule - status of actual quality against planned quality • Record of any deviations from planned activities and reason why
13-16	Change request	• Identifies purpose of change • Identifies request status (e.g., open, allocated, implemented, closed) • Identifies requester contact information • Impacted system(s) • Impact to operations of existing system(s) defined • Impact to associated documentation defined • Criticality of the request, due date
13-19	Review record	• Provides the context information about the review: - what was reviewed - lists reviewers who attended - status of the review • Provides information about the coverage of the review: - checklists - review criteria - requirements - compliance to standards • Records information about: - the readiness for the review - preparation time spent for the review - time spent in the review

WP ID	WP Name	WP Characteristics
		- reviewers, roles and expertise • Review findings: - non-conformities - improvement suggestions • Identifies the required corrective actions: - risk identification - prioritized list of deviations and problems discovered - the actions, tasks to be performed to fix the problem - ownership for corrective action - status and target closure dates for identified problems
13-20	Risk action request	• Date of initiation • Scope • Subject • Request originator • Risk management process context: - this section may be provided once, and then referenced in subsequent action requests if no changes have occurred - process scope - stakeholder perspective - risk categories - risk thresholds - project objectives - project assumptions - project constraints • Risks: - this section may cover one risk or many, as the user chooses - where all the information above applies to the whole set of risks, one action request may suffice - where the information varies, each request

WP ID	WP Name	WP Characteristics
		may cover the risk or risks that share common information - risk description(s) - risk probability - risk value - risk consequences - expected timing of risk • Risk treatment alternatives: - Treatment option selected-avoid/reduce/transfer - alternative descriptions - recommended alternative(s) - justifications • Risk action request disposition: - each request should be annotated as to whether it is accepted, rejected or modified, and the rationale provided for whichever decision is taken
13-22	Traceability record	• All requirements (customer and internal) are to be traced • Identifies a mapping of requirement to lifecycle work products • Provides the linkage of requirements to work product decomposition (i.e., requirement, design, coding, testing, deliverables, etc.) • Provides forward and backwards mapping of requirements to associated work products throughout all phases of the lifecycle *NOTE: this may be included as a function of another defined work product (Example: A CASE tool for design decomposition may have a mapping ability as part of its features)*
13-24	Validation results	• Validation checklist • Passed items of validation

WP ID	WP Name	WP Characteristics
		• Failed items of validation • Pending items of validation • Problems identified during validation • Risk analysis • Recommendation of actions • Conclusions of validation • Signature of validation
13-25	Verification results	• Verification checklist • Passed items of verification • Failed items of verification • Pending items of verification • Problems identified during verification • Risk analysis • Recommendation of actions • Conclusions of verification • Signature of verification
13-50	Test result	• Level Test Log • Anomaly Report • Level Test Report (Summary) - test cases not passed - test cases not executed - information about the test execution (date, tester name etc.) Additionally where necessary: • Level Interim Test Status Report • Master Test Report (Summary)
14-02	Corrective action register	• Identifies the initial problem • Identifies the ownership for completion of defined action • Defines a solution (series of actions to fix problem) • Identifies the open date and target closure date • Contains a status indicator • Indicates follow up audit actions

WP ID	WP Name	WP Characteristics
14-05	Preferred suppliers register	• Subcontractor or supplier history • List of potential subcontractor/suppliers • Qualification information • Identification of their qualifications • Past history information when it exists
14-08	Tracking system	• Ability to record customer and process owner information • Ability to record related system configuration information • Ability to record information about problem or action needed: - date opened and target closure date - severity/criticality of item - status of any problem or actions needed - information about the problem or action owner - priority of problem resolution • Ability to record proposed resolution or action plan • Ability to provide management status information • Information is available to all with a need to know • Integrated change control system(s)/records
14-51	Cybersecurity scenario register	• Identifies: - Damage scenarios ○ ID ○ Title ○ Description ○ Impact category ▪ Safety ▪ Financial ▪ Operational ▪ Privacy ▪ Quality - Threat scenarios ○ ID

WP ID	WP Name	WP Characteristics
		○ Asset concerned ○ Security property ▪ Confidentiality ▪ Integrity ▪ Availability ○ Attack feasibility (high/medium/low/very low)
14-52	Asset library	• Identifies - title - description - security properties ○ Confidentiality ○ Integrity ○ Availability - stakeholders related to the asset
15-01	Analysis report	• What was analyzed? • Who did the analysis? • The analysis criteria used: - selection criteria or prioritization scheme used - decision criteria - quality criteria • Records the results: - what was decided/selected - reason for the selection - assumptions made - potential risks • Aspects of correctness to analyze include: - completeness - understandability - testability - verifiability - feasibility - validity

WP ID	WP Name	WP Characteristics
		- consistency - adequacy of content
15-08	Risk analysis report	• Identifies the risks analyzed - ID - impact scenario (e.g., damage scenario) • Records the results of the analysis: - potential ways to mitigate the risk - selected risk treatment option - assumptions made - probability of occurrence (e.g., attack feasibility) - risk value - constraints
15-09	Risk status report	• Identifies the status of an identified risk: - related project or activity - risk statement - condition - consequence - changes in priority - duration of mitigation, when started - risk mitigation activities in progress - responsibility - constraints
15-21	Supplier evaluation report	• States the purpose of evaluation • Method and instrument (checklist, tool) used for evaluation • Requirements used for the evaluation • Assumptions and limitations • Identifies the context and scope information required (e.g., date of evaluation, parties involved) • Fulfillment of evaluation requirements
15-50	Vulnerability analysis report	• Identifies - ID

WP ID	WP Name	WP Characteristics
		- Description - Attack path concerned - Attack feasibility (e.g., CVSS rating (Common Vulnerability Scoring System)
17-11	Software requirements specification	• Includes functional and non-functional cybersecurity software requirements • Associated to one or more cybersecurity goal • Cybersecurity requirements are recognizable and categorized as such
17-12	System requirements specification	• Includes functional and non-functional cybersecurity system requirements • Associated to one or more cybersecurity goal • Cybersecurity requirements are recognizable and categorized as such
17-51	Cybersecurity goals	• Describe a property of an asset, that is necessary to guarantee cybersecurity • Associated to one or more threat scenarios
17-52	Cybersecurity controls	• Technical solutions to avoid, detect, counteract, or minimize cybersecurity risks • Associated to one or more cybersecurity requirement
18-50	Supplier evaluation criteria	• Expectations for conformity, to be fulfilled by competent suppliers • Links from the expectations to national/international/domains-specific standards/laws/regulations • Requirements conformity evidence to be provided by the potential suppliers or assessed by the acquiring organization • Provisions for tailoring or exception to the requirements
19-10	Verification strategy	• Verification methods, techniques, and tools • Work product or processes under verification • Degrees of independence for verification

WP ID	WP Name	WP Characteristics
		• Schedule for performing the above activities • Identifies what needs there are to be satisfied • Establishes the options and approach for satisfying the need • Establishes the evaluation criteria against which the strategic options are evaluated • Identifies any constraints/risks and how these will be addressed • Verification ending criteria • Verification start, abort and restart criteria
19-11	Validation strategy	• Validation methods, techniques, and tools • Work products under validation • Degrees of independence for validation • Schedule for performing the above activities • Identifies what needs there are to be satisfied • Establishes the options and approach for satisfying the need • Establishes the evaluation criteria against which the strategic options are evaluated • Identifies any constraints/risks and how these will be addressed

Annex C Terminology

Automotive SPICE follows the following precedence for use of terminology:

a) ISO/IEC 33001 for assessment-related terminology

b) ISO/IEC/IEEE 24765 and ISO/IEC/IEEE 29119 terminology (as contained in Annex C)

c) Terms introduced by Automotive SPICE (as contained in Annex C)

d) ISO/IEC/SAE 21434 for cybersecurity-related terminology

Annex C lists the applicable terminology references from ISO/IEC/IEEE 24765 and ISO/IEC/IEEE 29119. It also provides terms which are specifically defined within Automotive SPICE. Some of these definitions are based on ISO/IEC/IEEE 24765.

Table C.1 — Terminology

Term	Origin	Description
Acceptance testing	ISO/IEC/IEEE 24765	Formal testing conducted to enable a user, customer, or authorized entity to determine whether to accept a system or component.
Application parameter	Automotive SPICE V3.1	An application parameter is a parameter containing data applied to the system or software functions, behavior or properties. The notion of application parameter is expressed in two ways: firstly, the logical specification (including name, description, unit, value domain or threshold values or characteristic curves, respectively) and secondly, the actual quantitative data value it receives by means of data application.

Architecture element	Automotive SPICE V3.1	Result of the decomposition of the architecture on system and software level: • The system is decomposed into elements of the system architecture across appropriate hierarchical levels. • The software is decomposed into elements of the software architecture across appropriate hierarchical levels down to the software components (the lowest level elements of the software architecture).
Baseline	ISO/IEC/IEEE 24765	A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and can only be changed through formal change control procedures.
Black-box testing	Automotive SPICE V3.1	Method of requirement testing where tests are developed without knowledge of the internal structure and mechanisms of the tested item.
Code review	Automotive SPICE V3.1	A check of the code by one or more qualified persons to determine its suitability for its intended use and identify discrepancies from specifications and standards.
Coding	ISO/IEC/IEEE 24765	The transforming of logic and data from design specifications (design descriptions) into programming language.
Consistency	Automotive SPICE V3.1	Consistency addresses content and semantics and ensures that work

		products are not in contradiction to each other. Consistency is supported by bidirectional traceability.
Defect		→ [FAULT]
Dynamic analysis	ISO/IEC/IEEE 24765	A process of evaluating a system or component based on its behavior during execution.
Element	Automotive SPICE V3.1	Elements are all structural objects on architectural and design level on the left side of the "V". Such elements can be further decomposed into more fine-grained sub-elements of the architecture or design across appropriate hierarchical levels.
Error	ISO/IEC/IEEE 24765	The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.
Fault	ISO/IEC/IEEE 24765	A manifestation of an error in software.
Functional requirement	ISO/IEC/IEEE 24765	A statement that identifies what a product or process must accomplish to produce required behavior and/or results.
Functional specification	ISO/IEC/IEEE 24765	A document that specifies the functions that a system or component must perform. Often part of a requirements specification.
Functional testing	ISO/IEC/IEEE 24765	Testing conducted to evaluate the compliance of a system or component with specified functional requirements.

Hardware	ISO/IEC/IEEE 24765	Physical equipment used to process, store, or transmit computer programs or data.
Hardware item	Automotive SPICE V3.1	A physical representation of a hardware element.
Integration	Automotive SPICE V3.1	A process of combining items to larger items up to an overall system.
Integrated software item	Automotive SPICE V3.1	A set of software units or items that are integrated into a larger assembly for the purpose of integration testing.
Integration testing	Automotive SPICE V3.1	Testing in which items (software items, hardware items, or system items) are combined and tested to evaluate the interaction among them.
Integrated system item	Automotive SPICE V3.1	A set of items that are integrated into a larger assembly for the purpose of integration testing.
Quality assurance	ISO/IEC/IEEE 24765	A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements.
Regression testing	Automotive SPICE V3.1	Selective retesting of a system or item to verify that modifications have not caused unintended effects and that the system or item still complies with its specified requirements.
Requirement	Automotive SPICE V3.1	A property or capability that must be achieved or possessed by a system, system item, product or service to satisfy a contract, standard, specification or other formally imposed documents.

Requirements specification	Automotive SPICE V3.1	A document that specifies the requirements for a system or item. Typically included are functional requirements, performance requirements, interface requirements, design requirements, and development standards.
Software	ISO/IEC/IEEE 24765	Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system.
Software component	Automotive SPICE V3.1	In Automotive SPICE V3.1 the term "software component" is used for the lowest level elements of the software architecture for which finally the detailed design is defined. A software "component" consists of one or more software "units". → [ARCHITECTURE ELEMENT], [UNIT]
Software element		→ [ARCHITECTURE ELEMENT]
Software item	ISO/IEC/IEEE 24765	Identifiable part of a software product.
Software unit		→ [UNIT]
Static analysis	Automotive SPICE V3.1	A process of evaluating an item based on its form, structure, content or documentation.
System	Automotive SPICE V3.1	A collection of interacting items organized to accomplish a specific function or set of functions within a specific environment.
System item	Automotive SPICE V3.1	Identifiable part of the system.

System test	ISO/IEC/IEEE 24765	Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements.
Testing	Automotive SPICE V3.1	Activity in which an item (system, hardware, or software) is executed under specific conditions; and the results are recorded, summarized and communicated.
Traceability	ISO/IEC/IEEE 24765	The degree to which a relationship can be established between two or more products of the development process, especially products having a predecessor-successor or master-subordinate relationship to one another.
Unit	Automotive SPICE V3.1	Part of a software component which is not further subdivided. → [SOFTWARE COMPONENT]
Unit test	Automotive SPICE V3.1	The testing of individual software units or a set of combined software units.
Validation	ISO/IEC/IEEE 29119	Validation demonstrates that the work item can be used by the users for their specific tasks.
Verification	ISO/IEC/IEEE 29119	Verification is confirmation, through the provision of objective evidence, that specified requirements have been fulfilled in a given work item.
White-box testing	Automotive SPICE V3.1	Method of testing where tests are developed based on the knowledge of the internal structure and mechanisms of the tested item.

Table C.2 — Abbreviations

AS	**A**utomotive **SPICE**
BP	**B**ase **P**ractice
CAN	**C**ontroller **A**rea **N**etwork
CASE	**C**omputer-**A**ided **S**oftware **E**ngineering,
CCB	**C**hange **C**ontrol **B**oard
CFP	**C**all **F**or **P**roposals
CPU	**C**entral **P**rocessing **U**nit
ECU	**E**lectronic **C**ontrol **U**nit
EEPROM	**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory
GP	**G**eneric **P**ractice
GR	**G**eneric **R**esource
IEC	**I**nternational **E**lectrotechnical **C**ommission
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
I/O	**I**nput/**O**utput
ISO	**I**nternational **O**rganization for **S**tandardization
ITT	**I**nvitation **T**o **T**ender
LIN	**L**ocal **I**nterconnect **N**etwork
MISRA	**M**otor **I**ndustry **S**oftware **R**eliability **A**ssociation
MOST	**M**edia **O**riented **S**ystems **T**ransport
PA	**P**rocess **A**ttribute
PAM	**P**rocess **A**ssessment **M**odel
PRM	**P**rocess **R**eference **M**odel
PWM	**P**ulse **W**idth **M**odulation
RAM	**R**andom **A**ccess **M**emory
ROM	**R**ead **O**nly **M**emory
SPICE	**S**oftware **P**rocess **I**mprovement and **C**apability d**E**termination
SUG	**S**pice **U**ser **G**roup
USB	**U**niversal **S**erial **B**us
WP	**W**ork **P**roduct
WPC	**W**ork **P**roduct **C**haracteristic

Annex D Homologation-Relevant Rating

The homologation relevant rating guideline provides the necessary requirements and rules for the cybersecurity homologation-relevant rating of an Automotive Cybersecurity SPICE assessment. It defines a schema which enables an assessor to determine the rating result on basis of a capability profile of an executed Automotive Cybersecurity SPICE assessment.

To enable the rating, the capability profile of an Automotive SPICE assessment has to be available for the SEC Scope and the VDA Scope. The SEC Scope contains MAN.7, SEC.1 – SEC.4 and in case of cybersecurity relevant suppliers also ACQ.2 and ACQ.4. The Assessment of the SEC scope and VDA scope can be split.

Meaning of Homologation-Relevant Rating:

Automotive Cybersecurity SPICE Assessment: **PASSED**

Identified gaps have low process-related quality risk and VDA scope processes are performed.

SEC processes are fully performed and corresponding work products managed.

Automotive Cybersecurity SPICE Assessment: **PASSED WITH CONDITIONS**

Identified gaps have low process-related quality risk. VDA scope processes are performed.

SEC processes are performed and corresponding work products managed.

Improvement measures are agreed between lead assessor and assessed organization at the end of the Automotive Cybersecurity Assessment to close the corresponding gaps within an appropriate time frame.

Automotive Cybersecurity SPICE Assessment: **NOT PASSED**
Applies in case “passed” and “passed with conditions” is not achieved.

The homologation relevant rating is done according to the following table:

Assessment Scope		**Homologation Recommendation**
VDA Scope	SEC Scope	
Target Level >= 1	Target Level 2	**PASSED, if** VDA Scope: all PA 1.1 minimum Largely & all engineering PA 2.2 minimum Largely SEC Scope: all PA 1.1 Fully & PA2.2 minimum Largely
		PASSED WITH CONDITIONS, if VDA Scope: all PA 1.1 minimum Largely SEC Scope: all PA 1.1 minimum Largely & PA2.2 minimum Largely
		Or else **NOT PASSED**