LGE Internal Use Only

VS CSMS Standard

Standard	VS CSMS Standard
Standard No.	LG(46)-A-5013
Enactment date	4 Mar. 2021
Revision date	5 Mar. 2024
Revision No.	3
Version	v 3.0
Approver	Cyber Security Chief Officer
Management Department	Cyber Security Governance Unit

History

Revision	Date	Description	Author	Approver
v1.0	2021.03.02	Initial version CSMS standard process of Vehicle component Solutions Company	CSMS Task	Head of Vehicle component Solutions Company
V1.1	2021.05.10	Add processes for the Organizational Cybersecurity Management Modify the definition of some roles Move the process for the cybersecurity audit	VS Cyber Security Risk Management Team	CyberSecurity Governance Officer (CSGO)
V1.2	2022.09.08	Modify and Add processes based on the TuV pre-Audit Open Items	VS Cyber Security Governance Unit	-
V1.3	2022.09.30	Modify and Add processes(Chapter1) based on the TuV pre-Audit Open Items	VS Cyber Security Governance Unit	
V1.4	2022.11.18	• Delete the Cybersecurity Assessor from Responsibility / authority by role and management department • Add “A” in PA 1-14. and PA 1-15 • Modify 5.5 Reuse Analysis • [#11] Added acknowledgment to RASIC table for each step. • The definition of Assessor in 4pgae has been replaced by Assessor on page 5. Assessor on page 4 has been deleted. • [#15] Reuse-related items listed in ISO 21434 have been added to the Process document. We also created a reuse analysis report. • [#9_New] Yes no has been added to 1-2, 1-12~14, 5-12~14, and 6-6. • [#15_New] In process document 6-3, "If OEMs are not responsible for reviewing cybersecurity case cybersecurity case is reviewed internally by assessor." I added text and indicated the contents in the diagram. • [#3] Added HW DEV/HWA/HWQT Manager to pages 3-5(Responsibility / authority by role and management department). • [#3] Added HW Test to page 10 (VS CSMS activity summary). • [#3]Added HW Cybersecurity Verification to pages 11 and 12 (VS CSMS activity definition, Relation between LGE SW Development Standard Process and VS CSMS Standard).	VS Cyber Security Governance Unit	

History

Revision	Date	Description	Author	Approver
V1.4	2022.11.18	[#3]Added and modified HW Test to pages 58~69 (Cybersecurity HW Development Phase). [#4] Cal rating-related URL has been added to page 22(CAL Rating) of the process document, and the content in the URL will be submitted as a PDF(CAL_Rating.pdf). [#5] Points related to CSMS Assessemt have been updated on page 103(Cybersecurity Assessment (2/3)). The contents of the URL will be shown as a PDF(CSMS Assessment.pdf). [#26] On page 22(CAL Rating), it was added that CAL Rating is set as the overall requirements. [#new_13] Modified to CSM on page 118(Production Control Plan). [#7] Modifying Guideline 4 in CSMS standard document. (G4.) 1) Delete the Escalation process for "common cybersecurity issues" slide of the existing OIL1 version 2) Create Management of cybersecurity issue menu in Guideline 3) Instead of 1), adding the types of CS issues and classification criteria (general Cybersecurity related issues and Critical Cybersecurity incident issues) 4) Adding the escalation mechanism and management process of 3) 5) Attached the collab page document mentioned in the description as pdf 7_02. Cybersecurity Monitoring Guideline.pdf 7_20. Incident Response Management_Process.pdf 7_Incident response & TARA.pdf 7_Cybersecurity_IR_VLM.JPG [#10] PA 7-5, Adding the mention of LGE Tool Management Report (1) input file/ 2) output file / 3)firtst dot in Description in detail) The contents of LGE Tool Management Report and http://collab.lge.com/main/x/f21-Sg are the same, and by adding Vulnerability result and Tool Review Result column for Tool, evaluate the securedness of the tool. (The actual contents of the tool are internal information, so they are not filled out separately, only the management form is attached). 10_LGE_Tool_Management_Report.xlsx [#new_11] PA. 1-11, Added the link to TARA's Guide collab page Extracted http://collab.lge.com/main/x/OSdgXg as a attached file new11_TARA Guideline.pdf	VS Cyber Security Governance Unit	

History

Revision	Date	Description	Author	Approver
V1.4	2022.11.18	[♯new_12] In PA 1-7/PA 1-8/PA 1-9 /PA 1-10 , adding link of the collab site link about TARA Rating criteria & Risk Matrix. http://collab.lge.com/main/x/ETg3Tw link is extracted&attached as a file new12_TARA Rating criteria & VS Risk Matrix.pdf [♯16] Out-of-Context related items listed in ISO 21434 have been added to the Process document. We also created a Out-of-Context Validation report. See Templates [♯17] Off-the-Shelf related items listed in ISO 21434 have been added to the Process document. We also created a Off-the-Shelf Analysis report. See Templates [♯19] No process document update. See Templates [♯20] An independence related Post-development was defined in the Process document. We also updated a post-development report . See Templates [♯21] Chapter6 was changed so that it covers all product life cycle from development to production and maintenance (The first 6 pages of CH6) [♯27, ♯30] Risk assessment, treatment and tracing of managed vulnerabilities have been added with related links (PA 4-11, PA 6-7) [♯28] Description for test coverage has been added to CS SW integration test (PA 4-8) [♯35] This phrase is added in chapter 2-10(system) Penetration Test The phase is like "Penetration test is conducted by referring to the Vulnerability test plan document (LGE_Penetration_TestPlan)" You can also refer to detail process in "LGE_Penetration_TestPlan.pdf" [♯35]This phrase is added in chapter 2-13.Fuzz Test.The phase is like "Fuzz test is conducted by referring to the Vulnerability test plan document (Vulnerability_Fuzz Test Plan)" You can also refer to detail process in "Vulnerability_Fuzz Test Plan.pdf" [♯4] PA 5-2, Supplier Evaluation Check List is added in Output	VS Cyber Security Governance Unit	
V1.5	2022.12.22	Modify and Add processes based on the TuV pre-Audit 3rd Open Items	VS Cyber Security Governance Unit	
V2.0	2023.01.11	Granted CSMS TuV Certification Passed 2022 Internal Audit To improve TuV Open Items and Internal Audit Findings Microsoft Word ¹®¼	VS Cyber Security Governance Unit	Cyber Security Governance Officer

History

Revision	Date	Description	Author	Approver
V2.1	2023.03.31	Adjust and reflect roles as requested by VS Development Quality Assurance Department	VS Cyber Security Governance Unit	
V2.2	2023.05.19	Release for the work of internal audit preparation	VS Cyber Security Governance Unit	
V3.0	2024.03.05	▪ Responsibility / authority by role and management department CSVTM, IRM content revised and CSEG added (p. 8, 9) ▪ Changed and added Term and Abbreviation (p. 12) ▪ Modify Location in guidance & Template links and pictures (p. 20) ▪ Modify Location in assessment guide/items & ISO 21434 Checklist picture (p. 21) ▪ Modify Related ISO/SAE 21434 standard for cybersecurity concept definition Option (p. 24, 25) ▪ Redefine Activities to Define CALs by Security Requirements (p. 44, 50, 51, 52, 70, 71, 72, 85, 86, 87, 90) ▪ Modify 2.System Development Phase, 3.HW Development Phase, 4.SW Development Phase, 5.Management & Supporting RASIC(p. 47, 48, 67, 68, 82, 83, 101, 102) - http://vlm.lge.com/issue/browse/LGCSAUDIT-105 ▪ Modify PA 4-11 the Cybersecurity Vulnerability Test link (p. 95) ▪ Modify PA 6-1 Production Control Plan (p. 126) ▪ Modify PA 6-4 Cybersecurity Information monitoring (p. 129) ▪ Modify PA 6-5 Initial Vulnerability analysis (p. 130) ▪ Modify PA 6-6 Triggers Incident Response (p. 131) ▪ Modify PA 6-7 Detailed incident analysis (p. 132) ▪ Modify PA 6-8 Prepare incident countermeasure (p. 133) ▪ Modify PA 6-9 Post-Incident Response Activities (p. 134)	VS Cyber Security Governance Unit	Cyber Security Governance Officer

History

Revision	Date	Description	Author	Approver
V3.0	2024.03.05	▪ Modify Collab links (p. 134, 151) ▪ Modify PA6-10 Emergency Incident Response (p. 135) ▪ Modify PA6-11 SW update for products in development (p. 136) ▪ Modify PA7-5 Tool Management (p. 144) ▪ Updated PA7-6 Information Security Management(p. 145) ▪ Modify G4. Management of cybersecurity issues (p. 153, 154, 155, 156)	VS Cyber Security Governance Unit	Cyber Security Governance Officer

Related standard

- VS CSMS standard defines the activities necessary to develop cybersecurity items based on the following standard documents.

Standard name	Revision	Enactment date	Author
ISO/SAE 21434 (Road vehicles - Cybersecurity engineering)	v 1.0	2021.08	INTERNATIONAL STANDARD
[LG(10)-A-9117] LGE SW Product Security Activities (LG-SDL) Standard	v 3.5	2021.03.08	Software Center Software Engineering R&D Lab. SW Security Task
LG(35)-A-5907] Smart Division SW Development Standard Process Regulation	V 2.2	2020-05-11	VS Smart SW Development Division SW Process Unit
[LG(10)-A-5012] LGE Regulation of the SW Development Standard Process	v 10.0	2021-02-18	Quality Management Center SW Development Quality Evaluation Task
LGE VS One Q Process	-	2021-02-01	VS One Q Standard Process Task

VS CSMS standard application

- VS CSMS standard is applied to cybersecurity items following LG Electronics' VS Smart product development process since June, `21.
- CSMS VTA (Vehicle Type Approval) Projects are subject to VS CSMS standard.
- CAL (Cybersecurity Assurance Level) within 1 to 4 is assigned to CSMS VTA Project

Responsibility / authority by role and management department (1/4)

Role	Abbreviation	Responsibility & authority	Management department
Cybersecurity Governance Manager	CSGM	Cybersecurity Policy & Process Establishment Cybersecurity Training & Culture Establishment Cybersecurity Strategy	Cyber Security Governance Unit
Cybersecurity Manager	CSM	Project manager related to cybersecurity Consultation with customer (OEM) and supplier's cybersecurity engineer Project function cybersecurity application planning and status management Cybersecurity work product review, cybersecurity case development	Cyber Security Management Unit
Cybersecurity Architect	CSA	* Security Specialist : LGE Internal Certification Cybersecurity architect Cybersecurity architects perform TARA(threat analysis and risk assessment) Cybersecurity risk assessment, cybersecurity requirements/design analysis & review Development of cybersecurity concept (CSC)	Cyber Security Management Unit
Requirement Manager	RM	Acquire the requirements by OEM and, register requirements to the requirement management system (eg. CodeBeamer) Establish the structure of requirements in the requirement management system Add a field for security in the requirement management system Facilitate the verification review for SysRS and SRS Guide how to describe the SysRS and SRS to developers	Requirement Engineering Unit
System Architect	SysA	Establish the structure of system architecture design in the design management system (eg. CodeBeamer) Add a field for security in the design management system Describe the system architecture design Facilitate the verification review for SysAD	System Expert Task
SW Architect	SWA	Establish the structure of software architecture design in the design management system (eg. CodeBeamer) Add a field for security in the design management system Facilitate the verification review for SAD	SW Architect Unit
HW Architect	HWA	Establish the structure of hardware architecture design in the design management system (eg. CodeBeamer) Add a field for security in the design management system	HW Development Division

Responsibility / authority by role and management department (2/4)

Role	Abbreviation	Responsibility & authority	Management department
Static Analysis Manager	SAM	Static analysis tool management Establish and set up the environment of the static analysis tool Perform static analysis Review the tool to expand the scope of the coverage of secure rule set Review the OEM requirements and communicate the ruleset with OEM Define the ruleset for the project and adapt the ruleset agreed with OEM to the project Review the impact of static analysis issues and set the severity of static analysis issues Guide how to modify the issues reported by static analysis environment	CI/CT Unit
Developer	DEV	Cybersecurity development engineer Cybersecurity requirements, architecture designs, and detailed designs Implementation, software unit cybersecurity test case and test Cybersecurity system/software integration test case specification Cybersecurity system/software integration test Cybersecurity system/software integration testing defect monitoring and management Cybersecurity system/software integration test result report Cybersecurity system/software test case specification	SW Development Division
HW Developer	HW DEV	Cybersecurity hardware integration test case specification Cybersecurity hardware integration test Cybersecurity hardware integration testing defect monitoring and management Cybersecurity hardware integration test result report Cybersecurity hardware test case specification	HW Development Division
Cybersecurity Vulnerability Test Manager	CSVTM	Cybersecurity vulnerability manage Cybersecurity item field monitoring Contact point of vulnerability management. Collect information and initial vulnerability based on information. Upgrade and manage vulnerability Cybersecurity vulnerability test and result report	Cyber Security Analysis Unit
Penetration Test Manager	PTM	Penetration test and result report	Cyber Security Analysis Unit

Responsibility / authority by role and management department (3/4)

Role	Abbreviation	Responsibility & authority	Management department
Cybersecurity Assessor	-	Confirmation review planning, checklist development, and confirmation review Cybersecurity assessment planning, Cybersecurity assessment checklist development and Cybersecurity assessment Cybersecurity requirement, design, implementation, approval gate reviews	VS Cyber Security Governance Unit
Cybersecurity Auditor	-	Cybersecurity audit planning, Cybersecurity audit checklist development and Cybersecurity audit Manage and revise the CSMS standard	VS Cyber Security Audit Team
Production Manager	-	Establishment of production plan for cybersecurity items Cybersecurity item production monitoring	VS Quality Management Division
Incident Response Manager	IR Manager	Each cybersecurity incident manage Contact point of incident response. Collect information and initial incident analysis based on information. Upgrade and manage incident response process, tool, policy	Cyber Security Analysis Unit
Cyber Security Expert Group	CSEG	Classify Cybersecurity relevant requirements from OEM requirement and allocate feasible Security Control to them. Review Cybersecurity Requirement derived from TARA work product. Request and Operate Developer/Function Owner (FO) review session Develop and Review requirement/design specifications regarding Cybersecurity Relevant requirements. *Responsible CSA, Cybersecurity Assessor and CSM assigned to the project could not play CSEG role at the same time	Cyber Security Development

Responsibility / authority by role and management department (4/4)

Role	Abbreviation	Responsibility & authority	Management department
SW Qualification Test Manager	SWQT Manager	Cybersecurity software qualification test case (SWQTC) specification Cybersecurity software qualification test (SWQT) Cybersecurity software qualification testing defect monitoring and management Cybersecurity software qualification test result report	Validation Environment Unit
HW Qualification Test Manager	HWQT Manager	Cybersecurity hardware qualification test case specification Cybersecurity hardware qualification test Cybersecurity hardware qualification testing defect monitoring and management Cybersecurity hardware qualification test result report	Test Design Unit VS Development Quality Assurance team
System Integration Test Manager	SysIT Manager	Cybersecurity system integration test case (SysITC) specification Cybersecurity system integration test (SysIT) Cybersecurity system integration testing defect monitoring and improvement review Cybersecurity system integration test result report	Test Design Unit
System Qualification Test Manager	SysQT Manager	Cybersecurity system qualification test case (SysQTC) specification Cybersecurity system qualification test (SysQT) Cybersecurity system qualification test defect monitoring and improvement review Cybersecurity system qualification test result report	Test Design Unit VS Development Quality Assurance team
Configuration Manager	CM	• Create and manage CMP document, Identification of configuration items • Configuration items and storage management, Definition of configuration management process • Establish and change baseline, Baseline revision management • Ensure team members comply with the configuration management plan • Regular backup of configuration items, report the results	Requirement Engineering Unit
Project leader	PL	• Leads and manages the overall development process.	
Software project leader	SW PL	• Lead SW development and review SW documents • Manage Test Master Plan, Review Configuration Management documents and Report Quality Metrics	SW PL Unit
Hardware project leader	HW PL	• Lead HW Developers, take care of HW development activities, and review HW engineering documents	HW Development Department

Legend

Notation	Description
Reference Process	Item-based development process activities This refers to the ASPICE or CMMI development process used by the organization for reference purposes as to when the functional cybersecurity activities are performed.
Cybersecurity activity	Display of activities defined in the functional cybersecurity standard
Cybersecurity activity	Notation for describing the pre- and post-relationship of functional cybersecurity activities It expresses the previous step / after step of the describing process
——→	Direction of the activity
- - - - - - - - -→	Optional direction of the activity
◇ Judgement	Notation of review or judgment activities

Term and Abbreviation (1/2)

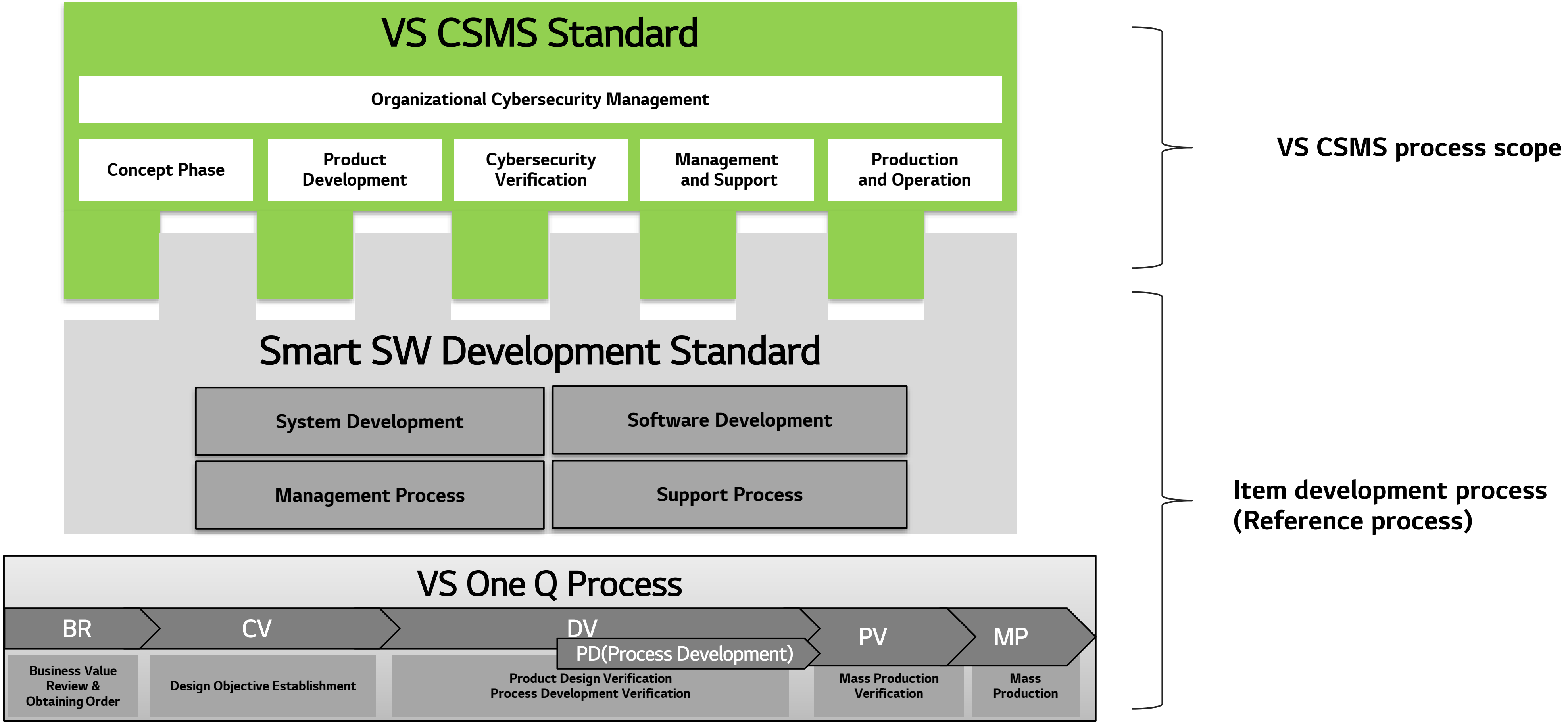
Term	Description
LG-SDL	• Secure Development Lifecycle • LG-SDL is the SW development process by adding SW security activities to enhance security for SW of LGE products. LGSDL process is established based on MS-SDL, fixed and supplemented to meet LGE's development environment. • It is the lifecycle of secure development that detects/eliminates SW security vulnerabilities at an early stage by performing core security activities in each SW development stage.
Product Security Certification	• Product Security Certification • It is the activity to issue the certificate after checking final results after executing all the SW product security activities (LGSDL) according to the determined security level of the product.
Attack Surface	• It is part of the SW product program that can be accessed by unauthorized user or external program (incl. process communications via IPC) • Example) Open network port, user interface, etc.
Threat	• It is an act of penetrating into the SW product with malicious intention.
Vulnerability	• It can be exploited by one or more threats.
Incident	• It is a cybersecurity issue that affected product is after SOP.
Mitigation	• A plan to reduce threats on the product by eliminating security vulnerabilities in the SW product.
Fuzz Testing	• This testing can be done in a random or negative automated way - running a number of wrong data to a system (web, file, network protocol and memory) to check if there occur any memory leak, crash, or other security issues.
Penetration Testing	• This test is intended to find the security vulnerabilities by executing the penetrating test on the SW product in order to improve SW product security.
Cybersecurity Design	• SW design that includes cybersecurity requirements
CIA	• Cybersecurity interface agreement • Agreement between customer and supplier stating responsibility for functional cybersecurity activities and deliverables
E/E system	• Electrical and electronic systems • A system comprising a programmable electrical / electronic element
FMEA	• Failure mode and effect analysis • Inductive analysis method used for system cybersecurity analysis

Term and Abbreviation (2/2)

Term	Description
SRS	• Software requirements specification
SAD	• Software architecture design
SDD	• Software detailed design
SWUT	• Software unit test
SWIT	• Software integration test
SWQT	• Software qualification test
HWIT	• Hardware integration test
HWQT	• Hardware qualification test
SysRS	• System requirements specification
SysAD	• System architecture design
SysIT	• System integration test
SysQT	• System qualification test
BR	• Business review phase
CV	• Concept verification phase
DV	• Development verification phase
PD	• Process development phase
PV	• Mass production verification phase
MP	• Mass production approval phase

VS CSMS standard composition

- The scope of the VS CSMS standard is limited to the cybersecurity area based on UNECE Cybersecurity Regulation, ISO/SAE 21434 and LGE Regulation of the SW Development Standard Process.
- To enable cybersecurity engineering, an organization institutes and maintains cybersecurity governance and cybersecurity culture. This involves specifying organization-specific rules and processes covering concept, development, production, operation, maintenance and decommissioning, including cybersecurity risk management, information sharing, vulnerability disclosure, cybersecurity monitoring, and incident response.
- Reference process applies the development process used by VS business unit.



VS CSMS Standard

Organizational Cybersecurity Management

Concept Phase

Product Development

Cybersecurity Verification

Management and Support

Production and Operation

VS CSMS process scope

Smart SW Development Standard

System Development

Software Development

Management Process

Support Process

VS One Q Process

BR

CV

DV

PD(Process Development)

PV

MP

Business Value Review & Obtaining Order

Design Objective Establishment

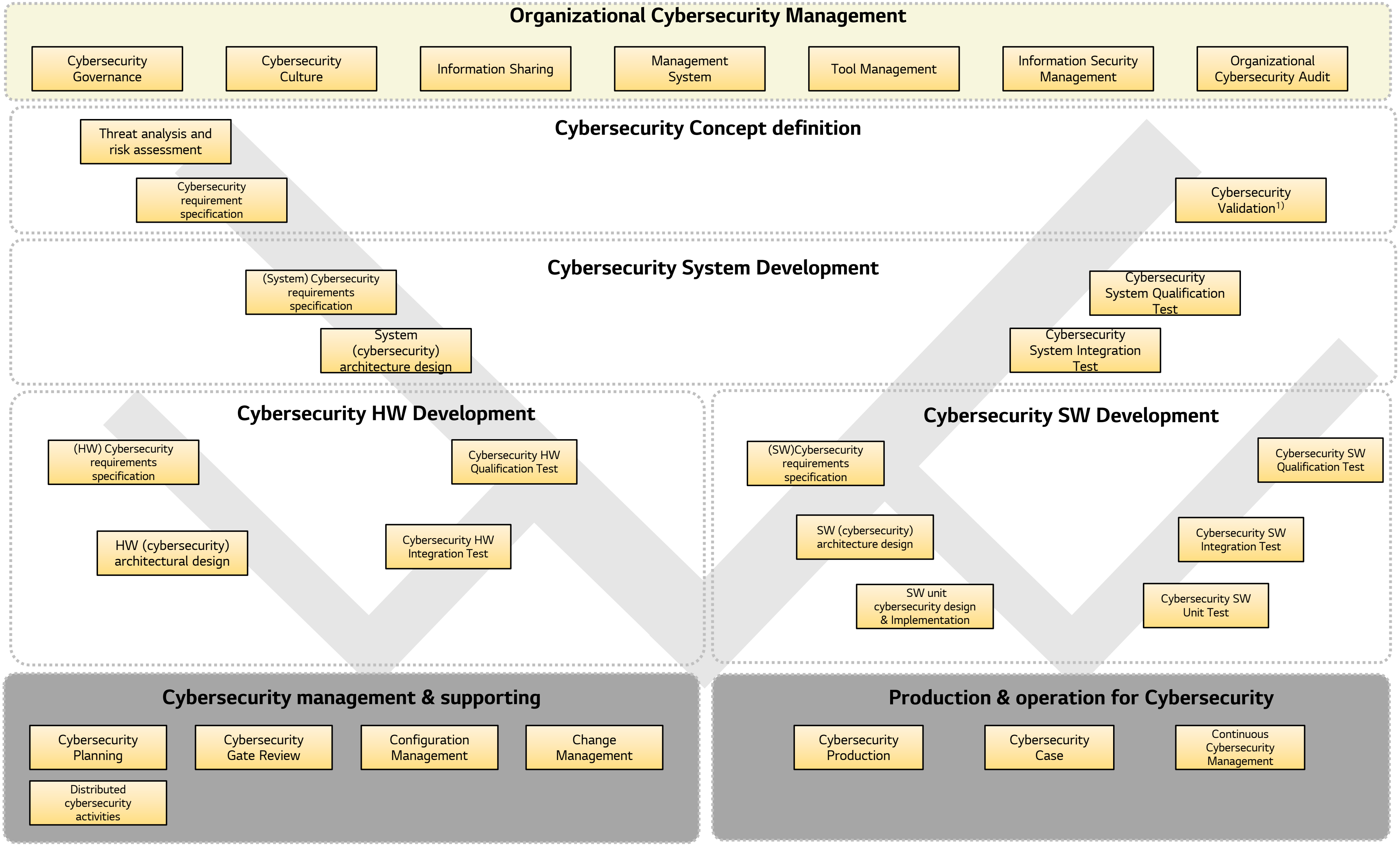
Product Design Verification
Process Development Verification

Mass Production Verification

Mass Production

Item development process (Reference process)

VS CSMS activity summary



Organizational Cybersecurity Management

- Cybersecurity Governance
- Cybersecurity Culture
- Information Sharing
- Management System
- Tool Management
- Information Security Management
- Organizational Cybersecurity Audit

Cybersecurity Concept definition

- Threat analysis and risk assessment
- Cybersecurity requirement specification
- Cybersecurity Validation[1]

Cybersecurity System Development

- (System) Cybersecurity requirements specification
- System (cybersecurity) architecture design
- Cybersecurity System Integration Test
- Cybersecurity System Qualification Test

Cybersecurity HW Development

- (HW) Cybersecurity requirements specification
- HW (cybersecurity) architectural design
- Cybersecurity HW Integration Test
- Cybersecurity HW Qualification Test

Cybersecurity SW Development

- (SW)Cybersecurity requirements specification
- SW (cybersecurity) architecture design
- SW unit cybersecurity design & Implementation
- Cybersecurity SW Unit Test
- Cybersecurity SW Integration Test
- Cybersecurity SW Qualification Test

Cybersecurity management & supporting

- Cybersecurity Planning
- Cybersecurity Gate Review
- Configuration Management
- Change Management
- Distributed cybersecurity activities

Production & operation for Cybersecurity

- Cybersecurity Production
- Cybersecurity Case
- Continuous Cybersecurity Management

[1] Cybersecurity Validation : Basically, validation activities are related to the test in the vehicle, so these are generally performed by OEM.

VS CSMS activity definition

Organizational Cybersecurity Management

Organizational Cybersecurity Management

Cybersecurity Governance
Cybersecurity Culture
Information Sharing

Management System
Tool Management
Information Security Management

Organizational Cybersecurity Audit

Cybersecurity Concept Definition

Definition of Cybersecurity goals

Item Definition
Threat analysis and risk assessment(TARA)
Cybersecurity Goals specification

Definition of Cybersecurity requirements

Cybersecurity Requirements specification
Obtaining Cybersecurity requirements
Review Cybersecurity requirements

Cybersecurity System Development

Cybersecurity System design

Initiation of system development
(system)Cybersecurity requirements specification
Release of (system)cybersecurity requirements
System (cybersecurity) architectural design
Release of System (cybersecurity) architectural design
Cybersecurity System Integration test specification
Cybersecurity System Qualification test specification

Cybersecurity System Test & Validation

Cybersecurity System Integration Test
Cybersecurity System Qualification Test
(System) Penetration Test
Vehicle Validation
System Release

Cybersecurity HW Development

HW Cybersecurity Design

Initiation of HW development
(HW) cybersecurity requirements specification
Release of (HW) cybersecurity requirements
HW (cybersecurity) architecture design
HW (cybersecurity) design release
Cybersecurity HW Qualification Test Specification

HW Cybersecurity Verification

Cybersecurity HW Integration Test
Cybersecurity HW Qualification Test
HW release

Cybersecurity SW Development

SW Cybersecurity Design

Initiation of SW development
(SW)cybersecurity requirement specification
Release of (SW)cybersecurity requirement
SW (cybersecurity) architecture design
Release of SW (cybersecurity) architecture
SW unit cybersecurity design and implementation
Cybersecurity SW Qualification Test Specification

SW Cybersecurity Verification

Cybersecurity SW Unit Test
Cybersecurity SW Integration Test
Cybersecurity SW Qualification Test
Cybersecurity Vulnerability Test
SW Release

Cybersecurity Management & Supporting

Cybersecurity Management

Establish Release Cybersecurity Plan
Development of CIA & suppliers' CIA
Release of CIA
of Cybersecurity Plan
Establish Cybersecurity Audit
Establish Cybersecurity Assessment

Cybersecurity Gate Review(Q-Gate)

Requirements confirm review
Feature Complete Review
Qualification completion Review

Supporting

Configuration Management
Requirement Change Management
Vulnerabilities Change Management

Production & Operation for Cybersecurity

Cybersecurity production

Production control plan

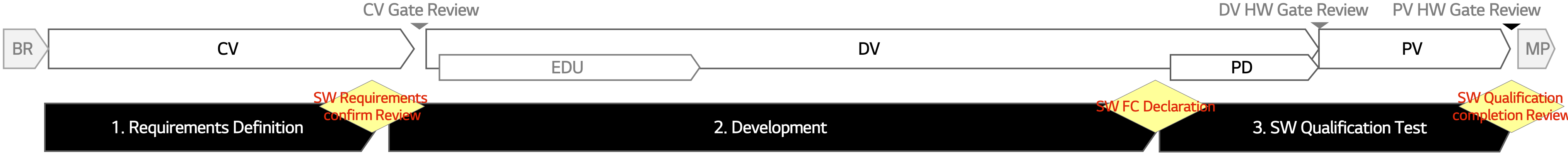
Continuous Cybersecurity Management

Cybersecurity threat monitoring
Initial incident analysis
Confirm affected products
Detailed threat analysis
Threat countermeasure development management
Prepare threat countermeasure
Post-Response Activities
End of Cybersecurity Support

Cybersecurity Case

Planning of Cybersecurity Case
Development of Cybersecurity Case

Relation between LGE Development Standard Process and VS CSMS Standard



Definition of Cybersecurity goals

Item Definition
Threat analysis and risk assessment(TARA)
Cybersecurity Goals specification

Definition of Cybersecurity requirements

Cybersecurity Requirements specification
Obtaining Cybersecurity requirements
Review Cybersecurity requirements

Cybersecurity planning

Establish Release Cybersecurity Plan
Development of CIA & suppliers' CIA
Release of CIA
Release of Cybersecurity Plan
Establish Cybersecurity Audit
Establish Cybersecurity Assessment

Q-Gate (Requirement confirm review)

Cybersecurity Requirement Gate Review
- Scope :
  1) CAL Rating
  2) Identification of cybersecurity threat
  3) Identification of customer cybersecurity requirements
  4) Cybersecurity Plan

- Submit CS assessment report

Cybersecurity System design

Initiation of system development
(system)Cybersecurity requirements specification
Release of (system)cybersecurity requirements
System (cybersecurity) architectural design
Release of System (cybersecurity) architectural design
Cybersecurity System Integration test specification
Cybersecurity System Qualification test specification

HW Cybersecurity Design

Initiation of HW development
(HW) cybersecurity requirements specification
Release of (HW) cybersecurity requirements
HW (cybersecurity) architecture design
HW (cybersecurity) design release

SW Cybersecurity Design

Initiation of SW development
(SW)cybersecurity requirement specification
Release of (SW)cybersecurity requirement
SW (cybersecurity) architecture design
Release of SW (cybersecurity) architecture
SW unit cybersecurity design and implementation
Cybersecurity SW Qualification Test Specification

Cybersecurity test plan & test specification

Cybersecurity System Qualification Test Specification
Cybersecurity System Integration Test Specification
Cybersecurity SW Qualification Test Specification

N-th iteration
Repetition according to item development characteristics (e.g. Sample release cycle)

System Cybersecurity verification

Cybersecurity System Integration Test
Cybersecurity System Qualification Test
(System) Penetration Test
Vehicle Validation
System Release

HW Cybersecurity Verification

Cybersecurity HW Integration Test
Cybersecurity HW Qualification Test
HW release

SW Cybersecurity Verification

Cybersecurity SW Unit Test
Cybersecurity SW Integration Test
Cybersecurity SW Qualification Test
Cybersecurity Vulnerability Report
SW Release

N-th iteration
Repetition according to item development characteristics (e.g. Sample release cycle)

Q-Gate (Feature complete review)

Cybersecurity Design Gate Review
- Scope :
  1) Identification of cybersecurity threat
  2) Specifying SysRS/SRS about cybersecurity requirements and obtaining traceability
  3) Cybersecurity architecture design and reducing the risk
  4) System/SW test specification and test result
  5) SW vulnerability scanning result

- Submit CS assessment report

System Cybersecurity verification

Cybersecurity System Integration Test
Cybersecurity System Qualification Test
(System) Penetration Test
Vehicle Validation
System Release

SW Cybersecurity Verification

Cybersecurity SW Unit Test
Cybersecurity SW Integration Test
Cybersecurity SW Qualification Test
Cybersecurity Vulnerability Test
SW Release

Cybersecurity Case development

Planning of Cybersecurity Case
Development of Cybersecurity Case

Cybersecurity production & operation planning

Production control plan

N-th iteration
Repetition according to item development characteristics (e.g. Sample release cycle)

Q-Gate (Qualification completion Review)

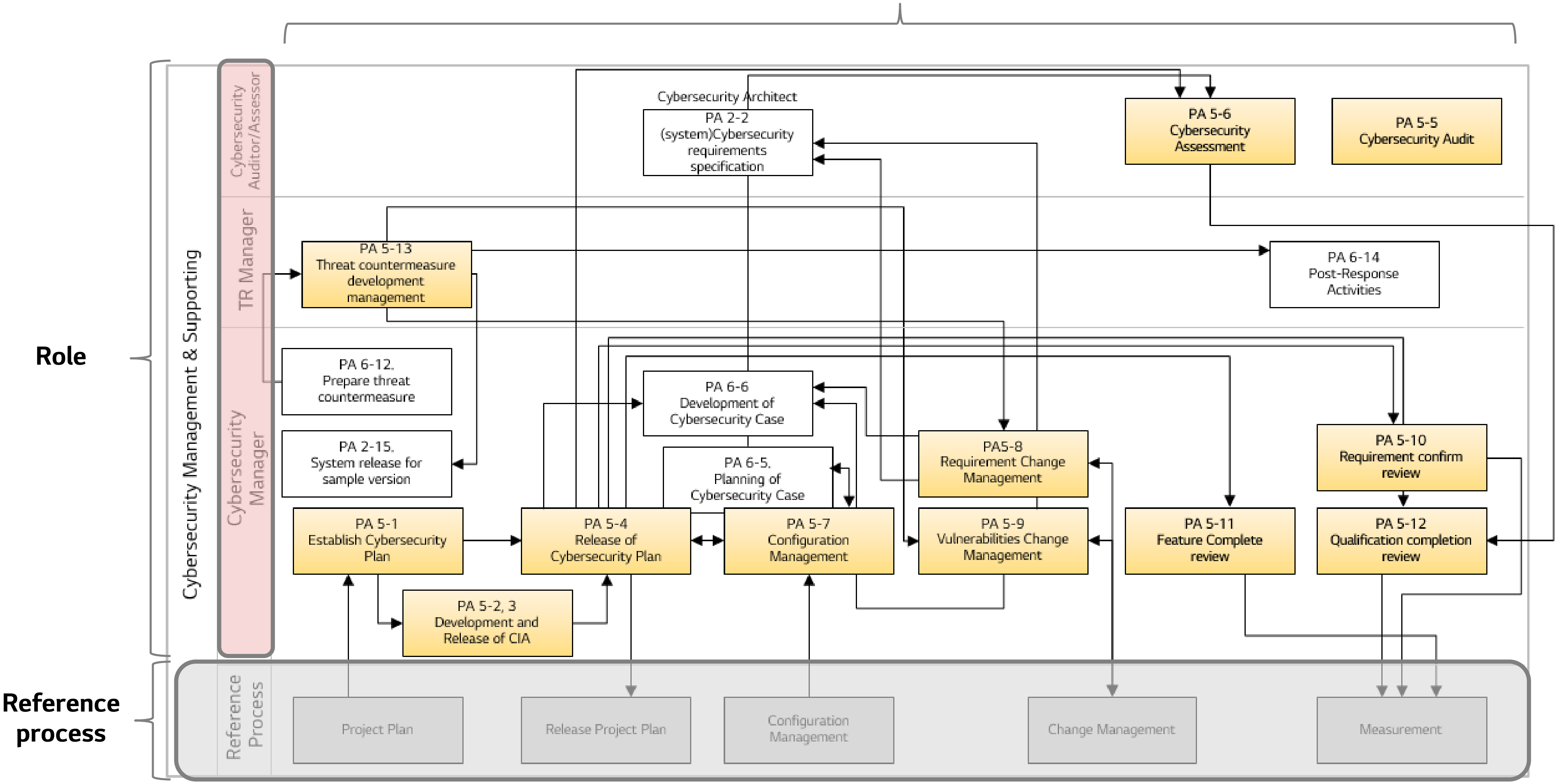
Cybersecurity Approval Gate Review
- Scope :
  1) Work products consistency/completion
  2) Production control plan
  3) Post-development report

- Submission QP assessment report

VS CSMS Standard composition(1/2)

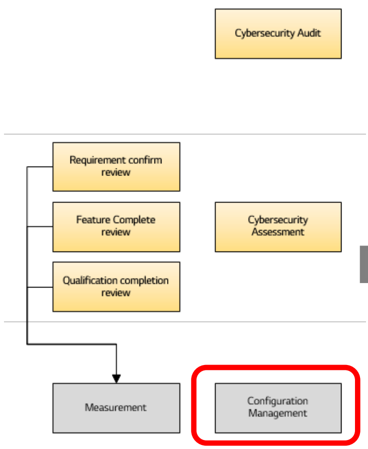
- VS CSMS standard has six process areas, and provides a process map for each process area.
- The process map is provided in the form of the following and provides the relationship between the person in charge of cybersecurity and cybersecurity activities, and the reference process.

Relationship flow between CSMS activities

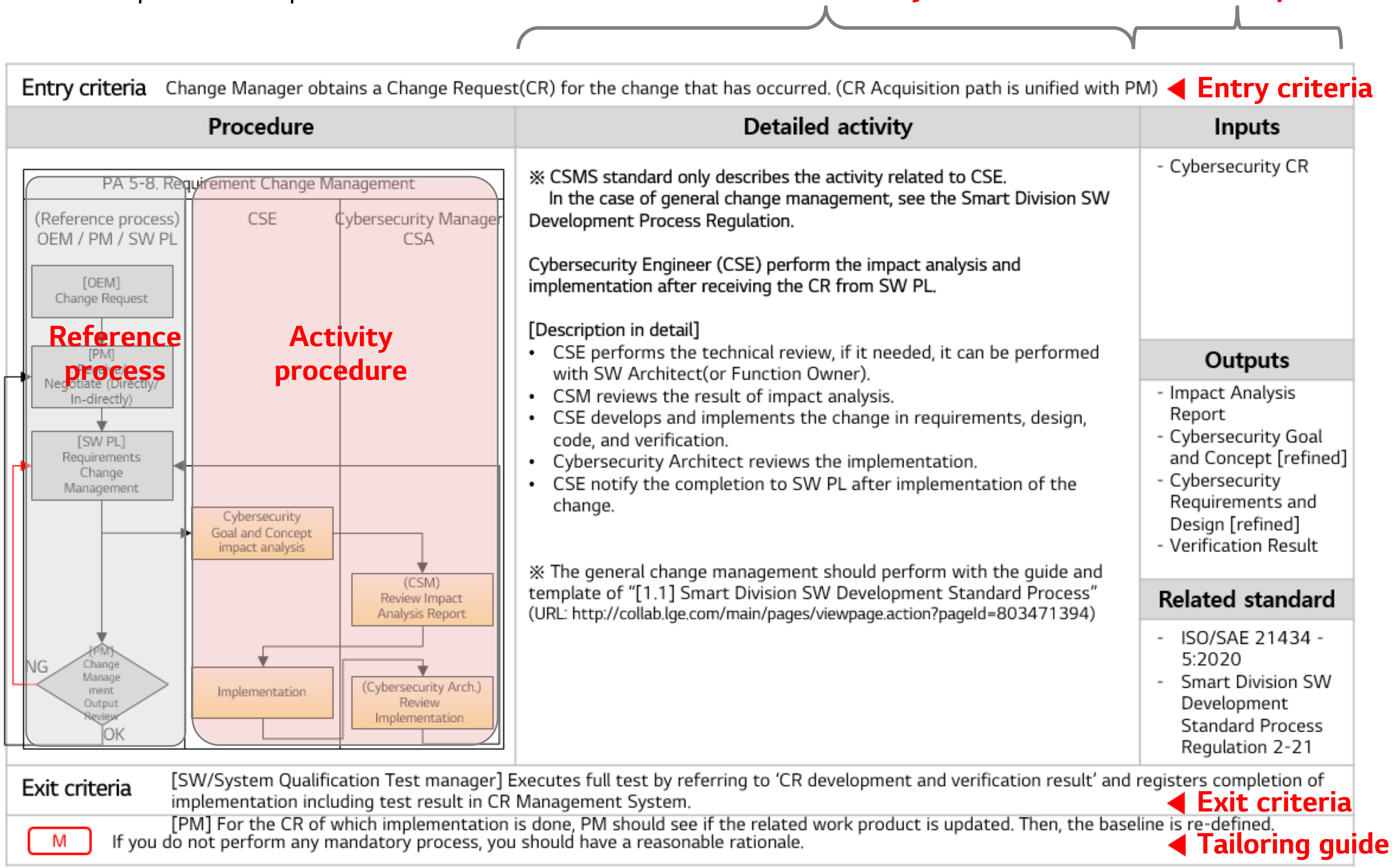

Role
Reference process
Cybersecurity Management & Supporting
Cybersecurity Auditor/Assessor
TR Manager
Cybersecurity Manager
Reference Process
Cybersecurity Architect
PA 2-2 (system)Cybersecurity requirements specification
PA 5-6 Cybersecurity Assessment
PA 5-5 Cybersecurity Audit
PA 5-13 Threat countermeasure development management
PA 6-14 Post-Response Activities
PA 6-12. Prepare threat countermeasure
PA 2-15. System release for sample version
PA 6-6 Development of Cybersecurity Case
PA 6-5. Planning of Cybersecurity Case
PA5-8 Requirement Change Management
PA 5-10 Requirement confirm review
PA 5-1 Establish Cybersecurity Plan
PA 5-4 Release of Cybersecurity Plan
PA 5-7 Configuration Management
PA 5-9 Vulnerabilities Change Management
PA 5-11 Feature Complete review
PA 5-12 Qualification completion review
PA 5-2, 3 Development and Release of CIA
Project Plan
Release Project Plan
Configuration Management
Change Management
Measurement

VS CSMS Standard composition(2/2)

- Detailed specification of activities as a unit of work is provided.
- Each development task has an entry and exit criteria, and it defines inputs and outputs that are needed to perform activities.
- Detailed activity describes detailed action procedures so that the activity flow can be viewed.
- The reference process is provided to present the point in time of CSMS activities.



Process Map


Detailed activity
In/out work product
Entry criteria
Exit criteria
Tailoring guide
PA 5-8. Requirement Change Management
(Reference process) OEM / PM / SW PL
CSE
Cybersecurity Manager CSA
[OEM] Change Request
[PM] Receive/ Negotiate (Directly/ In-directly)
[SW PL] Requirements Change Management
[PM] Change Management Output Review
NG
OK
Cybersecurity Goal and Concept impact analysis
(CSM) Review Impact Analysis Report
Implementation
(Cybersecurity Arch.) Review Implementation
Reference process
Activity procedure

Entry criteria Change Manager obtains a Change Request(CR) for the change that has occurred. (CR Acquisition path is unified with PM)

Procedure	Detailed activity	Inputs
	※ CSMS standard only describes the activity related to CSE. In the case of general change management, see the Smart Division SW Development Process Regulation. Cybersecurity Engineer (CSE) perform the impact analysis and implementation after receiving the CR from SW PL. [Description in detail] • CSE performs the technical review, if it needed, it can be performed with SW Architect(or Function Owner). • CSM reviews the result of impact analysis. • CSE develops and implements the change in requirements, design, code, and verification. • Cybersecurity Architect reviews the implementation. • CSE notify the completion to SW PL after implementation of the change. ※ The general change management should perform with the guide and template of "[1.1] Smart Division SW Development Standard Process" (URL: http://collab.lge.com/main/pages/viewpage.action?pageId=803471394)	- Cybersecurity CR **Outputs** - Impact Analysis Report - Cybersecurity Goal and Concept [refined] - Cybersecurity Requirements and Design [refined] - Verification Result **Related standard** - ISO/SAE 21434 - 5:2020 - Smart Division SW Development Standard Process Regulation 2-21

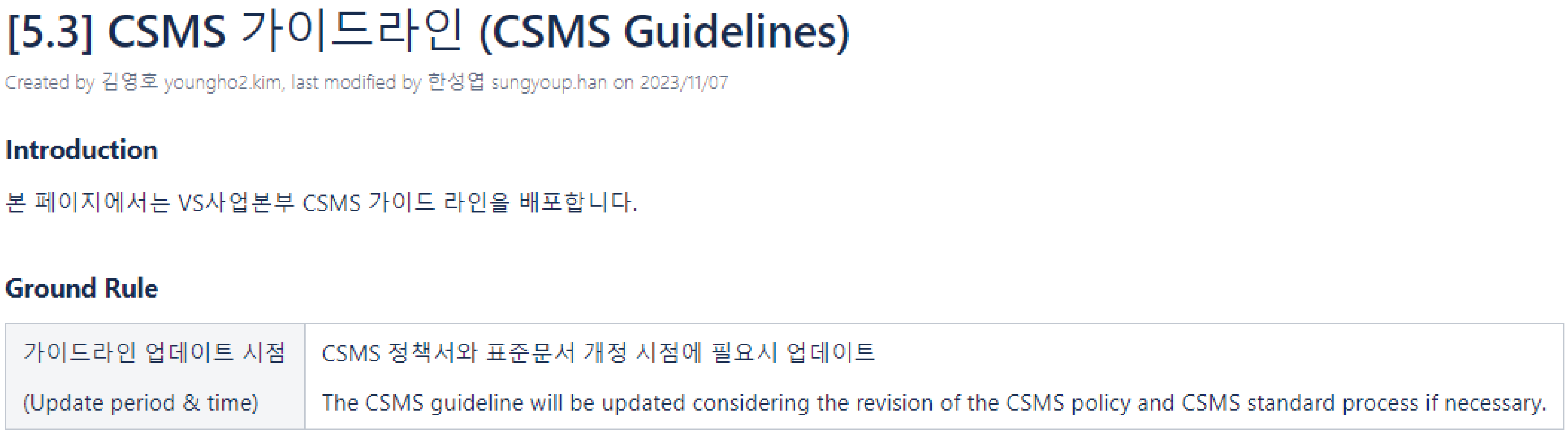
Exit criteria [SW/System Qualification Test manager] Executes full test by referring to 'CR development and verification result' and registers completion of implementation including test result in CR Management System.
[PM] For the CR of which implementation is done, PM should see if the related work product is updated. Then, the baseline is re-defined.

M If you do not perform any mandatory process, you should have a reasonable rationale.

Detailed activity

Location in guidance & Template

- Please refer to guidance & template for CSMS preparation
- Guidance & template which are aligned with CMBook.
  Guidance Collab : http://collab.lge.com/main/x/fW1-Sg
  Template Collab : http://collab.lge.com/main/x/DaGwh



[5.3] CSMS 가이드라인 (CSMS Guidelines)

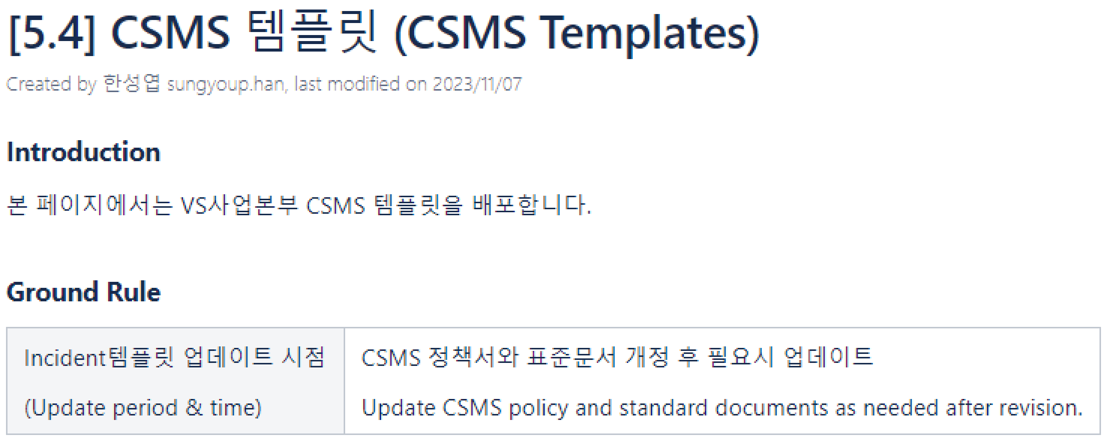
Created by 김영호 youngho2.kim, last modified by 한성엽 sungyoup.han on 2023/11/07

Introduction

본 페이지에서는 VS사업본부 CSMS 가이드 라인을 배포합니다.

Ground Rule

가이드라인 업데이트 시점 (Update period & time)	CSMS 정책서와 표준문서 개정 시점에 필요시 업데이트 The CSMS guideline will be updated considering the revision of the CSMS policy and CSMS standard process if necessary.



[5.4] CSMS 템플릿 (CSMS Templates)

Created by 한성엽 sungyoup.han, last modified on 2023/11/07

Introduction

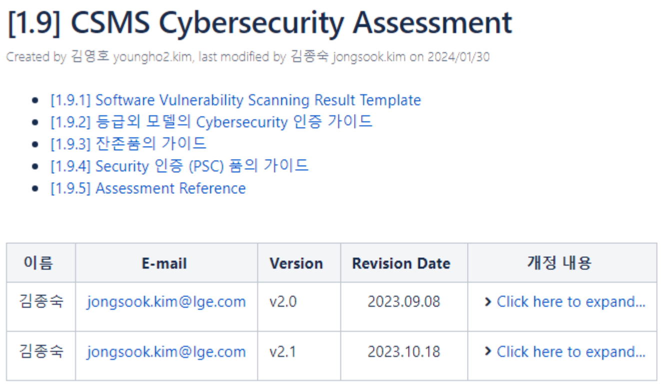
본 페이지에서는 VS사업본부 CSMS 템플릿을 배포합니다.

Ground Rule

Incident템플릿 업데이트 시점 (Update period & time)	CSMS 정책서와 표준문서 개정 후 필요시 업데이트 Update CSMS policy and standard documents as needed after revision.

Location in assessment guide/items & ISO 21434 Check list

- Assessment guide & items
  http://collab.lge.com/main/x/wLNjUw



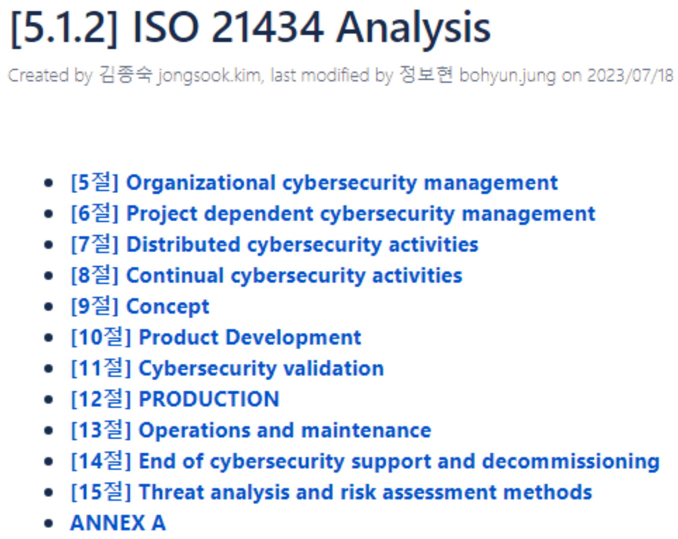
[1.9] CSMS Cybersecurity Assessment

Created by 김영호 youngho2.kim, last modified by 김종숙 jongsook.kim on 2024/01/30

- [1.9.1] Software Vulnerability Scanning Result Template
- [1.9.2] 등급외 모델의 Cybersecurity 인증 가이드
- [1.9.3] 잔존품의 가이드
- [1.9.4] Security 인증 (PSC) 품의 가이드
- [1.9.5] Assessment Reference

이름	E-mail	Version	Revision Date	개정 내용
김종숙	jongsook.kim@lge.com	v2.0	2023.09.08	› Click here to expand...
김종숙	jongsook.kim@lge.com	v2.1	2023.10.18	› Click here to expand...

- ISO 21434 Check list to understand CSMS
  http://collab.lge.com/main/x/8PrWUg



[5.1.2] ISO 21434 Analysis

Created by 김종숙 jongsook.kim, last modified by 정보현 bohyun.jung on 2023/07/18

- [5절] Organizational cybersecurity management
- [6절] Project dependent cybersecurity management
- [7절] Distributed cybersecurity activities
- [8절] Continual cybersecurity activities
- [9절] Concept
- [10절] Product Development
- [11절] Cybersecurity validation
- [12절] PRODUCTION
- [13절] Operations and maintenance
- [14절] End of cybersecurity support and decommissioning
- [15절] Threat analysis and risk assessment methods
- ANNEX A

1 Cybersecurity Concept Definition Phase

- **Objective**

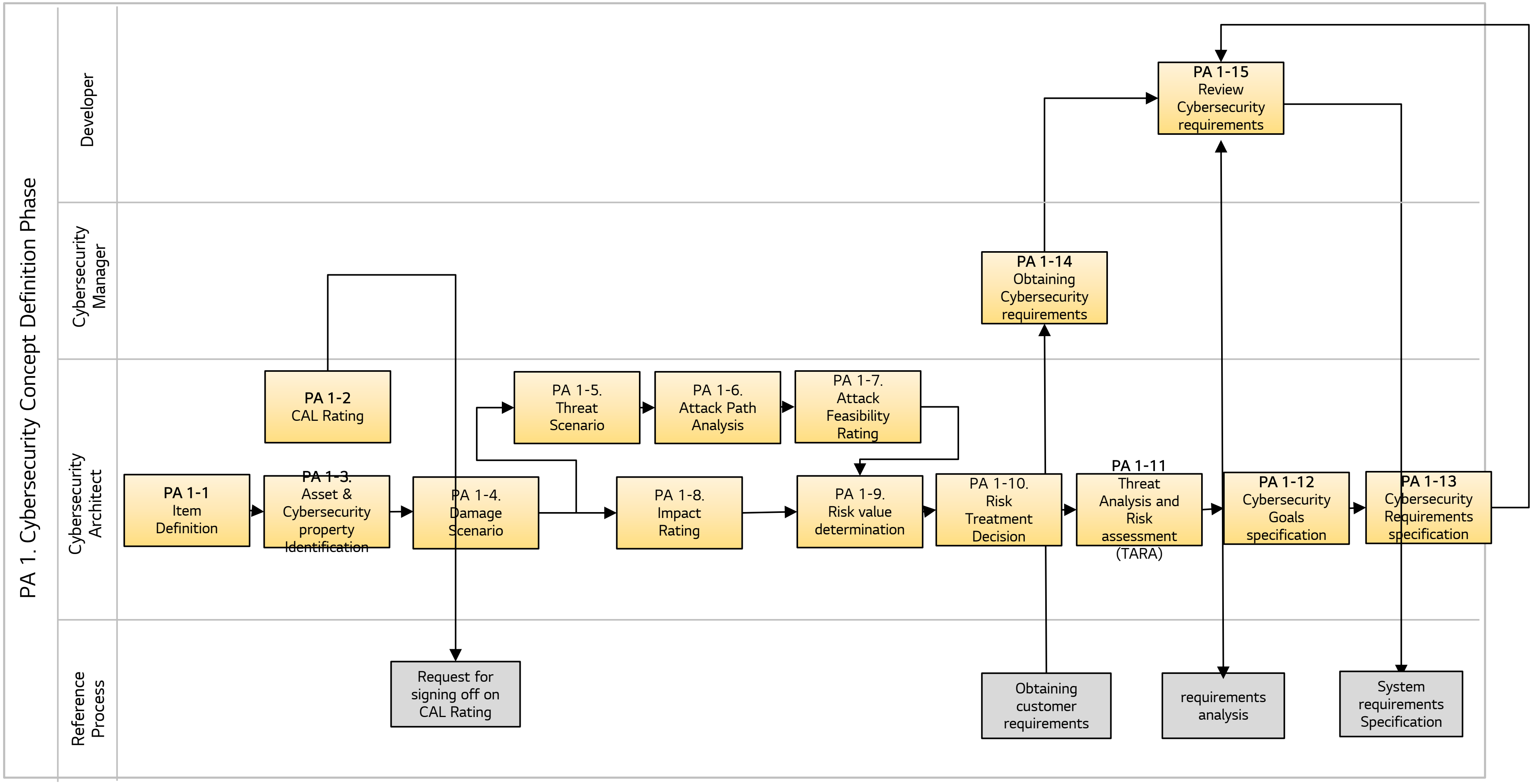
  Define the item concept definition phase from the cybersecurity point of view and define key activities and criteria for each step.

- **Scope**

  Developing an item that applies cybersecurity among electrical and electronic system (E / E system) developed by VS company. Cybersecurity concept definition is the OEM's role, but if the OEM requests LGE to define it, LGE can define it.

1 Cybersecurity Concept Definition Phase

Define the necessary activities and criteria when LGE develops the functional cybersecurity required E/E system, if the OEM doesn't give the cybersecurity concept of the system or LGE develops the system without OEMs.


PA 1. Cybersecurity Concept Definition Phase
Developer
Cybersecurity Manager
Cybersecurity Architect
Reference Process
PA 1-1 Item Definition
PA 1-2 CAL Rating
PA 1-3. Asset & Cybersecurity property Identification
PA 1-4. Damage Scenario
PA 1-5. Threat Scenario
PA 1-6. Attack Path Analysis
PA 1-7. Attack Feasibility Rating
PA 1-8. Impact Rating
PA 1-9. Risk value determination
PA 1-10. Risk Treatment Decision
PA 1-11 Threat Analysis and Risk assessment (TARA)
PA 1-12 Cybersecurity Goals specification
PA 1-13 Cybersecurity Requirements specification
PA 1-14 Obtaining Cybersecurity requirements
PA 1-15 Review Cybersecurity requirements
Request for signing off on CAL Rating
Obtaining customer requirements
requirements analysis
System requirements Specification

LGE Internal Use Only

1 Related ISO/SAE 21434 standard for cybersecurity concept definition

Cybersecurity Concept Definition

Option	Process Area	Description	Role	Work product	Related standard
M	**PA 1-1.** Item Definition	Identifies the item, the operational environment and its interaction with other items.	Cybersecurity Architect	• Item definition	• ISO SAE 21434-9 : v1.0
M	**PA 1-2** CAL Rating	Review project information and share CAL rating with CSM	Cybersecurity Architect	• CAL Rating with rationale • Signing off CAL Rating	• ISO SAE 21434-9 : v1.0
M	**PA 1-3** Asset & Cybersecurity property Identification	Determines the risk response by identifying the possible Threats on the vehicle..	Cybersecurity Architect	• Identified assets and cybersecurity properties	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0
M	**PA 1-4** Damage Scenario	Determines the risk response by identifying the possible Threats on the vehicle..	Cybersecurity Architect	• Damage Scenario	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0
M	**PA 1-5** Threat Scenario	Determines the risk response by identifying the possible Threats on the vehicle.	Cybersecurity Architect	• Threat Scenario	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0
M	**PA 1-6** Attack Path Analysis	Analyze possible attack paths on the vehicle	Cybersecurity Architect	• Identified attack paths	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0
M	**PA 1-7** Attack Feasibility Rating	Determines the risk response by identifying the possible Threats on the vehicle.	Cybersecurity Architect	• Attack Feasibility Rating	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0
M	**PA 1-8** Impact Rating	Determines the risk response by identifying the possible Threats on the vehicle.	Cybersecurity Architect	• Impact rating, including the associated impact categories of the damage scenarios	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0

M Mandatory O Optional

[Cybersecurity concept phase application guide]

- LGE could skip the PA1 phase if OEM performs it instead. However, it must be clearly stated to the CIA

1 Related ISO/SAE 21434 standard for cybersecurity concept definition

Cybersecurity Concept Definition

Option	Process Area	Description	Role	Work product	Related standard
M	PA 1-9 Risk value determination	Determines the risk response by identifying the possible Threats on the vehicle.	Cybersecurity Architect	• Risk value	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0
M	PA 1-10 Risk Treatment Decision	Determines the risk response by identifying the possible Threats on the vehicle.	Cybersecurity Architect	• Risk treatment decision per threat scenario	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0
M	PA 1-11. Threat Analysis and Risk Assessment	Determines the risk response by identifying the possible Threats on the vehicle	Cybersecurity Architect	• TATA report	• ISO/SAE 21434-15: v1.0 • ISO/SAE 21434-9: v1.0
M	PA 1-12 Cybersecurity Goals specification	Describes cybersecurity goals and cybersecurity claims according to risk assessment results	Cybersecurity Architect	• Cybersecurity goals • Cybersecurity claims • Verification report of cybersecurity concept	• ISO SAE 21434-9 : v1.0
M	PA 1-13 Cybersecurity Requirements specification	Specifies cybersecurity requirements and allocate them to the item and/or the operational environment.	Developer	• Cybersecurity concept • Verification report of cybersecurity concept	• ISO SAE 21434-9 : v1.0
M	PA 1-14 Obtaining Cybersecurity requirements	Obtains cybersecurity requirements from the customer in accordance with the development schedule.	Cybersecurity Manager	• Cybersecurity goal • Cybersecurity requirements (CSR)	• ISO SAE 21434-9 : v1.0
M	PA 1-15 Review Cybersecurity requirements	reviews the feasibility of obtaining Cybersecurity requirements from customers.	Cybersecurity Manager	• Feasibility report for Cybersecurity requirements	• ISO SAE 21434-9 : v1.0

M Mandatory O Optional

[Cybersecurity concept phase application guide]

- LGE could skip the PA1 phase if OEM performs it instead. However, it must be clearly stated to the CIA

1 Cybersecurity Concept Definition Phase Role & Responsibility

Process Area	Work Product	CSM	CSA	DEV	SW PL
PA 1-1. Item Definition	• Item definition	I	R	-	-
PA 1-2 CAL Rating	• CAL Rating with rationale • Signing off CAL Rating	I	R	-	-
PA 1-3 Asset & Cybersecurity property Identification	• Identified assets and cybersecurity properties	I	R	-	I
PA 1-4 Damage Scenario	• Damage Scenario	I	R	-	-
PA 1-5 Threat Scenario	• Threat Scenario	I	R	-	-
PA 1-6 Attack Path Analysis	• Identified attack paths	I	R	-	-

R : Responsibility , A : Approval, S : Support , I : Informed

1 Cybersecurity Concept Definition Phase Role & Responsibility

Process Area	Work Product	CSM	CSA	DEV	SW PL
PA 1-7 Attack Feasibility Rating	• Attack Feasibility Rating	I	R	-	-
PA 1-8 Impact Rating	• Impact rating, including the associated impact categories of the damage scenarios	I	R	-	-
PA 1-9 Risk value determination	• Risk value	I	R	-	-
PA 1-10 Risk Treatment Decision	• Risk treatment decision per threat scenario	I	R	-	-
PA 1-11. Threat Analysis and Risk Assessment	• TARA report	I	R	-	-
PA 1-12 Cybersecurity Goals specification	- Cybersecurity goals - Cybersecurity claims - Verification report of cybersecurity concept	I	R	-	-
PA 1-13 Cybersecurity Requirements specification	• Cybersecurity concept • Verification report of cybersecurity concept	I	A	R	-
PA 1-14. Obtaining Cybersecurity requirements	• Cybersecurity goal • Cybersecurity requirements (CSR)	R	S	-	-
PA 1-15 Review Cybersecurity requirements	• Feasibility report for Cybersecurity requirements	R	S	S	-

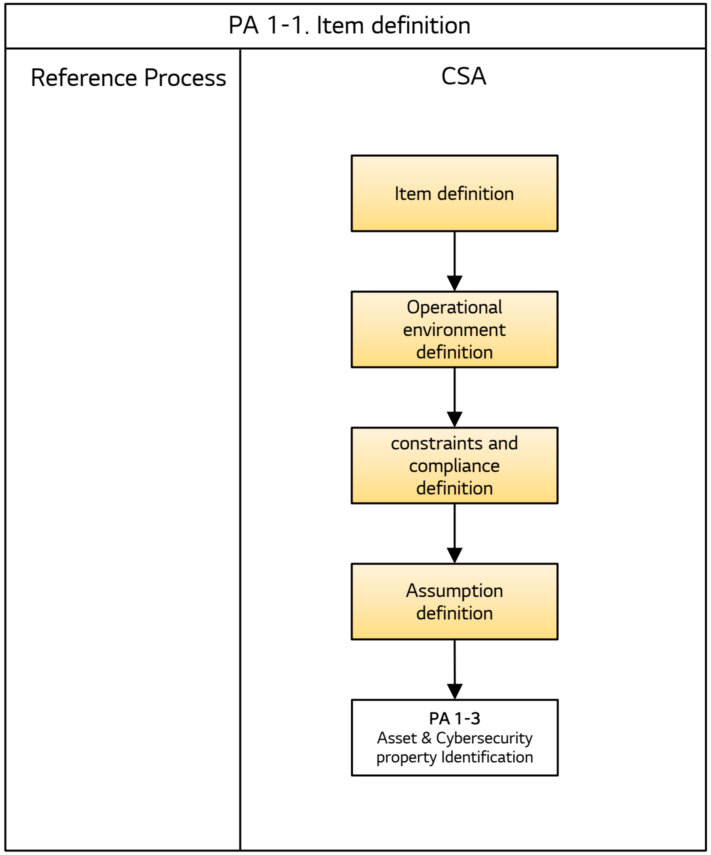
R : Responsibility , A : Approval, S : Support , I : Informed

1- 1. Item definition

◆ **Cybersecurity Architect identifies the item, the operational environment and its interaction with other items in the context of cybersecurity.**

Entry criteria none

Procedure



PA 1-1. Item definition

Reference Process

CSA

Item definition

Operational environment definition

constraints and compliance definition

Assumption definition

PA 1-3 Asset & Cybersecurity property Identification

Detailed activity

Cybersecurity Architect identifies the item, the operational environment and its interaction with other items in the context of cybersecurity.

[Description in detail]

- System and SW architect provides basic information for CSA to identify Item.
- CSA identifies item boundary and function and preliminary architecture.
- CSA describes the operational environment of item with regard to cybersecurity.
- CSA identifies constraints and compliance needs.
- CSA identifies assumptions about the item and the operational environment of the item.

Inputs

- Existing information regarding the item and the operational environment can be considered.

Outputs

- Item definition

Related standard

- ISO SAE 21434-9 :V1.0

Exit criteria [Cybersecurity Architect] Define item and operational environment to TARA(Threat Analysis and Risk Assessment).

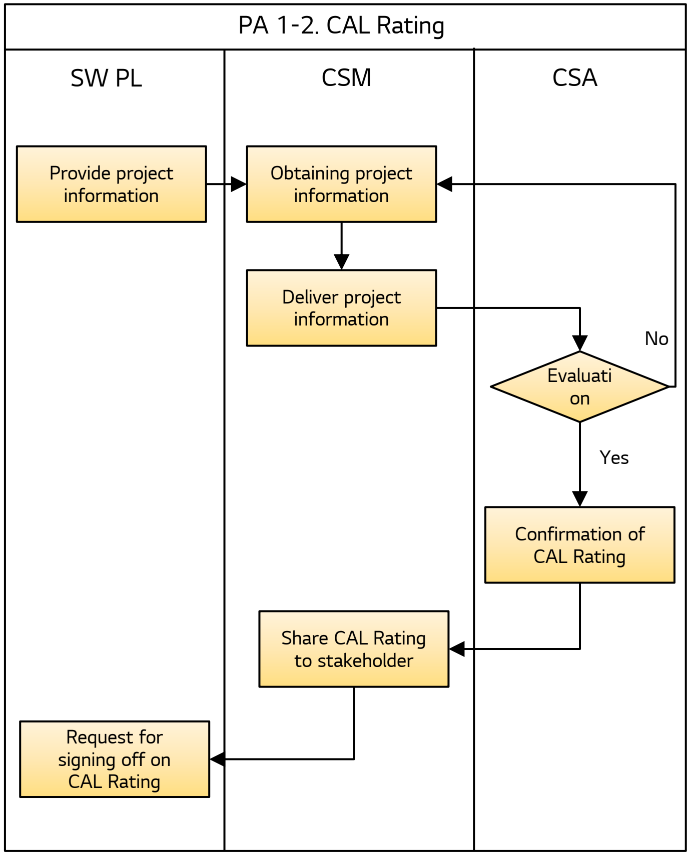
O This is OEM's responsibility, so only performed when OEM requests or the item is developed without OEM.

1-2. CAL Rating

◆ Cybersecurity Architect review project information and share CAL rating with CSM

Entry criteria High level project diagram should be prepared.

Procedure


PA 1-2. CAL Rating
SW PL
CSM
CSA
Provide project information
Obtaining project information
Deliver project information
Evaluation
No
Yes
Confirmation of CAL Rating
Share CAL Rating to stakeholder
Request for signing off on CAL Rating

Detailed activity

CSM announce CAL Rating of project

[Description in detail]

- CSM obtain project information such as HW block diagram
- CSM share project information with CSA
- CSA review project information and confirm CAL Rating
- CSM share CAL rating to stakeholder
- CAL Rating : http://collab.lge.com/main/display/VCSWINFO/%5B5.3.0%5D+CAL+Rating
  CAL Rating is determined by the overall requirements. It is not determined for each requirement.
- SW PL request signing off on CAL rating to related leaders

Inputs

- High level diagram
- Product family
- Main feature

Outputs

- CAL Rating with rationale
- Signing off CAL Rating

Related standard

- ISO SAE 21434-9 : v1.0

Exit criteria [SW PL] SW PL should request for signing off on CAL Rating to related leaders

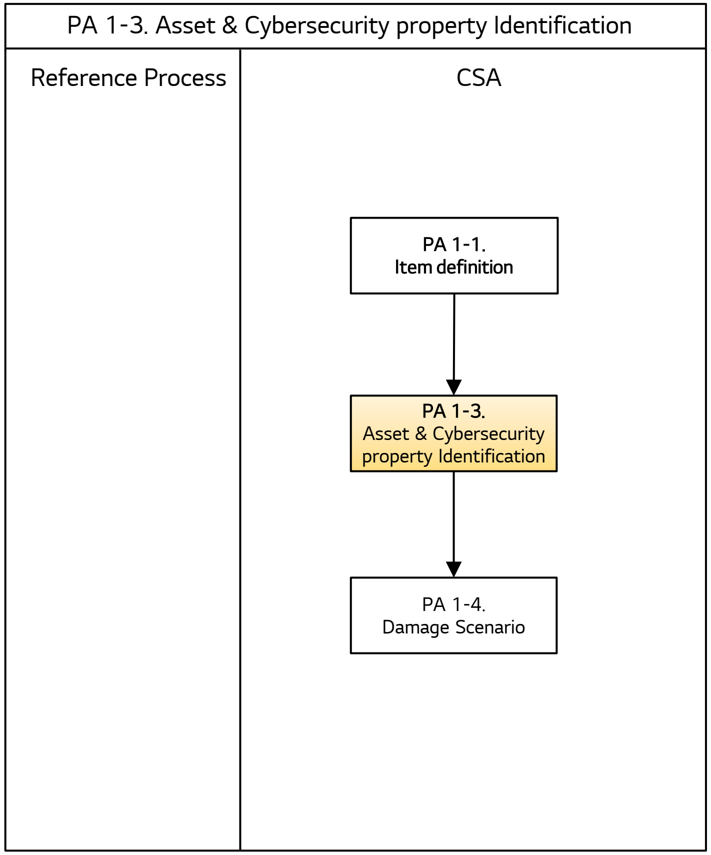
M If you do not perform any mandatory process, you should have a reasonable rationale.

1-3. Asset & Cybersecurity property Identification

◆ **Cybersecurity Architect determines the risk response by identifying the possible Threats on the vehicle.**

Entry criteria Item definition to analyze threat must be completed.

Procedure


PA 1-3. Asset & Cybersecurity property Identification
Reference Process
CSA
PA 1-1.
Item definition
PA 1-3.
Asset & Cybersecurity property Identification
PA 1-4.
Damage Scenario

Detailed activity

Cybersecurity Architect identify assets and cybersecurity properties.

[Description in detail]

- CSA analyzes and lists items or components as assets with cybersecurity properties.
- CSA extract assets and cybersecurity properties from the architecture design.

Inputs

- Item Definition
- Existing information such as item or component architecture design

Outputs

- Identified assets and cybersecurity properties

Related standard

- ISO/SAE21434-15: v1.0
- ISO/SAE21434-9: v1.0

Exit criteria [Cybersecurity Architect] Identify assets and cybersecurity properties.

O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

1-4. Damage Scenario

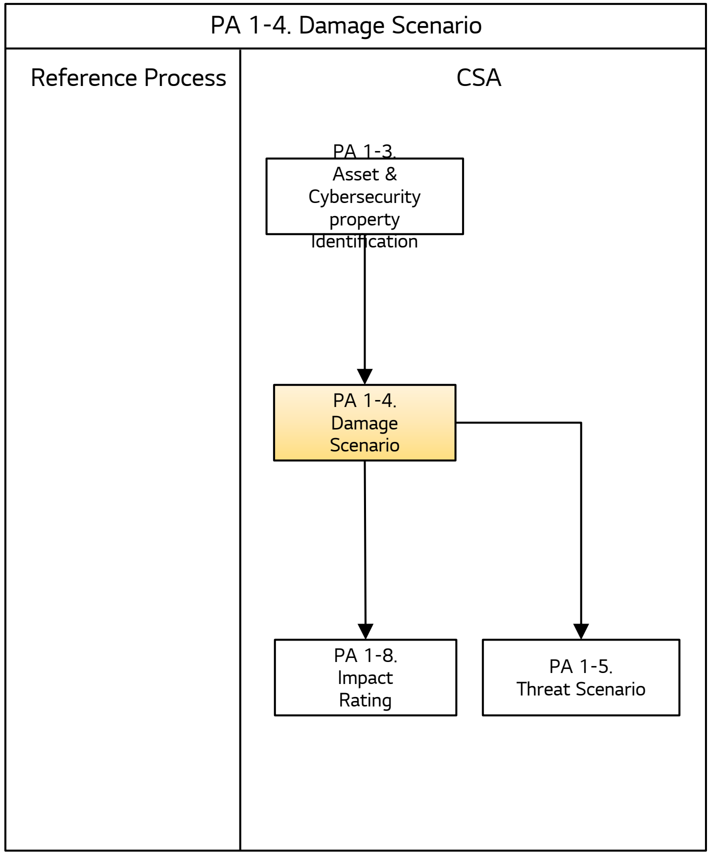
LGE Internal Use Only

Cybersecurity Concept Definition

◆ Cybersecurity Architect determines the risk response by identifying the possible Threats on the vehicle.

Entry criteria Asset & Cybersecurity property Identification must be completed.

Procedure



Detailed activity

Cybersecurity Architect makes damage scenario.

[Description in detail]

- CSA should create the damage scenarios with identified assets and cybersecurity properties (based on loss of security property of asset).
- CSA can include relation between the functionality of the item and the adverse consequence to damage scenarios
- CSA can include description of harm to the road user and/or relevant assets to damage scenarios

Inputs

- Asset & Cybersecurity property Identification

Outputs

- Damage Scenario

Related standard

- ISO/SAE21434-15: v1.0
- ISO/SAE21434-9: v1.0

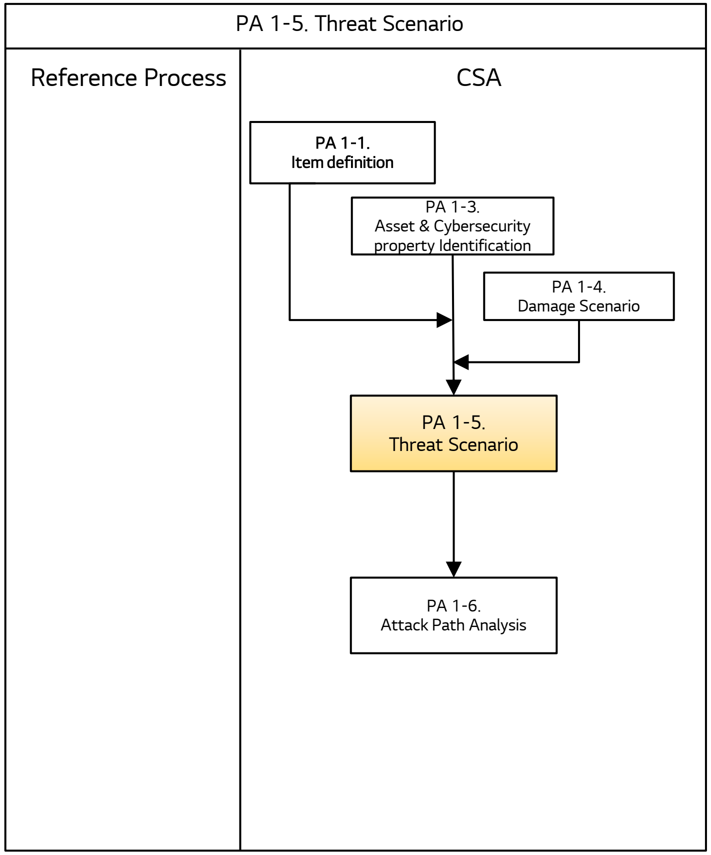
Exit criteria [Cybersecurity **Architect**] Identified assets and cybersecurity properties should be included in damage scenario. Damage scenarios should be made

O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

1-5. Threat Scenario

◆ Cybersecurity Architect determines the risk response by identifying the possible Threats on the vehicle.

Entry criteria Asset Identification should exist.

Procedure	Detailed activity	Inputs
 PA 1-5. Threat Scenario Reference Process CSA PA 1-1. Item definition PA 1-3. Asset & Cybersecurity property Identification PA 1-4. Damage Scenario PA 1-5. Threat Scenario PA 1-6. Attack Path Analysis	Cybersecurity Architect defines threat scenario [Description in detail] • CSA analyze the damage scenario. • CSA analyze relations and dependencies between assets. • CSA analyze documents threat initiator, method, tools, and entry points to inform the risk assessment process. (e.g. attack path analysis, attack feasibility) • CSA define threat scenario.	- Item definition & architecture design - Asset & Cybersecurity property Identification - Damage Scenario **Outputs** - Threat Scenario **Related standard** - ISO/SAE21434-15: v1.0 - ISO/SAE21434-9: v1.0

Exit criteria [Cybersecurity Architect] Threat scenarios should be defined including target assets, compromised cybersecurity properties and the action to achieve the damage scenario.

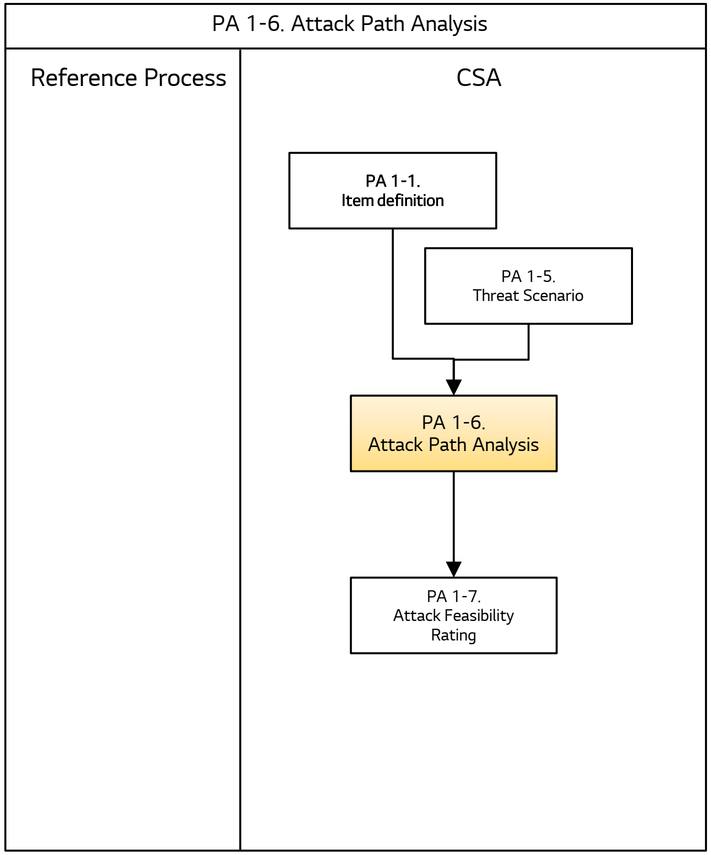
O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

1-6. Attack Path Analysis

◆ **Cybersecurity Architect analyze possible attack paths on the vehicle.**

Entry criteria Threat scenario should exist.

Procedure


PA 1-6. Attack Path Analysis
Reference Process
CSA
PA 1-1. Item definition
PA 1-5. Threat Scenario
PA 1-6. Attack Path Analysis
PA 1-7. Attack Feasibility Rating

Detailed activity

Cybersecurity Architect analyze attack path

[Description in detail]

- CSA analyzes threat scenario and describe possible attack paths.
- CSA documents the applied attack path.
- CSA refers to the threat scenarios that can be realized by the attack path.
- CSA updates the attack paths as more information becomes available over the lifecycle (e.g. after a vulnerability analysis)

Inputs

- item definition
- threat scenarios

Outputs

- Identified attack paths

Related standard

- ISO/SAE21434-15: v1.0
- ISO/SAE21434-9: v1.0

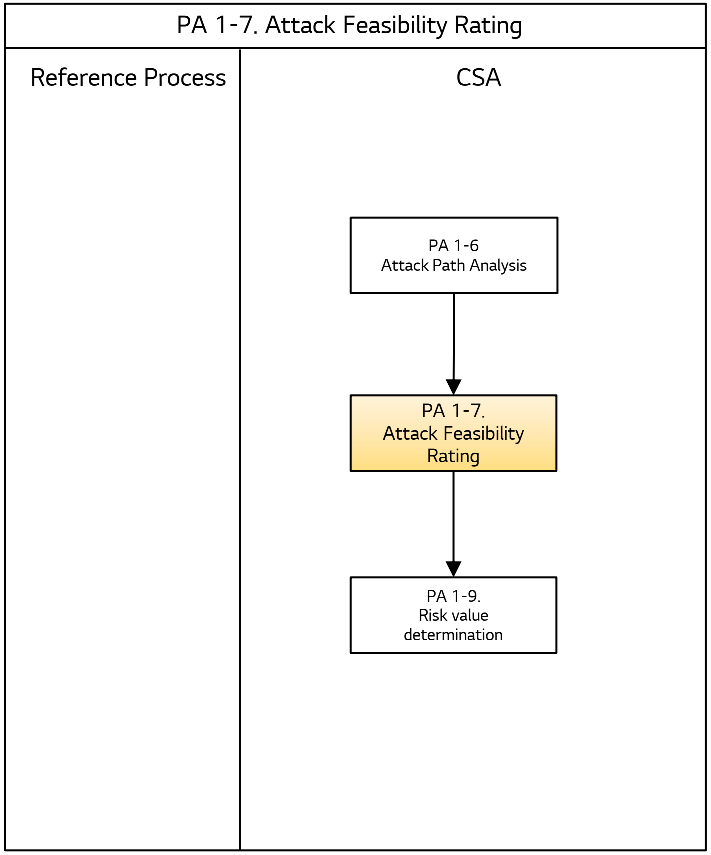
Exit criteria [**Cybersecurity Architect**] The attack path should be identified within the threat scenario.

O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

1-7. Attack Feasibility Rating

◆ Cybersecurity Architect determines the risk response by identifying the possible Threats on the vehicle.

Entry criteria Attack paths should exist.

Procedure	Detailed activity	Inputs
	**Cybersecurity Architect determine attack feasibility rating** **[Description in detail]** • CSA decides the attack feasibility rating by High, Medium, Low, and Very Low. • CSA uses attack potential-based approach for the assessment approach. • CSA determines the attack feasibility rating based on core factors including elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, and equipment. • The core attack potential factors can be derived from ISO/IEC 18045. ※ The TARA rating criteria and Risk Matrix are described on the following collaboration page. - http://collab.lge.com/main/x/ETg3Tw	- Attack Path Analysis **Outputs** - Attack Feasibility Rating **Related standard** - ISO/SAE21434-15: v1.0 - ISO/SAE21434-9: v1.0

PA 1-7. Attack Feasibility Rating
Reference Process
CSA
PA 1-6 Attack Path Analysis
PA 1-7. Attack Feasibility Rating
PA 1-9. Risk value determination

Exit criteria **[Cybersecurity Architect]** Attack feasibility rating should be determined.

O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

1-8. Impact Rating

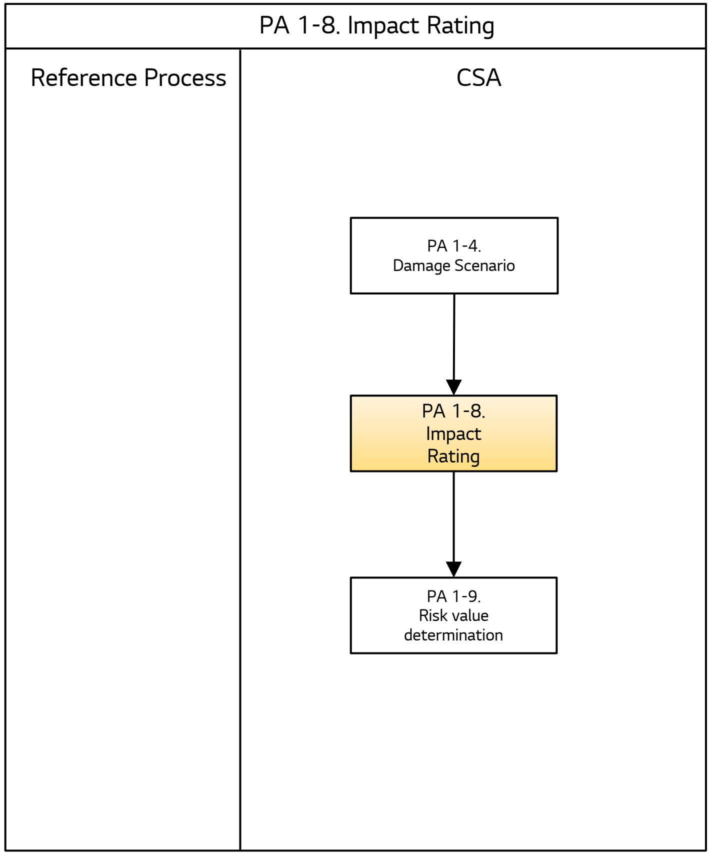
LGE Internal Use Only

Cybersecurity Concept Definition

◆ **Cybersecurity Architect determines the risk response by identifying the possible Threats on the vehicle.**

Entry criteria Damage scenario should exist.

Procedure


PA 1-8. Impact Rating

Reference Process | CSA

PA 1-4. Damage Scenario → PA 1-8. Impact Rating → PA 1-9. Risk value determination

Detailed activity

Cybersecurity Architect determine impact rating

[Description in detail]

- CSA assess the damage scenario against potential adverse consequences for stakeholders in the independent impact categories of safety, financial, operational, and privacy (S, F, O, P).
- CSA documents any impact categories other than S, F, O, and P.
- CSA determines the impact ratings as a Severe, Major, Moderate, Negligible.

※ The TARA rating criteria and Risk Matrix are described on the following collaboration page.

- http://collab.lge.com/main/x/ETg3Tw

Inputs

- Damage scenario

Outputs

- Impact rating, including the associated impact categories of the damage scenarios

Related standard

- ISO/SAE21434-15: v1.0
- ISO/SAE21434-9: v1.0

Exit criteria **[Cybersecurity Architect]** Impact rating should be created with the associated impact categories in the damage scenarios

O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

LGE Internal Use Only

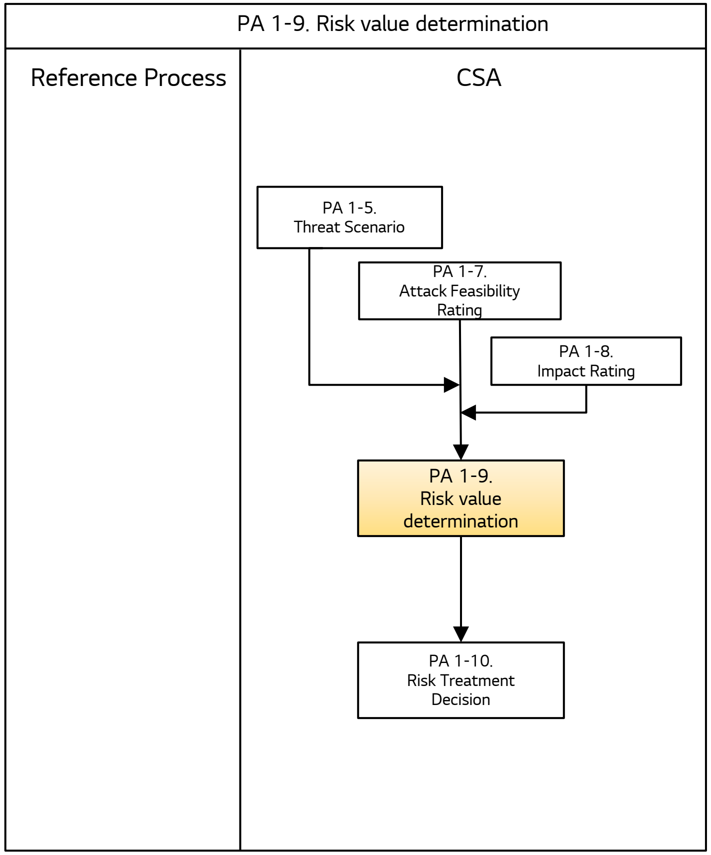
1-9. Risk value determination

Cybersecurity Concept Definition

◆ **Cybersecurity Architect determines the risk response by identifying the possible Threats on the vehicle.**

Entry criteria Impact rating and Attack feasibility rating should determine.

Procedure



PA 1-9. Risk value determination
Reference Process
CSA
PA 1-5. Threat Scenario
PA 1-7. Attack Feasibility Rating
PA 1-8. Impact Rating
PA 1-9. Risk value determination
PA 1-10. Risk Treatment Decision

Detailed activity

Cybersecurity Architect decide risk value

[Description in detail]

- CSA analyzes the impact of the associated damage scenario.
- CSA analyzes the attack feasibility of the associated attack paths.
- For each threat scenario the risk value shall be determined from the impact of the associated damage scenarios and the attack feasibility of the associated attack paths
- CSA determines the risk value based on risk matrices.
- The value 1 is the lowest risk and value 5 is the highest risk.
- Depending on the threat scenario that corresponds to more than one attack path, the attack feasibility may be different.
- (e.g. the threat scenario is assigned the maximum of the feasibility levels of the corresponding attack paths.)

※ The TARA rating criteria and Risk Matrix are described on the following collaboration page.

- http://collab.lge.com/main/x/ETg3Tw

Inputs

- Threat scenario
- impact rating
- attack feasibility rating

Outputs

- Risk value

Related standard

- ISO/SAE21434-15: v1.0
- ISO/SAE21434-9: v1.0

Exit criteria [Cybersecurity Architect] Risk value should be decided.

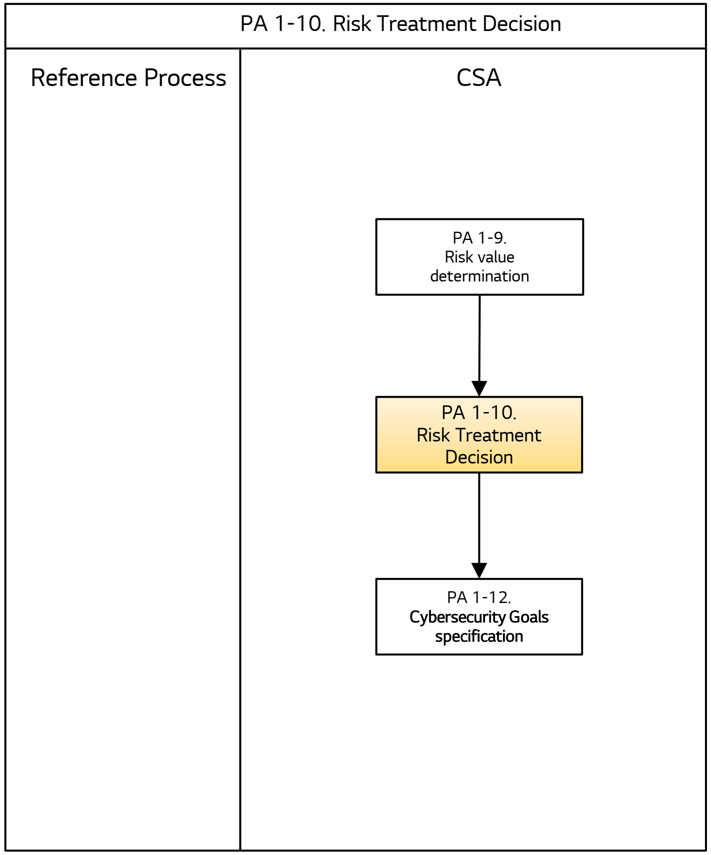
O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

1-10. Risk Treatment Decision

◆ **Cybersecurity Architect determines the risk response by identifying the possible Threats on the vehicle.**

Entry criteria Threat scenario with risk value should exist

Procedure


PA 1-10. Risk Treatment Decision
Reference Process
CSA
PA 1-9. Risk value determination
PA 1-10. Risk Treatment Decision
PA 1-12. Cybersecurity Goals specification

Detailed activity

Cybersecurity Architect establish risk treatment

[Description in detail]

- CSA analyzes impact categories, attack paths, and the results from risk determination.
- CSA determines and documents the risk treatment.
- Risk treatment options are determined by:

1. avoid the risk by removing the risk sources, or deciding not to start or continue with the activity that gives rise to the risk
2. reduce the risk
3. share or transfer the risk (e.g. through contracts, buying insurance).
4. accept or retain the risk

※ The TARA rating criteria and Risk Matrix are described on the following collaboration page.

- http://collab.lge.com/main/x/ETg3Tw

Inputs

- Item definition shall be available
- Impact categories from impact rating shall be available
- Threat scenarios shall be available
- Identified attack paths shall be available
- Corresponding risk values shall be available

Outputs

- Risk treatment decision per threat scenario

Related standard

- ISO/SAE21434-15: v1.0
- ISO/SAE21434-9: v1.0

Exit criteria [**Cybersecurity Architect**] Risk treatment should be established.

O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

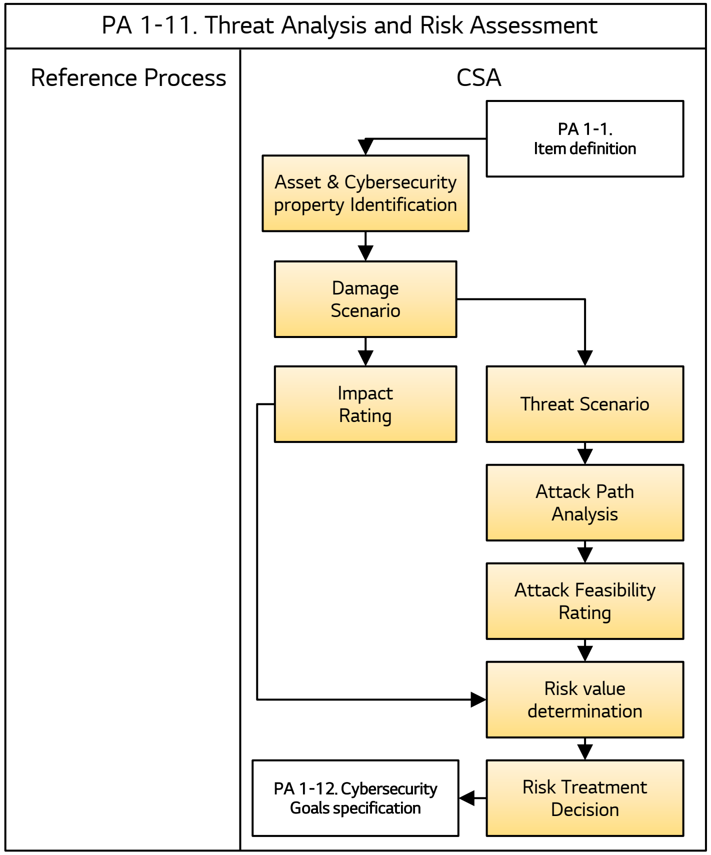
1-11. Threat Analysis and Risk Assessment

Cybersecurity Concept Definition

◆ **Cybersecurity Architect determines the risk response by identifying the possible Threats on the vehicle.**

Entry criteria Item definition to analyze threat must be completed.

Procedure


PA 1-11. Threat Analysis and Risk Assessment

Reference Process

CSA

PA 1-1. Item definition

Asset & Cybersecurity property Identification

Damage Scenario

Impact Rating

Threat Scenario

Attack Path Analysis

Attack Feasibility Rating

Risk value determination

Risk Treatment Decision

PA 1-12. Cybersecurity Goals specification

Detailed activity

Summary page for PA 1-3 ~ PA 1-10

Cybersecurity Architect determines the Risk Treatment by deriving assets from higher level(items), identifying and analyzing possible Threats.

[Description in detail]

- CSA identifies assets and cybersecurity attributes from higher level (item).
- CSA should create the damage scenarios with identified assets and cybersecurity properties (based on loss of security property of asset).
- CSA measures Impact Rating from the identified Damage Scenario.
- CSA derives Threat Scenario from the identified Damage Scenario.
- CSA analyzes the Attack Path from Threat Scenario and derives it. (Consider past weakness and derive the attack path.)
- CSA determines the Attack Feasibility Rating by measuring the feasibility of an attack from Attack Path.
- CSA measures Risk Value based on Impact Rating and Attack Feasibility Rating.
- CSA determines Risk Treatment based on Threat Scenario with consideration of impact ratings with impact categories, attack path, attack feasibility rating.

※ The TARA Guideline is described on the following collaboration page.
- http://collab.lge.com/main/x/OSdgXg

※ When CSA requests information necessary for TARA process, System and SW architect will provide it.

Inputs

- Item Definition
- Damage Scenario
- Identified assets and cybersecurity properties
- Threat Scenario
- Impact Rating
- Attack Path
- Attack Feasibility Rating
- Risk Value
- Risk treatment decision

Outputs

- TARA report

Related standard

- ISO/SAE21434-15:v1.0
- ISO/SAE21434-9:v1.0

Exit criteria [Cybersecurity Architect] All possible Threats in the item should be analyzed, and the related risk treatment should selected and determined.

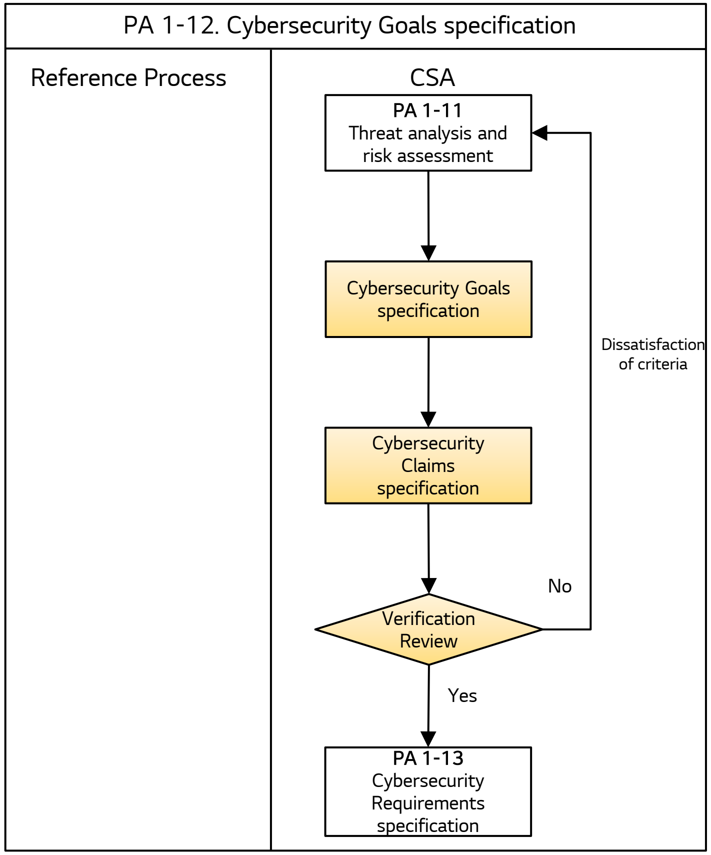
O This is performed by applying the threat analysis of OEMs or if the requirements of OEMs exist.

1-12. Cybersecurity Goals specification

◆ **Cybersecurity Architect describes cybersecurity goals and cybersecurity claims according to risk assessment results.**

Entry criteria Threat Analysis and Risk assessment (TARA) should be completed for the item.

Procedure



PA 1-12. Cybersecurity Goals specification

Reference Process

CSA

PA 1-11 Threat analysis and risk assessment

Cybersecurity Goals specification

Cybersecurity Claims specification

Verification Review

No

Dissatisfaction of criteria

Yes

PA 1-13 Cybersecurity Requirements specification

Detailed activity

Cybersecurity Architect describes cybersecurity goals and cybersecurity claims according to risk assessment results.

[Description in detail]

- CSA specifies one or more cybersecurity goals for the threat scenario about determined risk reduction item.
- CSA describes cybersecurity claims for the threat scenario about determined risk acceptance, transfer or share.
- CSA performs the Review about cybersecurity goals and claims.

[Review]
The activities to specify cybersecurity goals and cybersecurity claims shall be verified to:
a) confirm consistency of the analysis;
b) confirm consistency of the risk treatment decisions;
c) confirm consistency and completeness of the cybersecurity goals with respect to the threat scenarios;
d) consistency between different cybersecurity goals.

Inputs

- Item definition
- TARA report
- Risk treatment decision result

Outputs

- Cybersecurity goals
- Cybersecurity claims
- Verification report of cybersecurity concept

Related standard

- ISO SAE 21434-9 : v1.0

Exit criteria [Cybersecurity Architect] Cybersecurity goals and cybersecurity claims should be specified.

O This is OEM’s responsibility, so only performed when OEM requests or the item is developed without OEM.

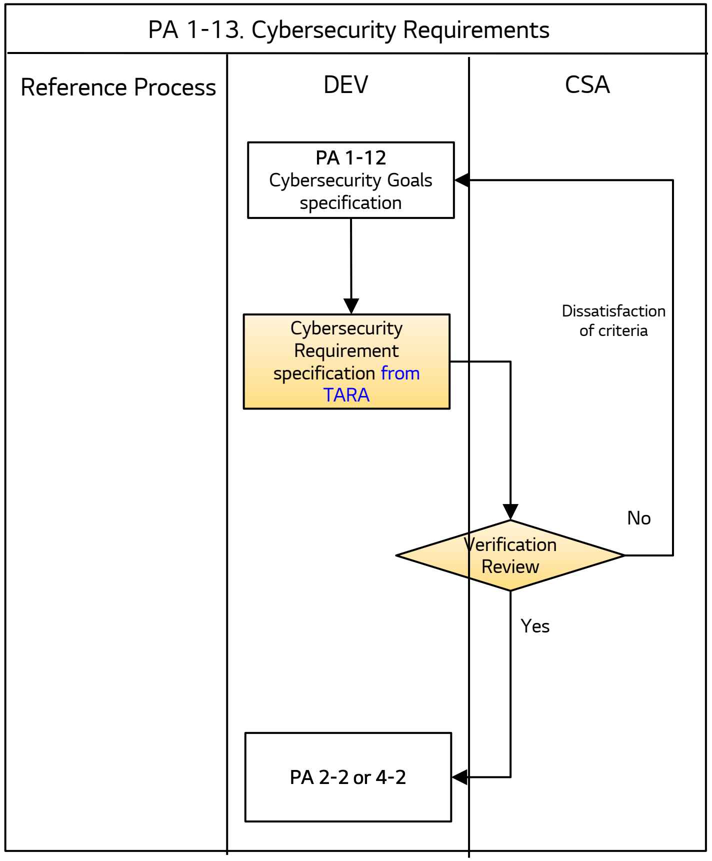
1-13. Cybersecurity Requirements specification

Cybersecurity Concept Definition

◆ Cybersecurity Architect specifies cybersecurity requirements and allocate them to the item and/or the operational environment.

Entry criteria cybersecurity goals and cybersecurity claims should be specified.

Procedure


PA 1-13. Cybersecurity Requirements
Reference Process
DEV
CSA
PA 1-12 Cybersecurity Goals specification
Cybersecurity Requirement specification from TARA
Dissatisfaction of criteria
No
Verification Review
Yes
PA 2-2 or 4-2

Detailed activity

Cybersecurity Architect specifies cybersecurity requirements and allocate them to the item and/or the operational environment.

[Description in detail]

- CSA describe cybersecurity controls and their interaction to achieve the cybersecurity goals.
- DEV derives cybersecurity requirements from the Cybersecurity goal and control.
- DEV analyzes the security objectives and specifies the security concepts to achieve them.
  - cybersecurity requirements include a rationale for the achievement of the cybersecurity goals.
  - Allocate cybersecurity requirements to one or more components of the item or to the operational environment.
- CSA perform the Review about cybersecurity requirements.

[Review]
The cybersecurity requirements and their allocation shall be verified to confirm:
a) consistency with the cybersecurity goals
b) completeness with respect to the cybersecurity goals
c) consistency and compatibility with the functionality of the item

Inputs

- Item definition
- TARA report
- Cybersecurity Goals

Outputs

- Cybersecurity concept
- Verification report of cybersecurity concept

Related standard

- ISO SAE 21434-9 : v1.0

Exit criteria [Developer] Cybersecurity requirements should be specified.

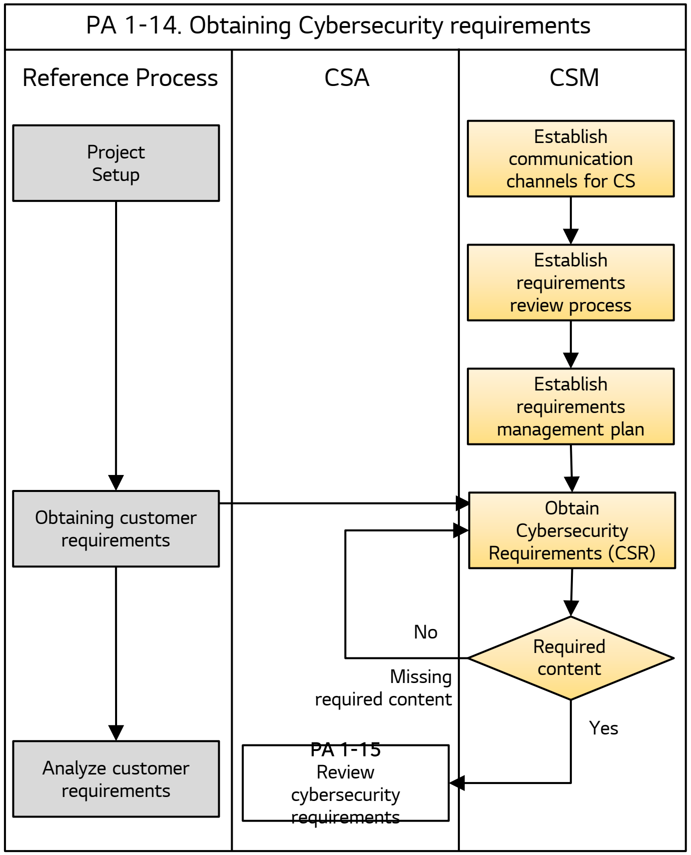
O This is OEM's responsibility, so only performed when OEM requests or the item is developed without OEM.

1- 14. Obtaining Cybersecurity requirements

◆ **Cybersecurity Manager obtains cybersecurity requirements from the customer in accordance with the development schedule.**

Entry criteria An organization should be organized to perform the project.

Procedure


PA 1-14. Obtaining Cybersecurity requirements
Reference Process
CSA
CSM
Project Setup
Establish communication channels for CS
Establish requirements review process
Establish requirements management plan
Obtaining customer requirements
Obtain Cybersecurity Requirements (CSR)
No
Required content
Missing required content
Yes
Analyze customer requirements
PA 1-15 Review cybersecurity requirements

Detailed activity

Cybersecurity Manager obtains cybersecurity requirements for the development of cybersecurity systems.

[Description in detail]

- CSM establishes a communication channel with the OEM for cybersecurity.
- CSM establishes the feasibility review process for OEM requirements.
- CSM agrees with OEMs how to manage cybersecurity requirements.
- CSM agrees with OEMs when to establish cybersecurity requirements.
- CSM obtains cybersecurity requirements(CSR).
- CSM reviews whether the cybersecurity requirement contains all the required content.

[Cybersecurity requirements shall include the following]

- Requirement identifier(ID)
- Cybersecurity goal (SG)
- Cybersecurity requirements
- CAL

Inputs

- Customer requirements

Outputs

- Cybersecurity goal
- Cybersecurity requirements (CSR)

Related standard

- ISO SAE 21434-9 :v1.0

Exit criteria [Cybersecurity Manager] Obtain cybersecurity requirements that include mandatory content and pass them to the CSA.

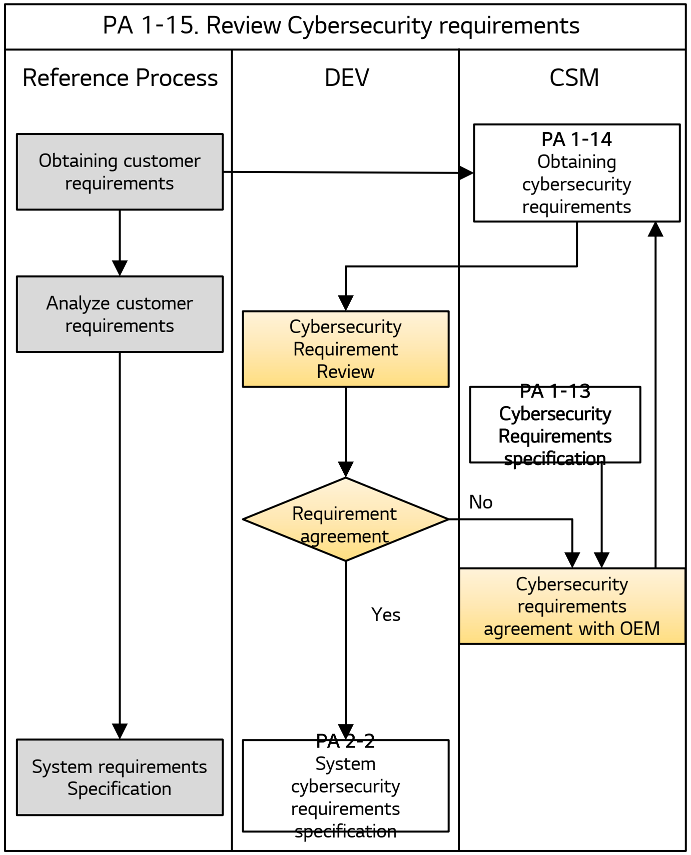
M If you do not perform any mandatory process, you should have a reasonable rationale.

1-15. Review Cybersecurity requirements

◆ Cybersecurity Architect reviews the feasibility of obtaining Cybersecurity requirements from customers.

Entry criteria Cybersecurity Manager should obtain cybersecurity requirements from the customer.

Procedure


PA 1-15. Review Cybersecurity requirements
Reference Process
DEV
CSM
Obtaining customer requirements
PA 1-14 Obtaining cybersecurity requirements
Analyze customer requirements
Cybersecurity Requirement Review
PA 1-13 Cybersecurity Requirements specification
Requirement agreement
No
Cybersecurity requirements agreement with OEM
Yes
System requirements Specification
PA 2-2 System cybersecurity requirements specification

Detailed activity

Cybersecurity Architect reviews the feasibility of cybersecurity requirements received from Cybersecurity Manager.

[Description in detail]

- Developer(DEV) reviews the feasibility of cybersecurity requirements.
- DEV classifies cybersecurity requirements and agrees with relevant domain experts on the results of the feasibility review.
- DEV notifies to Cybersecurity Manager of the requirements that impossible to implement.
- CSM discusses with OEMs whether or not the requirements derived through TARA results are reflected.
- CSM negotiates with OEMs on non-feasible Cybersecurity requirements.
- CSM obtains updated Cybersecurity requirements as a result of OEM negotiations.

Inputs

- Cybersecurity goal
- Cybersecurity requirements

Outputs

- Feasibility report for Cybersecurity requirements

Related standard

- ISO SAE 21434-9 :v1.0

Exit criteria [Cybersecurity Manager] A feasibility review should be completed for all cybersecurity requirements requested by the customer.

M If you do not perform any mandatory process, you should have a reasonable rationale.

2 Cybersecurity System Development Phase

- **Objective**

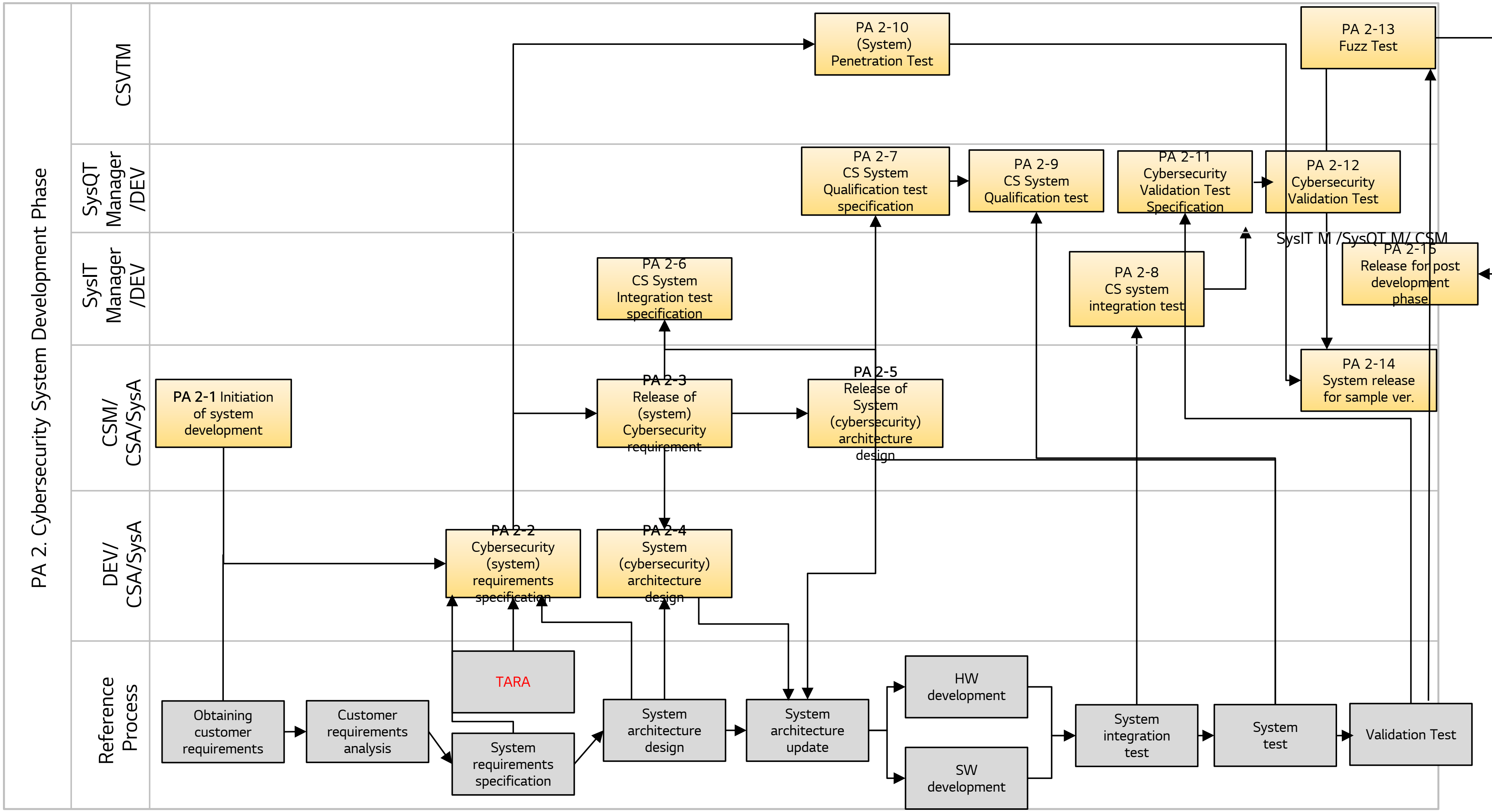
  Define system development steps to achieve cybersecurity goal and define key activities and criteria by stage.

- **Scope**

  This applies when developing an item that applies cybersecurity to the electrical and electronic(E/E) system.

2 Cybersecurity System Development Phase

Define the system development phase of the item to which cybersecurity is applied among the E/E system developed by the VS company, and define the main activities and standards by stages.


PA 2. Cybersecurity System Development Phase
CSVTM
SysQT Manager /DEV
SysIT Manager /DEV
CSM/ CSA/SysA
DEV/ CSA/SysA
Reference Process
PA 2-10 (System) Penetration Test
PA 2-13 Fuzz Test
PA 2-7 CS System Qualification test specification
PA 2-9 CS System Qualification test
PA 2-11 Cybersecurity Validation Test Specification
PA 2-12 Cybersecurity Validation Test
SysIT M /SysQT M/ CSM
PA 2-15 Release for post development phase
PA 2-6 CS System Integration test specification
PA 2-8 CS system integration test
PA 2-14 System release for sample ver.
PA 2-1 Initiation of system development
PA 2-3 Release of (system) Cybersecurity requirement
PA 2-5 Release of System (cybersecurity) architecture design
PA 2-2 Cybersecurity (system) requirements specification
PA 2-4 System (cybersecurity) architecture design
TARA
Obtaining customer requirements
Customer requirements analysis
System requirements specification
System architecture design
System architecture update
HW development
SW development
System integration test
System test
Validation Test

2 Related ISO/SAE 21434 standard for cybersecurity system development(1/2)

Option	Process Area	Description	Role	Work product	Related standard
M	**PA 2-1.** Initiation of system development	Determine the cybersecurity activities to be carried out in stages and system development plan.	Cybersecurity Manager	• Project plan [refined] • Cybersecurity plan [refined] • Test plan (SysIT, SysQT) • Verification review plan • Cybersecurity assessment plan [refined]	- ISO/SAE 21434- v1.0
M	**PA 2-2.** (system)Cybersecurity requirements specification	Analyze cybersecurity concept to create system-level cybersecurity requirements.	Developer	• (System)cybersecurity requirement • (Included) Cybersecurity requirement for post-development • Traceability matrix(Concept-SysCSR) • VR report(SysCSR) • Cybersecurity plan [refined]	- ISO/SAE 21434-10: v1.0
M	**PA 2-3.** Release of (system)cybersecurity requirements	Determine and distribute (system)cybersecurity requirements.	Cybersecurity Manager	• (System)cybersecurity requirements [confirmed] • Traceability matrix (Concept-SysCSR) [confirmed]	- ISO/SAE 21434-10: v1.0
M	**PA 2-4.** System (cybersecurity) architecture design	Design system cybersecurity architecture to meet (system)cybersecurity requirements.	System Architect	• System (cybersecurity) architecture design • HW-SW interface(HSI) [refined] • Cybersecurity plan [refined]	- ISO/SAE 21434-10: v1.0
M	**PA 2-5.** Release of System (cybersecurity) architecture design	Analyze and confirm that the system (cybersecurity) architecture design is at an appropriate level.	Cybersecurity Manager	• System (cybersecurity) architecture design [confirmed] • System architecture design [refined] • Cybersecurity case [refined]	- ISO/SAE 21434-10: v1.0
M	PA 2-6. Cybersecurity System Integration Test Specification	System Integration Test Manager prepares cybersecurity Integration test specification.	System Integration Test Manager	• System Integration Test Case	- ISO/SAE 21434-10: v1.0
M	PA 2-7. Cybersecurity System Qualification Test Specification	System Qualification Test Manager prepares cybersecurity qualification test specification.	System Qualification Test Manager	• System Qualification Test Case	- ISO/SAE 21434-10: v1.0
M	PA 2-8. Cybersecurity System Integration Test	System Integration Test Manager performs the System Integration Test.	System Integration Test Manager	• System Integration Test Report	- ISO/SAE 21434-10: v1.0 - Automotive SPICE Process Assessment / Reference Model SYS.4

M Mandatory O Optional

2 Related ISO/SAE 21434 standard for cybersecurity system development(2/2)

Option	Process Area	Description	Role	Work product	Related standard
M	PA 2-9. Cybersecurity System Qualification Test	System Qualification Test Manager performs the System Qualification Test.	System Qualification Test Manager	• System Qualification Test Report	- ISO/SAE 21434-10: v1.0 - Automotive SPICE Process Assessment / Reference Model SYS.5
M	PA 2-10. (System) Penetration Test	(System) Penetration Test engineer performs (system) penetration test.	Penetration Test Manager	• (System) Penetration Test report	- ISO/SAE 21434-10: v1.0
O	PA 2-11. Cybersecurity Validation Test Specific	(Cybersecurity) Penetration Test Manager specifies the test specification of validation	Penetration Test Manager	• Cybersecurity validation test specification	- ISO/SAE 21434-11: v1.0
O	PA 2-12. Cybersecurity Validation Test	(Cybersecurity) Penetration Test Manager performs a cybersecurity validation test	Penetration Test Manager	• Cybersecurity Validation Test report	- ISO/SAE 21434-11: v1.0
O	PA 2-13. Fuzz Test	(Vehicle/System) Fuzz Test manager performs vehicle or system fuzz test.	CSVTM	• Fuzz test report	- ISO/SAE 21434-11: v1.0
M	**PA 2-14.** System release for sample version	Deploys the system under development at the item sample release time.	Cybersecurity Manager	• System sample release report • Cybersecurity case [refined]	- ISO/SAE 21434-10: v1.0
M	**PA 2-15.** Release for post development phase	In order to mass-production the items, the system is released to the production department after reviewing the contents of the cybersecurity activities.	Cybersecurity Manager	• Post Development report	- ISO/SAE 21434-10: v1.0

M Mandatory O Optional

2 Role & responsibility for cybersecurity system development (1/2) Cybersecurity System Development Phase

Process Area	Work Product	CSM	CSA	Developer	System Architec t	SW Architec t	SysIT Manager	SysQT Manager	RM	Cybersec urity Assessor	SW PL/PL
PA 2-1. Initiation of system development	• Project plan [refined] • Cybersecurity plan [refined] • Test plan (SysIT, SysQT) • Verification review plan • Cybersecurity assessment plan [refined]	R	I	-	-	-	S	S	-	I	-
PA 2-2. (system)Cybersecurity requirements specification	• (System)cybersecurity requirement • (Included) Cybersecurity requirement for post-development • Traceability matrix(Concept-SysCSR) • VR report(SysCSR) • Cybersecurity plan [refined]	I	S	R	-	-	I	S	S	-	-
PA 2-3. Release of (system)cybersecurity requirements	• (System)cybersecurity requirements [confirmed] • Traceability matrix (Concept-SysCSR) [confirmed]	I	S	S	I	I	I	S	R	-	A
PA 2-4. System (cybersecurity) architecture design	• System (cybersecurity) architecture design • HW-SW interface(HSI) [refined] • Cybersecurity plan [refined]	I	S	S	R	S	S	I	I	-	-
PA 2-5. Release of System (cybersecurity) architecture design	• System (cybersecurity) architecture design [confirmed] • System architecture design [refined] • Cybersecurity case [refined]	I	S	S	R	I	S	I	I	-	A
PA 2-6. Cybersecurity System Integration Test Specification	• System Integration Test Case	I	S	S	S	-	R	I	-	-	-
PA 2-7. Cybersecurity System Qualification Test Specification	• System Qualification Test Case	I	S	S	S	-	I	R	-	-	-
PA 2-8. Cybersecurity System Integration Test	• System Integration Test Report	I	S	S	S	-	R	I	-	-	A
PA 2-9. Cybersecurity System Qualification Test	• System Qualification Test Report	I	S	S	S	-	I	R	-	-	A

R : Responsibility , A : Approval, S : Support , I : Informed

LGE Internal Use Only

2 Role & responsibility for cybersecurity system development (2/2) Cybersecurity System Development Phase

Process Area	Work Product	CSM	CSA	Developer	System Architect	SysIT Manager	SysQT Manager	DQA	PTM	CSVTM	Cybersecurity Assessor	SW PL/PL
PA 2-10. (System) Penetration Test	• (System) Penetration Test report	I	S	-	-	-	I	-	R	-	-	S
PA 2-11. Cybersecurity Validation Test Specification	• Cybersecurity validation test specification	I	I	-	-	-	R	-	-	-	-	-
PA 2-12. Cybersecurity Validation Test	• Cybersecurity Validation Test report	I	I	-	-	-	R	A	-	I	-	-
PA 2-13 (Vehicle) Fuzz Test	• Fuzz test report	I	S	-	-	-	-	-	-	R	-	-
PA 2-14. System release for sample version	• System sample release report • Cybersecurity case [refined]	S	S	S	S	I	S	-	-	I	I	R,A
PA 2-15. Release for post development phase	• Post Development report	S	S	S	S	I	S	-	-	I	S	R,A

R : Responsibility , A : Approval, S : Support , I : Informed

LGE Internal Use Only

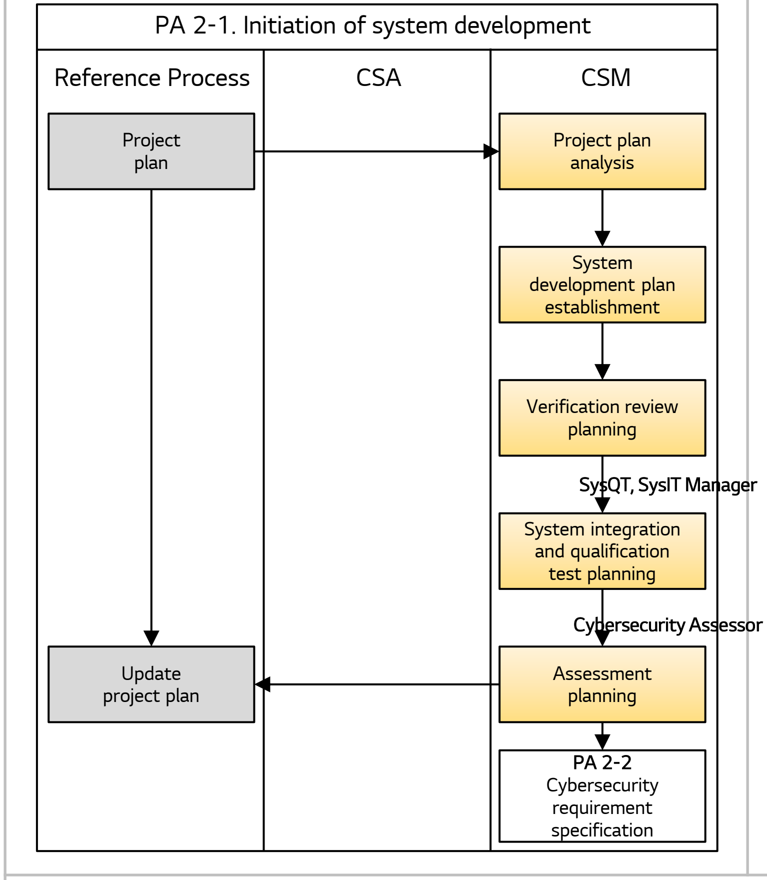
2-1. Initiation of system development

Cybersecurity System Development Phase

◆ Cybersecurity Manager determines and plans the cybersecurity activities to be performed during the system development phase.

Entry criteria An organization should be organized to perform the project.

Procedure



PA 2-1. Initiation of system development

Reference Process | CSA | CSM

Project plan

Project plan analysis

System development plan establishment

Verification review planning

SysQT, SysIT Manager

System integration and qualification test planning

Cybersecurity Assessor

Assessment planning

PA 2-2 Cybersecurity requirement specification

Update project plan

Detailed activity

Cybersecurity Manager determines and plans the cybersecurity activities required for development prior to system development.

[Description in detail]

- CSM analyzes the project plan and identifies the schedule required for system development.
- CSM tailors the contents of the standard process to establish a cybersecurity system development plan and update the cybersecurity plan.
- CSM establishes a VR plan for the work product of the system development phase and specifies it in the cybersecurity plan.
- System test managers establish a system level test plan and updates the test plan.
- Cybersecurity accessor establishes and updates the assessment plan.

Inputs

- Project plan
- Cybersecurity plan
- Cybersecurity concept
- Cybersecurity assessment plan

Outputs

- Project plan [refined]
- Cybersecurity plan [refined]
- Test plan (SysIT, SysQT)
- Verification review plan
- Cybersecurity assessment plan [refined]

Related standard

- ISO/SAE 21434-10: v1.0

Exit criteria [Cybersecurity Manager] All the system development plans should be reflected in the output required by PA 2-1.

M If you do not perform any mandatory process, you should have a reasonable rationale.

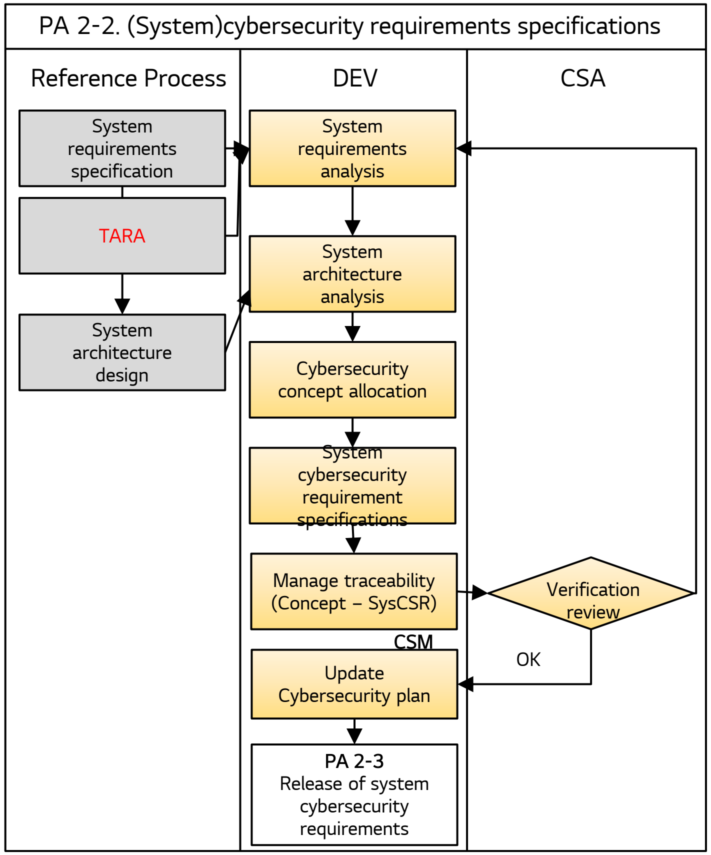
2- 2. (System)Cybersecurity requirements specifications

Cybersecurity System Development Phase

◆ **Developer specifies (system)cybersecurity requirements from a system point of view by analyzing cybersecurity concepts.**

Entry criteria A feasibility review should be completed for all cybersecurity concept requested by the customer.

Procedure



PA 2-2. (System)cybersecurity requirements specifications

Reference Process | DEV | CSA

System requirements specification

TARA

System architecture design

System requirements analysis

System architecture analysis

Cybersecurity concept allocation

System cybersecurity requirement specifications

Manage traceability (Concept – SysCSR)

Verification review

OK

CSM

Update Cybersecurity plan

PA 2-3 Release of system cybersecurity requirements

Detailed activity

Developer(DEV) **specifies the (system)cybersecurity requirements by analyzing the cybersecurity concepts for which the feasibility review has been completed.**

[Description in detail]

- DEV analyzes the cybersecurity concepts allocated from higher level.
- DEV analyzes the cybersecurity goals and claims and select security functions to apply component level elements.
- DEV analyzes system requirements to determine if there are any items that need to be included in cybersecurity requirements.
- DEV analyzes the cybersecurity concepts to determine which system element is responsible.
- DEV refines the cybersecurity requirements that an component level element should perform.
- DEV considers and update the cybersecurity implications of post-development phase during the refinement of cybersecurity requirements.
- DEV specifies and allocates to the relevant entities of the operational environment if specific procedures are required to ensure cybersecurity in post-development phases.
- DEV specifies the procedures to ensure cybersecurity after the development of the component if applicable.
- DEV links traceability between cybersecurity concepts and (system)cybersecurity requirements.
- CSA/RM performs verification review(VR) on (system)cybersecurity requirements.

Inputs

- Cybersecurity goal
- Cybersecurity claims(if applicable)
- Cybersecurity concept
- Known weaknesses and vulnerabilities from used systems(if applicable)

Outputs

- (System)cybersecurity requirement
- (Included) Cybersecurity requirement for post-development
- Traceability matrix (Concept-SysCSR)
- VR report(SysCSR)
- Cybersecurity plan [refined]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Developer] All cybersecurity requirements shall be specified as (system)cybersecurity requirements and shall pass verification review criteria

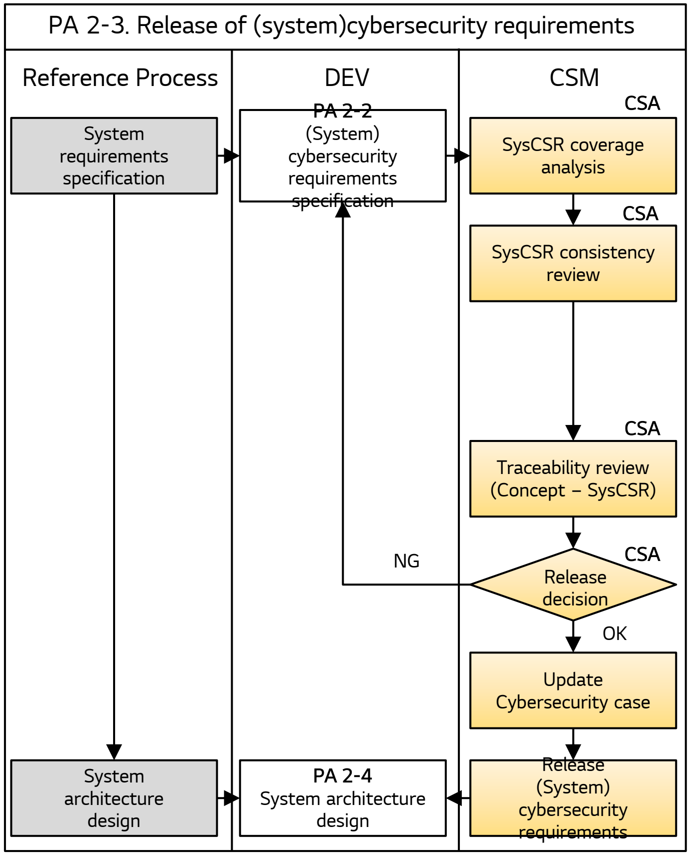
M If you do not perform any mandatory process, you should have a reasonable rationale.

2-3. Release of (system)cybersecurity requirements

◆ **Cybersecurity Architect reviews specified (system)cybersecurity requirements and Cybersecurity Manager confirms and releases them.**

Entry criteria The (system)cybersecurity requirements should pass the verification review criteria.

Procedure



PA 2-3. Release of (system)cybersecurity requirements

Reference Process
DEV
CSM
System requirements specification
PA 2-2 (System) cybersecurity requirements specification
CSA
SysCSR coverage analysis
CSA
SysCSR consistency review
CSA
Traceability review (Concept – SysCSR)
CSA
Release decision
NG
OK
Update Cybersecurity case
Release (System) cybersecurity requirements
System architecture design
PA 2-4 System architecture design

Detailed activity

Cybersecurity Architect reviews the completion of the (system)cybersecurity requirements and cybersecurity manager confirms them.

[Description in detail]

- CSA verifies the refined (system)cybersecurity requirements to ensure the completeness, correctness and adequacy with the cybersecurity concept from higher level.
- CSA reviews whether all cybersecurity concepts are specified as (system)cybersecurity requirements.
- CSA reviews each specified SysCSR to ensure that it is accurate and verifiable.
- CSM reviews each item in the SysCSR to see if a unique ID has been allocated.
- CSA reviews whether verification review(VR) is completed and VR results are reflected in SysCSR.
- CSA reviews the traceability between cybersecurity concept and SysCSR.
- CSM updates the argument of SysCSR to the cybersecurity case.
- CSM assigns a version to the SysCSR and releases it to the document management system.

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

- (System)cybersecurity requirement
- Traceability matrix (Concept-CSR)

Outputs

- (System)cybersecurity requirements [confirmed]
- Traceability matrix (Concept-SysCSR) [confirmed]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] (System)cybersecurity requirements should be assigned a version and released through the document management system.

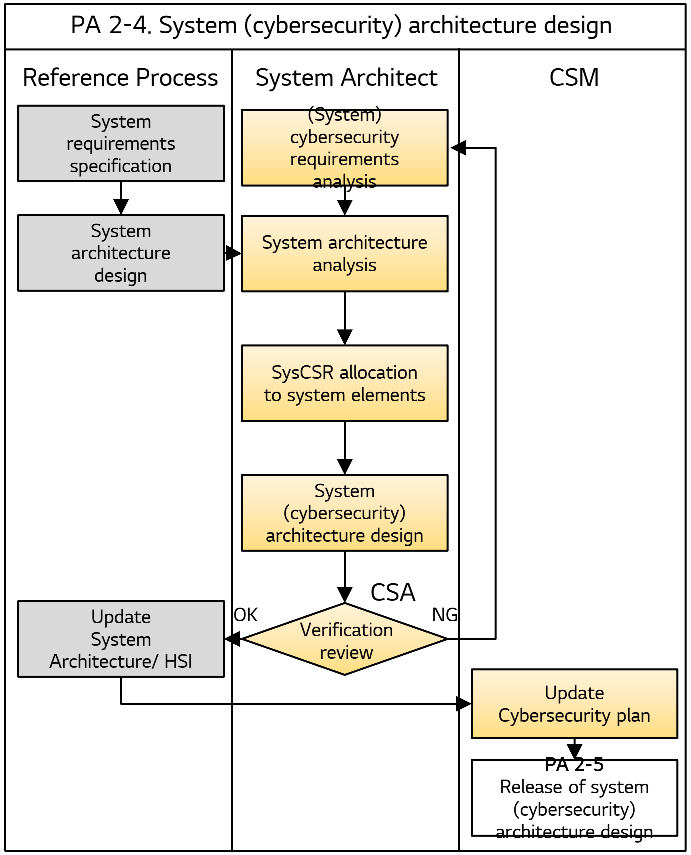
M If you do not perform any mandatory process, you should have a reasonable rationale.

2-4. System (cybersecurity) architecture design

◆ **System Architect designs system architecture to meet (system)cybersecurity requirements.**

Entry criteria (The system)cybersecurity requirements shall be finalized and released.

Procedure


PA 2-4. System (cybersecurity) architecture design
Reference Process
System Architect
CSM
System requirements specification
System architecture design
(System) cybersecurity requirements analysis
System architecture analysis
SysCSR allocation to system elements
System (cybersecurity) architecture design
CSA
OK
NG
Verification review
Update System Architecture/ HSI
Update Cybersecurity plan
PA 2-5
Release of system (cybersecurity) architecture design

Detailed activity

System Architect **designs the cybersecurity architecture of the system to achieve the (system)cybersecurity requirements(sysCSR).**

[Description in detail]

- SysA analyzes the initial architecture design and the cybersecurity controls (if applicable).
- SysA analyzes the refined system cybersecurity requirements and the higher level architecture design including the operational environment
- SysA allocates the defined cybersecurity requirements to components of the architectural design.
- SysA refines the architecture design to apply architecture design principles avoiding or minimizing the introduction of weaknesses
- SysA analyzes the system architecture and allocates the SysCSR, and adds the system element if there is no system element to allocate the SysCSR.
- SysA designs he interfaces between components of the refined architecture design related to the fulfillment of the refined cybersecurity requirements shall be identified and described including the purposes, usages, parameters (explicit inputs to and outputs from an interface) and allowed range of data in the interface.
- SysA designs the interface between hardware and software and refine in order to allow for the correct usage of cybersecurity control.
- SysA designs the Interfaces which can be a potential entry point for cybersecurity attacks.
- SysA specifies the role allocated to the system element.
- SysA updates cybersecurity design to the system architecture and HSI.
- CSA performs verification review(VR) on System (cybersecurity) architecture design. CSA ensures cybersecurity control for risks are correctly implemented and risks are mitigated

Inputs

- (System)cybersecurity requirements
- System architecture design (SysAD)
- Known weaknesses and vulnerabilities from the used systems

Outputs

- System (cybersecurity) architecture design
- HW-SW interface(HSI) [refined]
- Cybersecurity plan [refined]

Related standard

- ISO/SAE21434-10:v1.0

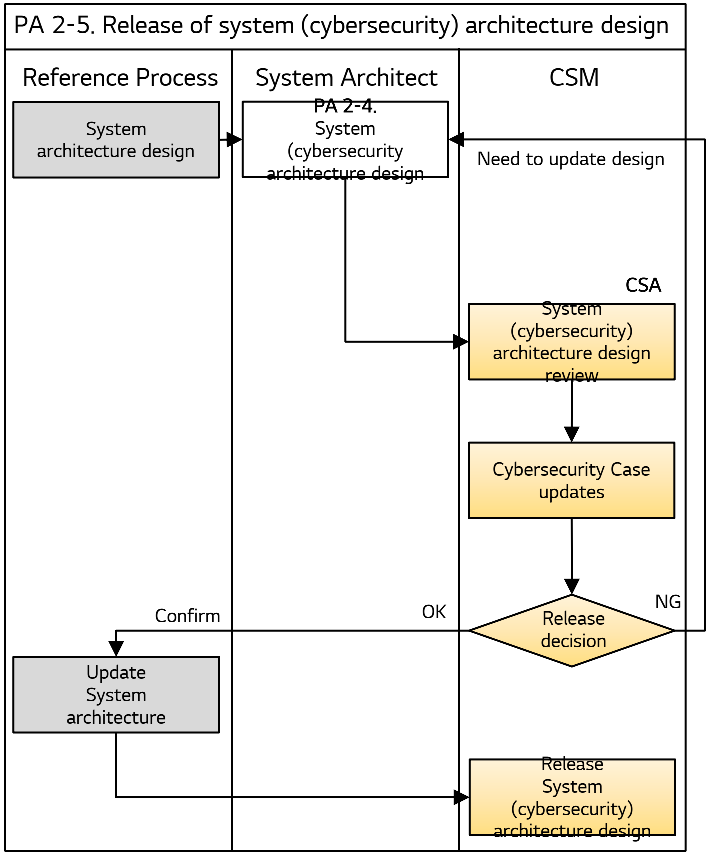
Exit criteria [System Architect] The (system cybersecurity) architecture design should be reflected in the system architecture.

M If you do not perform any mandatory process, you should have a reasonable rationale.

2-5. Release of system (cybersecurity) architecture design

◆ Cybersecurity Architect reviews the level of system (cybersecurity) architecture design and Cybersecurity Manager confirms and releases them.

Entry criteria The refined system (cybersecurity) architecture design should be passed the verification review criteria.

Procedure	Detailed activity	Inputs
	**Cybersecurity Architect reviews whether the system (cybersecurity) architecture design is properly designed and meets cybersecurity requirements and Cybersecurity Manager confirms them.** **[Description in detail]** • CSA reviews whether the system (cybersecurity) architecture design is properly designed to meet all the requirements of the cybersecurity. • CSM determines whether system (cybersecurity) architecture design is available for distribution. • CSM assigns a version to the system (cybersecurity) architecture design and releases it to the document management system. • System Architect updates the reflect changes in the system cybersecurity architecture design to the system architecture. • CSM releases system (cybersecurity) architecture design to the document management system. **※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.**	- System cybersecurity requirement - System (cybersecurity) architecture design - HW-SW interface(HSI) [refined] **Outputs** - System (cybersecurity) architecture design [confirmed] - System architecture design [refined] - Cybersecurity case [refined] **Related standard** - ISO/SAE21434-10:v1.0

PA 2-5. Release of system (cybersecurity) architecture design
Reference Process
System Architect
CSM
System architecture design
PA 2-4. System (cybersecurity architecture design
Need to update design
CSA
System (cybersecurity) architecture design review
Cybersecurity Case updates
Release decision
NG
OK
Confirm
Update System architecture
Release System (cybersecurity) architecture design

Exit criteria [Cybersecurity Manager] The technical cybersecurity concept should be assigned a version and released through a document management system

M If you do not perform any mandatory process, you should have a reasonable rationale.

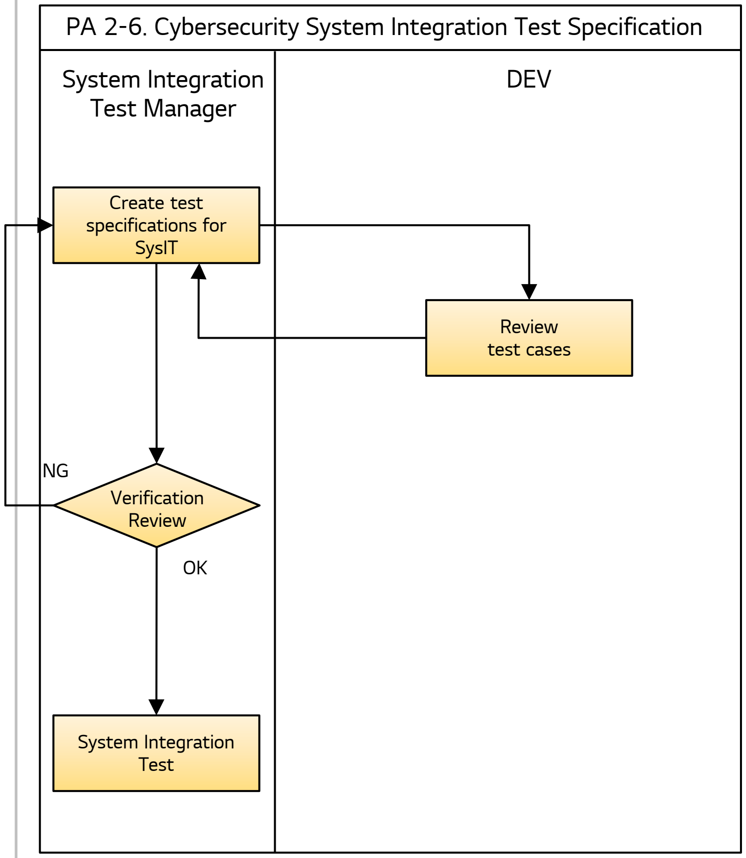
2-6. Cybersecurity System Integration Test Specification

Cybersecurity System Development Phase

◆ System Integration Test Manager prepares cybersecurity Integration test specification.

Entry criteria The system architectural design of cybersecurity should be existed and confirmed.

Procedure



PA 2-6. Cybersecurity System Integration Test Specification

System Integration Test Manager

DEV

Create test specifications for SysIT

Review test cases

Verification Review

NG

OK

System Integration Test

Detailed activity

System Integration test manager prepares the System Integration test through the following activities.

[Detail Activities]
Develop the System integration test case for cybersecurity.
Establish the environment for System integration test for cybersecurity.
Review test case.

[Description in detail]

- Develop the System integration test case for cybersecurity.
- Establish the environment for System integration test for cybersecurity.
- Review test case with DEV.

Mandatory items on System Integration test case.

[Items]
Requirement ID / TC ID
TC design type
Precondition
Input / expected output
Observed output
Pass / Fail / NA
Test method

Inputs

- System Architectural Design

Outputs

- System Integration Test Case

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [System Integration Test Manager] The verification review of the System Integration Test Specification is completed.

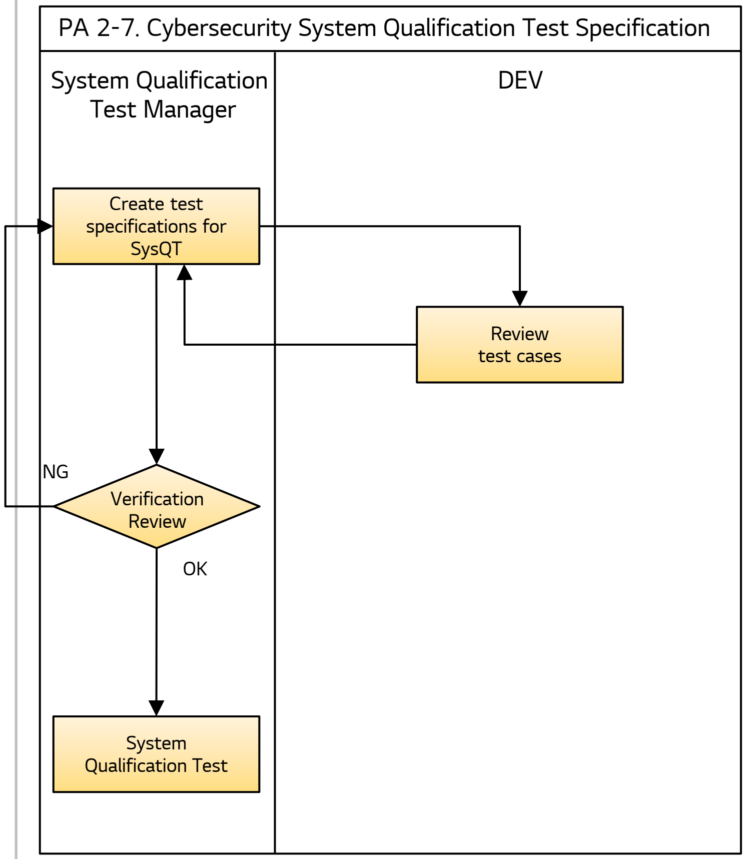
M If you do not perform any mandatory process, you should have a reasonable rationale.

2-7. Cybersecurity System Qualification Test Specification

◆ **System Qualification Test Manager prepares cybersecurity Integration test specification.**

Entry criteria The system requirements of cybersecurity should be existed and confirmed.

Procedure


PA 2-7. Cybersecurity System Qualification Test Specification
System Qualification Test Manager
DEV
Create test specifications for SysQT
Review test cases
NG
Verification Review
OK
System Qualification Test

Detailed activity

System Qualification test manager prepares the System Qualification test through the following activities.

[Detail Activities]
Develop the System qualification test case for cybersecurity.
Establish the environment for System Qualification test for cybersecurity.
Review test case.

[Description in detail]

- Develop the System qualification test case for cybersecurity.
- Establish the environment for System qualification test for cybersecurity.
- Review test case with DEV.

Mandatory items on System Qualification test case.

[Items]
Requirement ID / TC ID
TC design type
Precondition
Input / expected output
Observed output
Pass / Fail / NA
Test method

Inputs

- (Cybersecurity) System Requirements Specification

Outputs

- System Qualification Test Case

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [System Qualification Test Manager] The verification review of the System Qualification Test Specification is completed.

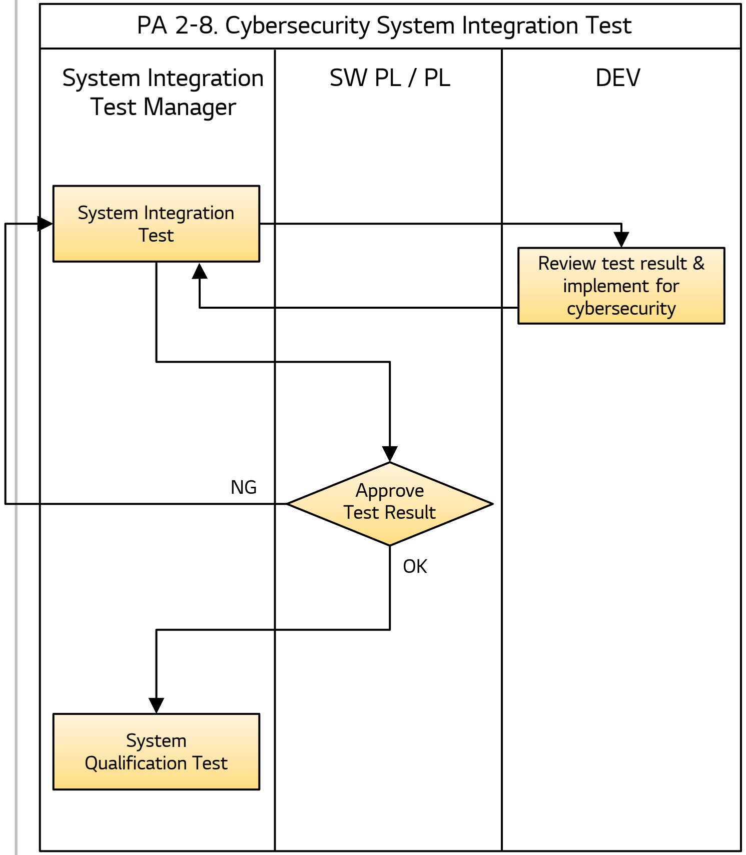
M If you do not perform any mandatory process, you should have a reasonable rationale.

2-8. Cybersecurity System Integration Test

◆ System Integration Test Manager performs the System Integration Test.

Entry criteria The test case for the system integration test is confirmed.

Procedure


PA 2-8. Cybersecurity System Integration Test
System Integration Test Manager
SW PL / PL
DEV
System Integration Test
Review test result & implement for cybersecurity
NG
Approve Test Result
OK
System Qualification Test

Detailed activity

System Integration test manager performs the System Integration test through the following activities and creates System Integration test result report.

[Description in detail]

- The test cases can be added / modified / deleted based on the system architectural design in consultation with Developers.
- Defects identified in the test run should be traced with related work products.
- Test result should be shared to related departments (dev. team, system test / qualification test).
- Repeat the test until test result is met the criteria.

Inputs

- System Integration Test Plan
- System Integration Test Case

Outputs

- System Integration Test Report

Related standard

- ISO/SAE21434-10:v1.0
- Automotive SPICE Process Assessment / Reference Model SYS.4

Exit criteria [System Integration Test Manager] The test result is met with the test criteria and has covered all system architectural designs.

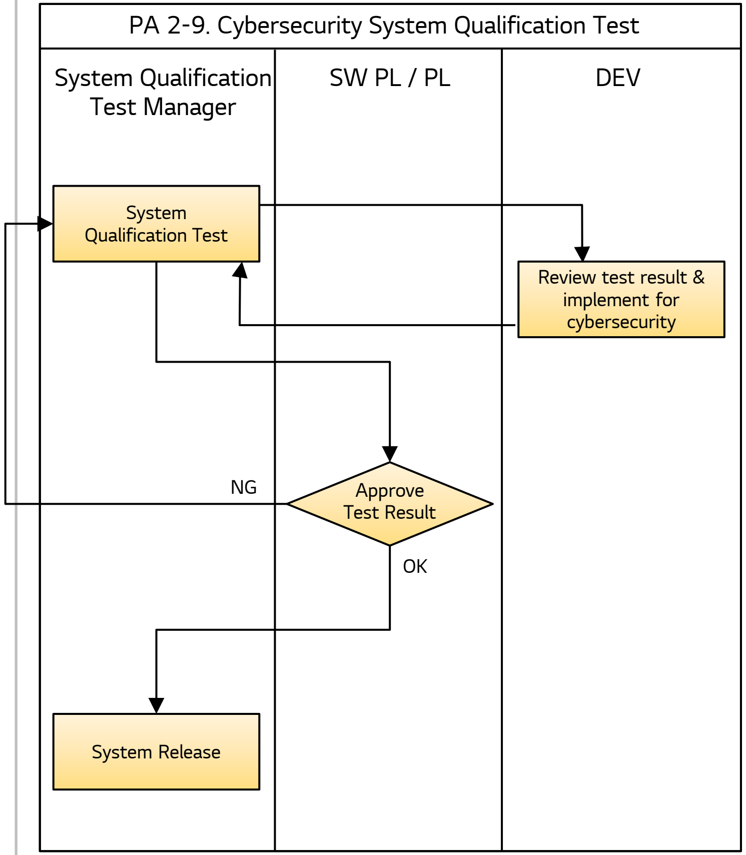
M If you do not perform any mandatory process, you should have a reasonable rationale.

2-9. Cybersecurity System Qualification Test

◆ System Qualification Test Manager performs the System Qualification Test.

Entry criteria The test case for the system qualification test is confirmed.

Procedure


PA 2-9. Cybersecurity System Qualification Test
System Qualification Test Manager
SW PL / PL
DEV
System Qualification Test
Review test result & implement for cybersecurity
NG
Approve Test Result
OK
System Release

Detailed activity

System Qualification test manager performs the System Qualification test through the following activities and creates System Qualification test result report.

[Description in detail]

- The test cases can be added / modified / deleted based on the system requirements specification in consultation with Developers.
- Defects identified in the test run should be traced with related work products.
- Test result should be shared to related departments (dev. team, system test / qualification test).
- Repeat the test until test result is met the criteria.

Inputs

- System Qualification Test Plan
- System Qualification Test Case

Outputs

- System Qualification Test Report

Related standard

- ISO/SAE21434-10:v1.0
- Automotive SPICE Process Assessment / Reference Model SYS.5

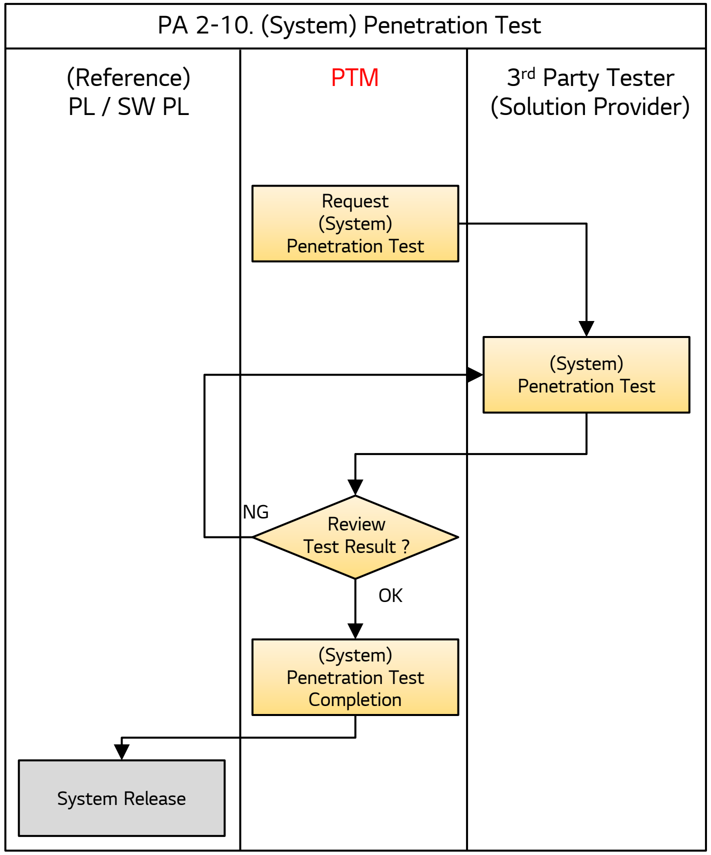
Exit criteria [System Qualification Test Manager] The test result is met with the test criteria and has covered all system requirements.

M If you do not perform any mandatory process, you should have a reasonable rationale.

2-10. (System) Penetration Test

◆ (System) Penetration Test Engineer performs (system) penetration test.

Entry criteria The environments and resources of penetration test must be prepared.

Procedure	Detailed activity	Inputs
	**PTM(Penetration Test Manager) requests the penetration test to 3rd Party Tester to perform (system) penetration test align with the schedule in the test plan and cybersecurity plan.** **[Description in detail]** (PTM) • Request a penetration test to the Penetration Test Engineer align with the schedule shared by Cybersecurity Manager • Review test result (3rd Party Tester) • Perform the penetration test • The issues should be registered in the defect management system • Monitor the issues with the defect management system • Perform tests until the criteria of completion is satisfied • Report the penetration test result in related departments • Penetration test is conducted by referring to the Vulnerability test plan document (LGE_Penetration_TestPlan)	- Test Plan - Cybersecurity Plan **Outputs** - (System) Penetration Test report **Related standard** - ISO/SAE21434-10:v1.0

PA 2-10. (System) Penetration Test
(Reference) PL / SW PL
PTM
3rd Party Tester (Solution Provider)
Request (System) Penetration Test
(System) Penetration Test
NG
Review Test Result ?
OK
(System) Penetration Test Completion
System Release

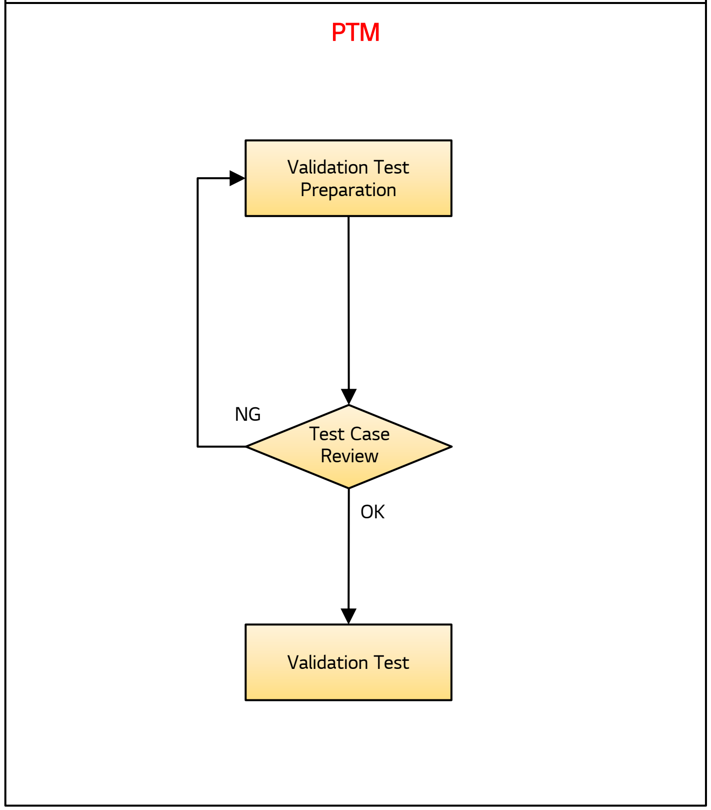
Exit criteria [PTM] Review the test result of the (system) Penetration Test and release the result to stakeholders.

M If you do not perform any mandatory process, you should have a reasonable rationale.

2-11. Cybersecurity Validation Test Specification

◆ (Cybersecurity) Penetration Test Manager specifies the test specification of validation.

Entry criteria The validation test plan is prepared and cybersecurity goals/claims are specified.

Procedure	Detailed activity	Inputs
PA 2-11. Cybersecurity Validation Test Specification  PTM Validation Test Preparation NG Test Case Review OK Validation Test	※ Basically, validation activities are related to the test in the vehicle, so these are generally performed by OEM. ※ Validation activities can be defined penetration testing and Penetration Test Manager can perform the activities of cybersecurity validation. (Cybersecurity) Penetration Test Manager specifies the cybersecurity validation test specifications. [Description in detail] • Check the environments of the cybersecurity validation test • Specify the cybersecurity validation test specifications • Review the specifications of cybersecurity validation test to ensure Cybersecurity Goals ※ The risks identified during the Concept and Product Development phases shall be confirmed with reasonable mitigation.	- Validation test plan - Cybersecurity goals/claims **Outputs** - Cybersecurity validation test specification **Related standard** - ISO/SAE21434-11:v1.0

Exit criteria [Penetration Test Manager] All requirements and validation specifications are specified. The verification review of the validation specification is completed

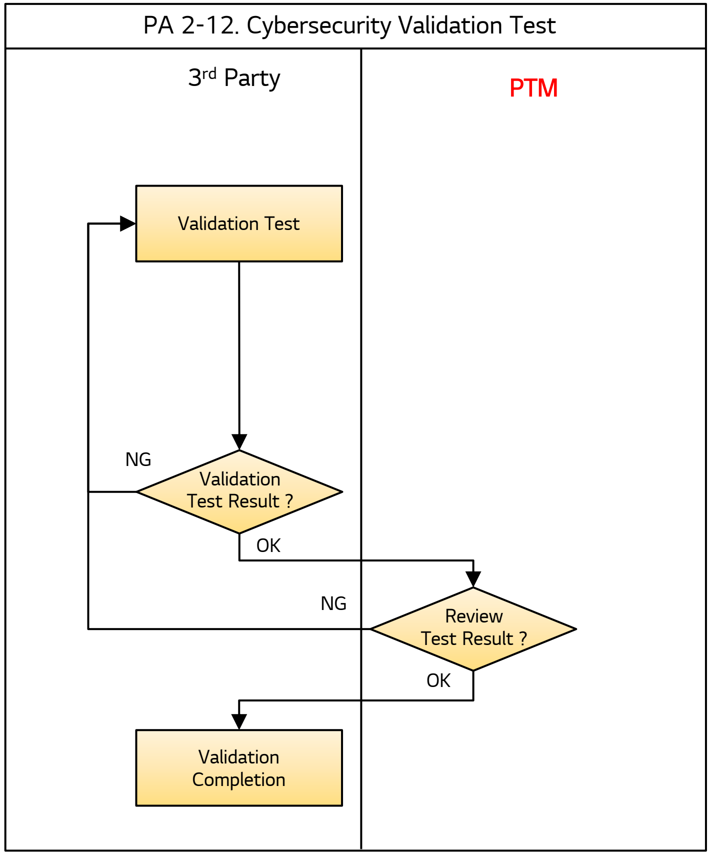
O (Vehicle) Validation activities are related to the test in the vehicle, so these are generally performed by OEM.

2-12. Cybersecurity Validation Test

◆ (Cybersecurity) Penetration Test Manager performs a cybersecurity validation test.

Entry criteria The verification review of the cybersecurity validation test specification should be completed.

Procedure



Detailed activity

※ **Basically, validation activities are related to the test in the vehicle, so these are generally performed by OEM.**
※ **Penetration Test Manager can perform the activities of cybersecurity validation.**

(Cybersecurity) Penetration Test Manager performs the test of cybersecurity validation with confirmed cybersecurity validation test specifications.

[Description in detail]

- Perform the test in compliance with the Validation plan
- The issues should be registered in the defect management system
- Monitor the issues with the defect management system
- Perform tests until the criteria of completion is satisfied
- Report the Validation test result in related departments

※ **The risks identified during the Concept and Product Development phases shall be confirmed with reasonable mitigation.**

Inputs

- Validation test plan
- Validation test specifications

Outputs

- Cybersecurity Validation Test report

Related standard

- ISO/SAE21434-11:v1.0

Exit criteria [Penetration Test Manager] obtains the approval for the test result of validation test by Penetration Test Manager after performing the validation test.

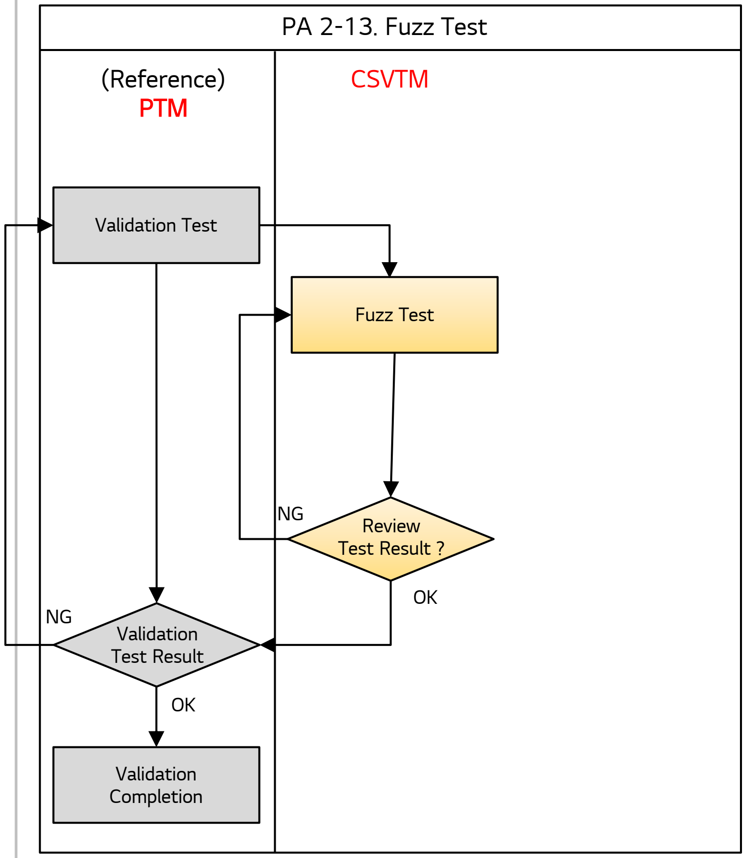
O (Vehicle) Validation activities are related to the test in the vehicle, so these are generally performed by OEM.

2-13. Fuzz Test

◆ **Fuzz Test manager performs vehicle or system fuzz test.**

Entry criteria The environments and resources of fuzz test must be prepared.

Procedure


PA 2-13. Fuzz Test

(Reference) PTM

CSVTM

Validation Test

Fuzz Test

Review Test Result ?

NG

OK

Validation Test Result

NG

OK

Validation Completion

Detailed activity

※ Basically, validation activities are related to the test in the vehicle, so these are generally performed by OEM.

CSVTM performs vehicle fuzz test align with the schedule in the validation test plan and cybersecurity plan.

[Description in detail]
(CSVTM)

- Conduct fuzz test aligned with the schedule shared by PTM
- Review test result
- Fuzz test is conducted by referring to the Vulnerability test plan document (Vulnerability_Fuzz Test Plan)

※ The risks identified during the Concept and Product Development phases shall be confirmed with reasonable mitigation.

Inputs

- Validation test plan

Outputs

- Fuzz Test report

Related standard

- ISO/SAE21434-11:v1.0

Exit criteria [CSVTM] Review the test result of the Fuzz Test and release the result to stakeholders.

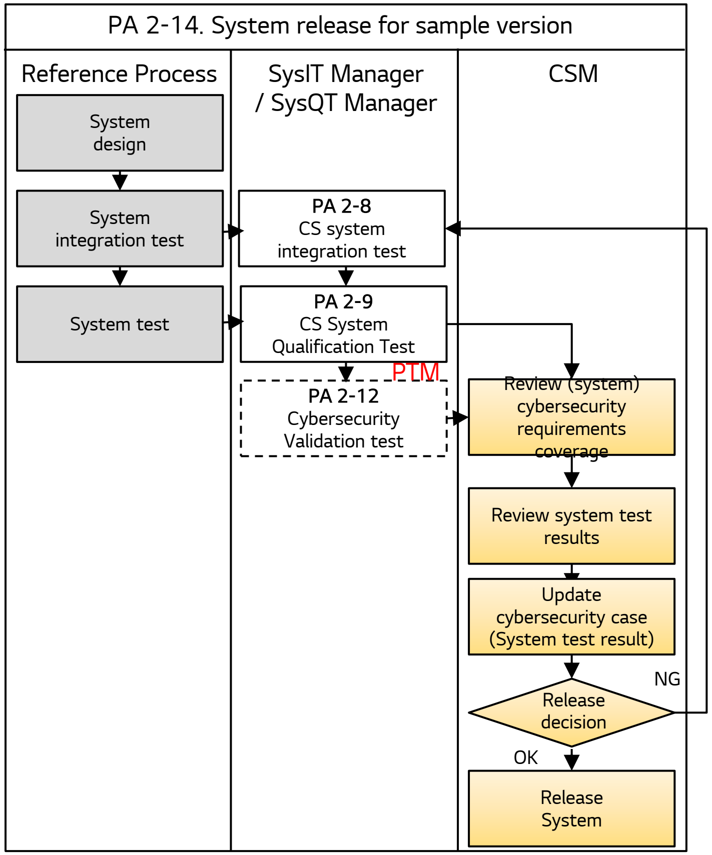
O Validation activities are related to the test in the vehicle, so these are generally performed by OEM.

2-14. System release for sample version

◆ **Cybersecurity Manager reviews cybersecurity test result for system level and releases the system of sample version.**

Entry criteria System vehicle integration verification should be completed.

Procedure



PA 2-14. System release for sample version

Reference Process

System design

System integration test

System test

SysIT Manager / SysQT Manager

PA 2-8 CS system integration test

PA 2-9 CS System Qualification Test

PTM

PA 2-12 Cybersecurity Validation test

CSM

Review (system) cybersecurity requirements coverage

Review system test results

Update cybersecurity case (System test result)

Release decision

NG

OK

Release System

Detailed activity

Cybersecurity Manager releases system sample version by reviewing cybersecurity test result for system level.

[Description in detail]

- Cybersecurity Manager reviews the implementation of all (system) cybersecurity requirements that must be released according to the feature release plan.
- Cybersecurity Manager reviews the results of the CS system test to see if the test has passed.
- Cybersecurity Manager updates system level test result to the cybersecurity case.
- Cybersecurity Manager decides (system) cybersecurity requirement coverage and test results to be appropriate for the level of sample release required by the OEM.
- Cybersecurity Manager assigns a version to the system and releases it

[System sample release report]

The system sample release report should include the following:
(if applicable)

- Version of system sample
- Released feature
- Summary of system test result
- Release date
- Release approver

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

- (System) cybersecurity requirements.
- System (cybersecurity) architecture design
- CS system integration test report
- CS system test report
- Vehicle integration test report

Outputs

- System sample release report
- Cybersecurity case [refined]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] Cybersecurity Manager gives a version to the sample system and releases the system sample release report with the system.

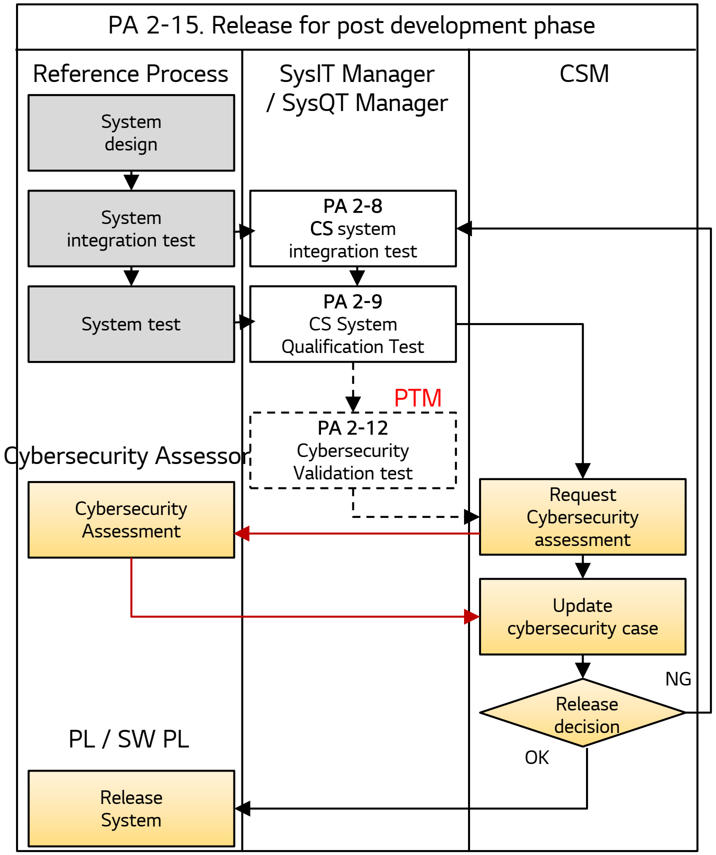
M If you do not perform any mandatory process, you should have a reasonable rationale.

2-15. Release for post development phase

◆ **Cybersecurity Manager reviews cybersecurity activity suitability and releases system for Item production.**

Entry criteria System vehicle integration verification should be completed.

Procedure


PA 2-15. Release for post development phase
Reference Process
SysIT Manager / SysQT Manager
CSM
System design
System integration test
System test
PA 2-8 CS system integration test
PA 2-9 CS System Qualification Test
PTM
PA 2-12 Cybersecurity Validation test
Cybersecurity Assessor
Cybersecurity Assessment
Request Cybersecurity assessment
Update cybersecurity case
NG
Release decision
OK
PL / SW PL
Release System

Detailed activity

Cybersecurity Manager reviews the suitability of cybersecurity activities for mass production of items and release the system to the production department and OEM.

[Description in detail]

- Cybersecurity Assessor performs the cybersecurity assessment after a request by Cybersecurity Manager.
- Cybersecurity Manager reviews the cybersecurity assessment report to ensure that any improvement requests are reflected in the system.
- Cybersecurity Manager reviews whether the cybersecurity case has passed the confirmation review.
- Cybersecurity Manager updates the result of cybersecurity assessment to the cybersecurity case.
- Cybersecurity Manager requests to the person in charge to correct any problems with the assessment report and cybersecurity case.
- Cybersecurity Manager creates post development release report.
- PL/SW PL review post development release report and releases the system for mass production.

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

- CS assessment report
- Cybersecurity case

Outputs

- Post Development report

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] The post development release report should be versioned and released.

M If you do not perform any mandatory process, you should have a reasonable rationale.

3 Cybersecurity HW Development Phase

- **Objective**

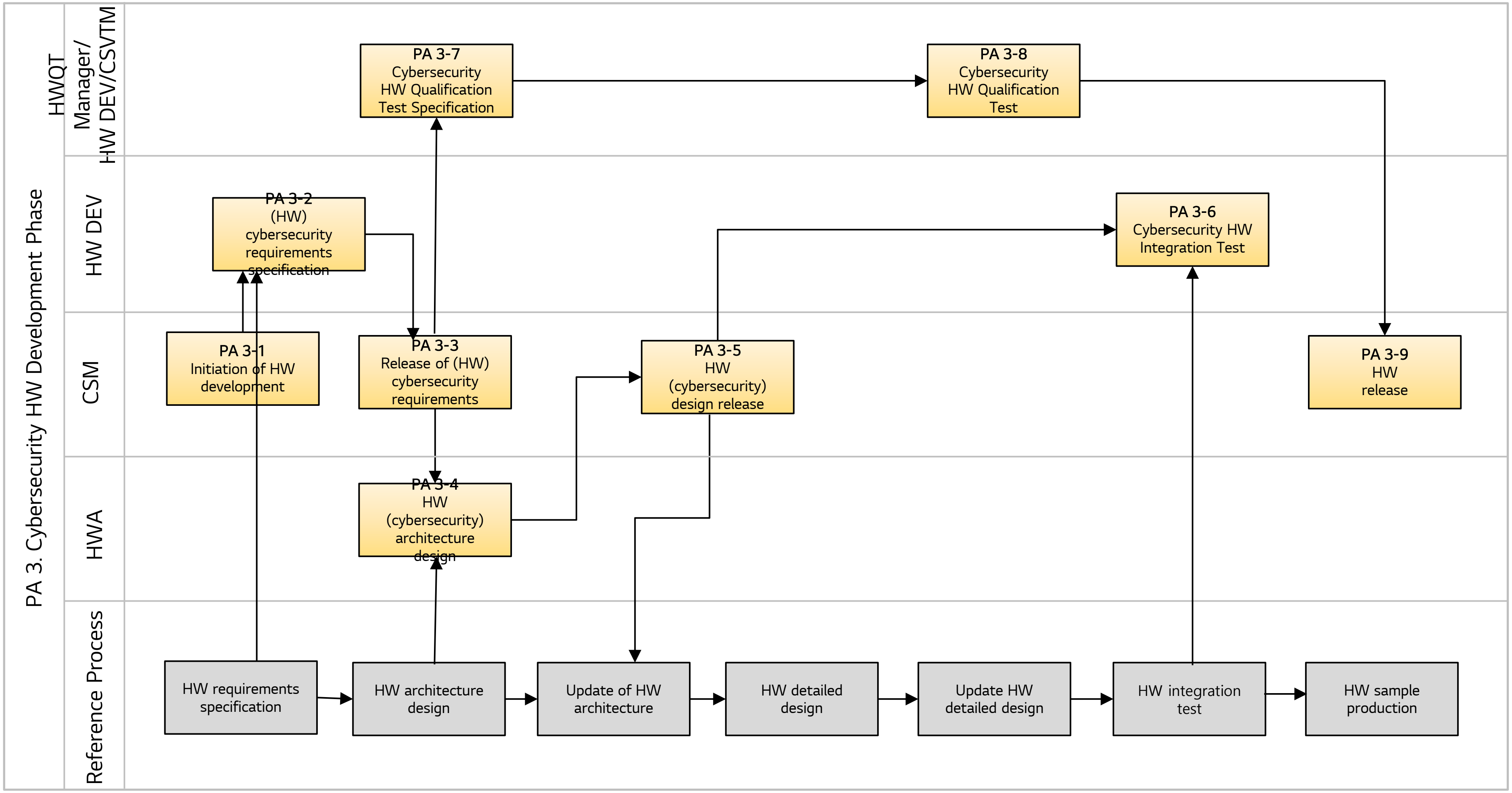
  Define a cybersecurity HW development phase to achieve cybersecurity objectives, and define key activities and criteria for each phase.

- **Scope**

  It is applied when developing the item to apply cybersecurity among electrical and electronic system (E / E system) developed by VS company.

3 Cybersecurity HW Development Phase

Define the HW development phase of the electrical and electronic system (E / E System) developed by VS company, and define the main activities and criteria for each phase.


PA 3. Cybersecurity HW Development Phase
HWQT Manager/ HW DEV/CSVTM
HW DEV
CSM
HWA
Reference Process
PA 3-7 Cybersecurity HW Qualification Test Specification
PA 3-8 Cybersecurity HW Qualification Test
PA 3-2 (HW) cybersecurity requirements specification
PA 3-6 Cybersecurity HW Integration Test
PA 3-1 Initiation of HW development
PA 3-3 Release of (HW) cybersecurity requirements
PA 3-5 HW (cybersecurity) design release
PA 3-9 HW release
PA 3-4 HW (cybersecurity) architecture design
HW requirements specification
HW architecture design
Update of HW architecture
HW detailed design
Update HW detailed design
HW integration test
HW sample production

3 Related ISO/SAE 21434 standard for cybersecurity HW development

Option	Process Area	Description	Role	Work product	Related standard
M	**PA 3-1.** Initiation of HW development	Determine the cybersecurity activities to be performed in the HW development phase and establish a plan.	Cybersecurity Manager	• Cybersecurity plan [refined] • HW verification review plan • HW test plan	- ISO/SAE 21434-10:v1.0
M	**PA 3-2.** (HW) cybersecurity requirements specification	The HW cybersecurity requirements are specified for the requirements allocated to the HW in system cybersecurity requirements (HWCSR).	HW Developer	• (HW) cybersecurity requirements • Traceability matrix (SysCSR-HWCSR) • VR report • Cybersecurity plan (refined)	- ISO/SAE 21434-10:v1.0
M	**PA 3-3.** Release of (HW) cybersecurity requirements	Confirm and distribute the specified HW cybersecurity requirements.	Cybersecurity Manager	• (HW) cybersecurity requirements • Traceability matrix (SysCSR-HWCSR) [refined] • Cybersecurity case [refined]	- ISO/SAE 21434-10:v1.0
M	**PA 3-4.** HW (cybersecurity) architecture design	Design HW architecture from the cybersecurity requirements.	HW Architect	• HW architecture (HwAD) • VR report (HWAD) • Traceability matrix (HWCSR-HWAD) • HW-SW interface (HSI) [refined] • Cybersecurity plan [refined]	- ISO/SAE 21434-10:v1.0
M	**PA 3-5.** HW (cybersecurity) design release	Analyze and confirm that the HW cybersecurity design is designed to the appropriate level.	Cybersecurity Manager	• HW (cybersecurity) architecture design (HWAD) • HW detailed design • Cybersecurity case [refined]	- ISO/SAE 21434-10:v1.0
M	**PA 3-6.** Cybersecurity HW Integration Test	HW DEV performs the Cybersecurity HW Integration Test using the Cybersecurity HW Integration Test Case.	HW Developer	• Cybersecurity HW Integration Test cases • HW Integration Test Report	- ISO/SAE 21434-10:v1.0
M	**PA 3-7.** Cybersecurity HW Qualification Test Specification	HW Qualification Test Manager prepares cybersecurity HW qualification test specification.	HW Qualification Test Manager	• HW Qualification Test Case	- ISO/SAE 21434-10:v1.0
M	**PA 3-8.** Cybersecurity HW Qualification Test	Cybersecurity HW Qualification test using the Test Case approved by the Test Case Review Board.	HW Qualification Test Manager	• HW Qualification Test Report	- ISO/SAE 21434-10:v1.0
M	**PA 3-9.** HW release	confirm and release of HW version.	Cybersecurity Manager	• HW release report • Cybersecurity case [refined]	- ISO/SAE 21434-10:v1.0

M Mandatory O Optional

3 Role & responsibility for cybersecurity HW development(1/2)

Process Area	Work Product	CSM	CSA	SysA	HWA	HW Dev	CSVTM	HWQT Manager	SysIT Manager	SysQT Manager	Cybersecurity Assessor	HW PL/PL
PA 3-1. Initiation of HW development	• Cybersecurity plan [refined] • HW verification review plan • HW test plan	R	-	-	-	I	-	-	-	-	-	-
PA 3-2. (HW) cybersecurity requirements specification	• (HW) cybersecurity requirements • Traceability matrix (SysCSR-HWCSR) • VR report • Cybersecurity plan (refined)	I	S	S	S	R	-	-	-	-	-	-
PA 3-3. Release of (HW) cybersecurity requirements	• (HW) cybersecurity requirements • Traceability matrix (SysCSR-HWCSR) [refined] • Cybersecurity case [refined]	I	S	-	S	R	-	-	-	-	-	A
PA 3-4. HW (cybersecurity) architecture design	• HW architecture (HwAD) • VR report (HWAD) • Traceability matrix (HWCSR-HWAD) • HW-SW interface (HSI) [refined] • Cybersecurity plan [refined]	I	S	S	R	S	-	-	-	-	-	-
PA 3-5. HW (cybersecurity) design release	• HW (cybersecurity) architecture design (HWAD) • HW detailed design • Cybersecurity case [refined]	I	S	-	S	R	-	-	-	-	-	A

R : Responsibility , A : Approval, S : Support , I : Informed

3 Role & responsibility for cybersecurity HW development(2/2)

Cybersecurity HW Development Phase

Process Area	Work Product	CS M	CS A	Sys A	HW A	HW Dev	CSVT M	HWQT Manage r	SysIT Manage r	SysQT Manage r	Cybersecurity Assessor	HW PL/PL
PA 3-6. Cybersecurity HW Integration Test	• Cybersecurity HW Integration Test cases • HW Integration Test Report	A	-	-	-	R	I	I	-	-	-	A
PA 3-7. Cybersecurity HW Qualification Test Specification	• HW Qualification Test Case	A	-	-	-	S	I	R	-	-	-	-
PA 3-8. Cybersecurity HW Qualification Test	• HW Qualification Test Report	A	-	-	-	S	I	R	-	-	-	A
PA 3-9. HW release	• HW release report • Cybersecurity case [refined]	I	S	-	-	S	S	-	I	I	I	A

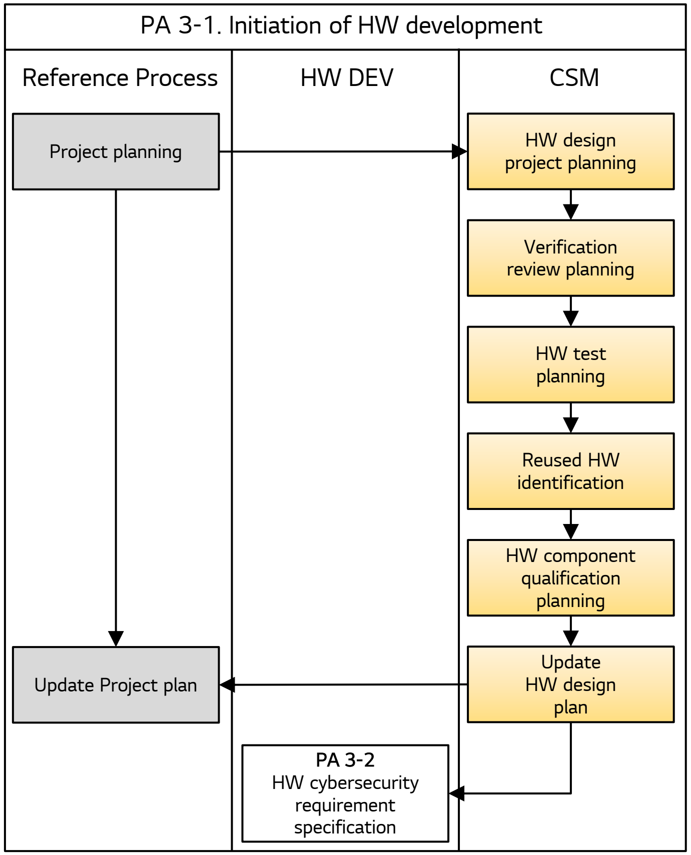
R : Responsibility , A : Approval, S : Support , I : Informed

3-1. Initiation of HW development

◆ **Cybersecurity Manager determines and plans the cybersecurity activities to be performed during the HW development phase.**

Entry criteria System development has been completed and the system cybersecurity activity plan should be completed.

Procedure



PA 3-1. Initiation of HW development

Reference Process
HW DEV
CSM
Project planning
HW design project planning
Verification review planning
HW test planning
Reused HW identification
HW component qualification planning
Update HW design plan
Update Project plan
PA 3-2 HW cybersecurity requirement specification

Detailed activity

Before developing HW, Cybersecurity Manager decides and plans the cybersecurity activities required for development.

[Description in detail]

- Cybersecurity Manager analyzes the project plan and establishes the HW development plan by tailoring the standard process to the project situation.
- Cybersecurity Manager establishes a VR plan for the HW development phase output and updates the cybersecurity plan.
- Cybersecurity Manager develops the HW test plan and updates the test plan.
- Cybersecurity Manager identifies the reusable HW components and establishes a qualification plan for the HW components / parts.
- Cybersecurity Manager updates the HW development plan based on the reuse and qualification plan of the HW component.

Inputs

- Project plan
- Cybersecurity plan
- Test plan(System integration test, System qualification test)

Outputs

- Cybersecurity plan [refined]
- HW verification review plan
- HW test plan

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] All HW development plans should be reflected in the output of PA 3-1.

M If you do not perform any mandatory process, you should have a reasonable rationale.

LGE Internal Use Only

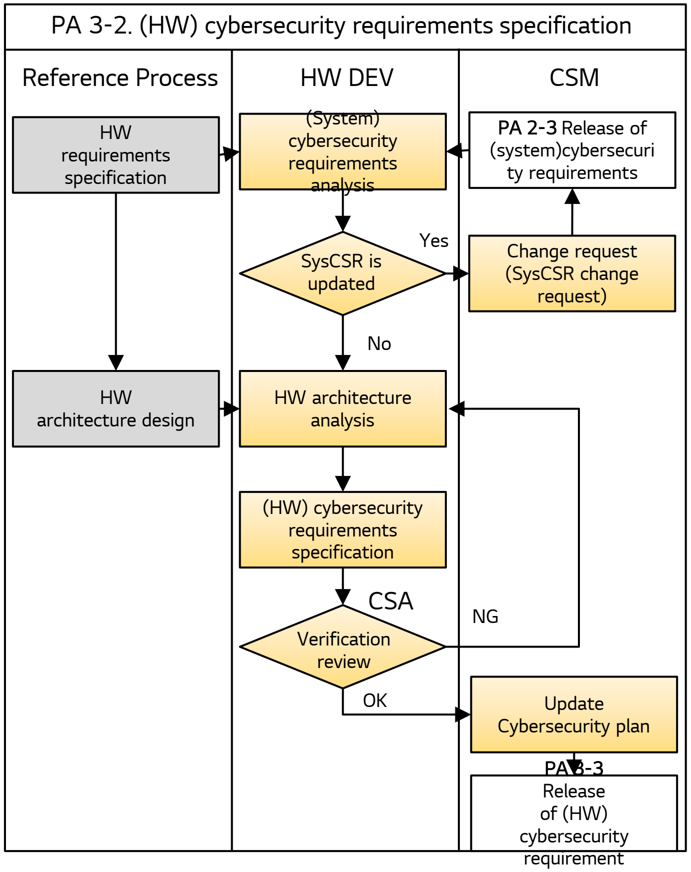
3-2. (HW) cybersecurity requirements specification

Cybersecurity HW Development Phase

◆ **HW Developer specifies the (HW)cybersecurity requirements allocated to the HW.**

Entry criteria Verification review should be completed for the (system)cybersecurity requirement derived from the system phase.

Procedure


PA 3-2. (HW) cybersecurity requirements specification
Reference Process
HW DEV
CSM
HW requirements specification
(System) cybersecurity requirements analysis
PA 2-3 Release of (system)cybersecurity requirements
Yes
SysCSR is updated
Change request (SysCSR change request)
No
HW architecture design
HW architecture analysis
(HW) cybersecurity requirements specification
CSA
NG
Verification review
OK
Update Cybersecurity plan
PA 3-3 Release of (HW) cybersecurity requirement

Detailed activity

HW Developer performs the following activities on the cybersecurity requirements allocated to hardware during the system development phase.

[Description in detail]

- HW Developer identifies HW level considerations by analyzing the cybersecurity requirements allocated to the hardware within the SysCSR.
- HW Developer analyzes whether there are any conflicts between the HW requirements specification and the SysCSRs.
- HW Developer requests the Cybersecurity Manager to request a change request for the SysCSR when there are requirements that are difficult to accommodate from the viewpoint of the HW among the SysCSRs allocated to the HW.
- HW Developer analyzes HW architecture design and assigns SysCSR to HW element.
- HW Developer specifies HW cybersecurity requirements on the basis of HW element.
- HW Developer analyzes considers and update the cybersecurity implications of post-development phase during the refinement of cybersecurity requirements.
- HW Developer specifies and allocates to the relevant entities of the operational environment if specific procedures are required to ensure cybersecurity in post-development phases.
- CSA performs a verification review of specified HW cybersecurity requirement. (if applicable).
- CSM updates the cybersecurity plan, taking into account the derived HW cybersecurity requirements.

Inputs

- (System)cybersecurity requirement
- System (cybersecurity) architecture design (SyAD)
- HW-SW interface (HSI)
- HW architecture design

Outputs

- (HW) cybersecurity requirements
- Traceability matrix (SysCSR-HWCSR)
- VR report
- Cybersecurity plan (refined)

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [HW DEV] For all (system) cybersecurity requirement allocated by the system to the hardware, it shall be specified as (HW) cybersecurity requirements and shall pass VR criteria.

M If you do not perform any mandatory process, you should have a reasonable rationale.

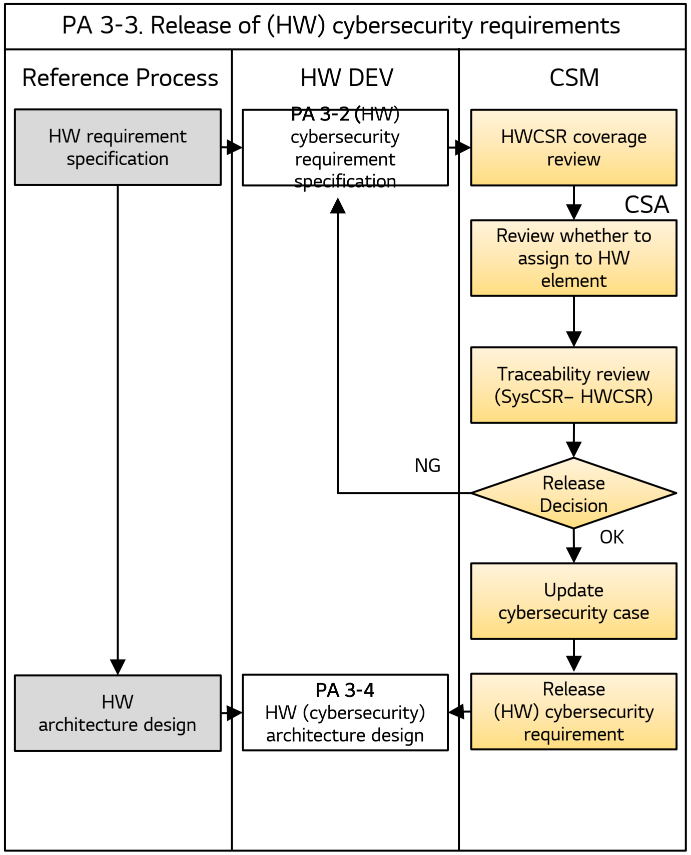
3-3. Release of (HW) cybersecurity requirements

Cybersecurity HW Development Phase

◆ Cybersecurity Architect reviews specified (HW)cybersecurity requirements and Cybersecurity Manager confirms and releases them.

Entry criteria HW cybersecurity requirements (HWCSR) should pass the verification review criteria.

Procedure



PA 3-3. Release of (HW) cybersecurity requirements

Reference Process | HW DEV | CSM

HW requirement specification

PA 3-2 (HW) cybersecurity requirement specification

HWCSR coverage review

CSA

Review whether to assign to HW element

Traceability review (SysCSR– HWCSR)

Release Decision

NG

OK

Update cybersecurity case

Release (HW) cybersecurity requirement

PA 3-4 HW (cybersecurity) architecture design

HW architecture design

Detailed activity

Cybersecurity Architect reviews the completion of the (system)cybersecurity requirements and cybersecurity manager confirms them.

[Description in detail]

- Cybersecurity Manager reviews all (system) cybersecurity requirement allocated to the HW as (HW) cybersecurity requirements.
- Cybersecurity Manager should review whether all (HW) cybersecurity requirements is clearly allocated to the HW element.
- Cybersecurity Manager reviews whether traceability is correctly established between System and (HW) cybersecurity requirement.
- Cybersecurity Manager assigns the version to the (HW) cybersecurity requirements and releases it to the document management system.

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

- (System) cybersecurity requirement
- (HW) cybersecurity requirements
- Traceability matrix (SysCSR-HWCSR)

Outputs

- (HW) cybersecurity requirements
- Traceability matrix (SysCSR-HWCSR) [refined]
- Cybersecurity case [refined]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] Cybersecurity Manager assigns the version to the (HW) cybersecurity requirements and releases it to the document management system.

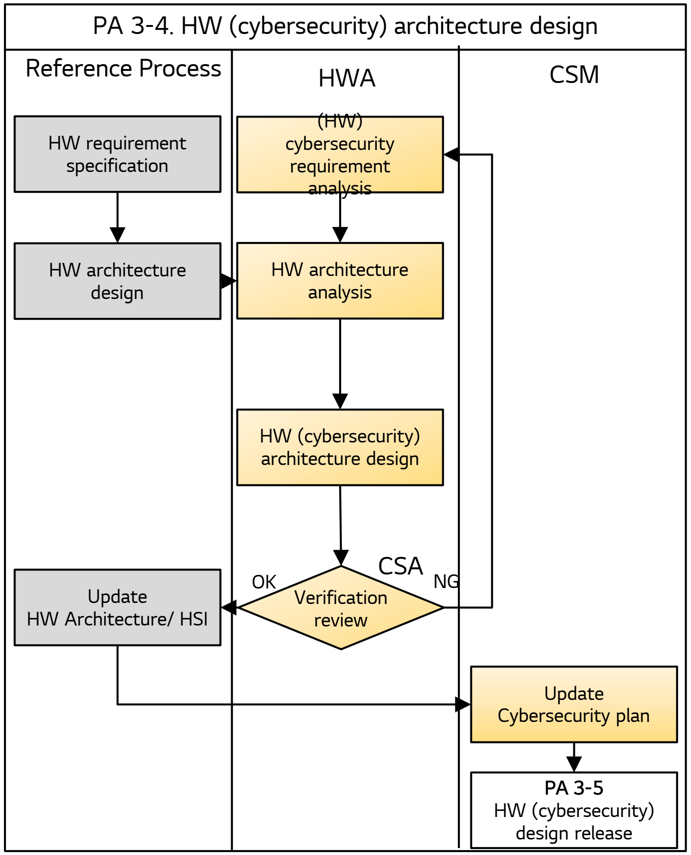
M If you do not perform any mandatory process, you should have a reasonable rationale.

3-4. HW (cybersecurity) architecture design

◆ **HW Architect designs the HW architecture to meet (HW) cybersecurity requirements.**

Entry criteria (HW) cybersecurity requirements shall be finalized and released.

Procedure


PA 3-4. HW (cybersecurity) architecture design
Reference Process
HWA
CSM
HW requirement specification
(HW) cybersecurity requirement analysis
HW architecture design
HW architecture analysis
HW (cybersecurity) architecture design
CSA
OK
NG
Verification review
Update HW Architecture/ HSI
Update Cybersecurity plan
PA 3-5 HW (cybersecurity) design release

Detailed activity

HW Architect designs HW cybersecurity architecture to achieve established (HW) cybersecurity requirements.

[Description in detail]

- HWA analyzes the established (HW) cybersecurity requirements to understand the objectives and functions that the HW should achieve.
- HWA analyzes the HW architecture design and reviews for any required architecture changes to meet CSR.
- HWA allocates the defined cybersecurity requirements to components of the architectural design.
- HWA designs HW architecture from a cybersecurity point of view to satisfy (HW) cybersecurity requirements.
- HWA updates the HW-SW interface (HSI) from the HW point of view.
- HWA requests to reflect the HW cybersecurity design in the HW architecture.
- CSA performs the verification review for HW (cybersecurity) architecture design.
- CSM updates the cybersecurity plan

Inputs

- (HW) cybersecurity requirements
- HW (cybersecurity) architecture (HWAD)
- HW-SW interface (HSI)

Outputs

- HW architecture (HwAD)
- VR report (HWAD)
- Traceability matrix (HWCSR-HWAD)
- HW-SW interface (HSI) [refined]
- Cybersecurity plan [refined]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [HWA] The HW architecture design should reflect all of the HW cybersecurity design..

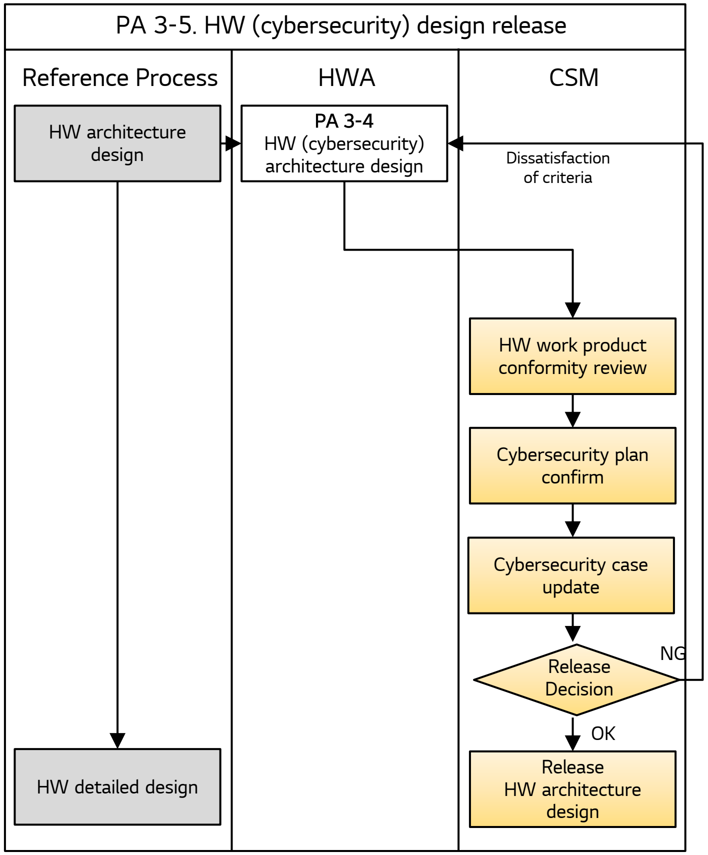
M If you do not perform any mandatory process, you should have a reasonable rationale.

3-5. HW (cybersecurity) design release

◆ Cybersecurity Architect reviews the HW (cybersecurity) architecture design and Cybersecurity Manager confirms and releases them.

Entry criteria HW cybersecurity analysis should be completed.

Procedure


PA 3-5. HW (cybersecurity) design release
Reference Process
HWA
CSM
HW architecture design
PA 3-4
HW (cybersecurity) architecture design
Dissatisfaction of criteria
HW work product conformity review
Cybersecurity plan confirm
Cybersecurity case update
NG
Release Decision
OK
HW detailed design
Release HW architecture design

Detailed activity

Cybersecurity Manager confirms cybersecurity design by reviewing to achieve cybersecurity target.

[Description in detail]

- CSA reviews whether the cybersecurity design covers all the requirements of the (HW) cybersecurity requirements.
- Cybersecurity Manager determines if the output is at release level.
- Cybersecurity Manager reflects the HW cybersecurity design content into the cybersecurity case.
- Cybersecurity Manager requests to the HWA to reflect any changes made in cybersecurity into the HW architecture design.
- Cybersecurity Manager assigns a version to the HW detailed design reflecting the HW cybersecurity design and releases it through the document management system.

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

- HW (cybersecurity) architecture design (HWAD)

Outputs

- HW (cybersecurity) architecture design (HWAD)
- HW detailed design
- Cybersecurity case [refined]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] HW detailed design should be given a version and released to the document management system.

M If you do not perform any mandatory process, you should have a reasonable rationale.

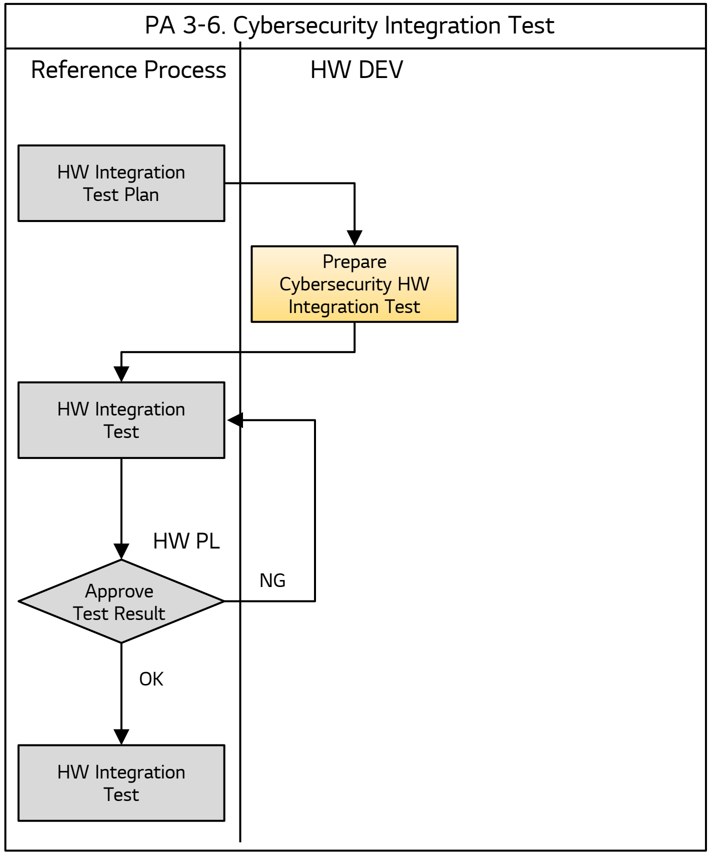
3-6. Cybersecurity HW Integration Test

Cybersecurity HW Development Phase

◆ **HW Developer(HW DEV) performs the Cybersecurity HW Integration Test using the Cybersecurity HW Integration Test Case.**

Entry criteria Complete the preparation of the system requirements statement. Complete HW test environment construction and HW test case development.

Procedure



Detailed activity

HW DEV prepare the test case of the cybersecurity HW Integration Test and perform the cybersecurity HW Integration Test.

[Description in detail]

- Check the HW release version at the time of the Cybersecurity HW integration test.
- Define the scope of the Cybersecurity HW integration testing in accordance with the test strategy described in the Cybersecurity HW Integration Test Plan.
- Send the results of the Cybersecurity HW integration test to the CSM and request approval.

Mandatory items on HW Cybersecurity HW Integration test case.

[Items]
Requirement ID / TC ID
TC design type
Precondition
Input / expected output
Observed output
Pass / Fail / NA
Test method

Inputs

- HW Integration Test Plan
- HW (cybersecurity) architecture design

Outputs

- Cybersecurity HW Integration Test cases
- HW Integration Test Report

Related standard

- ISO/SAE 21434-10:v1.0

Exit criteria [HW DEV] The test result is met with the test criteria and has covered all HW architecture designs.

M If you do not perform any mandatory process, you should have a reasonable rationale.

LGE Internal Use Only

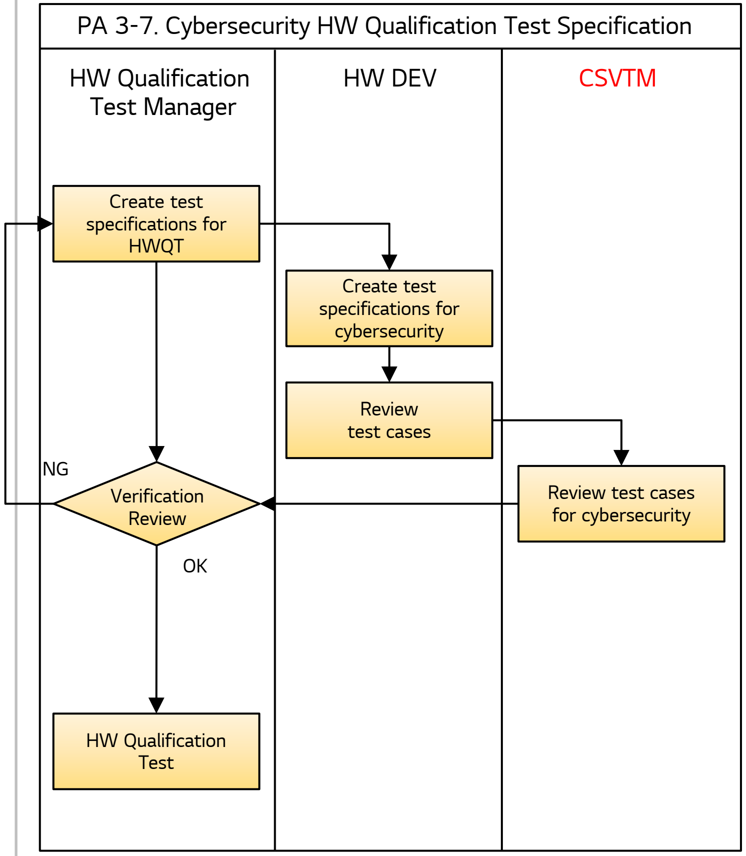
3-7. Cybersecurity HW Qualification Test Specification

Cybersecurity HW Development Phase

◆ HW Qualification Test Manager prepares cybersecurity HW qualification test specification.

Entry criteria The HW requirements of cybersecurity should be existed and confirmed.

Procedure



PA 3-7. Cybersecurity HW Qualification Test Specification

HW Qualification Test Manager

HW DEV

CSVTM

Create test specifications for HWQT

Create test specifications for cybersecurity

Review test cases

Review test cases for cybersecurity

Verification Review

NG

OK

HW Qualification Test

Detailed activity

HW Qualification test manager prepares the HW Qualification test through the following activities.

[Detail Activities]
Develop the HW qualification test case for cybersecurity.
Establish the environment for HW Qualification test for cybersecurity.
Review test case.

[Description in detail]

- HW DEV develops the HW qualification test case for cybersecurity.
- Establish the environment for HW qualification test for cybersecurity.
- Review test case with HW DEV.
- CSVTM reviews test cases for cybersecurity

Mandatory items on HW Qualification test case.

[Items]
Requirement ID / TC ID
TC design type
Precondition
Input / expected output
Observed output
Pass / Fail / NA
Test method

Inputs

- (Cybersecurity) HW Requirements Specification

Outputs

- HW Qualification Test Case

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [HW Qualification Test Manager] The verification review of the HW Qualification Test Specification is completed.

M If you do not perform any mandatory process, you should have a reasonable rationale.

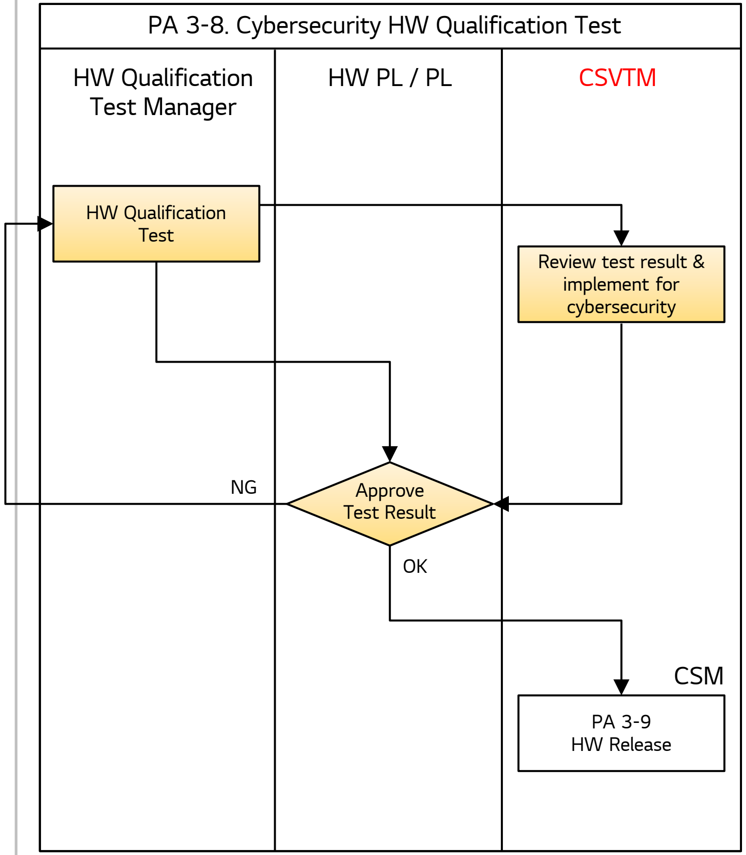
LGE Internal Use Only

3-8. Cybersecurity HW Qualification Test

Cybersecurity HW Development Phase

◆ HW Qualification Test Manager performs the HW Qualification Test.

Entry criteria The test case for the HW qualification test is confirmed.

Procedure	Detailed activity	Inputs
	**HW Qualification test manager performs the HW Qualification test through the following activities and creates HW Qualification test result report.** **[Description in detail]** • The test cases can be added / modified / deleted based on the HW requirements specification in consultation with HW PL/PL. • Defects identified in the test run should be traced with related work products. • Test result should be shared to related departments (dev. team, hw test / qualification test). • Repeat the test until test result is met the criteria. • CSVTM reviews test result for cybersecurity.	- HW Qualification Test Plan - HW Qualification Test Case **Outputs** - HW Qualification Test Report **Related standard** - ISO/SAE21434-10:v1.0

PA 3-8. Cybersecurity HW Qualification Test
HW Qualification Test Manager
HW PL / PL
CSVTM
HW Qualification Test
Review test result & implement for cybersecurity
Approve Test Result
NG
OK
CSM
PA 3-9 HW Release

Exit criteria [HW Qualification Test Manager] The test result is met with the test criteria and has covered all HW requirements.

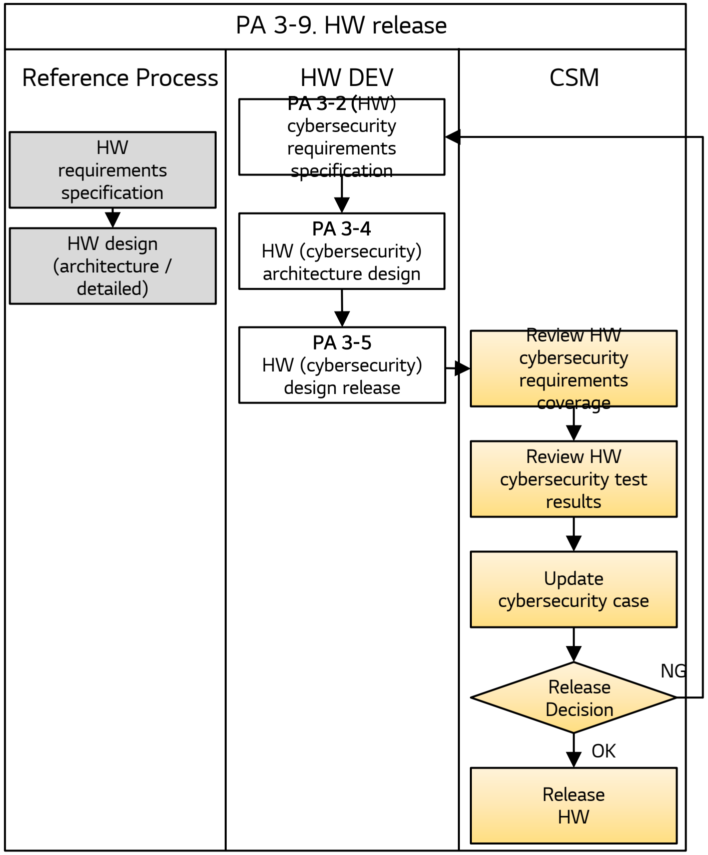
M If you do not perform any mandatory process, you should have a reasonable rationale.

3-9. HW release

◆ **Cybersecurity Manager reviews the HW cybersecurity work product and releases the HW.**

Entry criteria HW cybersecurity test should be completed.

Procedure



PA 3-9. HW release

Reference Process

HW requirements specification

HW design (architecture / detailed)

HW DEV

PA 3-2 (HW) cybersecurity requirements specification

PA 3-4 HW (cybersecurity) architecture design

PA 3-5 HW (cybersecurity) design release

CSM

Review HW cybersecurity requirements coverage

Review HW cybersecurity test results

Update cybersecurity case

Release Decision

NG

OK

Release HW

Detailed activity

Cybersecurity Manager reviews HW cybersecurity outputs, evaluates HW development levels, and releases HW.

[Description in detail]

- Cybersecurity Manager reviews whether the scope of the HW cybersecurity test covers all of the HW cybersecurity requirements (HWCSR).
- Cybersecurity Manager determines if the HW cybersecurity test results are within the release tolerance range.
- Cybersecurity Manager reflects HW verification results in the cybersecurity case.
- Cybersecurity Manager judges whether the cybersecurity requirement coverage and the result of the cybersecurity test are the level required by the OEM.
- Cybersecurity Manager assigns version to HW and releases HW.

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

- (HW) cybersecurity requirements
- HW (cybersecurity) architecture design (HWAD)
- Requirements traceability matrix (HWCSR – HWTC)
- HW cybersecurity test report

Outputs

- HW release report
- Cybersecurity case [refined]

Related standard

- ISO/SAE21434 10:v1.0

Exit criteria [Cybersecurity Manager] HW should be versioned and released.

M If you do not perform any mandatory process, you should have a reasonable rationale.

4 Cybersecurity SW Development Phase

- **Objective**

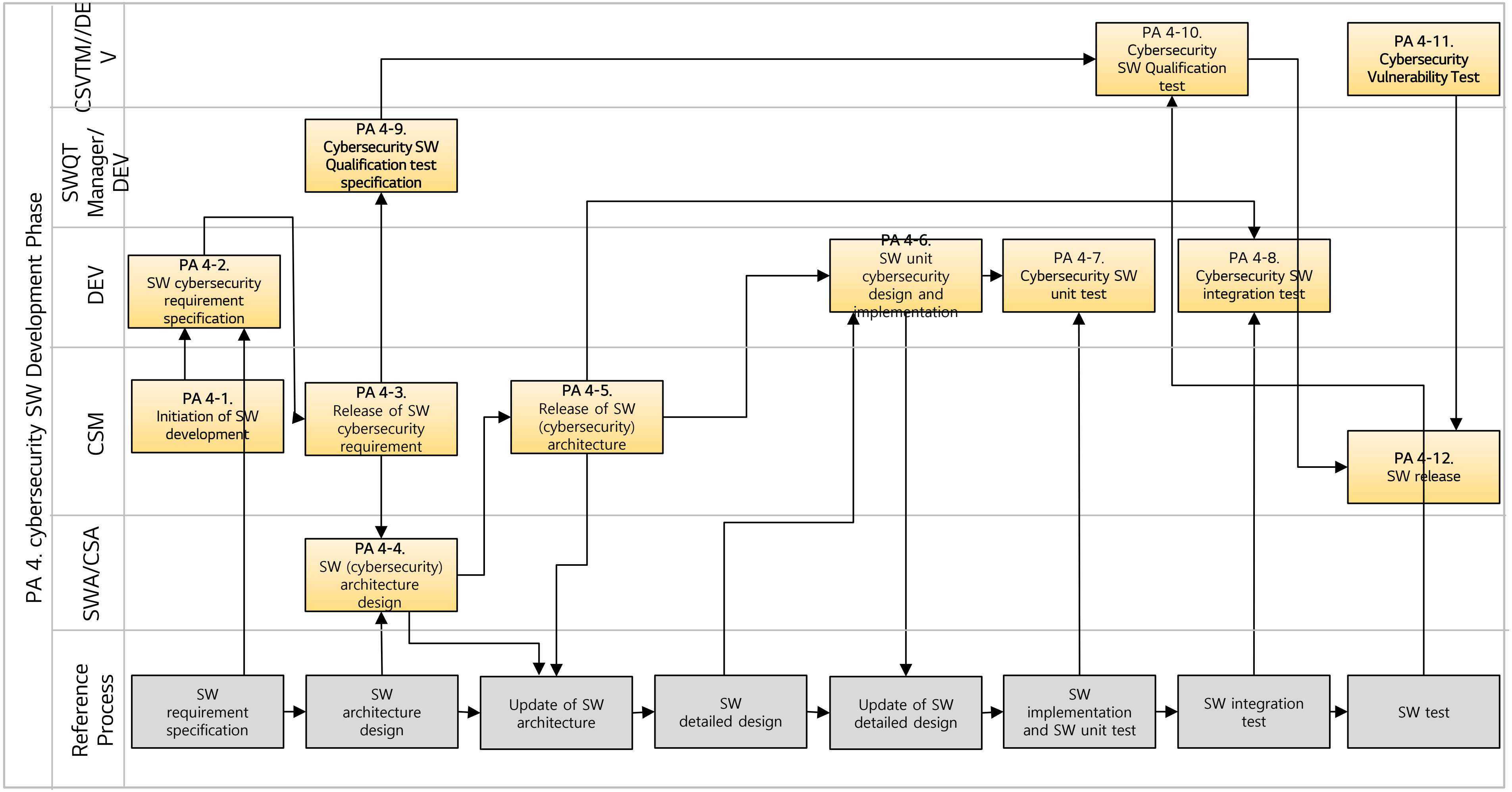
  Define cybersecurity software development phases to achieve cybersecurity goals and define key activities and criteria by stages.

- **Scope**

  This process is applied when developing an item that applies cybersecurity among electrical / electronic system developed by VS company.

4 Cybersecurity SW Development Phase

Define cybersecurity software development phase of the item that applies cybersecurity among electrical / electronic system developed by VS company and define key activities and criteria by stages.


PA 4. cybersecurity SW Development Phase
CSVTM/DEV
SWQT Manager/DEV
DEV
CSM
SWA/CSA
Reference Process
PA 4-10. Cybersecurity SW Qualification test
PA 4-11. Cybersecurity Vulnerability Test
PA 4-9. Cybersecurity SW Qualification test specification
PA 4-2. SW cybersecurity requirement specification
PA 4-6. SW unit cybersecurity design and implementation
PA 4-7. Cybersecurity SW unit test
PA 4-8. Cybersecurity SW integration test
PA 4-1. Initiation of SW development
PA 4-3. Release of SW cybersecurity requirement
PA 4-5. Release of SW (cybersecurity) architecture
PA 4-12. SW release
PA 4-4. SW (cybersecurity) architecture design
SW requirement specification
SW architecture design
Update of SW architecture
SW detailed design
Update of SW detailed design
SW implementation and SW unit test
SW integration test
SW test

4 Related ISO/SAE 21434 standard for cybersecurity SW development (1/2)

Option	Process Area	Description	Role	Work product	Related standard
M	**PA 4-1.** Initiation of SW development	Plan and initiate cybersecurity activities to be performed during SW development phase.	Cybersecurity Manager	• Cybersecurity plan [refined] • SW verification review plan • Test plan (SW Level) • Design and coding guideline • Static analysis rule set	- ISO/SAE 21434-10:v1.0
M	**PA 4-2.** (SW) cybersecurity requirement specification	The requirements allocated to the SW in the (system)cybersecurity requirements are detailed and specified from the SW point of view.	Developer	• SW cybersecurity requirement • VR Report (SWCSR) • Traceability Matrix (SysCSR-SWCSR) • HW-SW interface [refined] • Cybersecurity plan [refined] • SW Test plan [refined]	- ISO/SAE 21434-10:v1.0
M	**PA 4-3.** Release of (SW) cybersecurity requirement	Establish and distribute the specified (SW) cybersecurity requirements.	Cybersecurity Manager	• (SW)cybersecurity requirement • Traceability matrix (SysCSR-SWCSR) • HW-SW interface [refined] • Cybersecurity case [refined]	- ISO/SAE 21434-10:v1.0
M	**PA 4-4.** SW (cybersecurity) architecture design	Design SW architecture to achieve specified (SW) cybersecurity requirements.	SW Architect	• SW (cybersecurity) architecture design • Traceability matrix (SWCSR-SAD) • HW-SW interface [refined] • Cybersecurity plan [refined] • VR report (SAD)	- ISO/SAE 21434-10:v1.0
M	**PA 4-5.** Release of SW (cybersecurity) architecture	Analyze and confirm that SW (cybersecurity) architecture is designed to the appropriate level.	Cybersecurity Manager	• SW (cybersecurity) architecture design [refined] • HW-SW interface [refined] • Cybersecurity plan [refined] • Cybersecurity case [refined]	- ISO/SAE 21434-10:v1.0
M	**PA 4-6.** SW unit cybersecurity design and implementation	Design the SW cybersecurity unit at a level of detail.	Developer	• SW detailed design [refined] • VR report(SDD) • SW unit implementation source code • Static analysis report	- ISO/SAE 21434-10:v1.0

Mandatory O Optional

4 Related ISO/SAE 21434 standard for cybersecurity SW development (2/2)

Option	Process Area	Description	Role	Work product	Related standard
M	PA 4-7 Cybersecurity SW Unit Test	DEV develops test cases based on Cybersecurity SW unit test plans and establishes an environment for conducting tests.	Developer	• Cybersecurity SW Unit Test cases • SW Unit Test Report	- ISO/SAE 21434-10:v1.0 - Smart Division SW Development Standard Process Regulation 2-10
M	**PA 4-8.** Cybersecurity SW Integration Test	DEV performs the Cybersecurity SW Integration Test using the Cybersecurity SW Integration Test Case.	Developer	• Cybersecurity SW Integration Test cases • SW Integration Test Report	- ISO/SAE 21434-10:v1.0 - Smart Division SW Development Standard Process Regulation 2-12
M	PA 4-9. Cybersecurity SW Qualification Test Specification	SW Qualification Test Manager prepares cybersecurity SW qualification test specification.	SW Qualification Test Manager	• SW Qualification Test Case	- ISO/SAE 21434-10:v1.0
M	PA 4-10. Cybersecurity SW Qualification Test	Cybersecurity SW Qualification test using the Test Case approved by the Test Case Review Board.	SW Qualification Test Manager	• SW Qualification Test Report	- ISO/SAE 21434-10:v1.0 - Automotive SPICE Process Assessment / Reference Model SWE.6
M	**PA 4-11.** Cybersecurity Vulnerability Test	The Cybersecurity vulnerability test proceeds with the items defined in the requirements analysis stage.	CSVTM	• Cybersecurity Test Plan • Vulnerability Test Reports	- ISO/SAE 21434-10:v1.0
M	**PA 4-12.** SW release	Give the SW version and distribute it.	Cybersecurity Manager	• Cybersecurity case [refined] • SW release report	- ISO/SAE 21434-10:v1.0

M Mandatory O Optional

4 Role & responsibility for cybersecurity SW development (1/2)

Process Area	Work Product	CSM	CSA	DEV	SWA	SysA	CSVTM	SWQT Manager	SAM	SW PL/PL
PA 4-1. Initiation of SW development	• Cybersecurity plan [refined] • SW verification review plan • Test plan (SW Level) • Design and coding guideline • Static analysis rule set	R	-	I	-	-	S	S	S	-
PA 4-2. (SW)cybersecurity requirement specification	• SW cybersecurity requirement • VR Report (SWCSR) • Traceability Matrix (SysCSR-SWCSR) • HW-SW interface [refined] • Cybersecurity plan [refined] • SW Test plan [refined]	I	A	R	S	S	-	-	-	-
PA 4-3. Release of (SW)cybersecurity requirement	• (SW)cybersecurity requirement • Traceability matrix (SysCSR-SWCSR) • HW-SW interface [refined] • Cybersecurity case [refined]	I	S	R	S	-	-	-	-	A
PA 4-4. SW (cybersecurity) architecture design	• SW (cybersecurity) architecture design • Traceability matrix (SWCSR-SAD) • HW-SW interface [refined] • Cybersecurity plan [refined] • VR report (SAD)	I	S	S	R	S	-	-	-	-
PA 4-5. Release of SW (cybersecurity) architecture	• SW (cybersecurity) architecture design [refined] • HW-SW interface [refined] • Cybersecurity plan [refined] • Cybersecurity case [refined]	I	S	S	R	-	-	-	-	A
PA 4-6. SW unit cybersecurity design and implementation	• SW detailed design [refined] • VR report(SDD) • SW unit implementation source code • Static analysis report	I	-	R	-	-	-	-	S	-
PA 4-7 Cybersecurity SW Unit Test	• Cybersecurity SW Unit Test cases • SW Unit Test Report	I	-	R	-	-	I	I	-	A

R : Responsibility , A : Approval, S : Support , I : Informed

4 Role & responsibility for cybersecurity SW development (2/2)

Process Area	Work Product	CSM	CSA	DEV	CSVTM	SysIT Manager	SWQT Manager	Cybersecurity Assessor	SAM	SW PL/PL
PA 4-8. Cybersecurity SW Integration Test	• Cybersecurity SW Integration Test cases • SW Integration Test Report	I	-	R	I	-	I	-	-	A
PA 4-9. Cybersecurity SW Qualification Test Specification	• SW Qualification Test Case	I	-	S	I	-	R	-	-	-
PA 4-10. Cybersecurity SW Qualification Test	• SW Qualification Test Report	I	-	S	I	-	R	-	-	A
PA 4-11. Cybersecurity Vulnerability Test	• Cybersecurity Test Plan • Vulnerability Test Reports	A	-	S	R	-	-	-	-	-
PA 4-12. SW release	• Cybersecurity case [refined] • SW release report	S	S	S	S	I	I	I	-	R/A

R : Responsibility , A : Approval, S : Support , I : Informed

LGE Internal Use Only

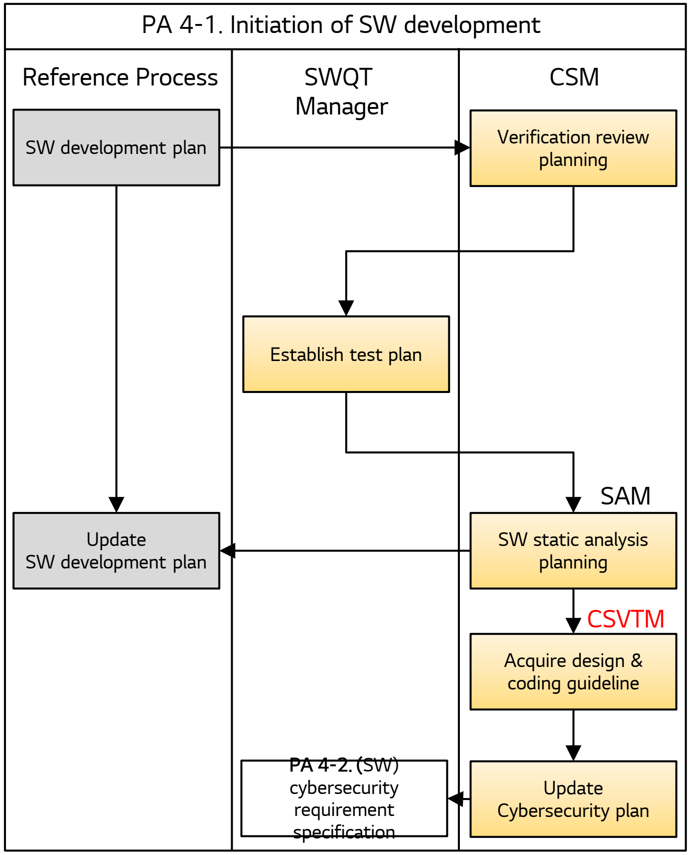
4-1. Initiation of SW development

Cybersecurity SW Development Phase

◆ Cybersecurity Manager determines and plans the cybersecurity activities to be performed during the SW development phase.

Entry criteria Initiation of system level development has been completed and the system cybersecurity activity plan should be completed.

Procedure


PA 4-1. Initiation of SW development
Reference Process
SWQT Manager
CSM
SW development plan
Verification review planning
Establish test plan
SAM
Update SW development plan
SW static analysis planning
CSVTM
Acquire design & coding guideline
PA 4-2. (SW) cybersecurity requirement specification
Update Cybersecurity plan

Detailed activity

Cybersecurity Manager determines and plans the cybersecurity activities required for SW development.

[Description in detail]

- CSM tailors the contents of the standard process to the project situation.(if needed)
- CSM updates the cybersecurity plan by establishing a VR plan for the SW development phase work products.
- SW qualification test manager develop SW test (SW unit test, SW integration test, SW qualification test) plans and updates the test plan.
- Static Analysis Manager(SAM) establishes the SW static analysis rules to be applied to the items and reflects the static analysis execution plan in the cybersecurity plan.
- CSVTM acquires design and coding guidelines to be used in SW design.
- CSM tailors VS standard coding guidelines to acquire coding guidelines for use in SW development.
- CSM makes a plan of SW component if there are some reused components. (if applicable)

[Design and coding guideline]

- Use of MISRA rules or CERT C according to the OEM requirement.
- When tailoring the modeling and coding guidelines to the project, apply the Topic as given in ISO 21434: v1.0, Annex E(Table 9) according to the CAL.

Inputs

- Project plan
- Cybersecurity plan
- (system) Cybersecurity requirement
- System (cybersecurity) architecture design
- Test plan (System integration test, System qualification test)

Outputs

- Cybersecurity plan [refined]
- SW verification review plan
- Test plan (SW Level)
- Design and coding guideline
- Static analysis rule set

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] The work products required in PA 4-1 should be reflected in the SW development plan.

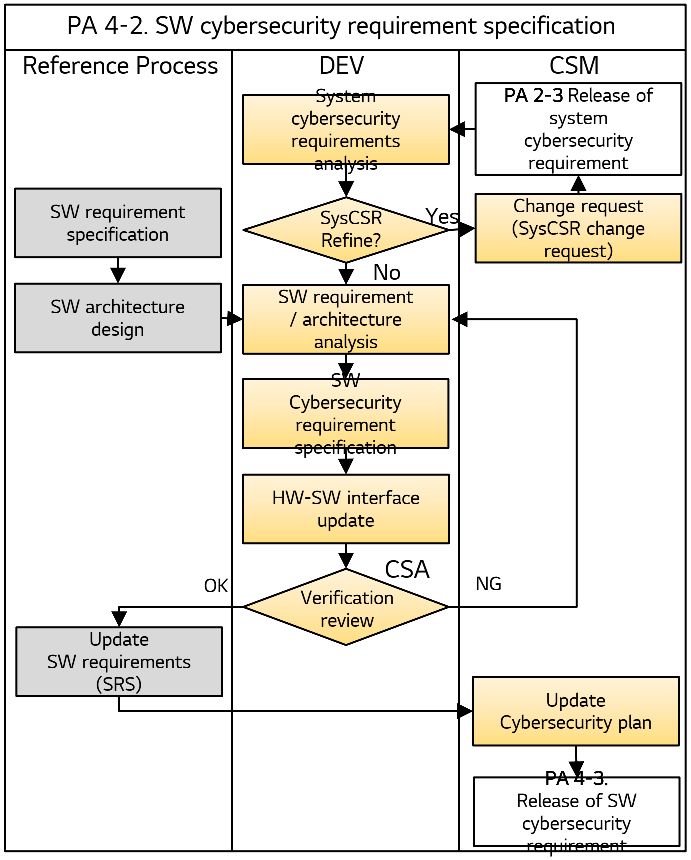
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-2. (SW) cybersecurity requirement specification

◆ Developer analyzes the requirements allocated to the SW in the system cybersecurity requirements and specifies SW requirements.

Entry criteria The verification review should be completed for the system cybersecurity requirements derived from the system phase.

Procedure


PA 4-2. SW cybersecurity requirement specification
Reference Process
DEV
CSM
System cybersecurity requirements analysis
PA 2-3 Release of system cybersecurity requirement
SW requirement specification
SysCSR Refine?
Yes
Change request (SysCSR change request)
No
SW architecture design
SW requirement / architecture analysis
SW Cybersecurity requirement specification
HW-SW interface update
CSA
OK
NG
Verification review
Update SW requirements (SRS)
Update Cybersecurity plan
PA 4-3. Release of SW cybersecurity requirement

Detailed activity

Developer(DEV) specifies the SW cybersecurity requirements for the system cybersecurity requirements allocated by the SW during the system development phase.

[Description in detail]

- DEV analyzes the system cybersecurity requirements allocated to the SW and analyzes the feasibility of implementing it in SW.
- DEV analyzes the SW requirements and analyzes the requirements related to or conflicting with the cybersecurity.
- DEV analyzes SW architecture and assigns system cybersecurity requirements to SW element.
- DEV specifies the system cybersecurity requirements allocated to the SW element to the extent that it can be implemented in SW.
- DEV analyzes considers and update the cybersecurity implications of post-development phase during the refinement of cybersecurity requirements.
- DEV specifies and allocates to the relevant entities of the operational environment if specific procedures are required to ensure cybersecurity in post-development phases.
- DEV creates traceability matrix between system cybersecurity requirements and SW cybersecurity requirements.
- DEV updates the HSI document by detailing the interface for the HW to be controlled at a level that can be controlled by the SW.
- CSA reviews the SW cybersecurity requirements.
- DEV requests updating the SW requirement that needs to be change by SW cybersecurity requirements.
- DEV reviews whether all SW requirements have been updated.
- DEV updates the SW test plan in consideration of the derived SW cybersecurity requirements.
- CSM updates the cybersecurity plan, taking into account the derived SW cybersecurity requirements.

Inputs

- System cybersecurity requirement
- System architecture design
- HW-SW interface
- SW architecture design
- Cybersecurity plan
- SW verification review plan

Outputs

- SW cybersecurity requirement
- VR Report (SWCSR)
- Traceability Matrix (SysCSR-SWCSR)
- HW-SW interface [refined]
- Cybersecurity plan [refined]
- SW Test plan [refined]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Developer] All system cybersecurity requirements allocated by the system to software should be specified as SW cybersecurity requirements and should satisfy VR criteria.

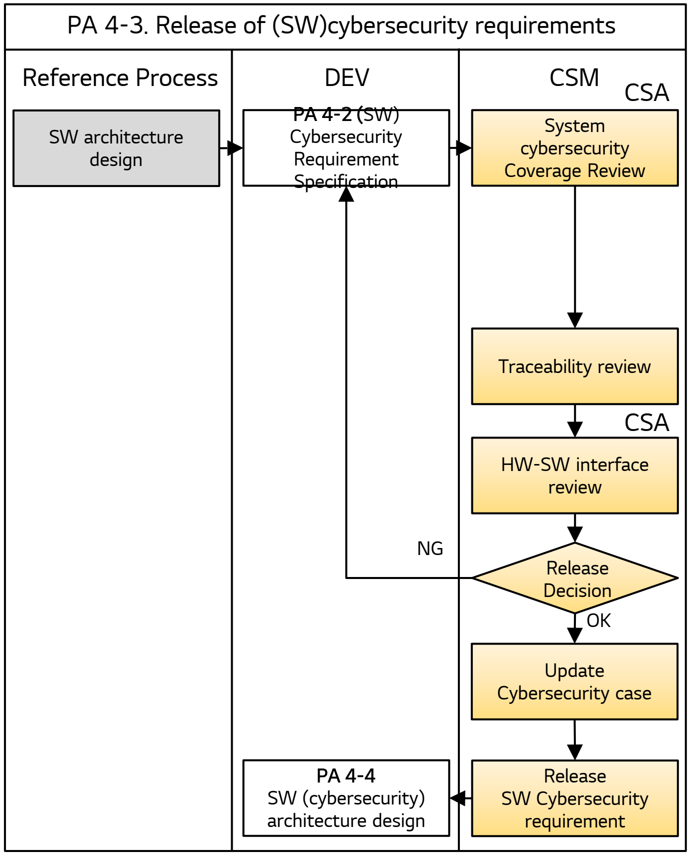
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-3. Release of (SW) cybersecurity requirements

◆ Cybersecurity Architect reviews specified (SW)cybersecurity requirements specified by the Developer and Cybersecurity Manager confirms and releases them.

Entry criteria The (SW) cybersecurity requirements pass verification review criteria.

Procedure


PA 4-3. Release of (SW)cybersecurity requirements
Reference Process
DEV
CSM
CSA
SW architecture design
PA 4-2 (SW) Cybersecurity Requirement Specification
System cybersecurity Coverage Review
Traceability review
CSA
HW-SW interface review
NG
Release Decision
OK
Update Cybersecurity case
PA 4-4 SW (cybersecurity) architecture design
Release SW Cybersecurity requirement

Detailed activity

Cybersecurity Architect reviews specified (SW)cybersecurity requirements specified by the Developer and Cybersecurity Manager confirms and releases them.

[Description in detail]

- CSA reviews if all system cybersecurity requirements allocated to the SW are specified as (SW)cybersecurity requirements.
- CSA reviews if (SW)cybersecurity requirements allocated to SW elements.
- CSA reviews whether traceability is correctly established between the system cybersecurity requirement and the SW cybersecurity requirement.
- Developer reviews whether (SW)cybersecurity requirement is deployable.
- CSM reflects (SW)cybersecurity requirement releases and decisions with OEMs in the cybersecurity case.
- CSM assigns a version to (SW)cybersecurity requirement, establishes baselines and distributes them to document management systems.

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

- (System)cybersecurity requirement
- SW architecture design
- (SW)cybersecurity requirement

Outputs

- (SW)cybersecurity requirement
- Traceability matrix (SysCSR-SWCSR)
- HW-SW interface [refined]
- Cybersecurity case [refined]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] Cybersecurity Manager assigns a version name to cybersecurity requirements and releases it to the document management system.

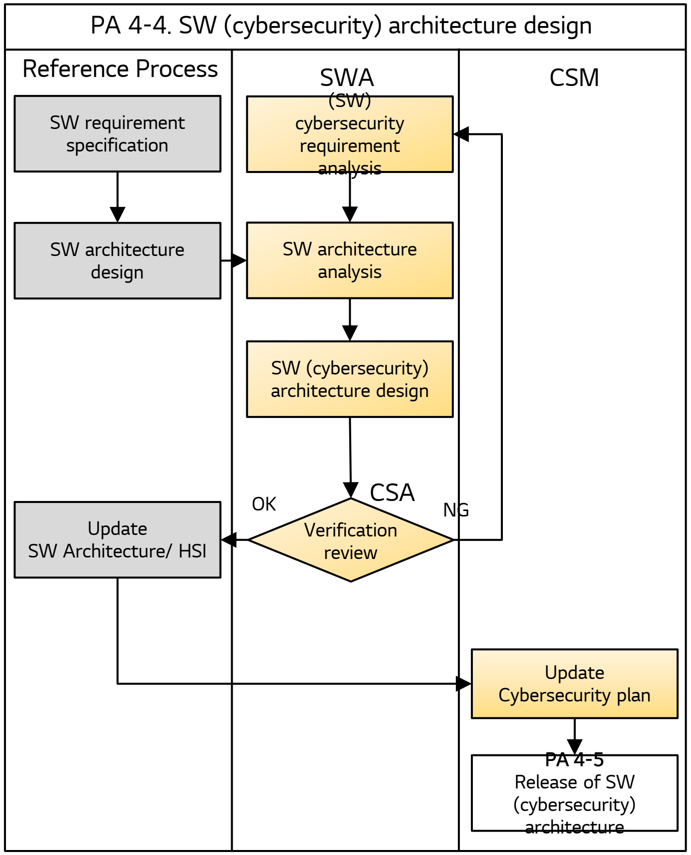
M If you do not perform any mandatory process, you should have a reasonable rationale.

4- 4. SW (cybersecurity) architecture design

◆ SW Architect designs SW architecture to meet (SW) cybersecurity requirements.

Entry criteria (SW) cybersecurity requirements should pass verification review criteria and be released formally.

Procedure



PA 4-4. SW (cybersecurity) architecture design

Reference Process | SWA | CSM

SW requirement specification

SW architecture design

Update SW Architecture/ HSI

(SW) cybersecurity requirement analysis

SW architecture analysis

SW (cybersecurity) architecture design

CSA

Verification review

OK

NG

Update Cybersecurity plan

PA 4-5 Release of SW (cybersecurity) architecture

Detailed activity

SW Architect designs SW cybersecurity architecture to achieve established SW cybersecurity requirements.

[Description in detail]

- SWA analyzes the (SW) cybersecurity requirements and identifies the cybersecurity goals and functions that the SW architecture should achieve.
- SWA analyzes SW architecture design for cybersecurity design.
- SWA allocates the defined cybersecurity requirements to components of the architectural design.
- SWA designs a SW architecture to implement (SW) cybersecurity requirements from a cybersecurity point of view.
- SWA analyzes the HW-SW interface created in the system phase and updates it from SW point of view.
- CSA performs verification review for (SW)cybersecurity design and HSI.
- CSA ensures cybersecurity control for risks are correctly implemented and risks are mitigated
- CSM updates the cybersecurity plan

[SW architecture design]

The UML notation should be used, which is a semi-formal notation.

Inputs

- (SW) cybersecurity requirement
- SW architecture design
- Cybersecurity plan
- Design and coding guideline
- Static analysis rule set
- HW-SW interface
- VR report (SWCSR)
- SW test plan

Outputs

- SW (cybersecurity) architecture design
- Traceability matrix (SWCSR-SAD)
- HW-SW interface [refined]
- Cybersecurity plan [refined]
- VR report (SAD)

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [SWA] The SW architecture should reflect all SW cybersecurity designs.

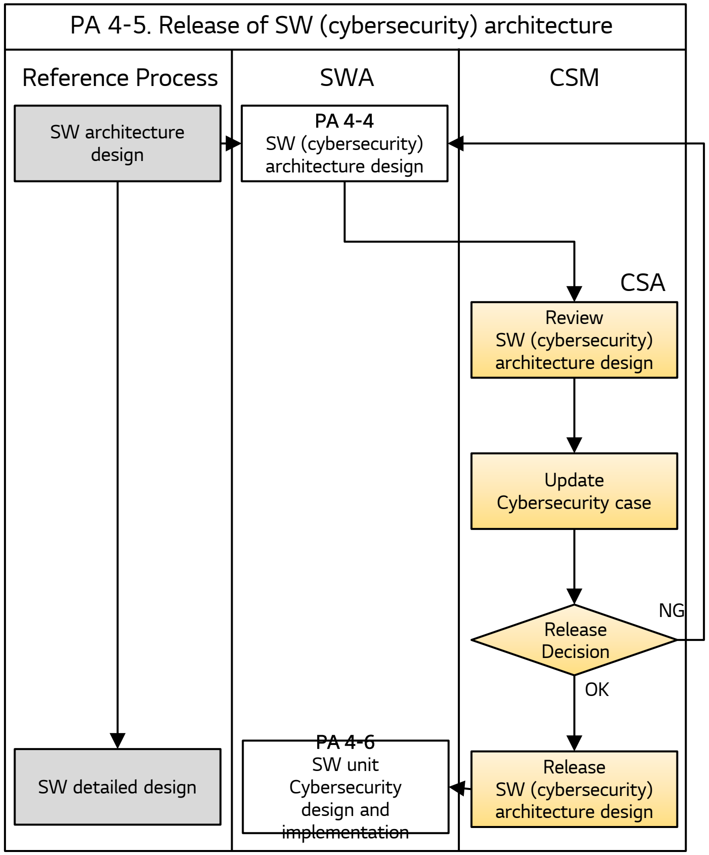
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-5. Release of SW (cybersecurity) architecture

◆ Cybersecurity Architect reviews the SW (cybersecurity) architecture design and Cybersecurity Manager confirms and releases them.

Entry criteria SW (cybersecurity) architecture design result should pass verification review criteria.

Procedure



PA 4-5. Release of SW (cybersecurity) architecture

Reference Process | SWA | CSM

CSA

SW architecture design

PA 4-4
SW (cybersecurity) architecture design

Review
SW (cybersecurity) architecture design

Update
Cybersecurity case

Release
Decision

NG

OK

Release
SW (cybersecurity) architecture design

SW detailed design

PA 4-6
SW unit Cybersecurity design and implementation

Detailed activity

Cybersecurity Architect reviews the SW (cybersecurity) design that reflects SW cybersecurity measure and Cybersecurity manager confirms and release them .

[Description in detail]

- CSA reviews whether the designed cybersecurity architecture is reflected in the SW architecture design.
- CSA reviews whether all the points of verification review are improved and reflected.
- CSA reviews whether the HW-SW interface has been properly updated from the SW point of view.
- CSM reviews and confirms the changed cybersecurity plan according to SW design.
- CSM reflects (SW) cybersecurity requirements, SW architecture design, HW-SW interface, and cybersecurity analysis results in the cybersecurity case.
- CSM assigns a baseline version to the SW (cybersecurity) architecture document and releases it to the document management system.

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

- SW (cybersecurity) architecture design
- HW-SW interface [refined]
- VR report(SAD)

Outputs

-SW (cybersecurity) architecture design [refined]
- HW-SW interface [refined]
- Cybersecurity plan [refined]
- Cybersecurity case [refined]

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] The SW (cybersecurity) architecture should be given a version and released to the document management system.

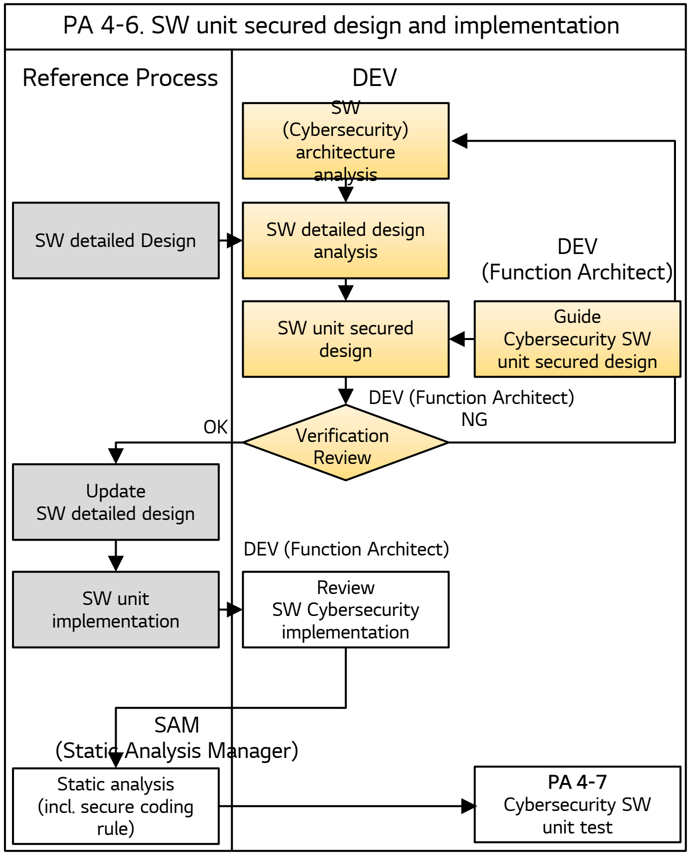
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-6. SW unit cybersecurity design and implementation (1/2)

◆ **Developer(DEV) performs the design for SW unit cybersecurity based on SW (cybersecurity) architecture design.**

Entry criteria SW (cybersecurity) architecture should be confirmed and released.

Procedure


PA 4-6. SW unit secured design and implementation

Reference Process

DEV

SW (Cybersecurity) architecture analysis

SW detailed Design

SW detailed design analysis

DEV (Function Architect)

SW unit secured design

Guide Cybersecurity SW unit secured design

DEV (Function Architect)

OK

NG

Verification Review

Update SW detailed design

DEV (Function Architect)

SW unit implementation

Review SW Cybersecurity implementation

SAM (Static Analysis Manager)

Static analysis (incl. secure coding rule)

PA 4-7 Cybersecurity SW unit test

Detailed activity

Developer(DEV) specifies SW unit cybersecurity design for implementing SW cybersecurity architecture.

[Description in detail]

- DEV analyzes the SW cybersecurity architectural design constraints that the SW unit should be secured.
- DEV reviews the SW detail design to ensure that it contains the latest design content and maintains consistency in the detail design.
- DEV analyzes the detailed structure of SW unit by analyzing SW detailed design.
- DEV(Function Architect) guides the cybersecurity SW unit secured design to developers.
- DEV performs SW unit secured design for the cybersecurity related element and the cybersecurity measure to satisfy the SW cybersecurity requirement.
- DEV(Function Architect) performs a verification review to ensure that the detailed design of the SW unit meets the SW cybersecurity requirement and design constraints.

Inputs

- SW cybersecurity requirement
- SW architecture design
- SW detailed design
- Cybersecurity plan
- VR plan(SDD)
- Design and coding guideline
- Calibration & Configuration Data
- Static analysis rule set

Outputs

- SW detailed design [refined]
- VR report(SDD)
- SW unit implementation source code
- Static analysis report

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Developer] Developer and Function Architect should apply all the detailed design of the SW cybersecurity design and confirm the design with verification review.

M If you do not perform any mandatory process, you should have a reasonable rationale.

LGE Internal Use Only

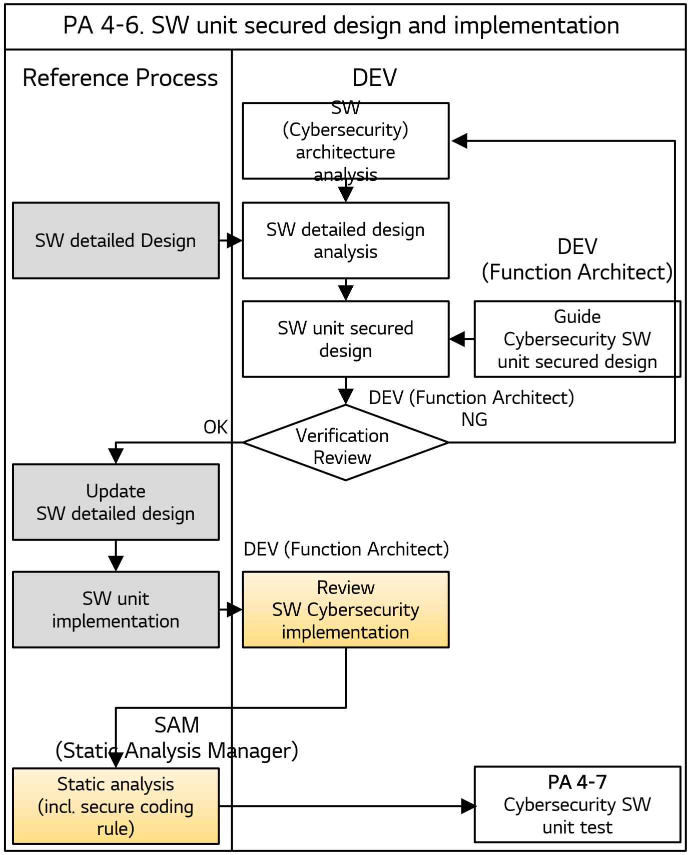
4-6. SW unit cybersecurity design and implementation (2/2)

Cybersecurity SW Development Phase

◆ **Developer(DEV) performs the design for SW unit cybersecurity based on SW (cybersecurity) architecture design.**

Entry criteria SW (cybersecurity) architecture should be confirmed and released.

Procedure


PA 4-6. SW unit secured design and implementation
Reference Process
DEV
SW (Cybersecurity) architecture analysis
SW detailed Design
SW detailed design analysis
DEV (Function Architect)
SW unit secured design
Guide Cybersecurity SW unit secured design
DEV (Function Architect)
NG
OK
Verification Review
Update SW detailed design
DEV (Function Architect)
SW unit implementation
Review SW Cybersecurity implementation
SAM (Static Analysis Manager)
Static analysis (incl. secure coding rule)
PA 4-7 Cybersecurity SW unit test

Detailed activity

Developer(DEV) specifies SW unit cybersecurity design for implementing SW cybersecurity architecture.

[Description in detail]

- DEV reviews whether cybersecurity design contents are reflected in SW detailed design.
- DEV implements the detailed design of the SW unit.
- ※ SW unit implementation reflects the restriction of coding guideline
- Static Analysis Manager(SAM) performs secure static code analysis with tool and guides how to resolve it to developers
- DEV performs secure static code analysis, analyzes and corrects problems of implemented codes.

Inputs

- SW cybersecurity requirement
- SW architecture design
- SW detailed design
- Cybersecurity plan
- VR plan(SDD)
- Design and coding guideline
- Calibration & Configuration Data
- Static analysis rule set

Outputs

- SW detailed design [refined]
- VR report(SDD)
- SW unit implementation source code
- Static analysis report

Related standard

- ISO/SAE21434-10:v1.0

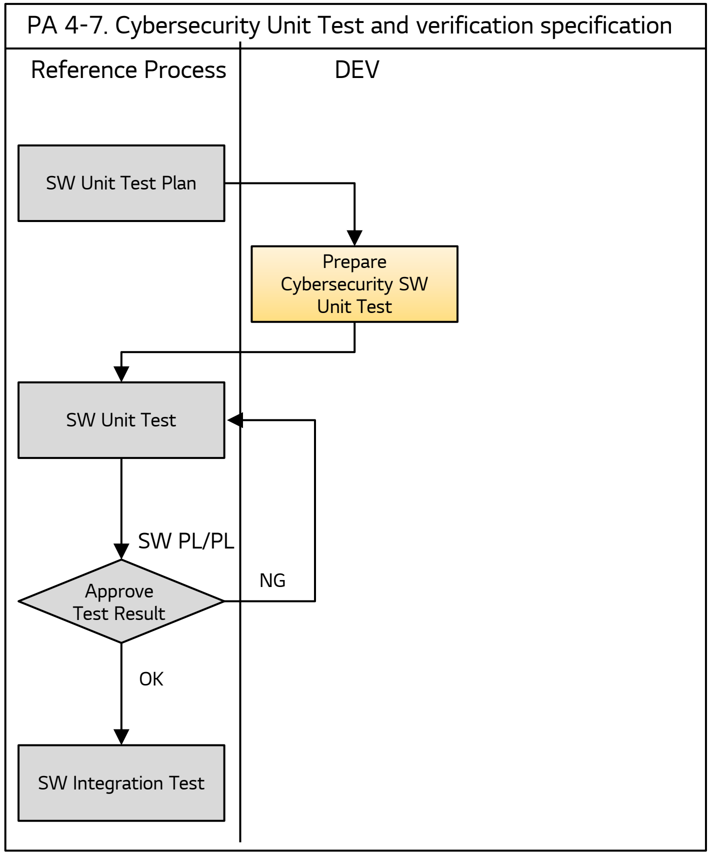
Exit criteria [Developer] Developer and Function Architect should apply all the detailed design of the SW cybersecurity design and confirm the design with verification review.

M If you do not perform any mandatory process, you should have a reasonable rationale.

4-7. Cybersecurity SW Unit Test

◆ Developer(DEV) develops test cases based on Cybersecurity SW unit test plan and performs the Cybersecurity SW unit test.

Entry criteria A confirmed cybersecurity unit test plan and detailed design shall exist.

Procedure	Detailed activity	Inputs
 PA 4-7. Cybersecurity Unit Test and verification specification Reference Process DEV SW Unit Test Plan Prepare Cybersecurity SW Unit Test SW Unit Test SW PL/PL NG Approve Test Result OK SW Integration Test	**DEV prepares and performs the Cybersecurity SW Unit test.** **[Description in detail]** Develop the SW unit test case for cybersecurity. Establish the environment for SW unit test for cybersecurity. Review test case. Mandatory items on SW Qualification test report. [Items] The version of SW release Executed SW component name and total number of functions The result of pass/fail based on test cases * Overall test process including test coverage is compliant with 'Unit Verification Plan' document	- SW Unit Test Plan - SW Detailed Design **Outputs** - Cybersecurity SW Unit Test cases - SW Unit Test Report **Related standard** - ISO/SAE 21434-10:v1.0 - Smart Division SW Development Standard Process Regulation 2-10

Exit criteria [Developer] The test result is met with the test criteria and has covered all SW detailed designs.

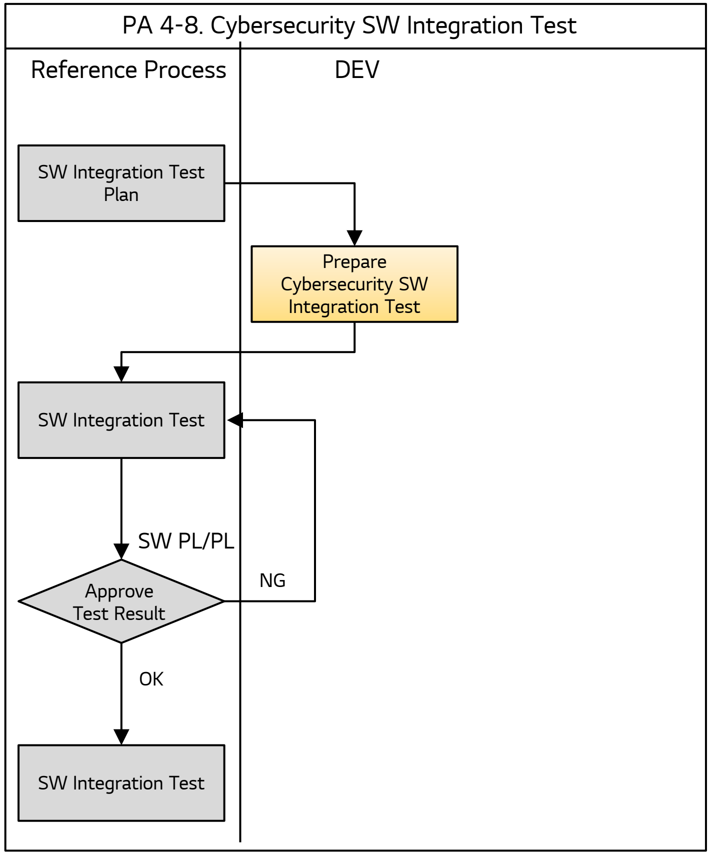
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-8. Cybersecurity SW Integration Test

Cybersecurity SW Development Phase

◆ Developer(DEV) performs the Cybersecurity SW Integration Test using the Cybersecurity SW Integration Test Case.

Entry criteria Complete the preparation of the system requirements statement. Complete SW test environment construction and SW test case development.

Procedure	Detailed activity	Inputs
 PA 4-8. Cybersecurity SW Integration Test Reference Process DEV SW Integration Test Plan Prepare Cybersecurity SW Integration Test SW Integration Test SW PL/PL Approve Test Result NG OK SW Integration Test	**DEV prepare the test case of the cybersecurity SW Integration Test and perform the cybersecurity SW Integration Test.** **[Description in detail]** • Check the SW release version at the time of the Cybersecurity SW integration test. • Define the scope of the Cybersecurity SW integration testing in accordance with the test strategy described in the Cybersecurity SW Integration Test Plan. • Send the results of the Cybersecurity SW integration test to the CSM and request approval. Mandatory items on SW Cybersecurity SW Integration test case. [Items] Requirement ID / TC ID TC design type Precondition Input / expected output Observed output Pass / Fail / NA Test method * Overall test process including test coverage is compliant with 'SW integration TestPlan' document	- SW Integration Test Plan - SW (cybersecurity) architecture design **Outputs** - Cybersecurity SW Integration Test cases - SW Integration Test Report **Related standard** - ISO/SAE 21434-10:v1.0 - Smart Division SW Development Standard Process Regulation 2-12

Exit criteria [Developer] The test result is met with the test criteria and has covered all SW architecture designs.

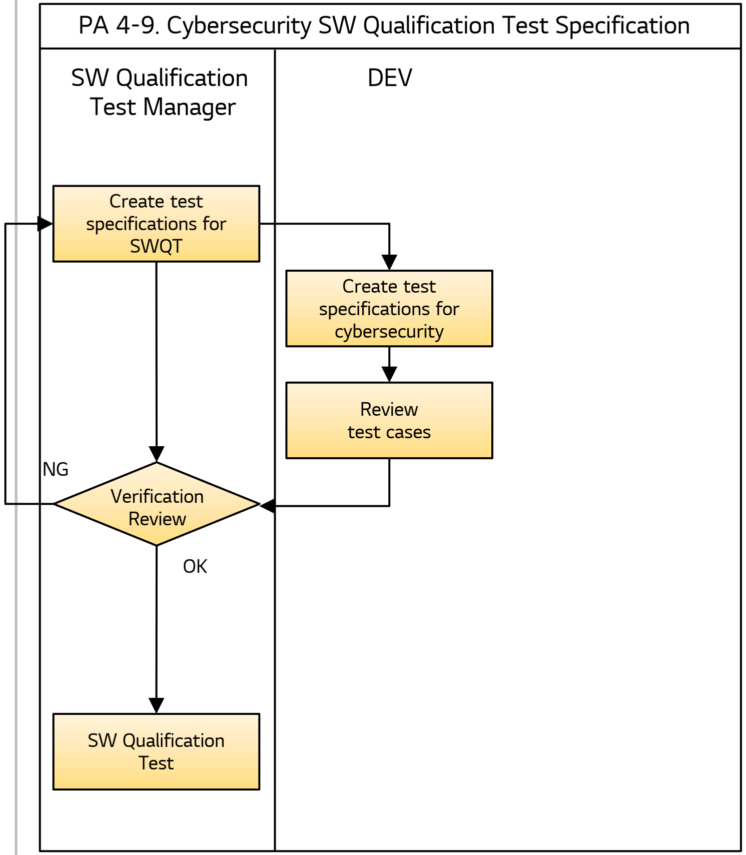
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-9. Cybersecurity SW Qualification Test Specification

◆ SW Qualification Test Manager prepares cybersecurity SW qualification test specification.

Entry criteria The SW requirements of cybersecurity should be existed and confirmed.

Procedure


PA 4-9. Cybersecurity SW Qualification Test Specification
SW Qualification Test Manager
DEV
Create test specifications for SWQT
Create test specifications for cybersecurity
Review test cases
NG
Verification Review
OK
SW Qualification Test

Detailed activity

SW Qualification test manager prepares the SW Qualification test through the following activities.

[Detail Activities]
Develop the SW qualification test case for cybersecurity.
Establish the environment for SW Qualification test for cybersecurity.
Review test case.

[Description in detail]

- DEV develops the SW qualification test case for cybersecurity.
- Establish the environment for SW qualification test for cybersecurity.
- Review test case with DEV.
- DEV reviews test cases for cybersecurity

Mandatory items on SW Qualification test case.

[Items]
Requirement ID / TC ID
TC design type
Precondition
Input / expected output
Observed output
Pass / Fail / NA
Test method

Inputs

- (Cybersecurity) SW Requirements Specification

Outputs

- SW Qualification Test Case

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [SW Qualification Test Manager] The verification review of the SW Qualification Test Specification is completed.

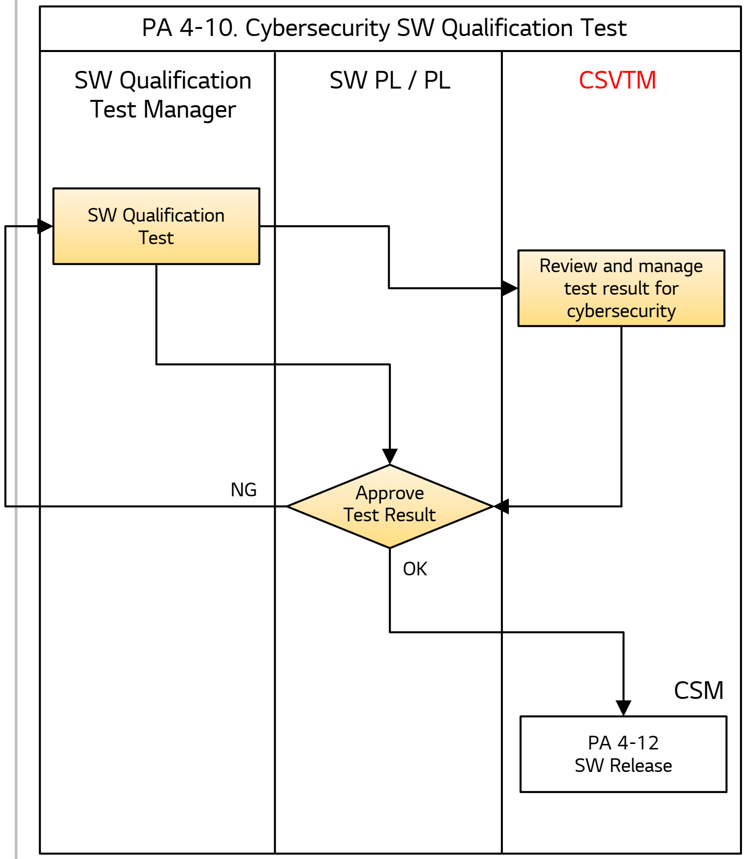
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-10. Cybersecurity SW Qualification Test

◆ **SW Qualification Test Manager performs the SW Qualification Test.**

Entry criteria Complete the preparation of the system requirements statement. Complete SW test environment construction and SW test case development.

Procedure



PA 4-10. Cybersecurity SW Qualification Test

SW Qualification Test Manager

SW PL / PL

CSVTM

SW Qualification Test

Review and manage test result for cybersecurity

NG

Approve Test Result

OK

CSM

PA 4-12 SW Release

Detailed activity

SW Qualification test manager perform the SW Qualification test through the following activities and creates SW Qualification test result report.

[Description in detail]

- The test cases can be added / modified / deleted based on the SW requirements specification in consultation with SW PL/PL.
- Defects identified in the test run should be traced with related work products.
- Test result should be shared to related departments (dev. team, sw test / qualification test).
- Repeat the test until test result is met the criteria.
- CSVTM reviews test result for cybersecurity.

Inputs

- SW Qualification Test Plan
- SW Qualification Test Case

Outputs

- SW Qualification Test Report

Related standard

- ISO/SAE 21434-10:v1.0
- Automotive SPICE Process Assessment / Reference Model SWE.6

Exit criteria [SW Qualification Test Manager] The test result is met with the test criteria and has covered all SW requirements.

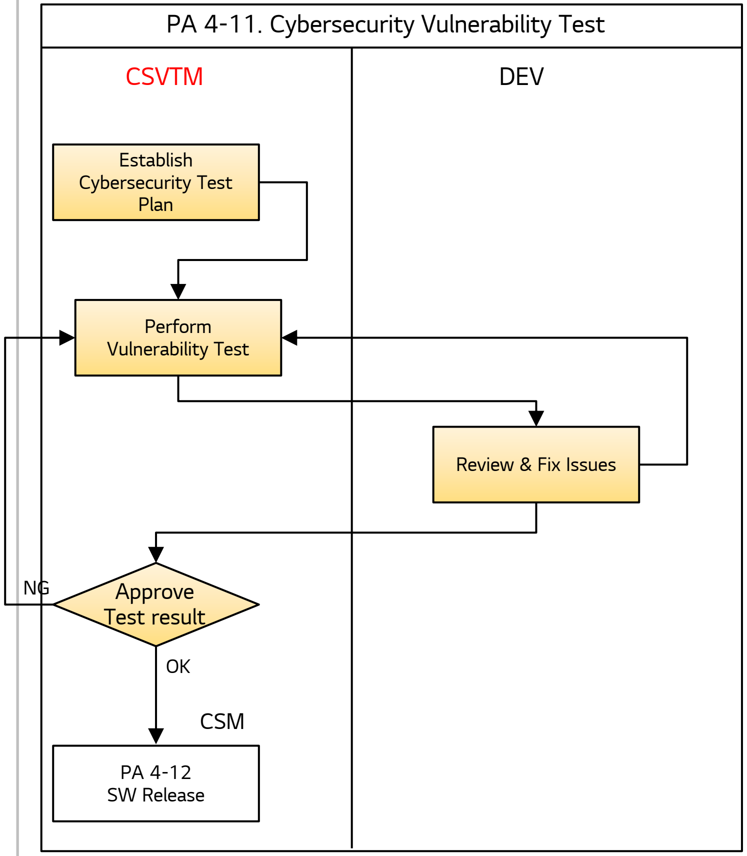
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-11. Cybersecurity Vulnerability Test

◆ **The Cybersecurity vulnerability test proceeds with the items defined in the requirements analysis stage.**

Entry criteria The environments and resources of vulnerability test must be prepared.

Procedure


PA 4-11. Cybersecurity Vulnerability Test

CSVTM

DEV

Establish Cybersecurity Test Plan

Perform Vulnerability Test

Review & Fix Issues

NG

Approve Test result

OK

CSM

PA 4-12 SW Release

Detailed activity

Measurements are made using a variety of tools to eliminate Security Vulnerability, and modifications proceed with the activity.

[Description in detail]

- CSVTM establishes a schedule for the Vulnerability analysis, allows to conduct measurement tests according to the schedule, and publishes reports.
- CSVTM performs tests align with the cybersecurity test plan.
- Developer(DEV) reviews and corrects the detected vulnerabilities.

[Cybersecurity Vulnerability Testing Item]

- Open Source Software Vulnerability Scanning
- Operational Security Hardening
- Exploit Mitigation via compile option setting

※ For the detailed process, refer to the following link
http://collab.lge.com/main/x/JDQHh

Inputs

- Cybersecurity Plan

Outputs

- Cybersecurity Test Plan
- Vulnerability Test Reports

Related standard

- ISO/SAE 21434-10:v1.0

Exit criteria [CSVTM] Release each vulnerability test result to the stakeholders.

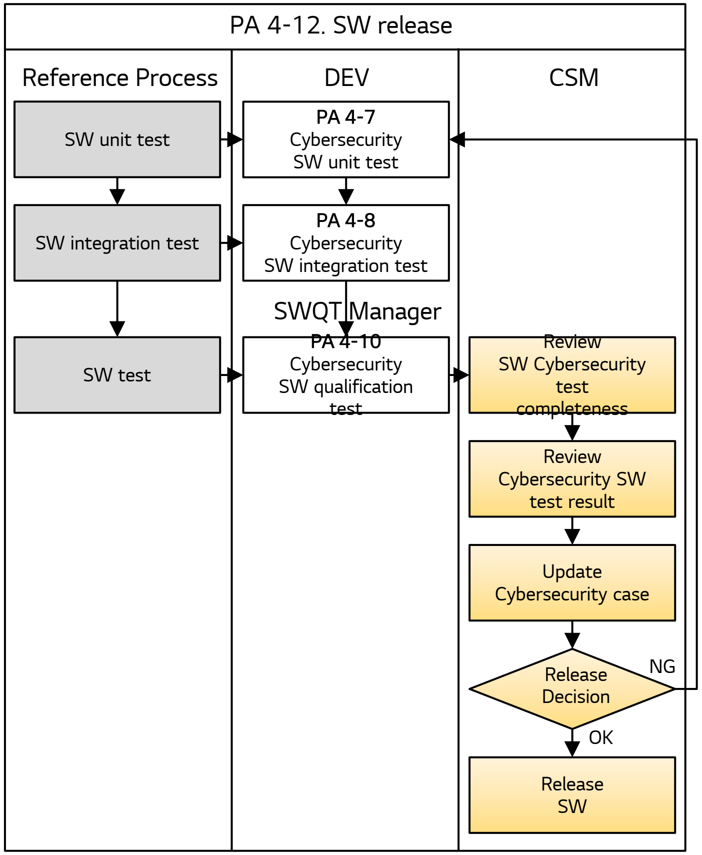
M If you do not perform any mandatory process, you should have a reasonable rationale.

4-12. SW release

◆ **Cybersecurity Manager decides that the implemented SW satisfies the cybersecurity requirement and then releases the SW.**

Entry criteria SW test should be completed.

Procedure


PA 4-12. SW release
Reference Process
DEV
CSM
SW unit test
SW integration test
SW test
PA 4-7
Cybersecurity
SW unit test
PA 4-8
Cybersecurity
SW integration test
SWQT Manager
PA 4-10
Cybersecurity
SW qualification
test
Review
SW Cybersecurity
test
completeness
Review
Cybersecurity SW
test result
Update
Cybersecurity case
Release
Decision
NG
OK
Release
SW

Detailed activity

Cybersecurity Manager releases the SW by examining whether it has been tested to achieve (SW) cybersecurity requirement for each SW level test.

[Description in detail]

- Cybersecurity Manager reviews whether each level of the test has achieved its agreed test objectives with the OEM.
- Cybersecurity Manager reviews the test results at each level to determine if it can be released to OEM.
- Cybersecurity Manager determines if the SW test results are releasable to the OEM. If the result of the test does not archive the expectation of OEM, the test is performed again or need a rationale for the test result not meeting the target value.
- Cybersecurity Manager updates the cybersecurity requirement test result (SW unit test, SW integration test, SW test) to the cybersecurity case.
- Cybersecurity Manager assigns a baseline version to the SW.

※ All cybersecurity work-products shall be approved by Cybersecurity Governance Manager before the official release to OEM.

Inputs

-SW unit test report
-SW integration test report
-SW test report
-Requirement traceability matrix

Outputs

- Cybersecurity case [refined]
- SW release report

Related standard

- ISO/SAE21434-10:v1.0

Exit criteria [Cybersecurity Manager] The SW should be versioned and released.

M If you do not perform any mandatory process, you should have a reasonable rationale.

5 Cybersecurity Management & Supporting

- **Objective**

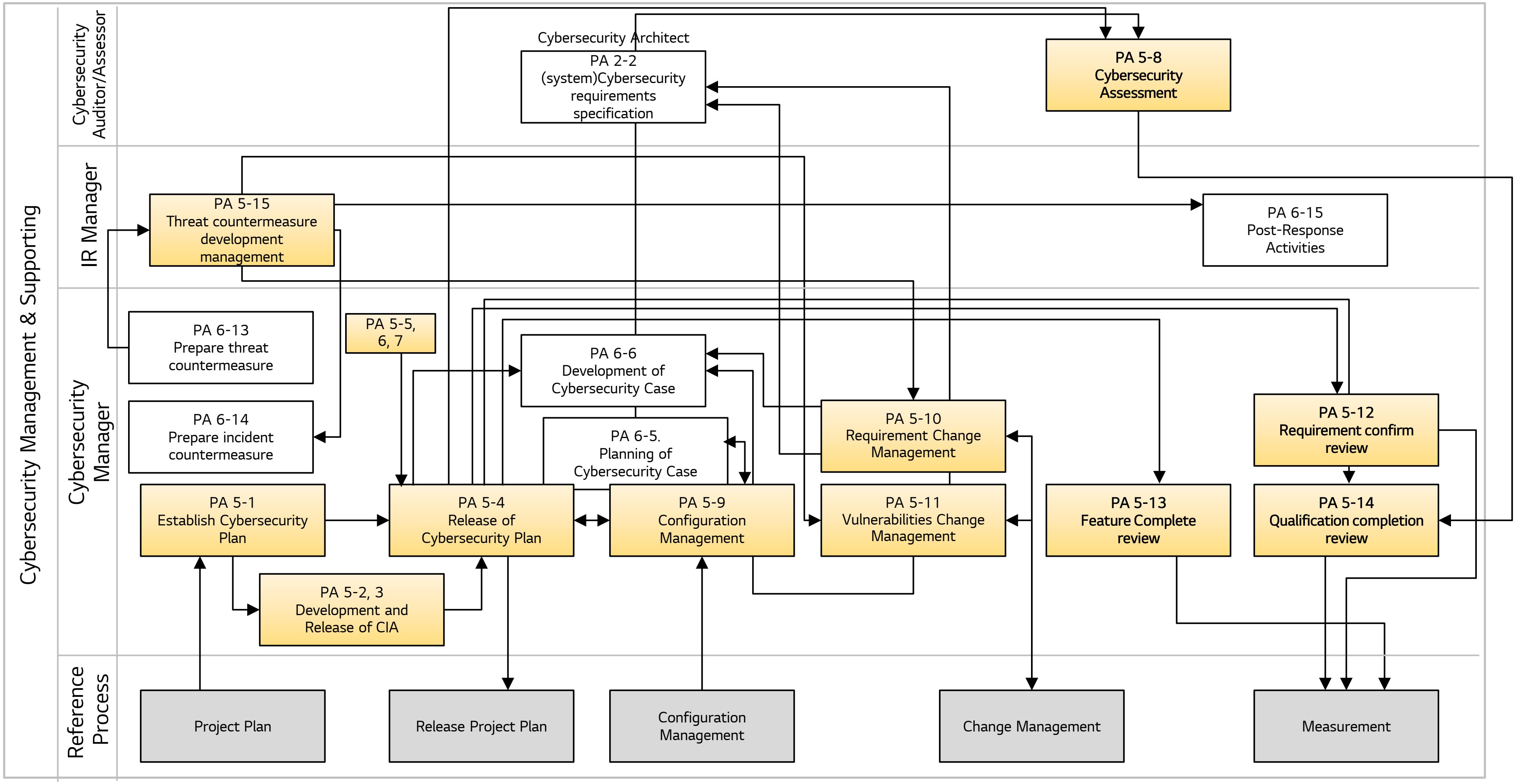
  Define the cybersecurity management & supporting phase of the item to which cybersecurity is applied among the E/E system developed by the VS company, and define the main activities and standards by stages.

- **Scope**

  It is applied when developing the item to apply cybersecurity among electrical and electronic system (E / E system) developed by VS company.

5 Cybersecurity Management & Supporting

Define the cybersecurity management & supporting phase of the item to which cybersecurity is applied among the E/E system developed by the VS company, and define the main activities and standards by stages.


Cybersecurity Management & Supporting
Cybersecurity Auditor/Assessor
IR Manager
Cybersecurity Manager
Reference Process
Cybersecurity Architect
PA 2-2 (system)Cybersecurity requirements specification
PA 5-8 Cybersecurity Assessment
PA 5-15 Threat countermeasure development management
PA 6-15 Post-Response Activities
PA 6-13 Prepare threat countermeasure
PA 5-5, 6, 7
PA 6-6 Development of Cybersecurity Case
PA 6-14 Prepare incident countermeasure
PA 6-5. Planning of Cybersecurity Case
PA 5-10 Requirement Change Management
PA 5-12 Requirement confirm review
PA 5-1 Establish Cybersecurity Plan
PA 5-4 Release of Cybersecurity Plan
PA 5-9 Configuration Management
PA 5-11 Vulnerabilities Change Management
PA 5-13 Feature Complete review
PA 5-14 Qualification completion review
PA 5-2, 3 Development and Release of CIA
Project Plan
Release Project Plan
Configuration Management
Change Management
Measurement

5 Related ISO/SAE 21434 standard for Cybersecurity Management & Supporting (1/2)

Option	Process Area	Description	Role	Work product	Related standard
M	PA 5-1. Establish Cybersecurity Plan	Cybersecurity Manager sets a cybersecurity activity plan in consideration of the project development plan	Cybersecurity Manager	• Cybersecurity Plan	- ISO/SAE 21434-6:v1.0
M	PA 5-2. Development of CIA & suppliers' CIA	The Cybersecurity Manager creates a cybersecurity activity plan for the CIA & suppliers' CIA required by the OEM.	Cybersecurity Manager	• CIA • Supplier_Evaluation_Checklist	- ISO/SAE 21434-7:v1.0
M	PA 5-3. Release of CIA	The Cybersecurity Manager agrees on the CIA with the OEM.	Cybersecurity Manager	• CIA [confirmed]	- ISO/SAE 21434-7:v1.0
M	PA 5-4. Release of Cybersecurity Plan	Cybersecurity Manager agrees a Cybersecurity Plan with OEM.	Cybersecurity Manager	• Cybersecurity Plan [confirmation]	- ISO/SAE 21434-6:v1.0
M	PA 5-5. Reuse Analysis	Identification of reused SW and obtaining HW block diagram should be complete.	Cybersecurity Architect	• Reuse Analysis Report • Risk reduction activity	- ISO/SAE 21434 -6:v1.0 - IATF 16949 - ISO 9001 - ISO 26262
M	PA 5-6. Out-of-Context Component Validation	Identification of Out-of-Context Component and obtaining 3rd Party Component list should be complete	Cybersecurity Manager	• Out-of-Context Validation Report	- ISO/SAE 21434 -6:v1.0 - IATF 16949 - ISO 9001 - ISO 26262
M	PA 5-7. Cybersecurity Activities for Off-the-Shelf	Identification of Off-the-Shelf Component and obtaining 3rd Party's Document should be complete.	Cybersecurity Manager	• 3rd Party Cybersecurity document	- ISO/SAE 21434 -6:v1.0 - IATF 16949 - ISO 9001 - ISO 26262
M	PA 5-8. Cybersecurity Assessment	The Cybersecurity Assessor establishes the assessment plan and performs the assessment.	Cybersecurity Assessor	• Assessment Report	- ISO/SAE 21434 -6:v1.0 - IATF 16949 - ISO 9001 - ISO 26262

M Mandatory O Optional

5 Related ISO/SAE 21434 standard for Cybersecurity Management & Supporting (2/2)

Option	Process Area	Description	Role	Work product	Related standard
M	PA 5-9. Configuration Management	Cybersecurity Manager (CSM) identifies the CI (Configuration Item) and manages it in compliance with the configuration management plan.	Cybersecurity Manager	• Configuration Item • Configuration Management Book • Configuration Management Plan [refined]	- ISO/SAE 21434-5:v1.0 - Smart Division SW Development Standard Process Regulation 2-18
M	PA 5-10. Requirement Change Management	Cybersecurity Architect(CSA), SW PL, and Developer perform the impact analysis and implementation after receiving the CR agreed with OEM from SW PL.	Cybersecurity Architect	• Technical Review report • Cybersecurity Requirements and Design [refined] • Verification Result	- ISO/SAE 21434-5:v1.0 - Smart Division SW Development Standard Process Regulation 2-21
M	PA 5-11. Vulnerabilities Change Management	Cybersecurity Architect(CSA) and Developer perform the impact analysis and implementation after receiving the CR related to new vulnerabilities agreed with OEM from SW PL.	Cybersecurity Architect	• CR • Impact Analysis Report • Cybersecurity Requirements and Design [refined] • Verification Result	- ISO/SAE 21434-5:v1.0 - Smart Division SW Development Standard Process Regulation 2-21
M	PA 5-12. SW Requirements confirm review	SW PL holds the SW Requirement Baseline Workshop and confirms the first baseline agreed with customer.	SW PL	• Requirements confirmation review report	- Smart Division SW Development Standard Process Regulation 1-6
M	PA 5-13. Feature complete review	SW PL holds the Feature Complete Declaration meeting and declares the Feature Complete after reviewing work-products with stakeholders.	SW PL	• Feature Complete Review Report	- Smart Division SW Development Standard Process Regulation 2-15
M	PA 5-14. Qualification completion Review	DQA confirms the version for production or release after complete the SW Qualification test(NPI process).	SW PL	• Qualification completion review report	- Smart Division SW Development Standard Process Regulation 4-11
M	PA 5-15. Threat countermeasure development management	CS Manager manages countermeasure development.	Incident Response Manager	• Threat response action plan [refined] • Cybersecurity Case [refined]	- ISO/SAE 21434 -8:v1.0

M Mandatory O Optional

Cybersecurity Management & Supporting Role & Responsibility (1/2)

Process Area	Work Product	CSM	CSA	DEV	Configuration Manager	PL/ SW PL	Cybersecurity Auditor	Cybersecurity Assessor
PA 5-1. Establish Cybersecurity Plan	• Cybersecurity Plan	R/A	I	I	I	I	-	I
PA 5-2. Development of CIA & suppliers' CIA	• CIA • Supplier_Evaluation_Checklist	R	S	I	I	A	S	I
PA 5-3. Release of CIA	• CIA [Confirmed]	R	S	I	I	A	-	I
PA 5-4. Release of Cybersecurity Plan	• Cybersecurity Plan [Confirmation]	R/A	I	I	I	I	-	I
PA 5-5. Reuse Analysis	• Reuse Analysis Report • Risk reduction activity	S	R A(Leader)	S	I	I	-	I
PA 5-6. Out-of-Context Component Validation	• Out-of-Context Validation Report	R	S	S	I	I	-	I
PA 5-7. Cybersecurity Activities for Off-the-Shelf	• 3rd Party Cybersecurity document	R	S	S	I	I	-	I
PA 5-8. Cybersecurity Assessment	• Assessment Report	S	I	S	I	A	-	R
PA 5-9. Configuration Management	• Configuration Item • Configuration Management Book • Configuration Management Plan [refined]	R	S	S	S	A	-	-
PA 5-10. Requirement Change Management	• Technical Review report • Cybersecurity Requirements and Design [refined] • Verification Result	A	R	S	I	S	-	-

R : Responsibility , A : Approval, S : Support , I : Informed

Cybersecurity Management & Supporting Role & Responsibility (2/2)

Process Area	Work Product	CSM	CSA	DEV	Configuration Manager	PL/ SW PL	DQA	IR Manager	PTM	CSVTM	SWQT Manager	SysIT Manager	SysQT Manager
PA 5-11. Vulnerabilities Change Management	• CR • Impact Analysis Report • Cybersecurity Requirements and Design [refined] • Verification Result	A	R	S	I	S	-	-	-	-	-	-	-
PA 5-12. SW Requirements confirm review	• Requirements confirmation review report	S	S	S	I	R	-	-	-	-	S	S	S
PA 5-13. Feature complete review	• Feature Complete Review Report	S	S	S	I	R	I	-	-	-	S	S	S
PA 5-14. Qualification completion Review	• Qualification completion review report	S	S	S	I	R	A	-	-	-	S	S	S
PA 5-15. Threat countermeasure development management	• Threat response action plan [refined] • Cybersecurity Case [refined]	S	S	S	I	I	S	S	S	R	S	S	S

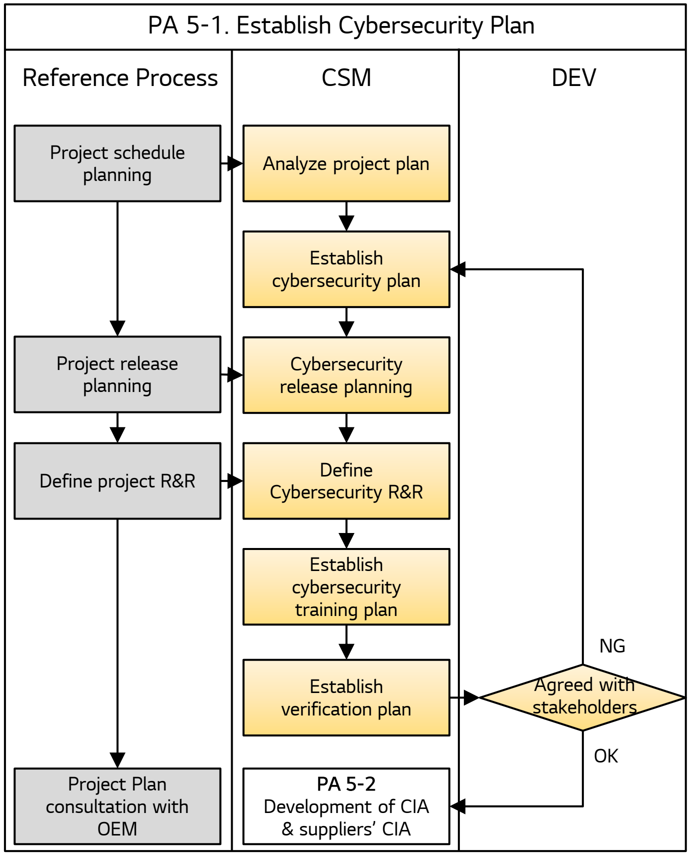
R : Responsibility , A : Approval, S : Support , I : Informed

5-1. Establish Cybersecurity Plan

◆ **Cybersecurity Manager sets a cybersecurity activity plan in consideration of the project development plan**

Entry criteria Project plan for item development should be obtained from the OEM.

Procedure



PA 5-1. Establish Cybersecurity Plan

Reference Process
CSM
DEV
Project schedule planning
Analyze project plan
Establish cybersecurity plan
Project release planning
Cybersecurity release planning
Define project R&R
Define Cybersecurity R&R
Establish cybersecurity training plan
Establish verification plan
NG
Agreed with stakeholders
OK
Project Plan consultation with OEM
PA 5-2 Development of CIA & suppliers' CIA

Detailed activity

Cybersecurity Manager sets a plan for performing cybersecurity activities based on the project development plan and agrees with cybersecurity officer of each area.

[Description in detail]

- CSM analyzes an item's project schedule to identify key milestones and feature release schedules.
- CSM tailors the cybersecurity process that is applied according to the project situation by referring to CSMS development criteria.
- CSM uses cybersecurity standard WBS to set detailed cybersecurity activity plan.
- CSM sets a cybersecurity release plan in conjunction with the project's key milestones.
- CSM defines the assignments and job roles to perform cybersecurity.
- CSM considers and applies reuse, component out of context and off-the-shelf component.
- CSM to perform reuse analysis by reviewing if the component to be reused is able to fulfill the cybersecurity requirements for the item or component and if existing documentation is sufficient to support integration of the component into an item or another component.
- CSM develops a plan to improve the capabilities of Developer(DEV).
- CSM sets verification plans and targets in consultation with System/HW/SW DEV.
- CSM agrees with stakeholders for the Cybersecurity Plan.

※ If necessary, cybersecurity plan could be modified during the project

Inputs

- Project Plan

Outputs

- Cybersecurity Plan

Related standard

- ISO/SAE 21434 - 6:v1.0

Exit criteria [Cybersecurity Manager] Cybersecurity plan should be agreed with stakeholders.

M If you do not perform any mandatory process, you should have a reasonable rationale.

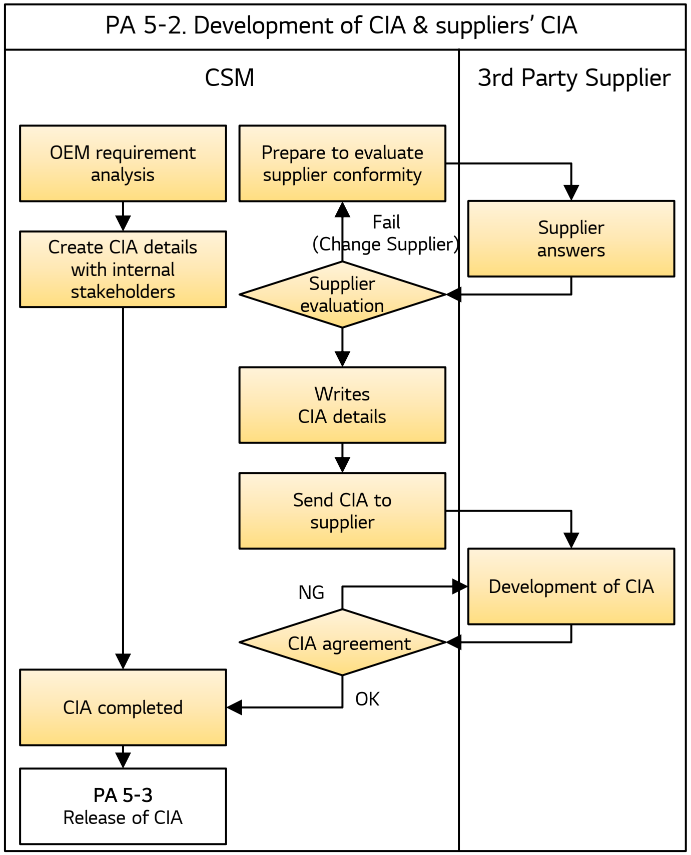
5-2. Development of CIA & suppliers' CIA

◆ **The Cybersecurity Manager writes for the CIA & suppliers' CIA required by the OEM.**

Entry criteria

1. The project development schedule has been agreed and the person responsible for the cybersecurity should be confirmed.
2. Selection of supplier should be completed.

Procedure



Detailed activity

Cybersecurity Manager(CSM) creates a cybersecurity activity plan for the CIA & suppliers' CIA required by the OEM.
CSM sends the requirements for the cybersecurity activities that should be performed by the supplier and create the CIA with the supplier's agreement.

[Description in detail]

※ Based on the use of the CIA template provided by the OEM, and if not supplied by the OEM, use the VS standard CIA template.

- CSM judges whether or not to carry out the items requested by OEM among CIA contents.
- CSM analyzes any missing items in the CIA and add missing items.
- CSM analyzes the CIA details and describe the action plan. (Whether to perform, completion date, person in charge, submittal of work product, method of delivery work product)
- CSM agrees with the internal stakeholders to ensure that the activity plan written in the CIA can be performed.
- CSM prepares checklists and questionnaires to assess the level of cybersecurity of selected supplier.
- The supplier provides answers to questions asked by CSM.
- CSM requests the Audit team to conduct an audit if the self-assessment result of the Supplier Evaluation Checklist is Fail.
- CSM obtains a remedial action plan for the insufficient areas from the supplier and encourages improvement. If the supplier fails to implement the remedial actions, the project's PL and contract team will be notified.
- CSM fills in the CIA details for the cybersecurity activities to be performed by the supplier.
- CSM sends the CIA document to the supplier.
- The supplier should modify the CIA and send it to LGE.
- CSM agrees on CIA with the supplier.

Inputs

- CIA template
- Supplier evaluation checklist
- Project plan

Outputs

- CIA
- Supplier_Evaluation_Checklist

Related standard

- ISO/SAE 21434 - 7:v1.0

Exit criteria [Cybersecurity Manager] The completed CIA document should be agreed by the internal stakeholders.

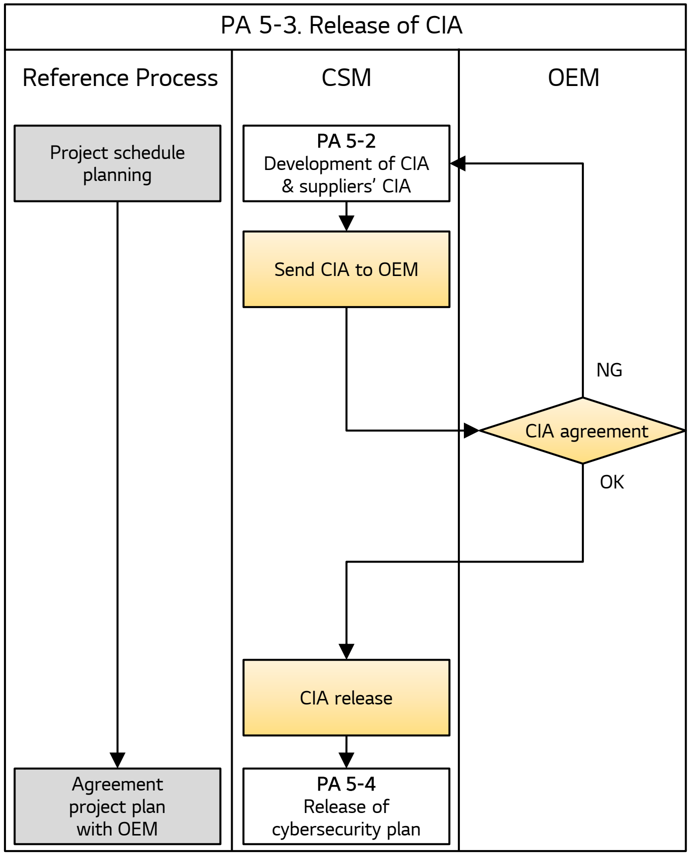
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-3. Release of CIA

◆ **The Cybersecurity Manager agrees on the CIA with the OEM.**

Entry criteria The CIA details should be agreed with the internal stake holders.

Procedure


PA 5-3. Release of CIA

Reference Process | CSM | OEM

Project schedule planning

PA 5-2 Development of CIA & suppliers' CIA

Send CIA to OEM

CIA agreement

NG

OK

CIA release

Agreement project plan with OEM

PA 5-4 Release of cybersecurity plan

Detailed activity

Cybersecurity Manager(CSM) reaches consensus on the details of the CIA with OEM and confirms the CIA

[Description in detail]

- CSM sends the created CIA document to OEM.
- CSM agrees on the CIA with OEM.
  ※ Offline workshop or online review based on OEM request
- CSM receives agreed CIA documents from OEM.
  ※ After CIA agreement, evidence of agreement should be kept.
  (Signed CIA document, agreed email notification, etc.)
- CSM releases the agreed CIA document to the document management system.

Inputs

- CIA

Outputs

- CIA [confirmed]

Related standard

- ISO/SAE 21434 - 7:v1.0

Exit criteria [Cybersecurity Manager] The Cybersecurity Manager should release the CIA document agreed with the OEM to the document management system.

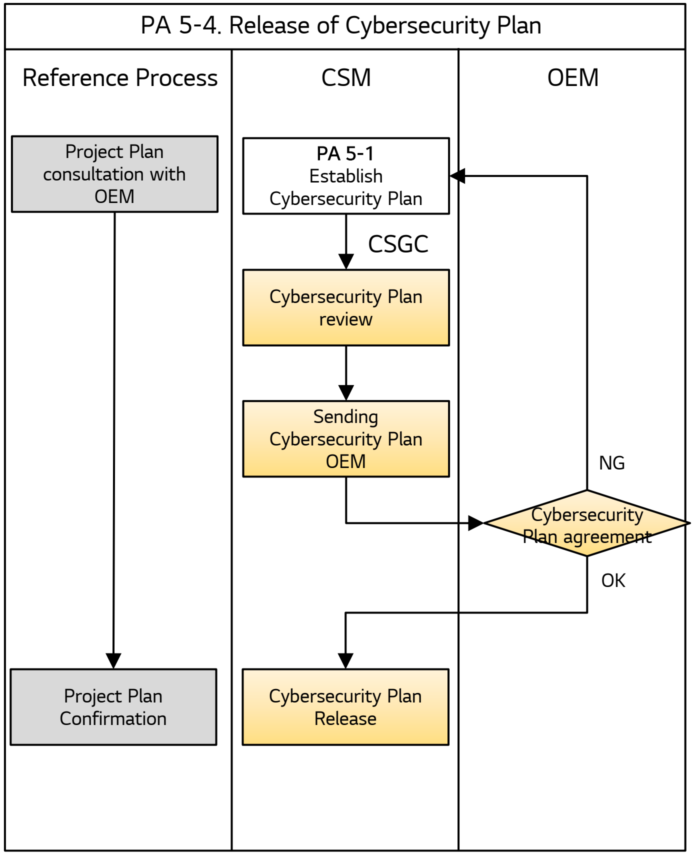
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-4. Release of Cybersecurity Plan

◆ Cybersecurity Manager agrees a Cybersecurity Plan with OEM

Entry criteria Cybersecurity Plan should be agreed with stakeholders.

Procedure


PA 5-4. Release of Cybersecurity Plan
Reference Process
CSM
OEM
Project Plan consultation with OEM
PA 5-1 Establish Cybersecurity Plan
CSGC
Cybersecurity Plan review
Sending Cybersecurity Plan OEM
NG
Cybersecurity Plan agreement
OK
Project Plan Confirmation
Cybersecurity Plan Release

Detailed activity

Cybersecurity Manager confirms by sending the Cybersecurity Plan to the OEM.

[Description in detail]

- CSGC reviews the detailed activity plan in the Cybersecurity Plan.
- CSGC reviews whether CIA's plans agreed with OEMs are reflected in the Cybersecurity Plan.
- CSM sends Cybersecurity Plan document with detailed activity plan to OEM
- CSM agrees on Cybersecurity Plan with OEM.
- CSM releases the agreed Cybersecurity Plan to the document management system.

※ Cybersecurity Plan documents can be integrated into Project Master Plan and managed as a single document.

Inputs

- Cybersecurity Plan

Outputs

- Cybersecurity Plan [Confirmation]

Related standard

- ISO/SAE 21434 - 6:v1.0

Exit criteria [Cybersecurity Manager] The Cybersecurity Plan document agreed with the OEM must be released to the document management system.

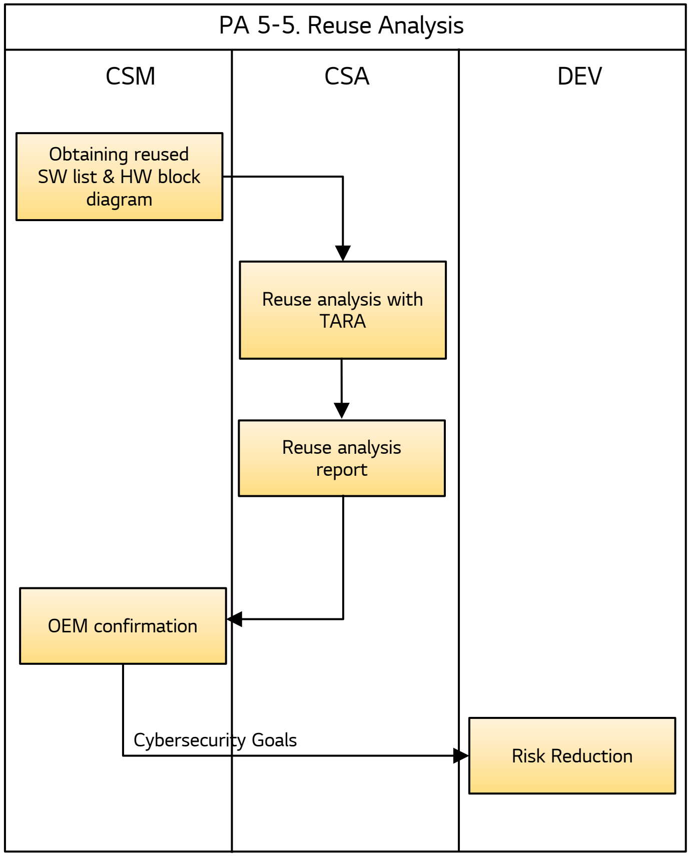
M If you do not perform any mandatory process, you should have a reasonable rationale.

5. Reuse Analysis

◆ CSA (Cybersecurity Architect) identifies vulnerabilities on reused SW

Entry criteria Identification of reused SW and obtaining HW block diagram should be complete.

Procedure



Detailed activity

CSA perform reuse analysis

[Description in detail]

- CSM obtain SW feature list, reused SW list and HW block diagram
- CSA perform reuse analysis for reused SW including TARA
- CSM communicate with OEM to confirm reuse analysis
- CSM identify the modifications to the item or component and the modifications of its operational environment;
- CSM analyze the cybersecurity implications of the modifications, including the effects on the validity of cybersecurity claims and previously made assumptions;
- CSM specify the cybersecurity activities necessary to conform with this document in the cybersecurity plan
- CSM identify the affected or missing work products
- CSA release reuse analysis report
- DEV perform risk reduction for vulnerabilities by applying requirements to design

Inputs

- Reused SW List
- Feature List
- HW Block Diagram
- Product Specification

Outputs

- Reuse Analysis Report
- Risk reduction activity

Related standard

- ISO/SAE 21434 - 6:v1.0
- IATF 16949
- ISO 9001
- ISO 26262

Exit criteria Reuse analysis for reused SW shall be performed.
Risk reduction on vulnerabilities (Cybersecurity goals) shall be complete.

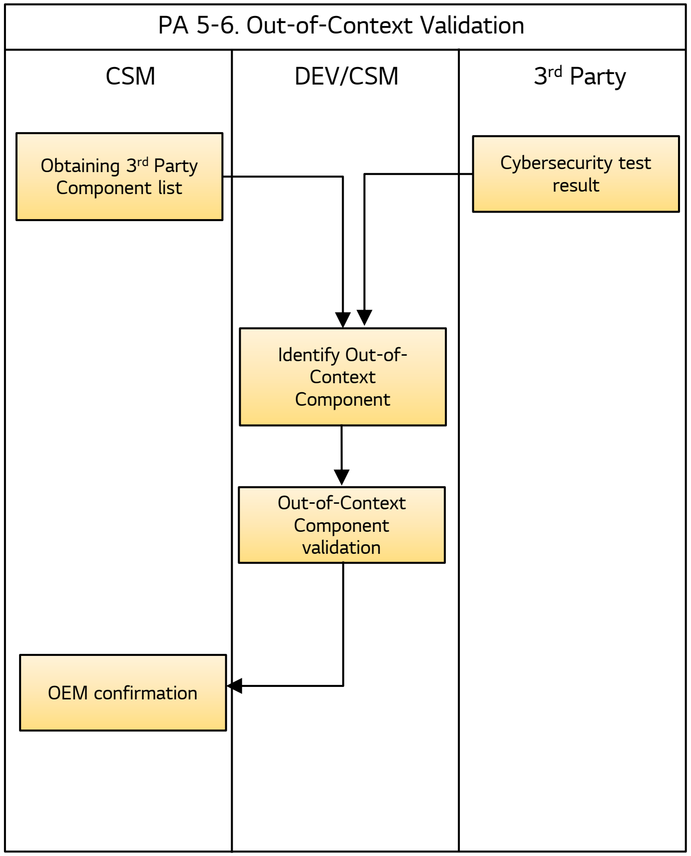
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-6. Out-of-Context Component Validation

◆ DEV/CSM identifies vulnerabilities on Out-of-Context Component

Entry criteria Identification of Out-of-Context Component and obtaining 3rd Party Component list should be complete.

Procedure


PA 5-6. Out-of-Context Validation
CSM
DEV/CSM
3rd Party
Obtaining 3rd Party Component list
Cybersecurity test result
Identify Out-of-Context Component
Out-of-Context Component validation
OEM confirmation

Detailed activity

DEV/CSM perform Out-of-Context validation including cybersecurity test results from 3rd party

[Description in detail]

- DEV/CSM obtain 3rd Party Component list
- DEV/CSM obtain Cybersecurity test result from 3rd party
- DEV/CSM identify Out-of-Context Component
- DEV/CSM Identify the assumptions on the intended use and context, including the external interfaces, shall be documented in the corresponding work products.
- DEV/CSM perform Out-of-Context validation including cybersecurity test result from 3rd party.
- CSM communicate with OEM to confirm Out-of-Context analysis

Inputs

- 3rd Party Component list
- Cybersecurity test result from 3rd party

Outputs

- Out-of-Context Validation Report

Related standard

- ISO/SAE 21434 - 6:v1.0
- IATF 16949
- ISO 9001
- ISO 26262

Exit criteria Out-of-Context validation shall be performed.
Request test results for vulnerabilities to 3rd party

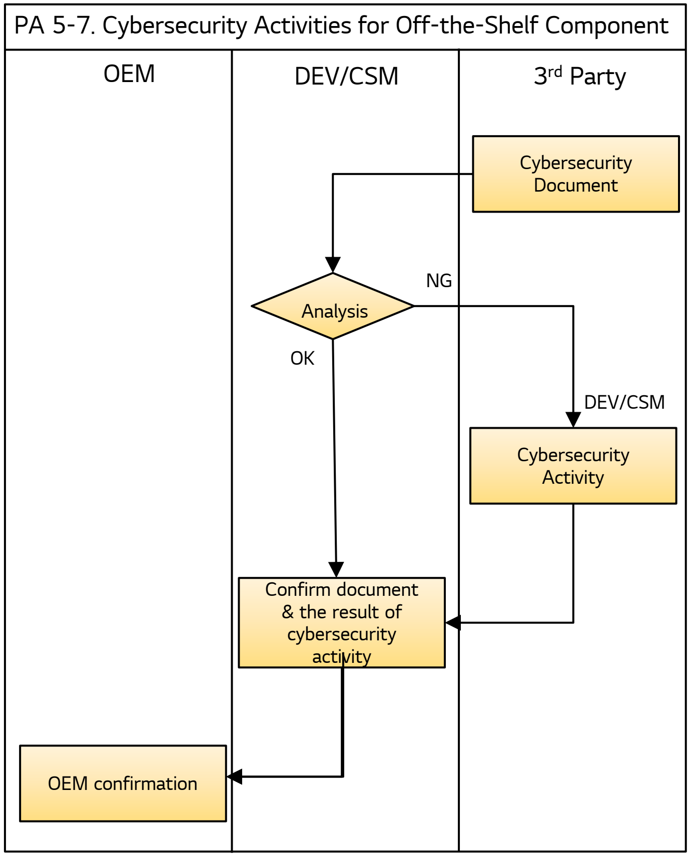
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-7. Cybersecurity Activities for Off-the-Shelf Component

◆ DEV/CSM identifies vulnerabilities on Off-the-Shelf Component

Entry criteria Identification of Off-the-Shelf Component and obtaining 3rd Party's Document should be complete.

Procedure



PA 5-7. Cybersecurity Activities for Off-the-Shelf Component

Detailed activity

DEV/CSM perform Off-the-Shelf validation including cybersecurity relevant document from 3rd party

[Description in detail]

- DEV/CSM obtain cybersecurity relevant document and analysis to determine necessary cybersecurity activity
- Analyze the Cybersecurity relevant document shall determine
  a) allocated cybersecurity requirements can be fulfilled
  b) the component is suitable for the specific application context of the intended use; and
  c) existing documentation is sufficient to support the cybersecurity activities.
- 3rd Party performs cybersecurity activity
- If necessary, DEV/CSM identify and performs cybersecurity activities to conform with the document.
- CSM communicate with OEM to confirm Off-the-Shelf validation

Inputs

- 3rd Party Cybersecurity document
- Cybersecurity Activity

Outputs

- 3rd Party Cybersecurity document

Related standard

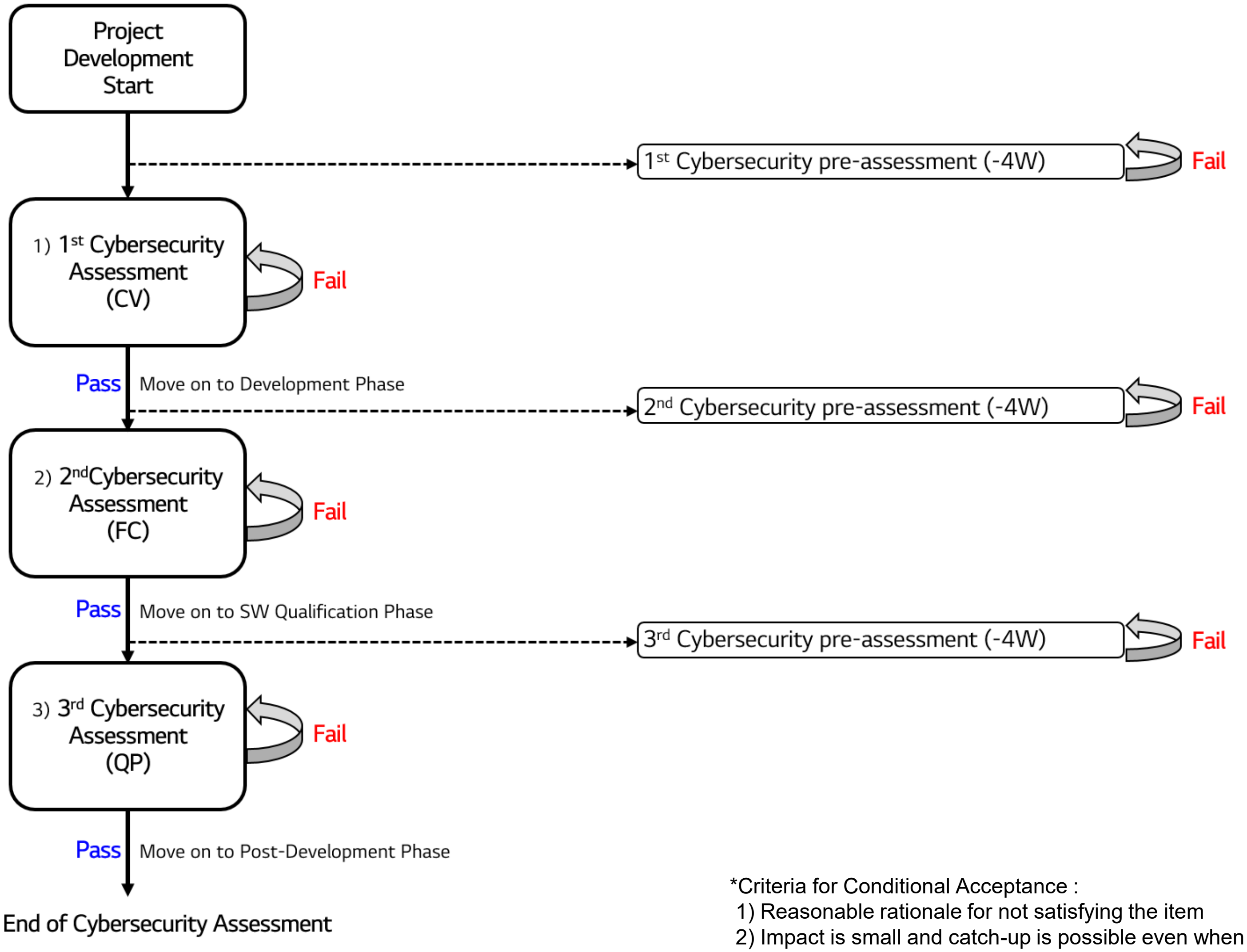
- ISO/SAE 21434 - 6:v1.0
- IATF 16949
- ISO 9001
- ISO 26262

Exit criteria Activity for Off-the-Shelf component shall be performed.
Request test results for vulnerabilities to 3rd party

M If you do not perform any mandatory process, you should have a reasonable rationale.

5-8. Cybersecurity Assessment (1/3)

◆ Summary of Cybersecurity Assessment Process



Project Development Start
1st Cybersecurity pre-assessment (-4W)
Fail
1) 1st Cybersecurity Assessment (CV)
Fail
Pass
Move on to Development Phase
2nd Cybersecurity pre-assessment (-4W)
Fail
2) 2ndCybersecurity Assessment (FC)
Fail
Pass
Move on to SW Qualification Phase
3rd Cybersecurity pre-assessment (-4W)
Fail
3) 3rd Cybersecurity Assessment (QP)
Fail
Pass
Move on to Post-Development Phase
End of Cybersecurity Assessment

*Criteria for Conditional Acceptance :
1) Reasonable rationale for not satisfying the item
2) Impact is small and catch-up is possible even when it goes with current state
3) Additional assessment shall be performed before the next assessment

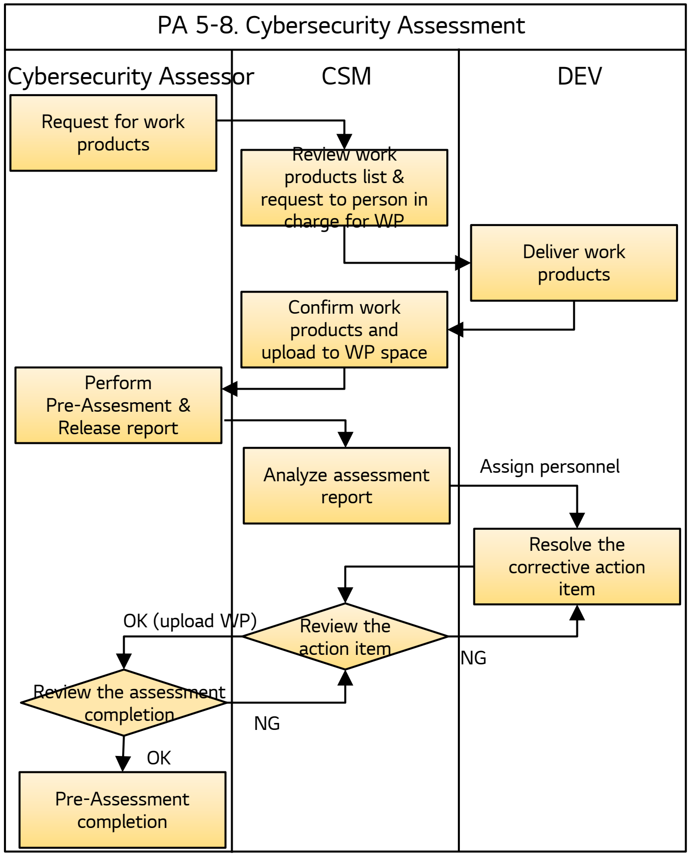
* The cybersecurity Internal audit department conducts regular cybersecurity audits to determine the organization's level of compliance with the CSMS.

5-8. Cybersecurity Assessment (2/3)

◆ The Cybersecurity Assessor perform Pre-Assessment 4 weeks before (official) assessment

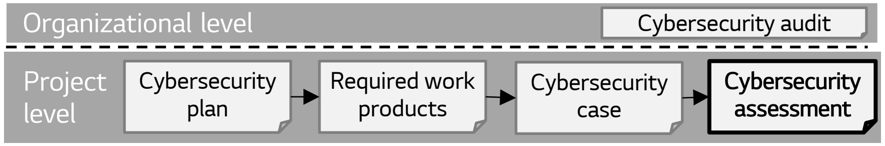
Entry criteria Pre-Assessment schedule should be planned.

Procedure


PA 5-8. Cybersecurity Assessment
Cybersecurity Assessor
CSM
DEV
Request for work products
Review work products list & request to person in charge for WP
Deliver work products
Confirm work products and upload to WP space
Perform Pre-Assessment & Release report
Analyze assessment report
Assign personnel
Resolve the corrective action item
Review the action item
OK (upload WP)
NG
Review the assessment completion
NG
OK
Pre-Assessment completion

Detailed activity

The cybersecurity assessment is performed at a project level as below.



[Description in detail]

- Assessor request work products for Pre-Assessment to CSM
- CSM gather work products from DEV and upload to WP space
- CSM notify and request Pre-Assessment to Assessor
- Assessor perform Pre-Assessment and release report to CSM
- CSM assign fail item to personnel
- DEV resolve fail item
- CSM review work product to confirm whether issues are fixed
- If there is no issue, CSM request to assessor for Pre-Assessment
- if issues are cleared, Assessor announce official assessment as planned.

*** The Cybersecurity Governance Unit independently performs the cybersecurity assessment.**
- Work product evaluation according to cybersecurity activity
***All work products shall be prepared for assessor to perform pre-assessment 4 weeks before (official) assessment**
***CSMS Assessment Guide :**
http://collab.lge.com/main/display/VCSWINFO/%5B5.7%5D+CSMS+Assessment

Inputs

- Project Plan
- Cybersecurity Plan
- Required work products

Outputs

- Pre-Assessment Report

Related standard

- ISO/SAE 21434 - 6:v1.0
- IATF 16949
- ISO 9001
- ISO 26262

Exit criteria After result of pre-assessment is acceptance, then official assessment can be performed as planned schedule.

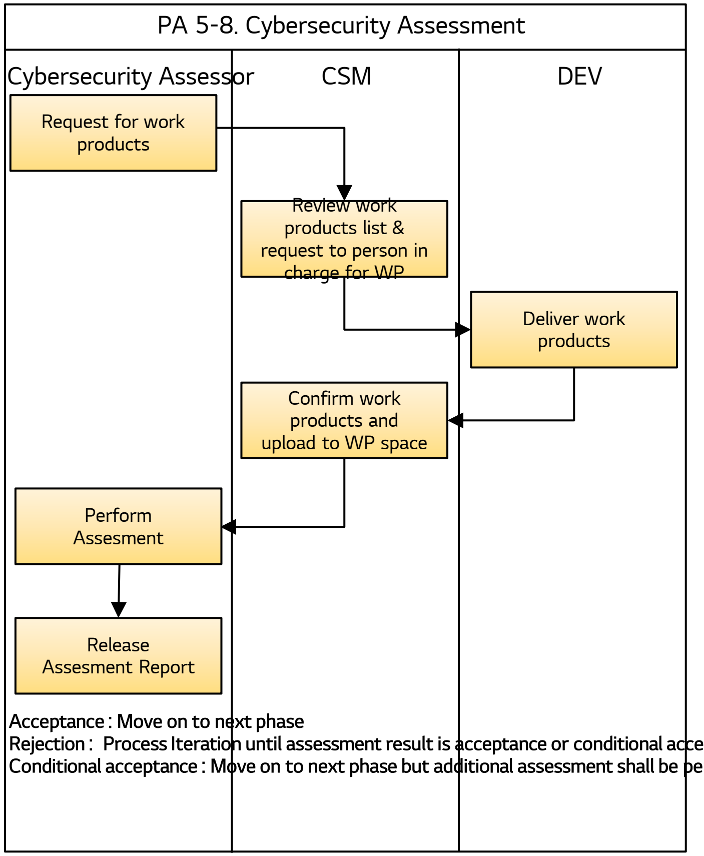
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-8. Cybersecurity Assessment (3/3)

◆ The Cybersecurity Assessor perform Assessment

Entry criteria Pre-Assessment is complete

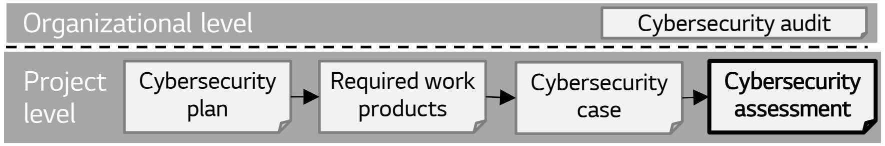
Procedure


PA 5-8. Cybersecurity Assessment
Cybersecurity Assessor
CSM
DEV
Request for work products
Review work products list & request to person in charge for WP
Deliver work products
Confirm work products and upload to WP space
Perform Assesment
Release Assesment Report

Acceptance : Move on to next phase
Rejection : Process Iteration until assessment result is acceptance or conditional acceptance
Conditional acceptance : Move on to next phase but additional assessment shall be performed before next assessment

Detailed activity

The cybersecurity assessment is performed at a project level as below.



[Description in detail]

- Assessor request work products for Pre-Assessment to CSM
- CSM gather work products from DEV and upload to WP space
- CSM notify and request assessment to Assessor
- Assessor perform assessment and release report
- If assessment result is acceptance, move on to next development phase
- If assessment result is rejection, iterate PA 5-9
- If assessment result is conditional acceptance, move on to next development phase but additional assessment shall be performed before next assessment

Inputs

- Required work products

Outputs

- Assessment Report

Related standard

- ISO/SAE 21434 - 6:v1.0
- IATF 16949
- ISO 9001
- ISO 26262

Exit criteria Move on to next phase if assessment result is (conditional) acceptance

M If you do not perform any mandatory process, you should have a reasonable rationale.

LGE Internal Use Only

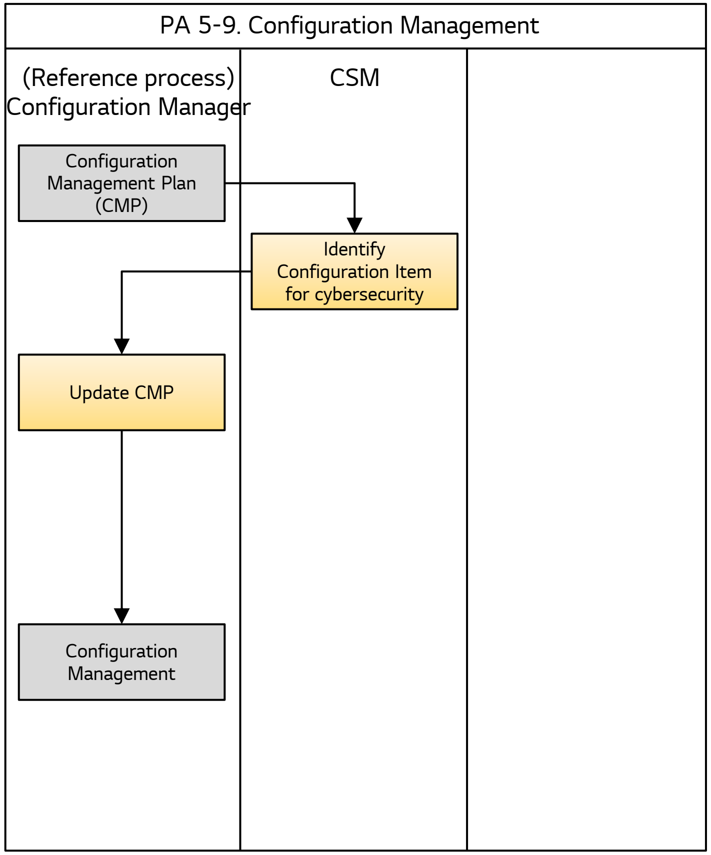
5-9. Configuration Management

Cybersecurity Management & Supporting

◆ **Cybersecurity Manager(CSM) identifies the CI (Configuration Item) and manages it in compliance with the configuration management plan.**

Entry criteria Configuration Management Plan that is should be completed.

Procedure



PA 5-9. Configuration Management

(Reference process) Configuration Manager

CSM

Configuration Management Plan (CMP)

Identify Configuration Item for cybersecurity

Update CMP

Configuration Management

Detailed activity

※ The general process of the configuration should be in compliance with the Smart Division SW Process except to identify the CI of Cybersecurity.
※ If the cybersecurity Cis are merged and managed with the general SW development work product, it can be managed with the SW process after describing it in the configuration management plan.

CSM identifies the cybersecurity CI(work-product) and informs it to the configuration manager. CSM should perform the development in compliance with the configuration management.

[Description in detail].

- If there is CI related to cybersecurity , CSM identifies the items that need to manage with version or baseline.
- CSM notifies the items to the configuration manager and requests to add the configuration item.

[Cybersecurity Configuration Item]

- (Cybersecurity) System/SW Requirements
- (Cybersecurity) System/SW Architectural Designs
- (Cybersecurity) SW Detailed Design
- (Cybersecurity) Plan
- Test Cases, Test/Verification Reports
- SW Code, Binary
- Cybersecurity cases, and etc.

※ The general configuration management should perform with the guide and template of “[1.1] Smart Division SW Development Standard Process” (URL: http://collab.lge.com/main/x/IgDkLw)

Inputs

- Configuration Management Plan

Outputs

- Configuration Item
- Configuration Management Book
- Configuration Management Plan [refined]

Related standard

- ISO/SAE 21434 - 5:v1.0
- Smart Division SW Development Standard Process Regulation 2-18

Exit criteria [CSM] CSM identifies the cybersecurity CI(work-product) and informs it to the configuration manager.

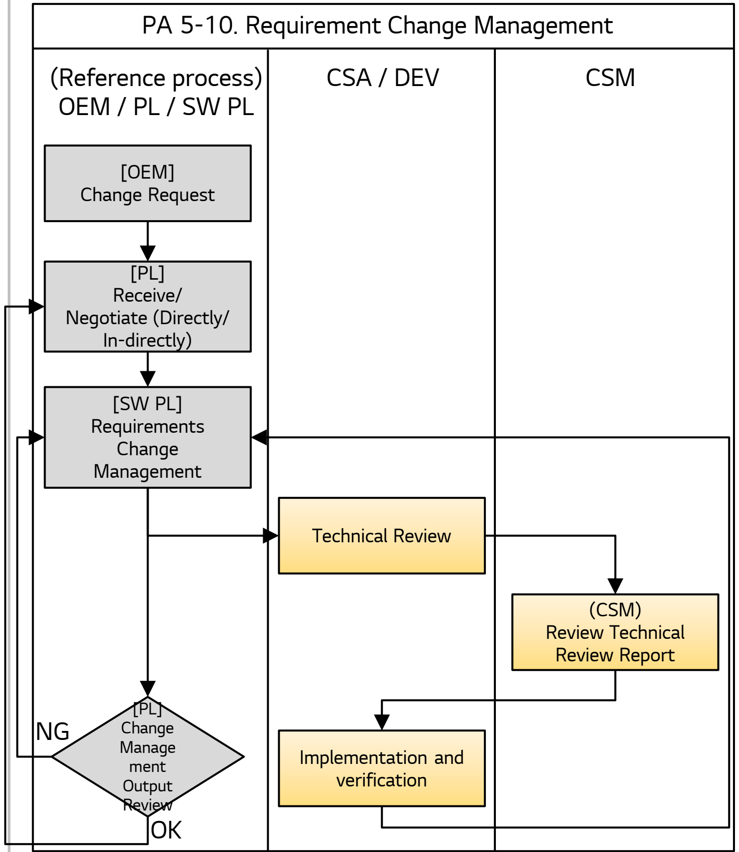
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-10. Requirement Change Management

◆ **Cybersecurity Architect(CSA) and Developer perform the technical review impact analysis and implementation after receiving the CR agreed with OEM from SW PL.**

Entry criteria Change Manager obtains a Change Request(CR) for the change that has occurred. (CR Acquisition path is unified with PM)

Procedure



PA 5-10. Requirement Change Management

(Reference process) OEM / PL / SW PL | CSA / DEV | CSM

[OEM] Change Request

[PL] Receive/ Negotiate (Directly/ In-directly)

[SW PL] Requirements Change Management

Technical Review

(CSM) Review Technical Review Report

Implementation and verification

[PL] Change Manage ment Output Review

NG

OK

Detailed activity

※ CSMS standard only describes the activity related to the cybersecurity activities.
In the case of general change management, see the Smart Division SW Development Process Regulation.

Cybersecurity Architect(CSA) and Developer(DEV) **perform the impact analysis and implementation after receiving the CR from SW PL.**

[Description in detail]

- CSA and DEV perform the technical review, if it needed, it can be performed with SW Architect(or Function Owner).
- CSM reviews the result of technical review report.
- DEV develops and implements the change in requirements, design, code, and verification.
- CSA and DEV notify the completion to SW PL after implementation of the change.

※ The general change management should perform with the guide and template of "[1.1] Smart Division SW Development Standard Process"
(URL: http://collab.lge.com/main/x/IgDkLw)

Inputs

- Cybersecurity CR

Outputs

- Technical Review report
- Cybersecurity Requirements and Design [refined]
- Verification Result

Related standard

- ISO/SAE 21434 - 5:v1.0
- Smart Division SW Development Standard Process Regulation 2-21

Exit criteria [SW/System Qualification Test manager] Executes full test by referring to 'CR development and verification result' and registers completion of implementation including test result in CR Management System.
[PL] For the CR of which implementation is done, PL should see if the related work product is updated. Then, the baseline is re-defined.

M If you do not perform any mandatory process, you should have a reasonable rationale.

LGE Internal Use Only

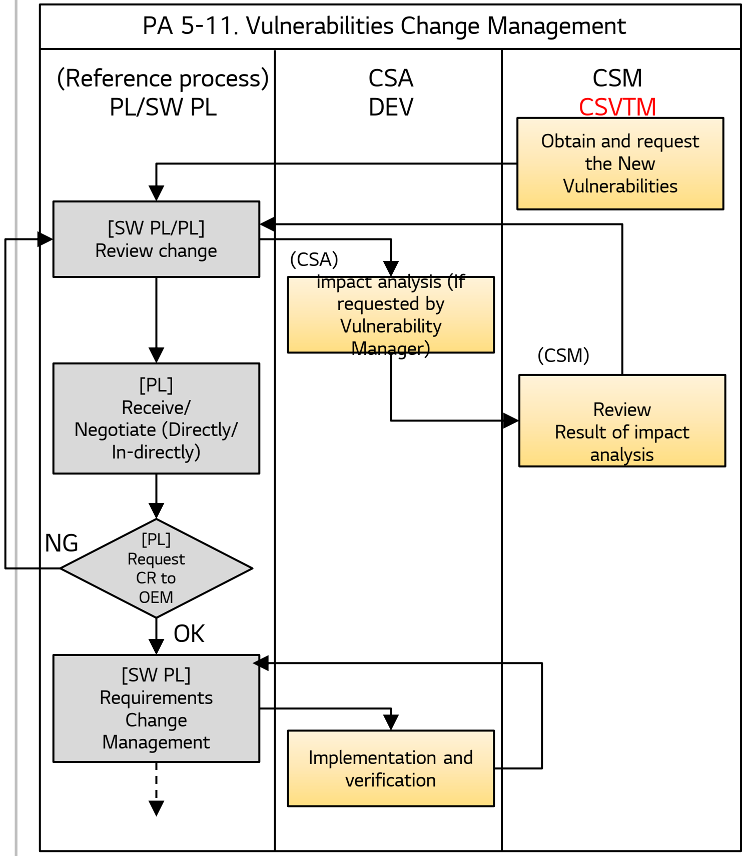
5-11. Vulnerabilities Change Management

Cybersecurity Management & Supporting

◆ Cybersecurity Architect(CSA) perform the impact analysis and CSA and DEV do implementation after receiving the CR related to new vulnerabilities agreed with OEM from SW PL.

Entry criteria CSM obtains the new vulnerabilities from the Incident Response manager.

Procedure



PA 5-11. Vulnerabilities Change Management

(Reference process) PL/SW PL

CSA DEV

CSM CSVTM

Obtain and request the New Vulnerabilities

[SW PL/PL] Review change

(CSA) Impact analysis (If requested by Vulnerability Manager)

(CSM) Review Result of impact analysis

[PL] Receive/ Negotiate (Directly/ In-directly)

[PL] Request CR to OEM

NG

OK

[SW PL] Requirements Change Management

Implementation and verification

Detailed activity

※ **CSMS standard only describes the activity related to the cybersecurity activities.**
In the case of general change management, see the Smart Division SW Development Process Regulation.

CSM obtains the new vulnerabilities from the internal or external CSVTM.
SW PL and PM officially request the new CR related to the new vulnerability to OEM.
SW PL requests the implementation of CR to Cybersecurity Architect(CSA) and Developer(DEV) **after receiving the CR agreed with OEM.**
CSA and DEV **perform the impact analysis and implementation of the CR.**

[Description in detail]

- CSA performs the impact analysis when CSVTM request impact analysis about new vulnerabilities, if it needed, it can be performed with SW Architect(or Function Owner).
- CSM reviews the result of impact analysis.
- DEV develops and implements the change in requirements, design, code, and verification.
- DEV notify the completion to SW PL after implementation of the change.

※ The general change management should perform with the guide and template of "[1.1] Smart Division SW Development Standard Process"
(URL: http://collab.lge.com/main/x/IgDkLw)

Inputs

- New Vulnerabilities

Outputs

- CR
- Impact Analysis Report
- Cybersecurity Requirements and Design [refined]
- Verification Result

Related standard

- ISO/SAE 21434 - 5:v1.0
- Smart Division SW Development Standard Process Regulation 2-21

Exit criteria [SW/System Qualification Test manager] Executes full test by referring to 'CR development and verification result' and registers completion of implementation including test result in CR Management System.
[PL] For the CR of which implementation is done, PM should see if the related work product is updated. Then, the baseline is re-defined.

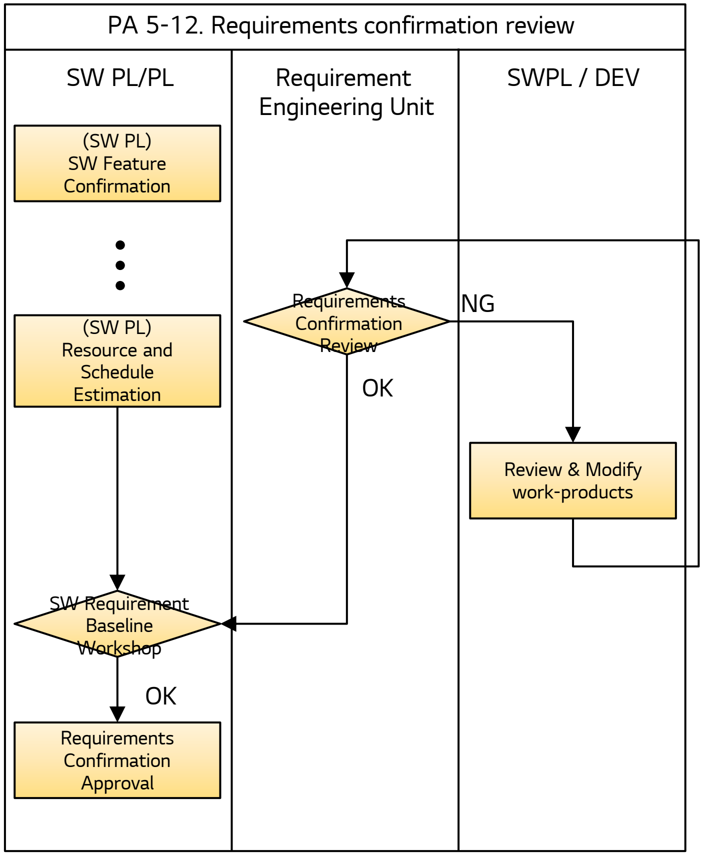
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-12. Requirements confirmation review

◆ SW PL holds the SW Requirement Baseline Workshop and confirms the first baseline agreed with customer.

Entry criteria Project plan for item development should be obtained from the OEM.

Procedure


PA 5-12. Requirements confirmation review

SW PL/PL

Requirement Engineering Unit

SWPL / DEV

(SW PL)
SW Feature Confirmation

(SW PL)
Resource and Schedule Estimation

Requirements Confirmation Review

NG

OK

Review & Modify work-products

SW Requirement Baseline Workshop

OK

Requirements Confirmation Approval

Detailed activity

SW PL holds the SW Requirement Baseline Workshop in compliance with Smart Division SW Development Standard Process.

REU performs the SW requirements confirmation review before the SW Requirement Baseline Workshop.

[Description in detail]

- Establish a baseline of requirements after agreeing on cybersecurity system requirements with PM/PL.
- If issues need to check again during the Requirement Confirmation Review, Requirement Engineering Unit requests SW PL and Developer(DEV) to check and modify work-products.
- Submit the Requirements Confirmation Review Report to SW PL.
- If it has unconfirmed features, it should be included detailed reasons and resolution in the result of the Requirements Confirmation Review.

[Requirements confirmation review criteria]

- TARA result
- Confirmed rate of Cybersecurity requirements
- Cybersecurity Plan

※ The Requirements Confirmation Approval should perform in compliance with "[1.1] Smart Division SW Development Standard Process"
(URL: http://collab.lge.com/main/x/rJjjGw)

Inputs

- System cybersecurity requirements

Outputs

- Requirements confirmation review report

Related standard

- Smart Division SW Development Standard Process Regulation 1-6

Exit criteria [SW PL] Review criteria of Requirement confirmation and share the result to related persons.
[PL] Approve the Requirement confirmation

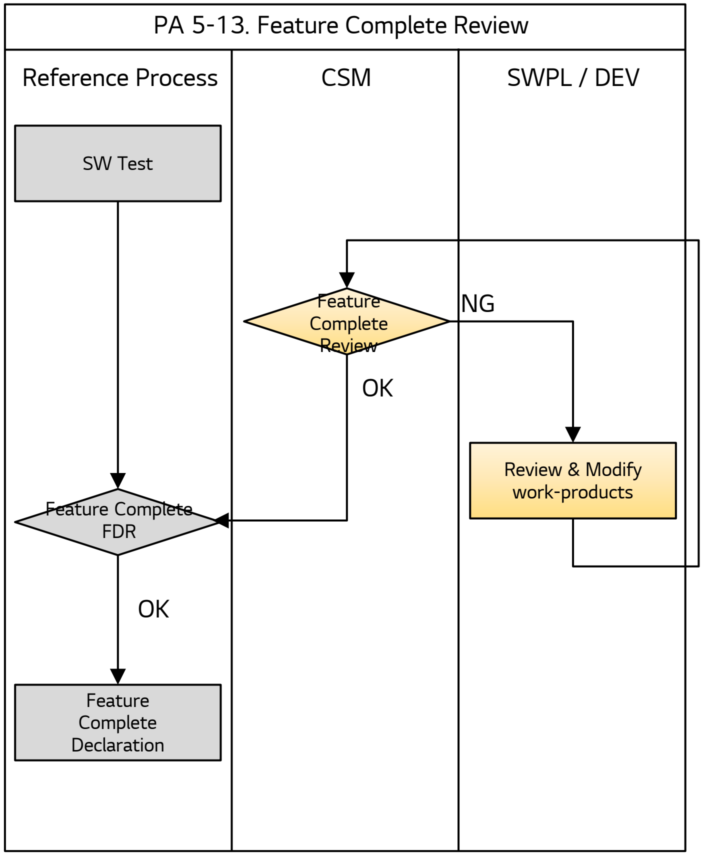
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-13. Feature Complete Review

◆ SW PL holds the Feature Complete Declaration meeting and declares the Feature Complete after reviewing work-products with stakeholders.

Entry criteria Project plan for item development should be obtained from the OEM.

Procedure


PA 5-13. Feature Complete Review
Reference Process
CSM
SWPL / DEV
SW Test
Feature Complete Review
NG
OK
Review & Modify work-products
Feature Complete FDR
OK
Feature Complete Declaration

Detailed activity

SW PL holds the Feature Complete Declaration in compliance with Smart Division SW Development Standard Process.

CSM performs the feature complete review before the Feature Complete Declaration.

[Description in detail]

- Check criteria of Feature Complete related to cybersecurity.
- If issues need to check again during the Feature Complete Review, CSM requests SW PL and Developer(DEV) to check and modify work-products.
- Submit the Feature Complete Review Report to SW PL.
- If it has unconfirmed features, it should be included detailed reasons and resolution in the result of the Requirements Confirmation Review.

[Feature complete review criteria]

- Cybersecurity requirements deployment consistency
- Review missing Cybersecurity design, conformity
- Conduct System/SW security analysis
- Completion of System/SW test specification
- Open Source Software Vulnerability Scanning result

※ The Feature Complete Declaration should perform in compliance with “[1.1] Smart Division SW Development Standard Process”
(URL: http://collab.lge.com/main/x/rJjjGw)

Inputs

- Project Plan

Outputs

- Feature Complete Review Report

Related standard

- Smart Division SW Development Standard Process Regulation 2-15

Exit criteria [SW PL] Perform the review meeting with related persons for checking the feature complete in compliance with the criteria.
Declare the Feature Complete after checking the criteria.

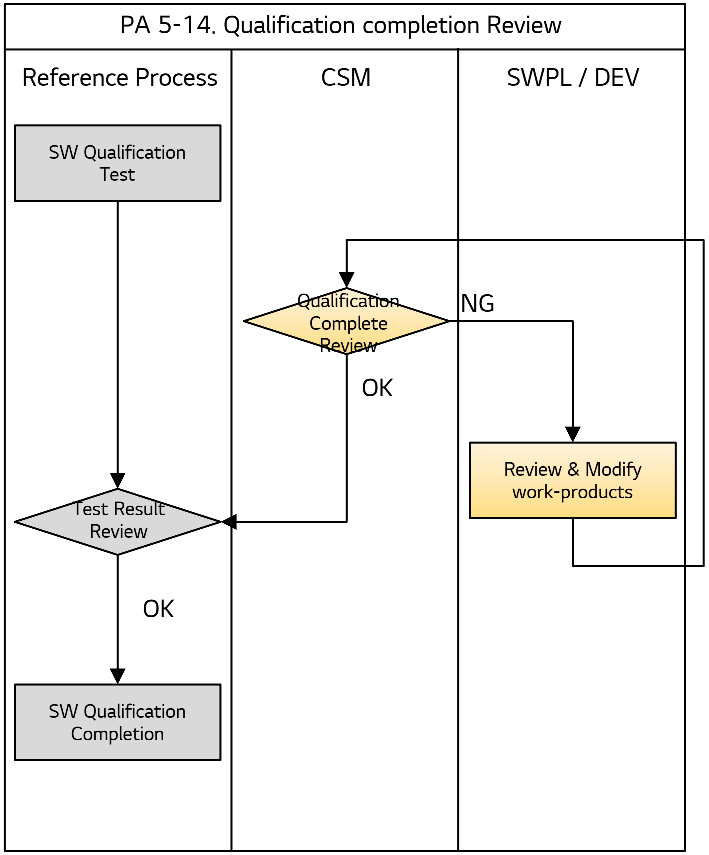
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-14. Qualification completion Review

◆ The Cybersecurity Assessor establishes the assessment plan and performs the assessment.

Entry criteria Project plan for item development should be obtained from the OEM.

Procedure


PA 5-14. Qualification completion Review
Reference Process
CSM
SWPL / DEV
SW Qualification Test
Qualification Complete Review
NG
OK
Review & Modify work-products
Test Result Review
OK
SW Qualification Completion

Detailed activity

DQA confirms the version for production or release after complete the SW Qualification test.

CSM performs the qualification complete review before the SW Qualification Completion.

[Description in detail]

- Check criteria of SW Qualification Completion related to cybersecurity.
- If issues need to check again during the Qualification Completion Review, CSM requests SW PL and Developer to check and modify work-products.
- Submit the Qualification Completion Review Report to SW PL and DQA.
- Review cybersecurity validation test results to ensure Cybersecurity requirements completeness and Cybersecurity Goals.

[Qualification completion Criteria]

- Production control plan
- Cybersecurity test defect Zero
- Post-development report
- PSC(Product Security Certification)
  - http://collab.lge.com/main/x/-pqHLw

※ The SW Qualification Completion should perform in compliance with "[1.1] Smart Division SW Development Standard Process"
(URL: http://collab.lge.com/main/x/rJjjGw)
※ When LGE performs the validation because of OEM's requests, all results of the validation are shall be included in the cybersecurity assessment report.

Inputs

- Project Plan
- Cybersecurity Assessment Report
- Post-development report

Outputs

- Qualification completion review report

Related standard

- Smart Division SW Development Standard Process Regulation 4-11

Exit criteria [DQA] Approval of the SW Qualification(NPI process) Test result by the DQA team leader.

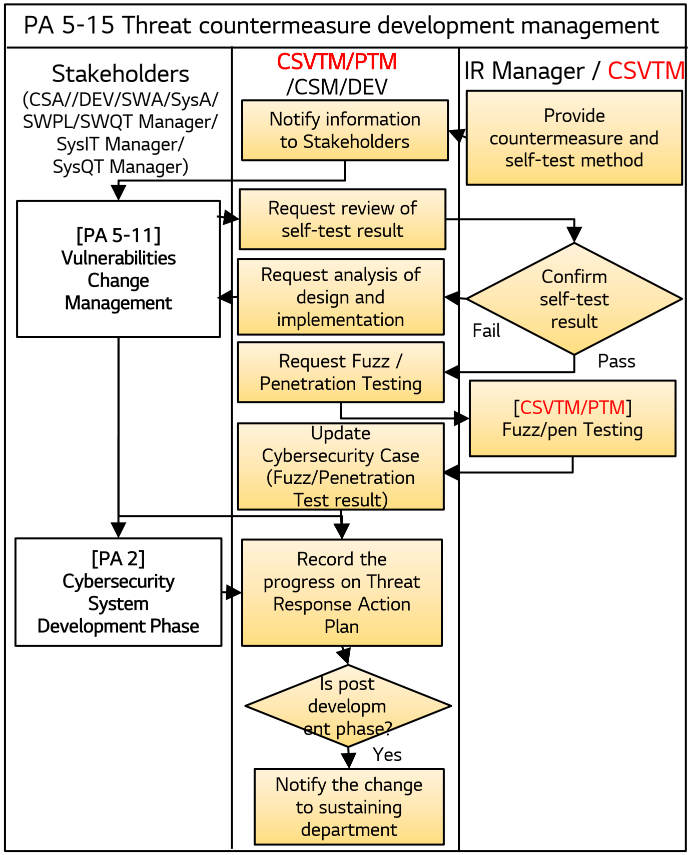
M If you do not perform any mandatory process, you should have a reasonable rationale.

5-15. Threat countermeasure development management

◆ CSVTM manages countermeasure development.

Entry criteria Threat response action plan shall be available.

Procedure


PA 5-15 Threat countermeasure development management
Stakeholders
(CSA//DEV/SWA/SysA/
SWPL/SWQT Manager/
SysIT Manager/
SysQT Manager)
CSVTM/PTM
/CSM/DEV
IR Manager / CSVTM
Notify information to Stakeholders
Provide countermeasure and self-test method
[PA 5-11] Vulnerabilities Change Management
Request review of self-test result
Request analysis of design and implementation
Confirm self-test result
Fail
Pass
Request Fuzz / Penetration Testing
[CSVTM/PTM] Fuzz/pen Testing
Update Cybersecurity Case (Fuzz/Penetration Test result)
[PA 2] Cybersecurity System Development Phase
Record the progress on Threat Response Action Plan
Is post developm ent phase?
Yes
Notify the change to sustaining department

Detailed activity

CSM manages countermeasure development.

[Description in detail]

- CSVTM provides countermeasure and self-test method.
- CSVTM notify information to Stakeholders and trigger PA 5-11 Vulnerabilities Change Management.
- When development is completed, Developer checks CSVTM's self-test method and then proceed with self-test.
- After completing the self-test, Developer request review for the self-test to Incident Response Manager.
- Once self-test result is failed, CSVTM requests review of design and implementation.
- Once self-test result is passed, CSVTM requests Fuzz Testing and PTM requests Penetration Testing for the relevant changes.
- CSM updates the Fuzz Test Result and Penetration Test Result on Cybersecurity Case.
- While PA 2 is proceed, CSVTM monitors and records the progress on Threat Response Action Plan.
- For the product in post development phase, CSVTM notify the change to sustaining department.

※ If discovered threat becomes available that invalidates the existing rationale, the vulnerability shall no longer be considered as managed.

Inputs

- Detail analysis report

Outputs

- Threat response action plan [refined]
- Cybersecurity Case [refined]

Related standard

- ISO/SAE 21434 - 8:v1.0

Exit criteria [CSVTM] Threat response action plan shall be refined.

M If you do not perform any mandatory process, you should have a reasonable rationale.

6 Continual Cybersecurity Activities including Production & Operation

- **Objective**

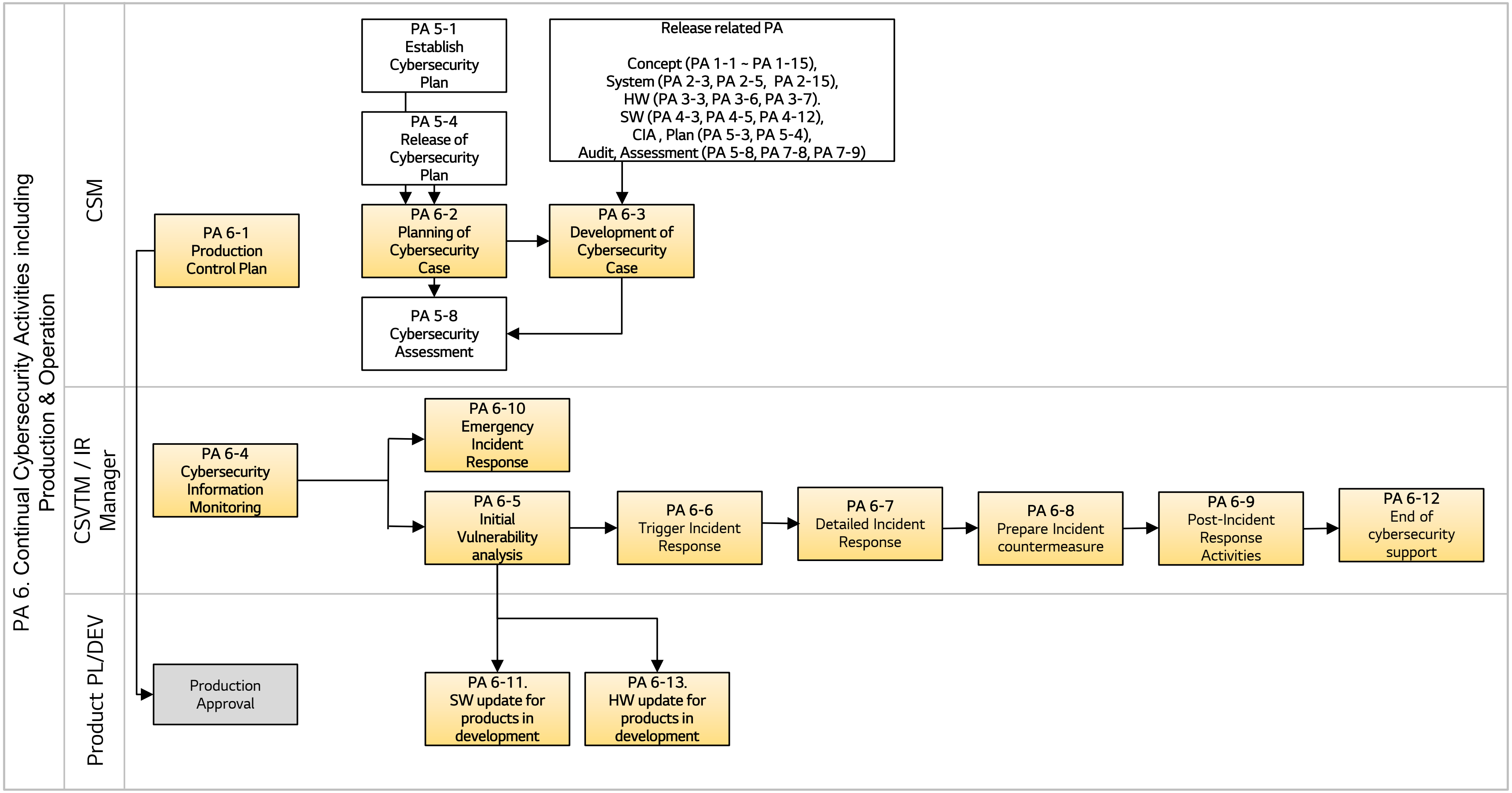
  Define Continual cybersecurity activities including production & operation phase for the items to which cybersecurity is applied among the E/E system developed by the VS company.

- **Scope**

  It is applied when developing the item to apply cybersecurity among electrical and electronic system (E / E system) developed by VS company.

6 Continual Cybersecurity Activities including Production & Operation

Define the necessary activities when LGE response the incident of vehicle product, whether complete development or not


PA 6. Continual Cybersecurity Activities including Production & Operation
CSM
CSVTM / IR Manager
Product PL/DEV
PA 5-1 Establish Cybersecurity Plan
PA 5-4 Release of Cybersecurity Plan
Release related PA
Concept (PA 1-1 ~ PA 1-15),
System (PA 2-3, PA 2-5, PA 2-15),
HW (PA 3-3, PA 3-6, PA 3-7).
SW (PA 4-3, PA 4-5, PA 4-12),
CIA , Plan (PA 5-3, PA 5-4),
Audit, Assessment (PA 5-8, PA 7-8, PA 7-9)
PA 6-1 Production Control Plan
PA 6-2 Planning of Cybersecurity Case
PA 6-3 Development of Cybersecurity Case
PA 5-8 Cybersecurity Assessment
PA 6-4 Cybersecurity Information Monitoring
PA 6-10 Emergency Incident Response
PA 6-5 Initial Vulnerability analysis
PA 6-6 Trigger Incident Response
PA 6-7 Detailed Incident Response
PA 6-8 Prepare Incident countermeasure
PA 6-9 Post-Incident Response Activities
PA 6-12 End of cybersecurity support
Production Approval
PA 6-11. SW update for products in development
PA 6-13. HW update for products in development

6 Related ISO/SAE 21434 standard for Continual Cybersecurity Activities including Production & Operation

Option	Process Area	Description	Role	Work product	Related standard
M	PA 6-1. Production control plan	The production shall securely manage the physical environment and production tools and data to meet the cybersecurity requirements.	Production Manager	• Production plan[refined]	- ISO/SAE 21434-12:v1.0
M	PA 6-2. Planning of Cybersecurity Case	Cybersecurity Manager consult with the OEM on how to develop the cybersecurity case and on the level of content.	Cybersecurity Manager	• Cybersecurity plan [refined] • Cybersecurity case [initial] • WBS [refined]	- ISO/SAE 21434-6:v1.0
M	PA 6-3. Development of Cybersecurity Case	Cybersecurity Manager creates a Cybersecurity case using the outputs of each development phase..	Cybersecurity Manager	• Cybersecurity case [confirmed]	- ISO/SAE 21434-6:v1.0
M	PA 6-4. Cybersecurity Information Monitoring	Vulnerability manager monitor cybersecurity information that affects LGE product from internal / external sources.	CSVTM	• Cybersecurity information • Cybersecurity events	- ISO/SAE 21434-7:v1.0
M	PA 6-5 Initial Vulnerability Analysis	Vulnerability manager analyzes threat and related vulnerabilities and determines the product scope the vulnerability is related to	CSVTM	• Initial threat analysis report • Affected product list	- ISO/SAE 21434-13:v1.0
M	PA 6-6 Triggers Incident Response	Incident Response Manager review initial analysis report and shares the report with related stakeholders	Incident Response Manager	• OEM (Governance, Project) contact point • Products list that affected by threat	- ISO/SAE 21434-13:v1.0
M	PA 6-7 Detailed incident analysis	Incident Response managers and domain experts conduct deep dive analysis to the affected product	Incident Response Manager	• Detailed analysis report	- ISO/SAE 21434-13:v1.0 - ISO/SAE 21434-8:v1.0
M	PA 6-8 Prepare incident countermeasure	Incident Response manager makes plan for incident response with stakeholder	Incident Response Manager	• Incident response action plan	- ISO/SAE 21434-13:v1.0
M	PA 6-9 Post-Incident Response Activities	Incident Response manager monitors threat response results and establishes countermeasures to prevent recurrence.	Incident Response Manager	• Threat monitoring report	- ISO/SAE 21434-13:v1.0

M Mandatory O Optional

6 Related ISO/SAE 21434 standard for Continual Cybersecurity Activities including Production & Operation

Option	Process Area	Description	Role	Work product	Related standard
M	PA 6-10 Emergency Incident Response	In case of an emergency, the incident response manager promptly shares information with the top manager and performs a quick response.	Incident Response Manager	• verification report	- ISO/SAE 21434-13:v1.0
M	PA 6-11 SW update for products in development	If identified vulnerability affect products under development, countermeasure should be applied in accordance with development process	CSVTM	• Verifying results of the mitigation for vulnerability	- ISO/SAE 21434-13:v1.0 - ISO/SAE 21434-8:v1.0
M	PA 6-12 End of Cybersecurity Support	Incident Response Manager notice end of cybersecurity support to OEM	Incident Response Manager	• End of cybersecurity support list	- ISO/SAE 21434-13:v1.0
M	PA 6-13 HW update for products in development	If identified vulnerability affect products under development, countermeasure should be applied in accordance with development process	CSVTM	• Verifying results of the mitigation for vulnerability	- ISO/SAE 21434-13:v1.0 - ISO/SAE 21434-8:v1.0

M Mandatory O Optional

6 Continual Cybersecurity Activities including Production & Operation (1/2)

Process Area	Work Product	CSM	CSA	SysA	SWA	CSVTM	DEV	SAM	DQA	SysIT Manager	SysQT Manager	Cybersecurity Assessor	Production Manager
PA. 6-1. Production control plan	• Production plan • Production cybersecurity checklist	I	-	-	-	-	-	-	-	-	-	I	R
PA. 6-2. Planning of Cybersecurity Case	• Cybersecurity plan [refined] • Cybersecurity case [initial] • WBS [refined]	R	S	S	S	S	S	S	S	S	S	-	-
PA. 6-3. Development of Cybersecurity Case	• Cybersecurity case [confirmed]	R	S	S	S	S	S	S	S	S	S	-	-

R : Responsibility , A : Approval, S : Support , I : Informed

6 Continual Cybersecurity Activities including Production & Operation (2/2)

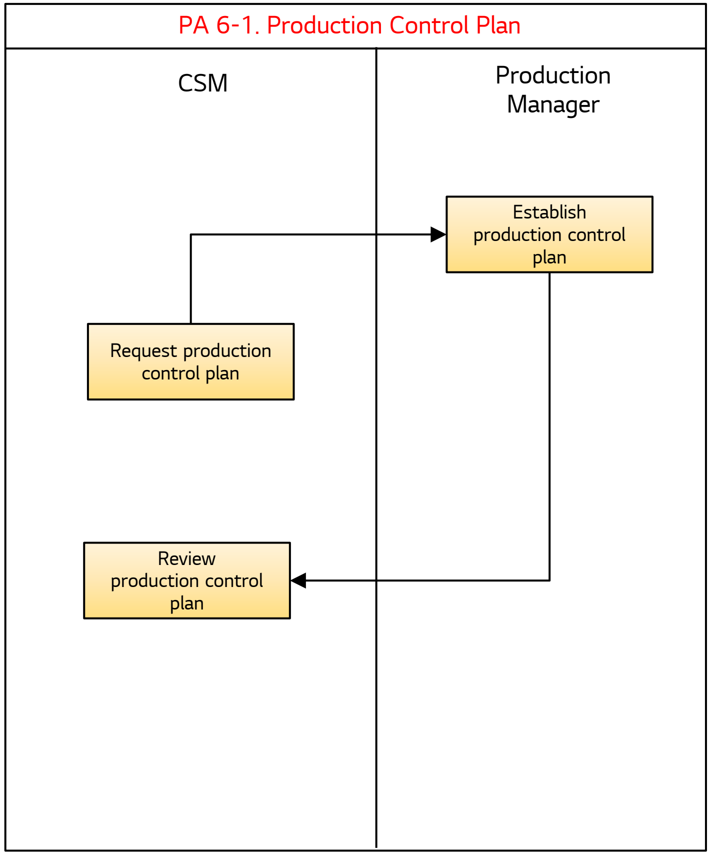
Process Area	Work Product	CSVTM	IR Manager	CSM	CSA	SWPL	HWPL	DEV	DQA	SysQT Manager	OEM CS Manager
PA 6-4. Cybersecurity Information monitoring	• Cybersecurity information • Cybersecurity events	R	S	I	-	-	-	-	-	-	I
PA 6-5. Initial Vulnerability analysis	• Initial threat analysis report • Affected product list	R	S	I	-	I	I	I	-	-	I
PA 6-6. Triggers Incident Response	• OEM (Governance, Project) contact point • Products list that affected by threat	S	R	I	-	I	I	I	-	-	I
PA 6-7. Detailed incident analysis	• Detailed analysis report	S	R	I	S	I	I	S	-	-	-
PA 6-8. Prepare incident countermeasure	• Incident response action plan	S	R	I	I	I	I	S	-	-	-
PA 6-9. Post-Incident Response Activities	• Threat monitoring report	S	R	S	I	I	I	I	-	-	I
PA 6-10. Emergency Incident Response	• verification report	S	R	S	S	I	I	S	-	-	I
PA 6-11. SW update for products in development	• Verifying results of the mitigation for vulnerability	R	S	I	S	A	I	S	-	-	-
PA 6-12. End of Cybersecurity Support	• End of cybersecurity support list	S	R	I	-	I	I	-	-	-	I
PA 6-13. HW update for products in development	• Verifying results of the mitigation for vulnerability	R	S	I	S	I	A	S	-	-	-

R : Responsibility , A : Approval, S : Support , I : Informed

6-1. Production Control Plan

◆ The production shall securely manage the physical environment and production tools and data to meet the cybersecurity requirements.

Entry criteria Approval of the SW Qualification(NPI process) by the DQA team leader.

Procedure	Detailed activity	Inputs
	※ Production control plan can be established with the process of "LG(35)-B-2592 Process control Plan". A production control plan shall be created that applies the cybersecurity requirements for post-development [Description in detail] • Production manager shall establish production control management plan • CSM shall verify the requirements described in Post-development report. • CSM requests Production Control plan from Production manager • Production manager reports mass production management status to CSM. • Production control plan can be included as part of an overall production plan • CSM reviews production control plan. ※ Please refer to the detailed information on the production approval procedure at "LG(35)-B-4516 Mass Production Approval Procedure".	- Production control plan - Post-development report **Outputs** - Production plan[refined] **Related standard** - ISO/SAE 21434-12:v1.0

PA 6-1. Production Control Plan
CSM
Production Manager
Establish production control plan
Request production control plan
Review production control plan

Exit criteria [Cybersecurity Manager] Review production Control plan.

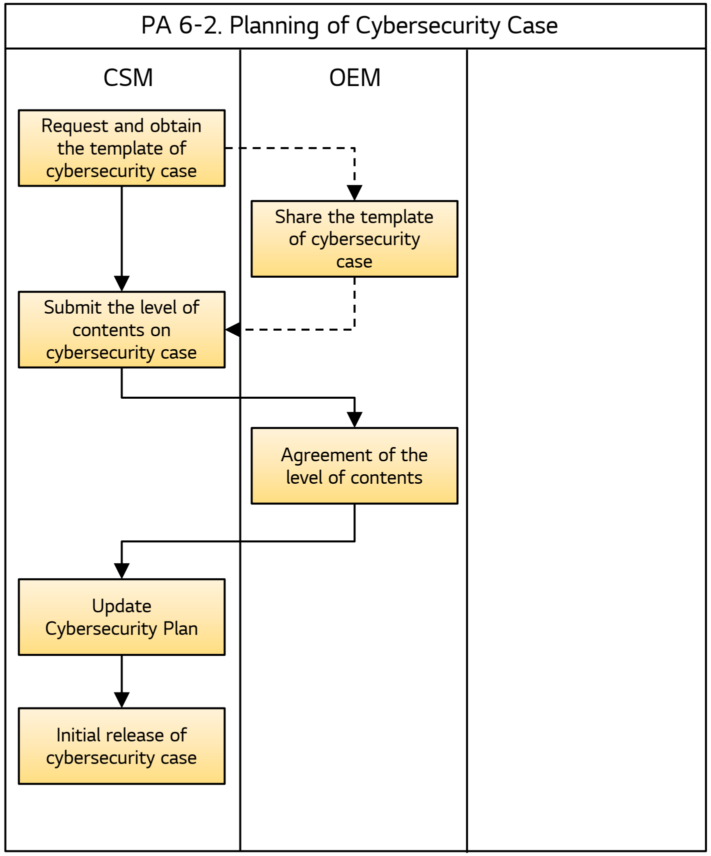
M If you do not perform any mandatory process, you should have a reasonable rationale.

6-2. Planning of Cybersecurity Case

◆ Cybersecurity Manager consult with the OEM on how to develop the cybersecurity case and on the level of content.

Entry criteria An OEM communication channel for cybersecurity activities should be established.

Procedure



PA 6-2. Planning of Cybersecurity Case

CSM

OEM

Request and obtain the template of cybersecurity case

Share the template of cybersecurity case

Submit the level of contents on cybersecurity case

Agreement of the level of contents

Update Cybersecurity Plan

Initial release of cybersecurity case

Detailed activity

Cybersecurity Manager(CSM) agrees with the OEM on how to arrange the cybersecurity case and drafts the cybersecurity case.

※ In the case of the preceding project without OEM, the initial release is drafted based on LGE's cybersecurity case template without any consultation.

[Description in detail]

- CSM ensures that the template provided to the OEM has a cybersecurity case template or a cybersecurity case guideline.
- CSM asks OEM if there is no data to prepare cybersecurity case.
- OEMs provide templates or guides for creating cybersecurity cases.
  ※ OEM should provide information on whether to make cybersecurity case and prepare it. If the hazard is not provided, it shall be arranged in units of cybersecurity goal.
- CSM analyzes the template to determine how to create a cybersecurity case.
- CSM requests an agreement from the OEM for the cybersecurity case.
  ※ If the contents related to the preparation of cybersecurity case are reflected in the CIA, it shall be replaced by the CIA agreement.
- The OEM agrees on the level of cybersecurity case.
- CSM establishes at what point in time the content of the cybersecurity case will be prepared and reflects it in the cybersecurity plan or WBS.
- CSM drafts a cybersecurity case with agreed contents.

Inputs

- Cybersecurity plan
- WBS

Outputs

- Cybersecurity plan [refined]
- Cybersecurity case [initial]
- WBS [refined]

Related standard

- ISO/SAE 21434-6:v1.0

Exit criteria [Cybersecurity Manager] The initial release of the cybersecurity case should be completed in an agreed manner with the OEM.

M If you do not perform any mandatory process, you should have a reasonable rationale.

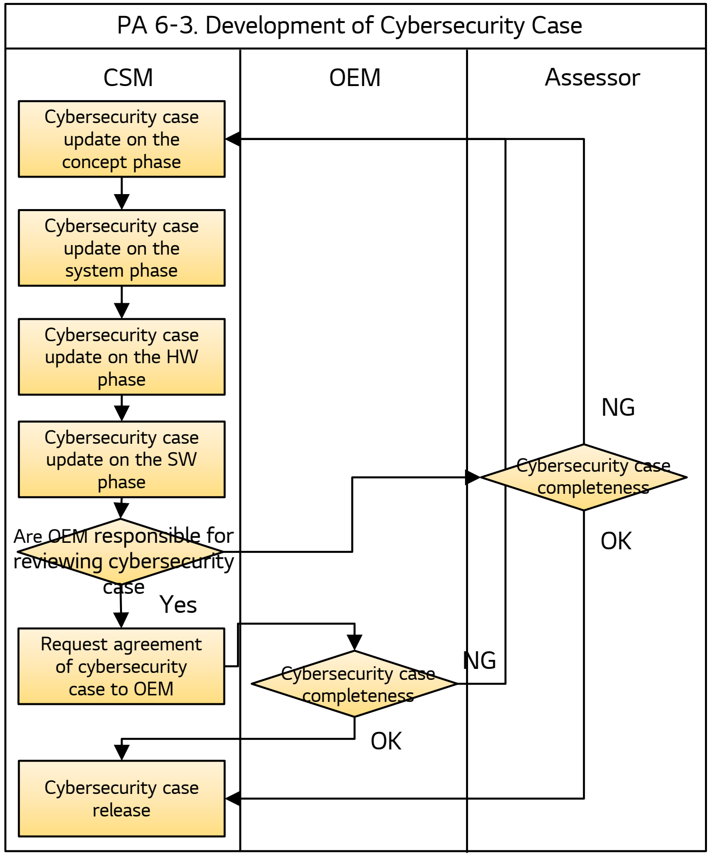
6-3. Development of Cybersecurity Case

Production & Operation for Cybersecurity

◆ Cybersecurity Manager creates a Cybersecurity case using the outputs of each development phase.

Entry criteria The level of Cybersecurity case contents should be agreed with the OEM.

Procedure



PA 6-3. Development of Cybersecurity Case

CSM | OEM | Assessor

Cybersecurity case update on the concept phase

Cybersecurity case update on the system phase

Cybersecurity case update on the HW phase

Cybersecurity case update on the SW phase

Are OEM responsible for reviewing cybersecurity case

Yes

Request agreement of cybersecurity case to OEM

Cybersecurity case completeness

NG

OK

Cybersecurity case completeness

NG

OK

Cybersecurity case release

Detailed activity

Cybersecurity Manager uses the work product of each phase of development to create the Cybersecurity case required by OEM.

※ The point of update of Cybersecurity case at each development phase is reflected in each development phase process.

[Description in detail]

- The Cybersecurity Manager reflects the concept phase work product to the Cybersecurity case.
- CSA, SysA, SWA, HWA, DEV request an update Cybersecurity case for the changes.
- Cybersecurity Manager reflects the outputs of the system development phase in the Cybersecurity case.
- Cybersecurity Manager reflects the outputs of the HW development phase to the Cybersecurity case.
- Cybersecurity Manager reflects the outputs of the SW development phase in the Cybersecurity case.
- Cybersecurity Manager sends the created Cybersecurity case to OEM and requests consent.
- The OEM reviews whether the Cybersecurity case meets the requirements and notify the consent.
- Cybersecurity Manager assigns the version to the agreed Cybersecurity case and distributes it to the document management system.
- If OEMs are not responsible for reviewing cybersecurity case cybersecurity case is reviewed internally by assessor.

Inputs

- Cybersecurity case [initial]

Outputs

- Cybersecurity case [confirmed]

Related standard

- ISO/SAE 21434-6:v1.0

Exit criteria [Cybersecurity Manager] Cybersecurity Manager assigns a version to the completed Cybersecurity case agreed with OEM and distributes it to the document management system.

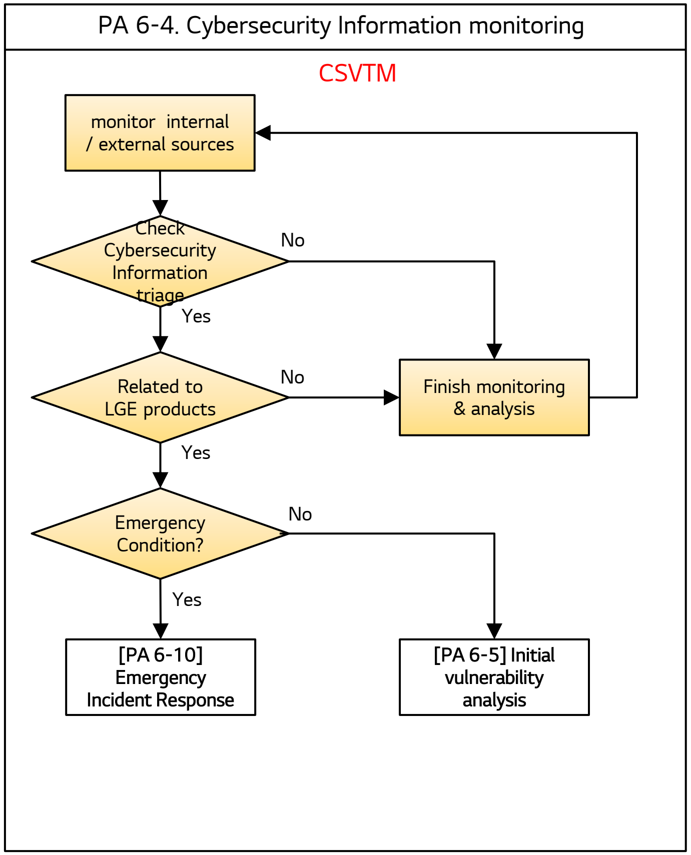
M If you do not perform any mandatory process, you should have a reasonable rationale.

6-4. Cybersecurity Information monitoring

◆ CSVTM monitor cybersecurity information that affects LGE product from internal / external sources.

Entry criteria None

Procedure



PA 6-4. Cybersecurity Information monitoring

CSVTM

monitor internal / external sources

Check Cybersecurity Information triage

No

Yes

Related to LGE products

No

Finish monitoring & analysis

Yes

Emergency Condition?

No

Yes

[PA 6-10] Emergency Incident Response

[PA 6-5] Initial vulnerability analysis

Detailed activity

CSVTM monitor internal / external source for collecting Cybersecurity information of LGE product. Vulnerability manager take actions if a Cybersecurity information affects LGE product

[Description in detail]

- CSVTM updates the list of internal and external sources for collection of cybersecurity information.
- CSVTM updates the list of triage for vulnerabilities that related LGE products.
- CSVTM manages criteria to determine cybersecurity event.
- CSVTM monitors cybersecurity information from internal and external sources.
- CSVTM triages cybersecurity information based on defined triggers.
- CSVTM identifies cybersecurity events if the Cybersecurity information related LGE product
- CSVTM determines if the cybersecurity events belongs to an emergency condition

[Emergency Condition]

- OEM or Government organization request emergency response.
- hacker successfully attacked LGE product through the media.

Inputs

- Cybersecurity information internal / external source list

Outputs

- Cybersecurity information
- cybersecurity events

* Weakness is included in the initial analysis report

Related standard

- ISO/SAE 21434-7:v1.0

Exit criteria [CSVTM] Identify the Cybersecurity information that need to analyze for vulnerability response.

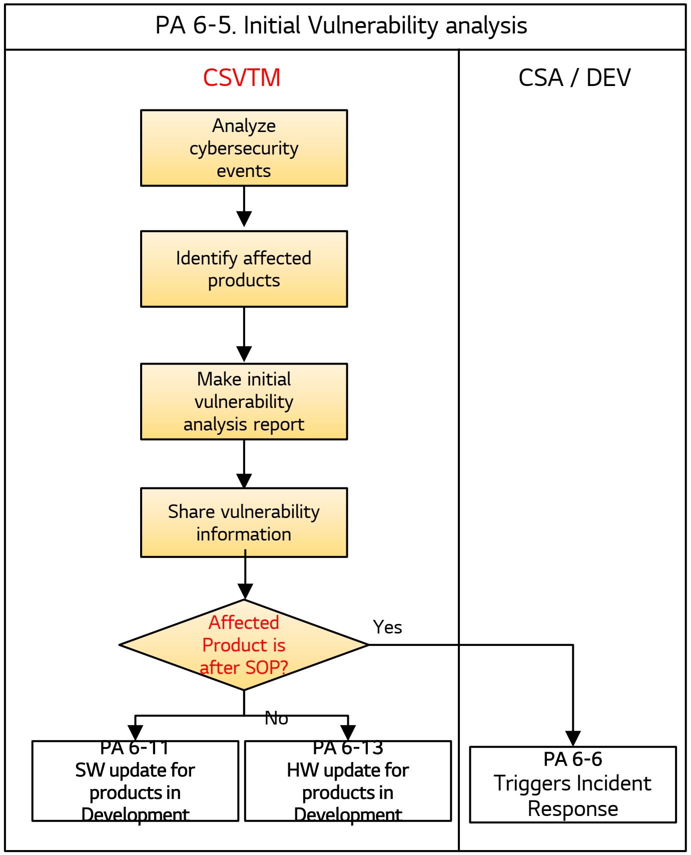
M If you do not perform any mandatory process, you should have a reasonable rationale.

6-5. Initial Vulnerability analysis

◆ CSVTM analyzes cybersecurity events for sharing results with cybersecurity managers

Entry criteria Cybersecurity event evaluation proved the Cybersecurity information affects LGE products

Procedure


PA 6-5. Initial Vulnerability analysis
CSVTM
CSA / DEV
Analyze cybersecurity events
Identify affected products
Make initial vulnerability analysis report
Share vulnerability information
Affected Product is after SOP?
Yes
No
PA 6-11 SW update for products in Development
PA 6-13 HW update for products in Development
PA 6-6 Triggers Incident Response

Detailed activity

CSVTM makes initial vulnerability analysis report based on cybersecurity events

[Description in detail]

- CSVTM conducts initial vulnerability analysis based on cybersecurity events
- CSVTM identifies affected products from cybersecurity events, if product has defect or characteristic that can lead to undesirable behavior.
- CSVTM makes initial vulnerability analysis report.
- CSVTM shares initial vulnerability analysis report with CSM together with affected products
- CSM share vulnerability information with OEM for products in Development, if coming from the OEM.

[Initial vulnerability analysis report shall include the following]

- Related vulnerabilities information
- Technical analysis results from security point of view
- List of products that may be affected

[Cases of the affected product is a product in development.]

- During the analysis, if it is confirmed that the affected product is a product under development, it is processed in accordance with PA 6-11, PA 6-13.

Inputs

- cybersecurity events
- LGE product list
- Product information

Outputs

- Initial vulnerability analysis report
- Affected product list

Related standard

- ISO/SAE 21434-13:v1.0

Exit criteria [CSVTM] Completes initial analysis report and share with CSM.

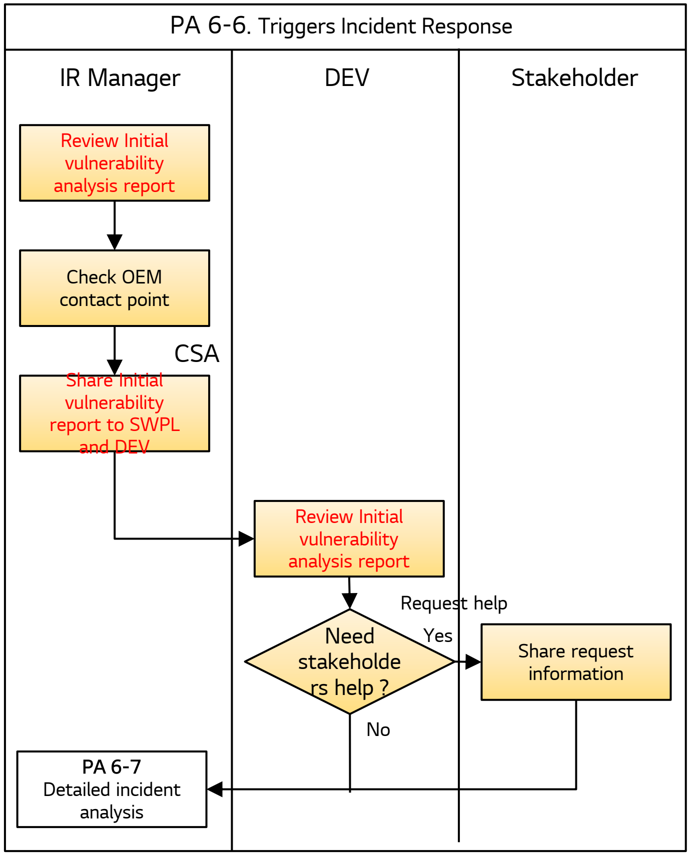
M If you do not perform any mandatory process, you should have a reasonable rationale.

6. Triggers Incident Response

◆ **Incident Response Manager review initial analysis report and confirm affected product for response.**

Entry criteria CSVTM shares initial analysis report to Cybersecurity Architect and Developer.

Procedure



PA 6-6. Triggers Incident Response

IR Manager

DEV

Stakeholder

Review Initial vulnerability analysis report

Check OEM contact point

CSA

Share initial vulnerability report to SWPL and DEV

Review Initial vulnerability analysis report

Request help

Need stakeholders help ?

Yes

No

Share request information

PA 6-7 Detailed incident analysis

Detailed activity

Cybersecurity Architect(CSA) and DEV confirm affected LGE product based on initial analysis report and If this is sure to affect products, IR Manager share initial vulnerability analysis report to CSA and DEV and stakeholders.

[Description in detail]

- CSA and DEV review initial vulnerability analysis report
- IR Manager check communication channel with (Governance, Project) cybersecurity manager in OEM
- CSA share and analyze initial vulnerability analysis report with DEV and stakeholders, if vulnerabilities affect products
- DEV and stakeholders review initial vulnerability analysis report.
- CSA and stakeholders confirm affected product by the information in the initial vulnerability analysis report

[Attention]

- Initial vulnerability analysis report should not be shared to OEM directly
- IR Manager communicates with OEM contact point for vulnerability response.

- Stakeholder: IR manager, legal, qualification, marketing department, developer, ETC (all member related vulnerability) http://collab.lge.com/main/x/d_nUew

Inputs

- Initial vulnerability analysis report
- Related product list
- Related domain experts list
- Related Stakeholders list

Outputs

- OEM (Governance, Project) contact point
- Products list that affected by vulnerability

Related standard

- ISO/SAE 21434-13:v1.0

Exit criteria [IR Manager] Complete review and Completion of determining whether or not products are affected

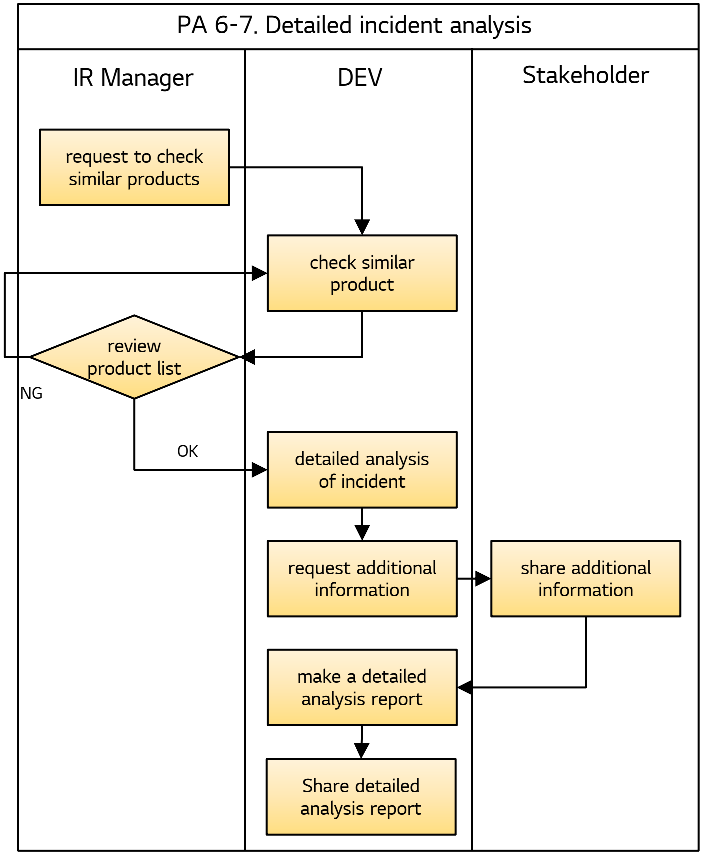
M If you do not perform any mandatory process, you should have a reasonable rationale.

6-7. Detailed incident analysis

◆ Incident Response managers and domain experts conduct deep dive analysis to the affected product.

Entry criteria Product affected by vulnerabilities in the initial analysis report and need deep dive analysis.

Procedure


PA 6-7. Detailed incident analysis
IR Manager
DEV
Stakeholder
request to check similar products
check similar product
review product list
NG
OK
detailed analysis of incident
request additional information
share additional information
make a detailed analysis report
Share detailed analysis report

Detailed activity

IR Manager and DEV (Developer) conduct deep dive analysis of vulnerabilities related incident. After that Developer make report of deep dive analysis.

[Description in detail]

- IR Manager request to Developer(DEV) checking similar products for incident response.
- DEV check similar product that can be affected.
- IR Manager confirm what product is affected.
- DEV request additional information to stakeholders if they need more information for analyzing incident.
- DEV specify detail information in the detailed analysis report.
- IR Manager share detailed analysis report to stakeholders

[detailed vulnerability report shall include the following]

- Affected module by the incidents
- Countermeasure opinion for incident response.
- Reason for incidents

- Stakeholder: http://collab.lge.com/main/x/d_nUew

※ A rationale for a weakness that is not identified as an incident shall be specified in Detailed analysis report.

※ For the unknown vulnerability, risk assessment and treatment are made. Refer to the following links for the details
http://collab.lge.com/main/x/Ys1PWg
http://collab.lge.com/main/x/9Ceogg
http://collab.lge.com/main/x/ETg3Tw

Inputs

- Initial analysis report
- Additional information related incident

Outputs

- Detailed analysis report

Related standard

- ISO/SAE 21434-13:v1.0
- ISO/SAE 21434-8:v1.0

Exit criteria [IR Manager] IR manager and Developer finish deep dive analysis of incident and make report

M If you do not perform any mandatory process, you should have a reasonable rationale.

LGE Internal Use Only

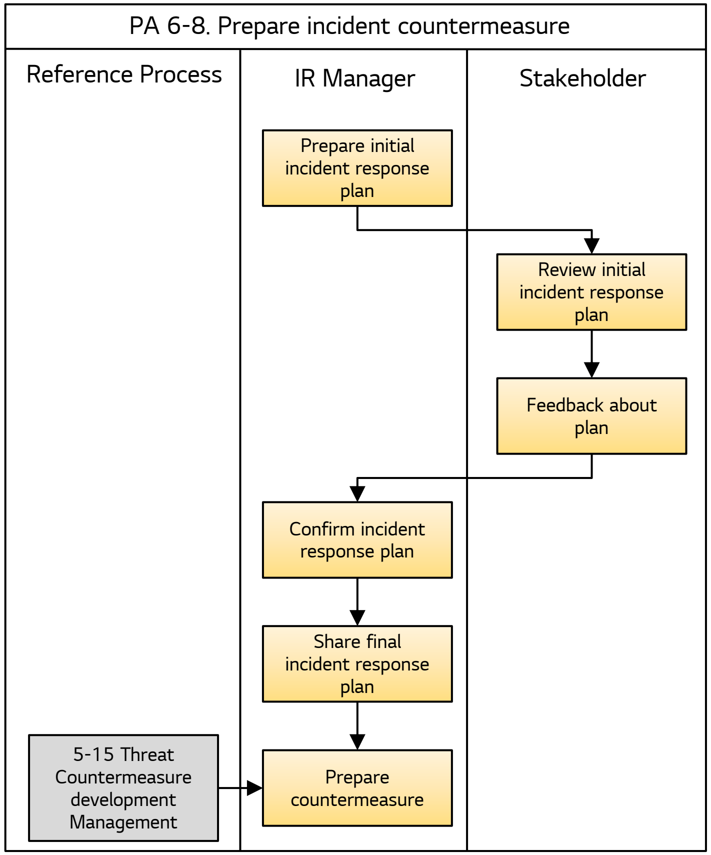
6-8. Prepare incident countermeasure

Production & Operation for Cybersecurity

◆ Incident Response **manager makes plan for incident response with stakeholder.**

Entry criteria Detailed analysis report for the affected products

Procedure


PA 6-8. Prepare incident countermeasure
Reference Process
IR Manager
Stakeholder
Prepare initial incident response plan
Review initial incident response plan
Feedback about plan
Confirm incident response plan
Share final incident response plan
5-15 Threat Countermeasure development Management
Prepare countermeasure

Detailed activity

IR Manager makes incident response plan of product and share the plan to stakeholders. Stakeholders review and send opinion to cybersecurity manager

[Description in detail]

- CSA and IR manager prepares countermeasures based on detailed analysis.
- IR manager contacts the OEM's response manager for sharing plan and countermeasures.
- The legal person in charge checks if necessary for legal issues in countermeasures and issues in contract
- Marketing staff prepares a response to the media for countermeasures.
- CSM prepares to implement countermeasures, if need implementation.

[Countermeasure plan shall include the following]

- Action plan
- Incident response schedule of product
- Detailed Countermeasure

- Stakeholder: http://collab.lge.com/main/x/d_nUew

Inputs

- Detailed analysis report of product

Outputs

- Incident response action plan

Related standard

- ISO/SAE 21434-13:v1.0

Exit criteria IR Manager makes final incident response plan and all stakeholder confirm action plan in the final incident response plan.

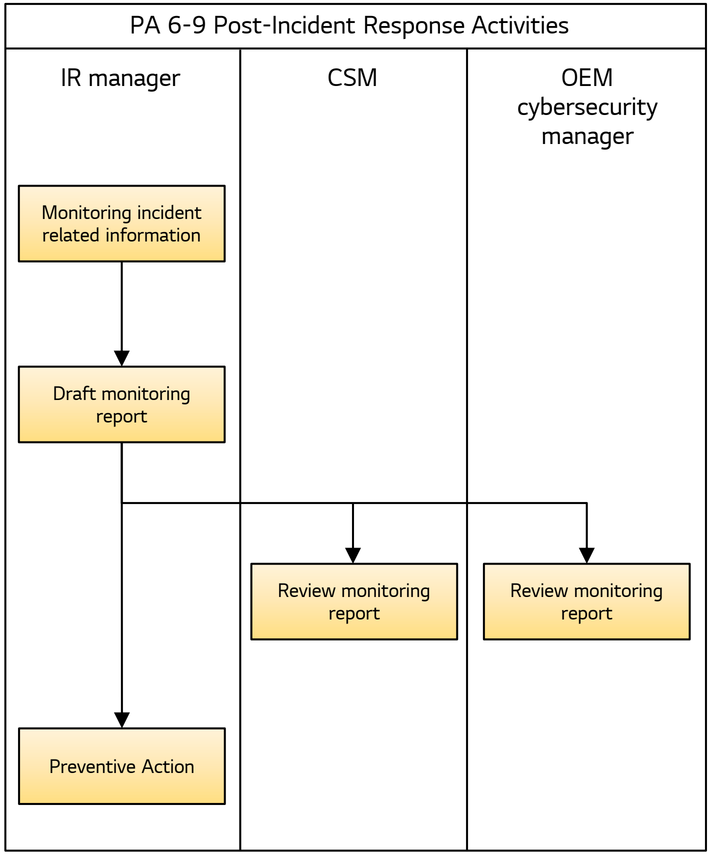
M If you do not perform any mandatory process, you should have a reasonable rationale.

6-9. Post-Incident Response Activities

◆ Incident Response **manager monitors incident response results and establishes countermeasures to prevent recurrence.**

Entry criteria LGE Send Official release to OEM including all vulnerabilities patched

Procedure


PA 6-9 Post-Incident Response Activities
IR manager
CSM
OEM cybersecurity manager
Monitoring incident related information
Draft monitoring report
Review monitoring report
Review monitoring report
Preventive Action

Detailed activity

IR manager continuously collects/analyzes information on products regarding vulnerabilities and incidents, shares them with internal parties, and reviews and applies recurrence prevention measures.

[Description in detail]

- Monitoring whether there is any updated contents of the incident-related vulnerability on the official vulnerability sharing site
- Monitoring hacking information related to LGE products on various hacking information sharing sites
- Periodic monitoring result report creation
- Sharing of information to the person concerned with the result report incident response
- Review and update cybersecurity concept to prevent incident recurrence
- Policy review and update to prevent recurrence of incident
- Review and update cybersecurity requirements to prevent recurrence

Inputs

- Information related to incident
- Countermeasure applying result report

Outputs

- Incident monitoring report

Related standard

- ISO/SAE 21434-13:v1.0

Exit criteria [IR Manager] There are no additional incident information after incident response during a month

M If you do not perform any mandatory process, you should have a reasonable rationale.

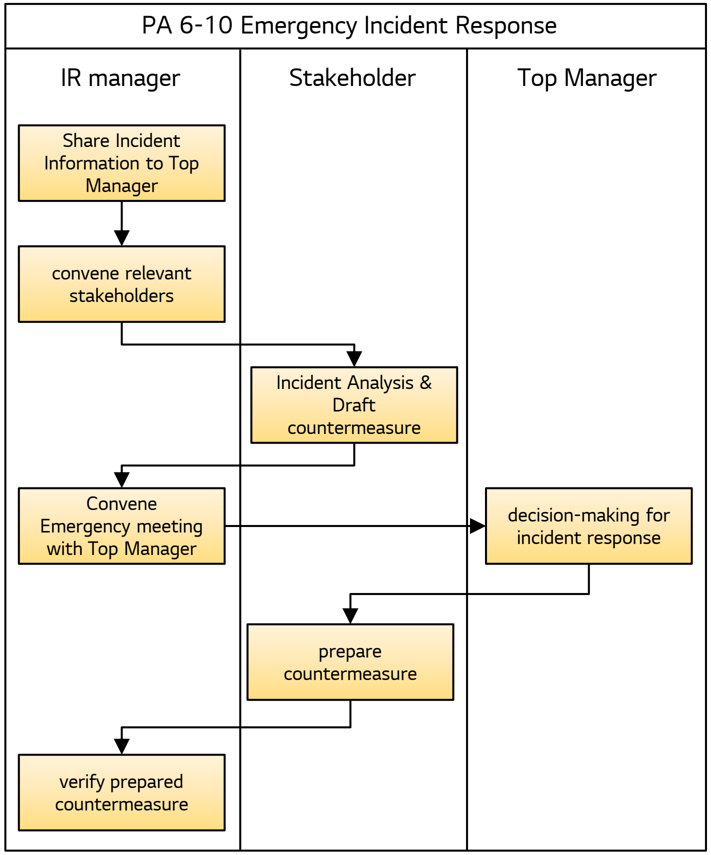
6-10. Emergency Incident Response

Production & Operation for Cybersecurity

◆ In case of an emergency, the incident response manager promptly shares information with the top manager and performs a quick response.

Entry criteria Vulnerability identified as requiring an emergency response.

Procedure



PA 6-10 Emergency Incident Response

IR manager | Stakeholder | Top Manager

Share Incident Information to Top Manager

convene relevant stakeholders

Incident Analysis & Draft countermeasure

Convene Emergency meeting with Top Manager

decision-making for incident response

prepare countermeasure

verify prepared countermeasure

Detailed activity

Incident Response manager promptly share cybersecurity information and convene stakeholders for emergency response. After completing countermeasures, verification follows the normal incident response process.

[Description in detail]

- Incident response manager promptly share cybersecurity information of incident to top manager(CS leader, CS Team leader, PL).
- Incident response manager convene emergency meeting for share cyber security information with stakeholder(CSA, Security FO, CSM, SWPL and developers).
- Stakeholders and Incident response manager analyze incident and draft countermeasures.
- Incident response manager convene emergency meeting for decision-making with top manager and OEM
- Top manager decide countermeasure for response
- Stakeholders prepare countermeasure based on decision.
- Incident response manager verify prepared countermeasure

[Due time of Emergency Incident Response]

- When an incident occurs, the IR Manager completes the analysis within 2 days and spreads it to the relevant people. The fixed version is released within 7 days of the incident.

- Stakeholder: http://collab.lge.com/main/x/d_nUew

Inputs

- Cybersecurity Information
- Stakeholders Information

Outputs

- verification report

Related standard

- ISO/SAE 21434-13:v1.0

Exit criteria [IR Manager] countermeasure is prepared by decision-making

M If you do not perform any mandatory process, you should have a reasonable rationale.

LGE Internal Use Only

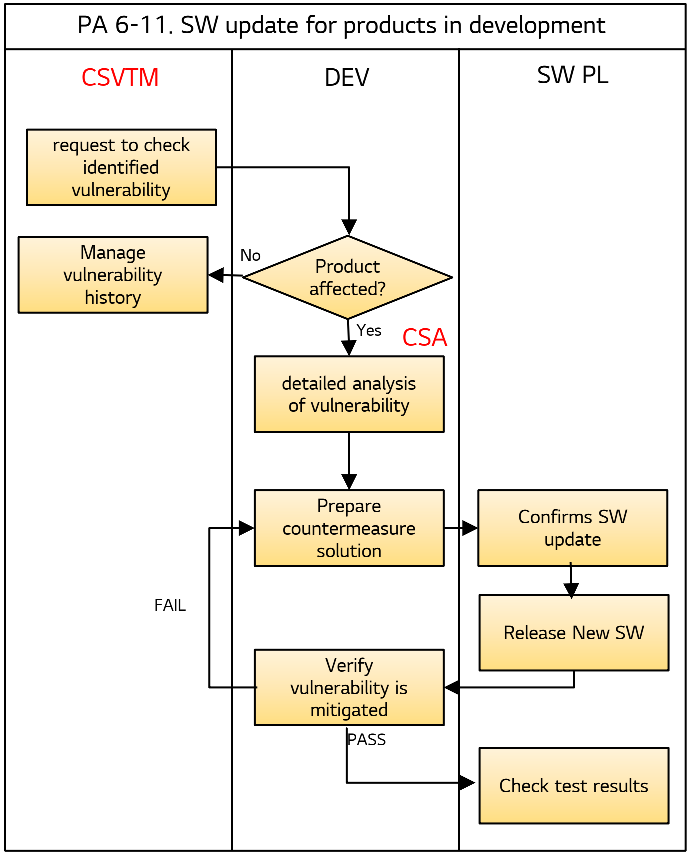
6-11. SW update for products in development

Production & Operation for Cybersecurity

◆ If identified vulnerability affect products under development, countermeasure should be applied in accordance with development process

Entry criteria Vulnerability identified affect products under development.

Procedure



PA 6-11. SW update for products in development

CSVTM | DEV | SW PL

request to check identified vulnerability

Product affected?

No

Manage vulnerability history

Yes

CSA

detailed analysis of vulnerability

Prepare countermeasure solution

Confirms SW update

Release New SW

FAIL

Verify vulnerability is mitigated

PASS

Check test results

Detailed activity

CSVTM and DEV (Developer) conduct deep dive analysis of vulnerabilities and prepare countermeasures. After that Developer makes sure solution is merged into new SW and verify the vulnerability is mitigated

[Description in detail]

- CSVTM requests Developer(DEV) checks identified vulnerability
- DEV confirms checks the reported vulnerability affects products under development
- CSVTM, CSA and DEV conduct detailed analysis of the vulnerability
- CSVTM and DEV prepares countermeasure solution
- DEV requests product PL to confirm SW update
- Product PL releases new SW that contains the countermeasure
- DEV verifies the vulnerability is mitigated with new SW
- DEV reports test results to product PL

※ For the unknown vulnerability, risk assessment and treatment are made. Refer to the following links for the details http://collab.lge.com/main/x/ETg3Tw

Inputs

- Initial analysis report

Outputs

- Verifying results of the mitigation for vulnerability

Related standard

- ISO/SAE 21434-13:v1.0
- ISO/SAE 21434-8:v1.0

Exit criteria [CSVTM] checks DEV verified vulnerability mitigation

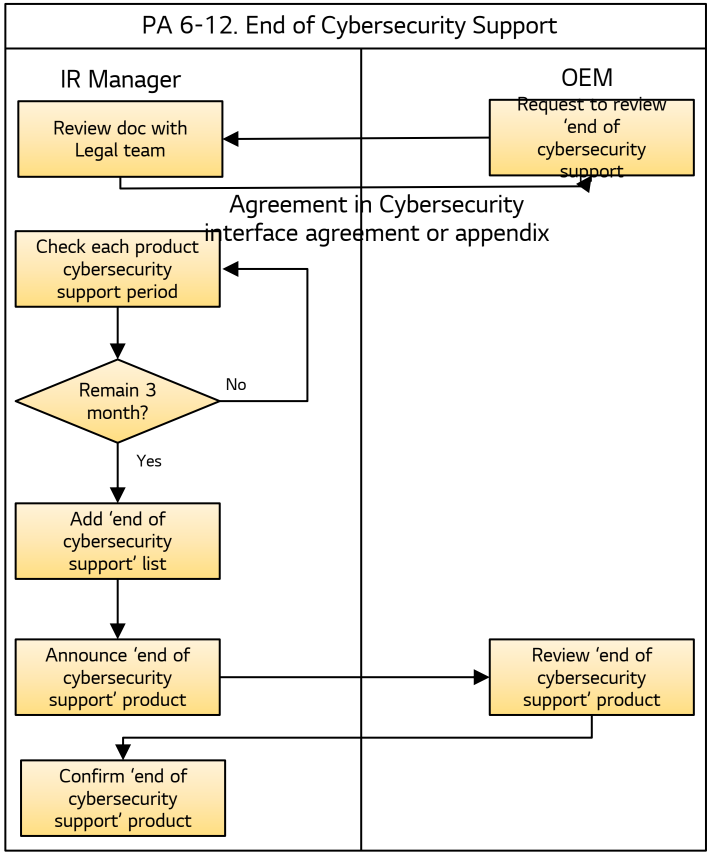
M If you do not perform any mandatory process, you should have a reasonable rationale.

6-12. End of Cybersecurity Support

◆ **Incident Response** Manager **notice end of cybersecurity support to OEM**

Entry criteria -

Procedure



PA 6-12. End of Cybersecurity Support

IR Manager

OEM

Request to review 'end of cybersecurity support

Review doc with Legal team

Agreement in Cybersecurity interface agreement or appendix

Check each product cybersecurity support period

Remain 3 month?

No

Yes

Add 'end of cybersecurity support' list

Announce 'end of cybersecurity support' product

Review 'end of cybersecurity support' product

Confirm 'end of cybersecurity support' product

Detailed activity

IR Manager check cybersecurity period of each product and announce products list to OEM for end of cybersecurity support

[Description in detail]

- If there is something to be negotiated with the OEM on cybersecurity support, LG goes through the consultation procedure with the OEM through a contract called Cybersecurity appendix
- Through the CIA consultation process, LG discusses the contents and period of end of cybersecurity support based on the contents described in its process and policy.
- when details are described through the cybersecurity appendix and delivered from the OEM, a final agreement is reached after review by LG's legal team
- IR Manager check all product cybersecurity support period remain 3 month
- IR Manager make end of cybersecurity support list.
- IR Manager announce 'end of cybersecurity support list' for end of cybersecurity support.
- OEM review 'end of cybersecurity support list' based on contract.
- IR Manager confirm 'end of cybersecurity support.
- several months prior to the expiration of the initial period, the parties may have a meeting and negotiation process to discuss the terms of the additional several years renewal period.

※ Product cybersecurity support check cycle : every month

Inputs

- Product period of cybersecurity support
- OEM contact point

Outputs

- End of cybersecurity support list

Related standard

- ISO/SAE 21434-13:v1.0

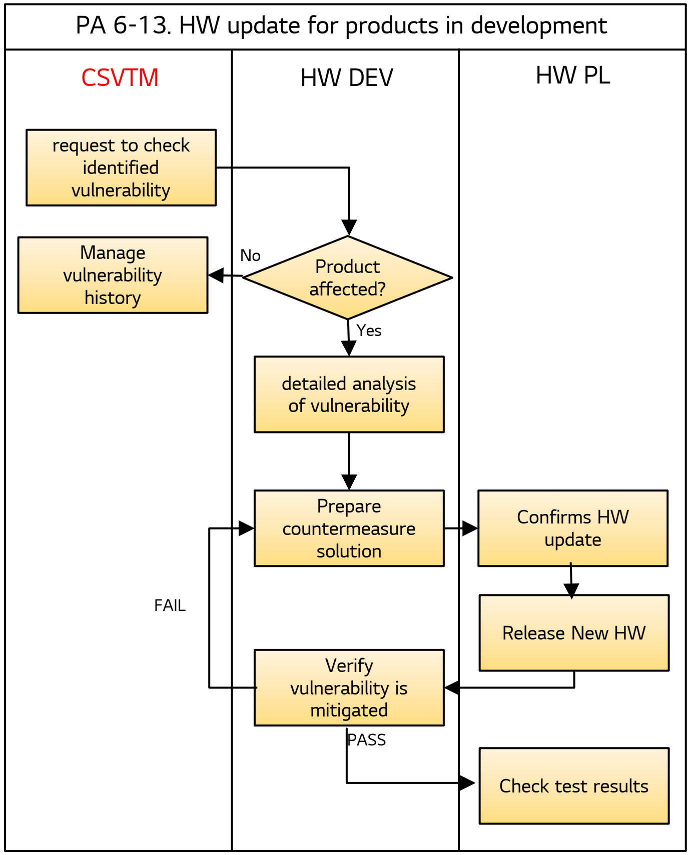
Exit criteria [IR Manager] Incident Response Manager update cybersecurity support status of all products.

M If you do not perform any mandatory process, you should have a reasonable rationale.

6-13. HW update for products in development

◆ If identified vulnerability affect products under development, countermeasure should be applied in accordance with development process

Entry criteria Vulnerability identified affect products under development.

Procedure	Detailed activity	Inputs
	**CSVTM and DEV (Developer) conduct deep dive analysis of vulnerabilities and prepare countermeasures. After that Developer makes sure solution is merged into new HW and verify the vulnerability is mitigated** **[Description in detail]** • CSVTM requests Developer(DEV) checks identified vulnerability • HW DEV confirms checks the reported vulnerability affects products under development • CSVTM and HW DEV conduct detailed analysis of the vulnerability • CSVTM and HW DEV prepares countermeasure solution • HW DEV requests product PL to confirm HW update • Product PL releases new HW that contains the countermeasure • HW DEV verifies the vulnerability is mitigated with new HW • HW DEV reports test results to product PL	- Initial analysis report **Outputs** - Verifying results of the mitigation for vulnerability **Related standard** - ISO/SAE 21434-13:v1.0 - ISO/SAE 21434-8:v1.0

PA 6-13. HW update for products in development
CSVTM
HW DEV
HW PL
request to check identified vulnerability
Product affected?
No
Yes
Manage vulnerability history
detailed analysis of vulnerability
Prepare countermeasure solution
Confirms HW update
Release New HW
FAIL
Verify vulnerability is mitigated
PASS
Check test results

Exit criteria [CSVTM] checks HW DEV verified vulnerability mitigation

M If you do not perform any mandatory process, you should have a reasonable rationale.

7 Organizational Cybersecurity Management

- **Objective**

  Define the organizational cybersecurity management of the item to which cybersecurity is applied among the E/E system developed by the VS company, and define the main activities and standards by stages.

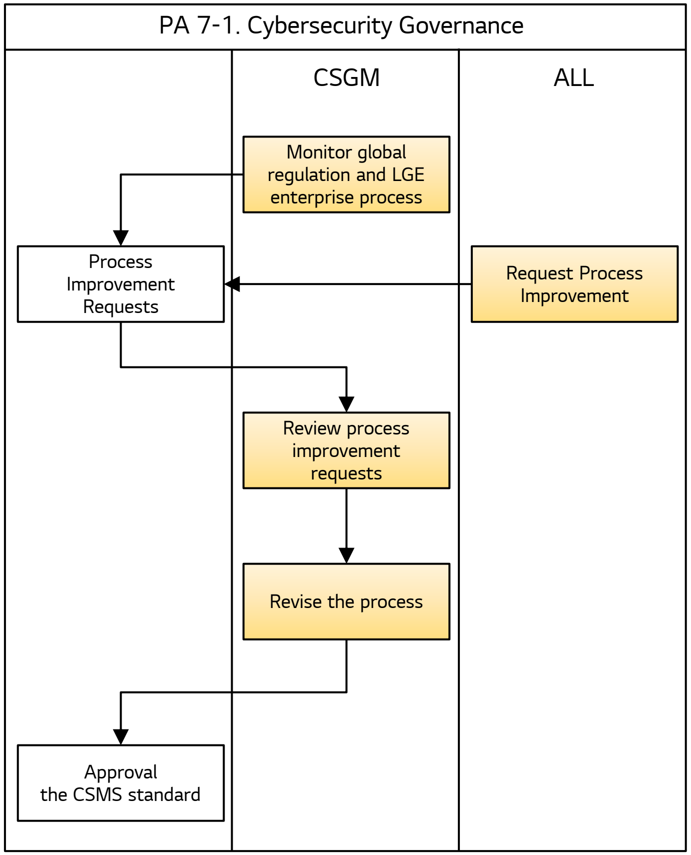
- **Scope**

  It is applied when developing the item to apply cybersecurity among electrical and electronic system (E / E system) developed by VS company.

7-1. Cybersecurity Governance

◆ Cybersecurity Governance Manager defines an organization-specific rules and processes for cybersecurity

Entry criteria Gathering the information of the global regulations, LGE enterprise processes, and process improvement requests every year

Procedure	Detailed activity	Inputs
	**CSGM defines an organization-specific rules and processes for cybersecurity. Basically, CSGM perform the revise of the CSMS standard every year with process improvement requests.** **[Description in detail]** • CSGM prepare items need to improve on the process, detail guideline, and templates for cybersecurity. [Process Improvement Requests] - Global Regulation - LGE Enterprise Process - Internal requests for the process improvement ※ Please refer to the detail activities and information for CSMS below collaboration page. - http://collab.lge.com/main/x/cm1-Sg	- CSMS Standard - Process Improvement Requests **Outputs** - CSMS Standard (refined) **Related standard** - ISO/SAE 21434 - 5:v1.0

PA 7-1. Cybersecurity Governance
CSGM
ALL
Monitor global regulation and LGE enterprise process
Process Improvement Requests
Request Process Improvement
Review process improvement requests
Revise the process
Approval the CSMS standard

Exit criteria [Cybersecurity Governance Manager] All possible process improvements are added and modified to the refined CSMS standard.

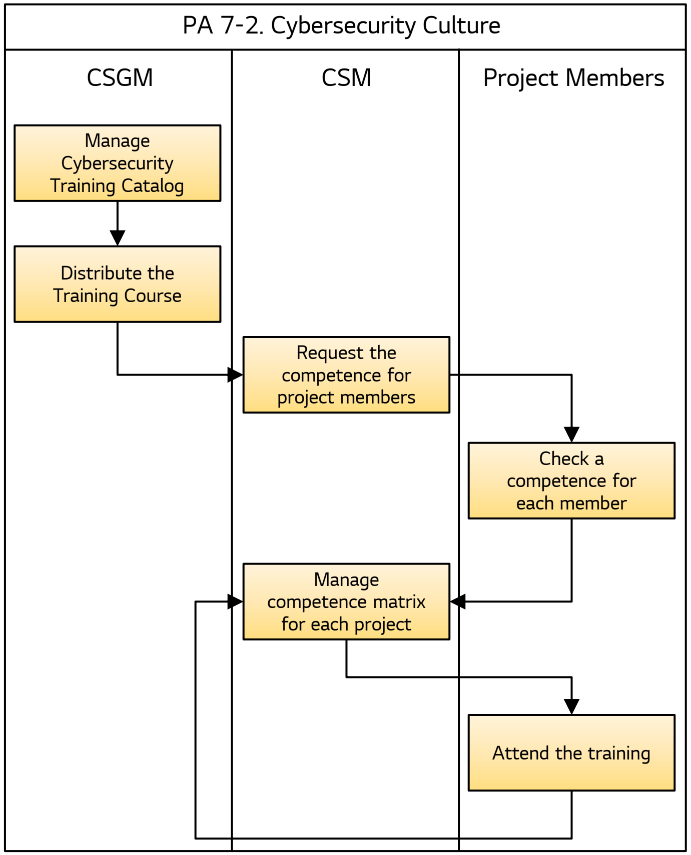
M If you do not perform any mandatory process, you should have a reasonable rationale.

7-2. Cybersecurity Culture

◆ **Cybersecurity Governance Manager and Cybersecurity Manager institute and maintain a cybersecurity culture, including competence management, awareness management.**

Entry criteria Cybersecurity training catalog is prepared

Procedure


PA 7-2. Cybersecurity Culture
CSGM
CSM
Project Members
Manage Cybersecurity Training Catalog
Distribute the Training Course
Request the competence for project members
Check a competence for each member
Manage competence matrix for each project
Attend the training

Detailed activity

CSGM and CSM institute and maintain a cybersecurity culture, including competence management, awareness management.

[Description in detail]

- CSGM manages the total training catalog for cybersecurity.
- CSGM distribute the training course to all members related to cybersecurity.
- CSM request the competence of project members and manages the competence management report.
- ALL project members check the competence of cybersecurity and update the competence management report.
- ALL project members attends the training with the schedule in the competence management report.

※ Please refer to the training catalog for cybersecurity below collaboration page.
- http://collab.lge.com/main/x/Rx44T
※ General training management is described in the enterprise process – “LG(10)-A-3120 교육훈련 규정”.
※ In addition to cybersecurity training, cybersecurity awareness education and publicity can be conducted through posters or letters.

Inputs

- Cybersecurity training catalog

Outputs

- Cybersecurity training catalog (refined)
- Competence management report (each project)
- Training evidences

Related standard

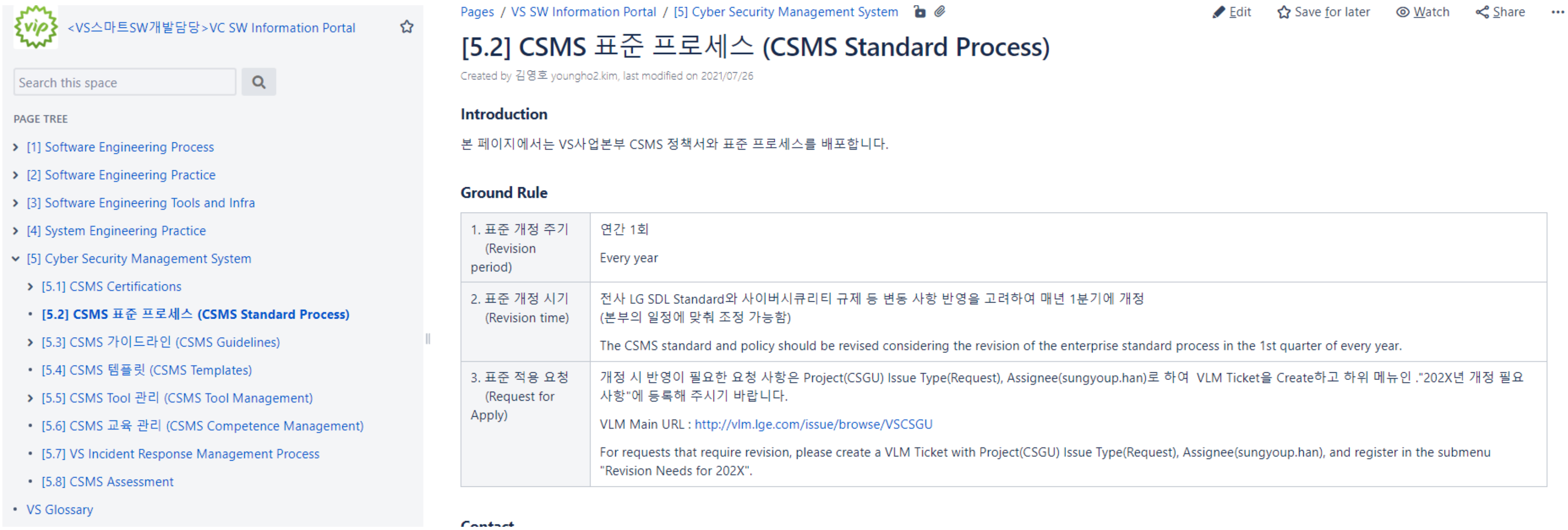
- ISO/SAE 21434
 -First edition:2021
- LG(10)-A-3120 교육훈련 규정

Exit criteria [CSM] CSM manages the competence of project members and monitors the completion of training schedules refer to the Cybersecurity Training Catalog.

M If you do not perform any mandatory process, you should have a reasonable rationale.

7-3. Information Sharing

◆ All information related to the CSMS(Cybersecurity) is managed "VIP(VS SW Information Portal) collaboration page".
- http://collab.lge.com/main/x/em1-Sg



<VS스마트SW개발담당>VC SW Information Portal
Search this space
PAGE TREE
[1] Software Engineering Process
[2] Software Engineering Practice
[3] Software Engineering Tools and Infra
[4] System Engineering Practice
[5] Cyber Security Management System
[5.1] CSMS Certifications
[5.2] CSMS 표준 프로세스 (CSMS Standard Process)
[5.3] CSMS 가이드라인 (CSMS Guidelines)
[5.4] CSMS 템플릿 (CSMS Templates)
[5.5] CSMS Tool 관리 (CSMS Tool Management)
[5.6] CSMS 교육 관리 (CSMS Competence Management)
[5.7] VS Incident Response Management Process
[5.8] CSMS Assessment
VS Glossary
Pages / VS SW Information Portal / [5] Cyber Security Management System
Edit
Save for later
Watch
Share

[5.2] CSMS 표준 프로세스 (CSMS Standard Process)

Created by 김영호 youngho2.kim, last modified on 2021/07/26

Introduction

본 페이지에서는 VS사업본부 CSMS 정책서와 표준 프로세스를 배포합니다.

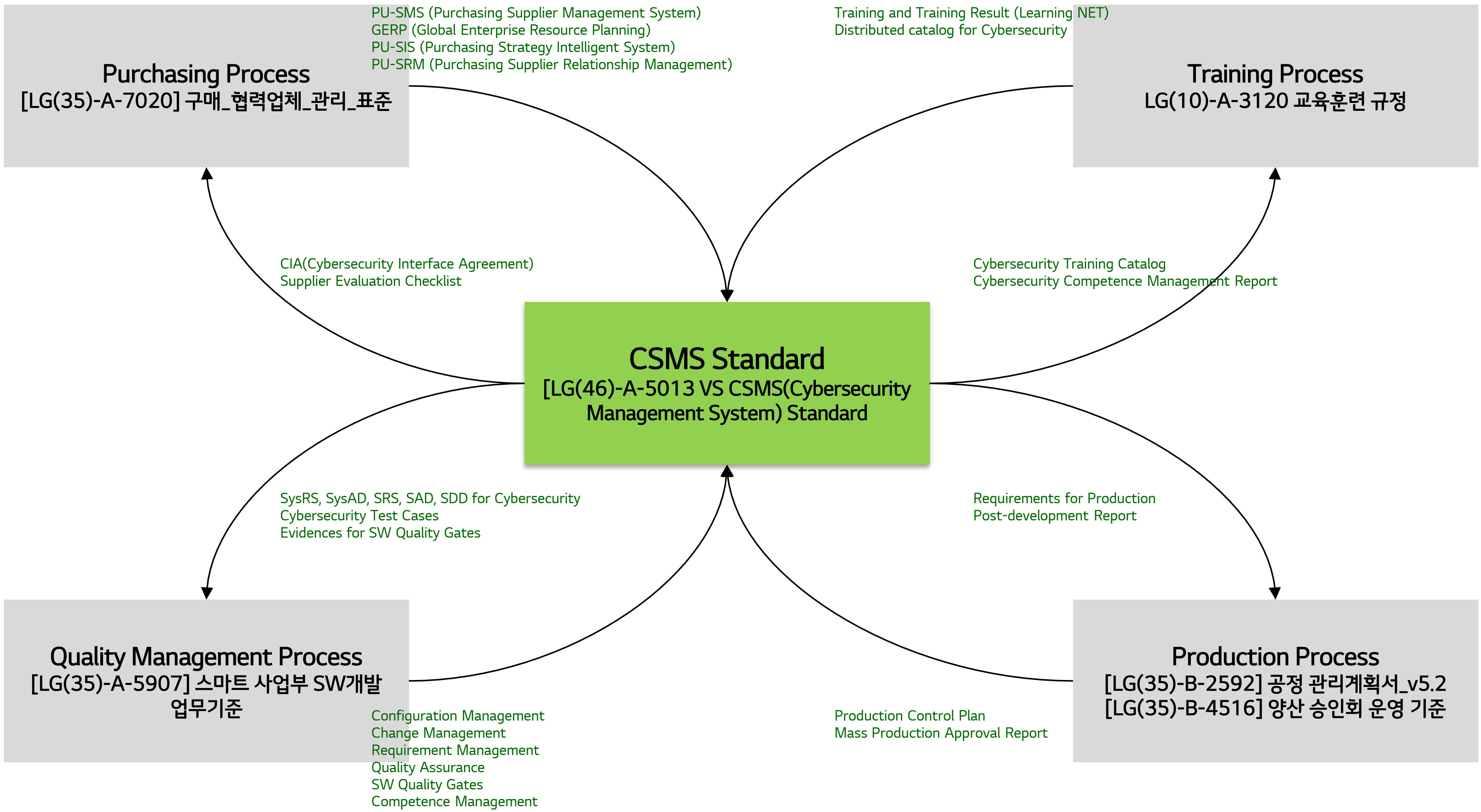
Ground Rule

1. 표준 개정 주기 (Revision period)	연간 1회 Every year
2. 표준 개정 시기 (Revision time)	전사 LG SDL Standard와 사이버시큐리티 규제 등 변동 사항 반영을 고려하여 매년 1분기에 개정 (본부의 일정에 맞춰 조정 가능함) The CSMS standard and policy should be revised considering the revision of the enterprise standard process in the 1st quarter of every year.
3. 표준 적용 요청 (Request for Apply)	개정 시 반영이 필요한 요청 사항은 Project(CSGU) Issue Type(Request), Assignee(sungyoup.han)로 하여 VLM Ticket을 Create하고 하위 메뉴인 ."202X년 개정 필요 사항"에 등록해 주시기 바랍니다. VLM Main URL : http://vlm.lge.com/issue/browse/VSCSGU For requests that require revision, please create a VLM Ticket with Project(CSGU) Issue Type(Request), Assignee(sungyoup.han), and register in the submenu "Revision Needs for 202X".

Contact

7-4. Management System

◆ Relations with existed LGE processes.



Purchasing Process
[LG(35)-A-7020] 구매_협력업체_관리_표준

PU-SMS (Purchasing Supplier Management System)
GERP (Global Enterprise Resource Planning)
PU-SIS (Purchasing Strategy Intelligent System)
PU-SRM (Purchasing Supplier Relationship Management)

Training and Training Result (Learning NET)
Distributed catalog for Cybersecurity

Training Process
LG(10)-A-3120 교육훈련 규정

CIA(Cybersecurity Interface Agreement)
Supplier Evaluation Checklist

Cybersecurity Training Catalog
Cybersecurity Competence Management Report

CSMS Standard
[LG(46)-A-5013 VS CSMS(Cybersecurity Management System) Standard

SysRS, SysAD, SRS, SAD, SDD for Cybersecurity
Cybersecurity Test Cases
Evidences for SW Quality Gates

Requirements for Production
Post-development Report

Quality Management Process
[LG(35)-A-5907] 스마트 사업부 SW개발 업무기준

Configuration Management
Change Management
Requirement Management
Quality Assurance
SW Quality Gates
Competence Management

Production Control Plan
Mass Production Approval Report

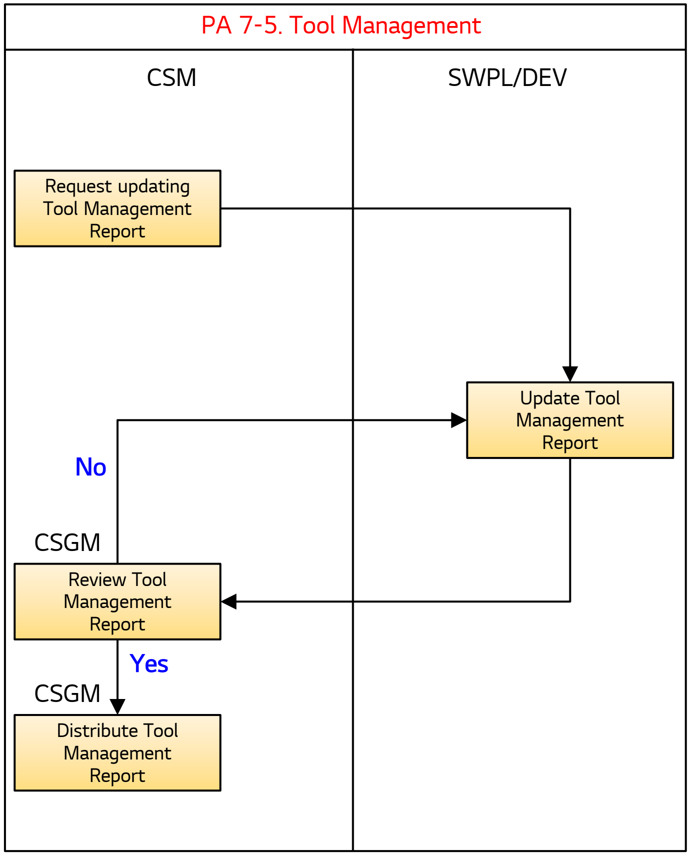
Production Process
[LG(35)-B-2592] 공정 관리계획서_v5.2
[LG(35)-B-4516] 양산 승인회 운영 기준

7-5. Tool Management

Based on project-specific tool information provided by CSM, the CSGM manages the latest version of the Tool List for the entire project.

Entry criteria Request updating tool management report

Procedure



PA 7-5. Tool Management
CSM
SWPL/DEV
Request updating Tool Management Report
Update Tool Management Report
No
CSGM
Review Tool Management Report
Yes
CSGM
Distribute Tool Management Report

Detailed activity

The CSGM maintains the latest version of the Tool List for the entire project.

[Description in detail]

- CSM request updating Tool Management Report.
- The Tool Management report includes the following items
  - Vulnerability result, Version name, etc
- SWPL request to contact person for each tool in DEV and ask them to update the tool management list.
- CSM obtain Tool Management Report
- CSGM reviews and update latest tool information

※ Please refer to the detail status of tool for CSMS below collaboration page.
- http://collab.lge.com/main/x/f21-Sg

Inputs

- Cybersecurity Tool Lists (Tool Management Report)

Outputs

- Cybersecurity Tool List (Tool Management Report) (refined)

Related standard

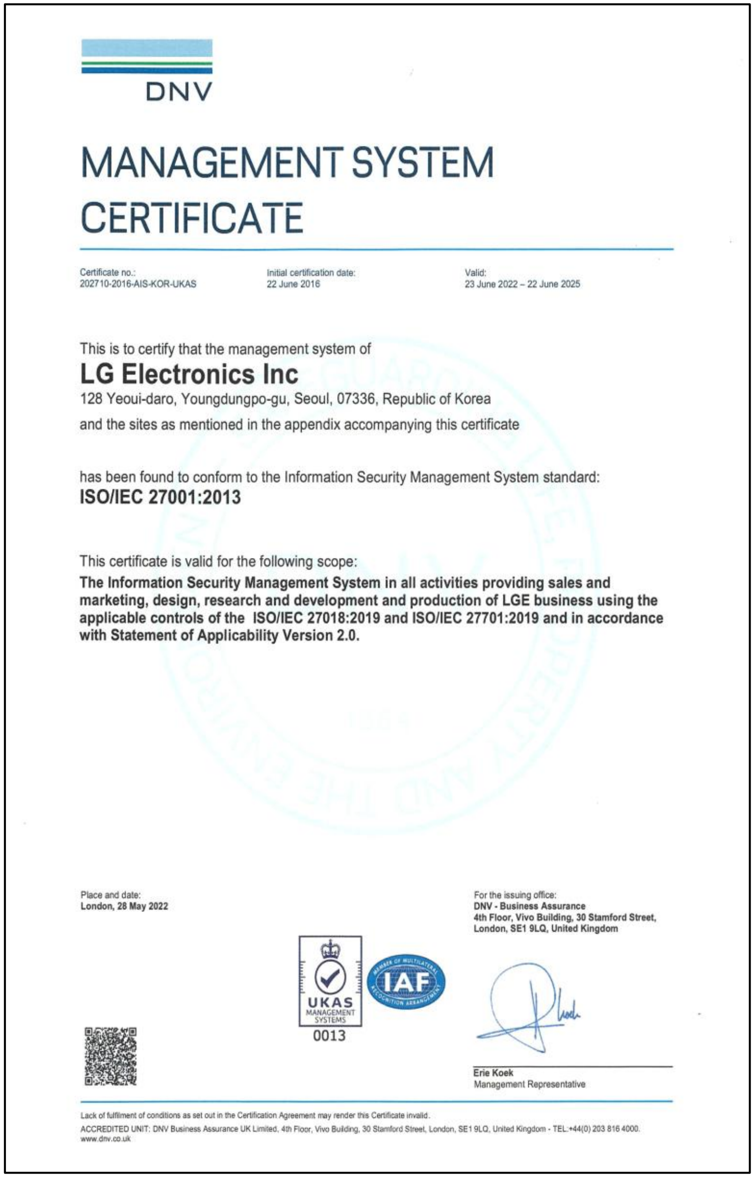
ISO/SAE 21434 – First edition:2021

Exit criteria [CSGM] CSGM reviews and update latest tool information.

M If you do not perform any mandatory process, you should have a reasonable rationale.

7-6. Information Security Management

◆ LG Electronics certified the Information Security Management System(ISO 27001).



DNV

MANAGEMENT SYSTEM CERTIFICATE

Certificate no.:	Initial certification date:	Valid:
202710-2016-AIS-KOR-UKAS	22 June 2016	23 June 2022 – 22 June 2025

This is to certify that the management system of

LG Electronics Inc

128 Yeoui-daro, Youngdungpo-gu, Seoul, 07336, Republic of Korea
and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Information Security Management System standard:
ISO/IEC 27001:2013

This certificate is valid for the following scope:
The Information Security Management System in all activities providing sales and marketing, design, research and development and production of LGE business using the applicable controls of the ISO/IEC 27018:2019 and ISO/IEC 27701:2019 and in accordance with Statement of Applicability Version 2.0.

Place and date:
London, 28 May 2022

UKAS MANAGEMENT SYSTEMS
0013

IAF

For the issuing office:
DNV - Business Assurance
4th Floor, Vivo Building, 30 Stamford Street,
London, SE1 9LQ, United Kingdom

Erie Koek
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.

ACCREDITED UNIT: DNV Business Assurance UK Limited, 4th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ, United Kingdom - TEL:+44(0) 203 816 4000.
www.dnv.co.uk

Information Security Regulation

[LG(10)-A-2151] LGE Information Security Regulations
[LG(10)-A-2152(7)] LGE Information Security Rules
[LG(10)-A-2153(7)] LGE Privacy Rules
[LG(10)-A-2152-05] 전사정보시스템(인프라) 보안 기준

LGE Information ecurity Regulation

LGE Information Security Rules

_GE Privacy Rules

Áα°¸½Ã½ºÅÛ(ÀÎÇÁ
¶ó)°¸¾È ±âÁØ

7. Adequate auditee determination

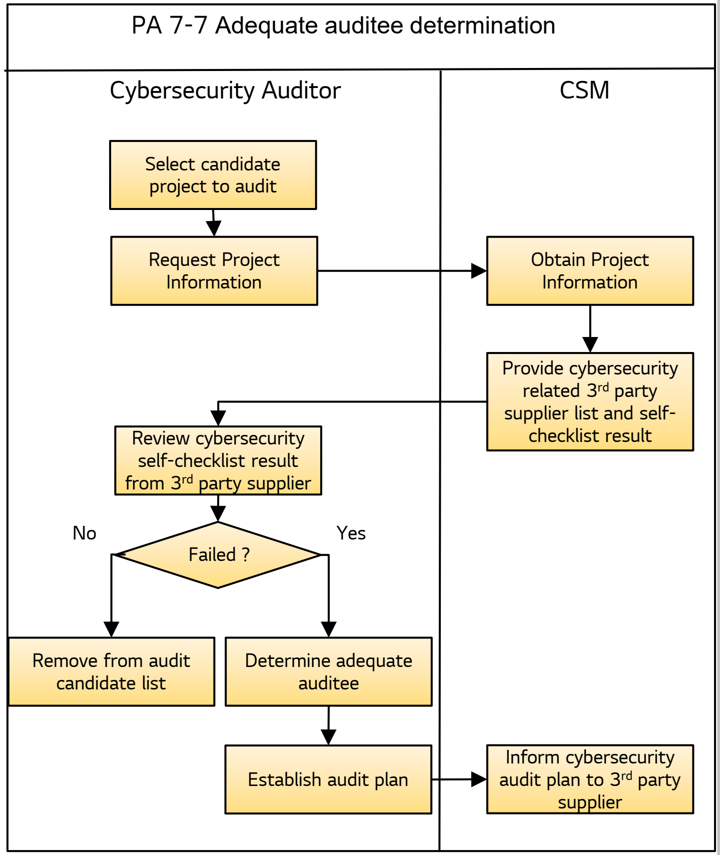
LGE Internal Use Only

Cybersecurity Audit

◆ The Cybersecurity Auditor determines project and 3rd party supplier list to audit

Entry criteria Initiating 3rd party supplier audit based on ISO PAS 5112.

Procedure



PA 7-7 Adequate auditee determination

Cybersecurity Auditor

CSM

Select candidate project to audit

Request Project Information

Obtain Project Information

Provide cybersecurity related 3rd party supplier list and self-checklist result

Review cybersecurity self-checklist result from 3rd party supplier

Failed ?

No

Yes

Remove from audit candidate list

Determine adequate auditee

Establish audit plan

Inform cybersecurity audit plan to 3rd party supplier

Detailed activity

[Description in detail]

- Cybersecurity Auditor performs PA 7-7 every quarter.
- Cybersecurity Auditor selects audit candidate project according to 'the condition' as written below
- Cybersecurity Auditor shall request project information to Cybersecurity Project Manager
- Cybersecurity Project Manager obtains project information, list cybersecurity related 3rd party suppliers and self-checklist result from 3rd party supplier
- Cybersecurity Auditor reviews cybersecurity activity self-checklist result from 3rd party supplier
- If the review result is failed, Cybersecurity Auditor determines the 3rd party supplier as adequate auditee
- If not, 3rd party supplier shall be removed from candidate list
- Once adequate 3rd party supplier auditee is determined, Cybersecurity Auditor will establish an audit plan
- Cybersecurity Project Manager shall inform cybersecurity audit plan to the auditee (3rd party supplier)

*'the condition' represents combination of conditions as following,

[1] Project, which is at DV phase or afterward

- However, audit could be conducted at CV phase according to priority of project

[2] Type of product

- Conduct audit per type of product at least once

[3] OEM

- Conduct audit per OEM at least once

* Precondition

- Cybersecurity relevance item shall be defined
- Cybersecurity Project Manager shall complete CIA with Tier 2 suppliers which has cybersecurity relevance item or component

Inputs

- CSMS Standard
- CSMS Policy
- CIA between LGE and 3rd party supplier

Outputs

- Auditee (project & 3rd party list)
- 3rd party supplier Cybersecurity audit plan

Related standard

- ISO/SAE 21434 – First edition:2021
- ISO 19011:2018
- IATF 16949
- ISO 9001
- ISO 26262

Exit criteria [Cybersecurity Auditor] After the audit is completed, an audit report should be issued that reflects audit findings.

M If you do not perform any mandatory process, you should have a reasonable rationale.

7-8. Organizational Cybersecurity Audit

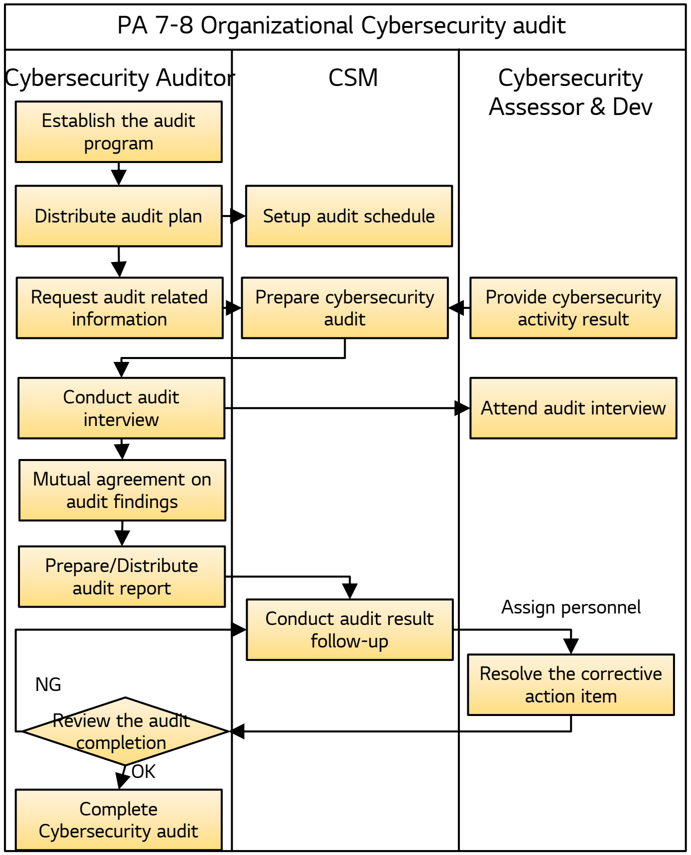
LGE Internal Use Only

Cybersecurity Audit

◆ The Cybersecurity Auditor conducts the audit of the automotive organization, in particular its Cybersecurity Management System

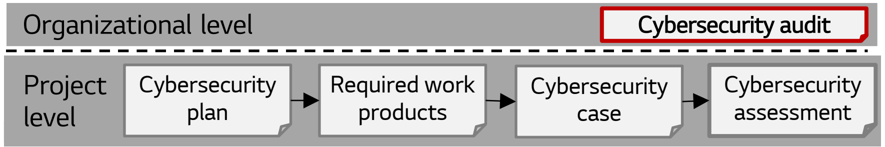
Entry criteria Initiating audit based on ISO PAS 5112.

Procedure


PA 7-8 Organizational Cybersecurity audit
Cybersecurity Auditor
CSM
Cybersecurity Assessor & Dev
Establish the audit program
Distribute audit plan
Setup audit schedule
Request audit related information
Prepare cybersecurity audit
Provide cybersecurity activity result
Conduct audit interview
Attend audit interview
Mutual agreement on audit findings
Prepare/Distribute audit report
Conduct audit result follow-up
Assign personnel
Resolve the corrective action item
NG
Review the audit completion
OK
Complete Cybersecurity audit

Detailed activity

The Cybersecurity audit is performed at an organizational level as below.



- Cybersecurity Auditor shall determine auditee according to PA 7-7
- Cybersecurity Auditor shall establish contact with auditee (Cybersecurity Project Manager)
- Cybersecurity Auditor shall mutually agree on audit scope and schedule with Cybersecurity Project Manager
- Cybersecurity Auditor distributes cybersecurity audit plan
- Cybersecurity Auditor requests audit related materials
- Cybersecurity Project Manager prepares the documented information for audit.
- Cybersecurity Auditor should conduct audit activities such as conducting opening meeting, communicating during audit, reviewing documented information, collecting and verifying information, interviewing Cybersecurity Assessor and generating audit findings
- Cybersecurity Auditor shares the audit findings with the auditee and mutual agreement on the audit findings shall be conducted
- Cybersecurity Auditor determines audit conclusion and conduct close meeting with the auditee.
- Cybersecurity Auditor distributes cybersecurity audit report.
- Cybersecurity Project Manager shall check the audit report and assign corrective action items to personnel.
- Developer(DEV) reviews and resolve action items and deliver them to Cybersecurity Project Manager.
- The Cybersecurity Auditor reviews whether any action items have been completed.

[Ensuring independence of Cybersecurity Auditor]
The Cybersecurity Auditor performing the audit shall ensure the independence required by ISO21434, 5.4.4, [RQ-05-11].

Inputs

- CSMS Standard
- CSMS Policy
- Assessment report

Outputs

- Cybersecurity audit plan
- Cybersecurity audit report
- Cybersecurity corrective action report

Related standard

- ISO/SAE 21434 – First edition:2021
- ISO 19011:2018
- IATF 16949
- ISO 9001
- ISO 26262

Exit criteria [**Cybersecurity** Auditor] After the audit is completed, a audit report should be issued that reflects the audit findings.

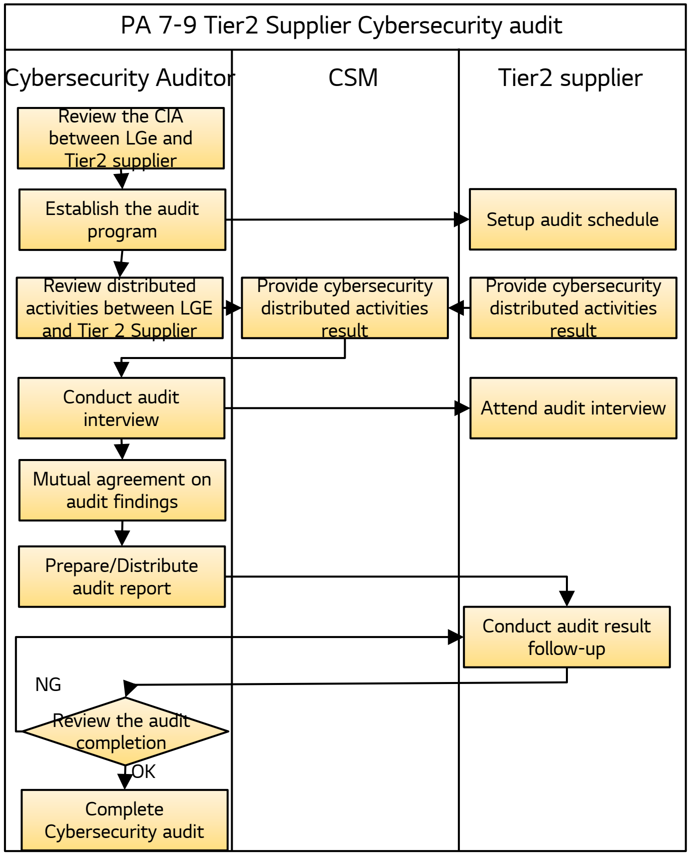
M If you do not perform any mandatory process, you should have a reasonable rationale.

7-9. Tier2 Supplier Cybersecurity Audit

◆ The Cybersecurity Auditor conducts the tier2 supplier audit, in particular its Cybersecurity Management System

Entry criteria Initiating audit based on ISO PAS 5112.

Procedure


PA 7-9 Tier2 Supplier Cybersecurity audit
Cybersecurity Auditor
CSM
Tier2 supplier
Review the CIA between LGe and Tier2 supplier
Establish the audit program
Setup audit schedule
Review distributed activities between LGE and Tier 2 Supplier
Provide cybersecurity distributed activities result
Provide cybersecurity distributed activities result
Conduct audit interview
Attend audit interview
Mutual agreement on audit findings
Prepare/Distribute audit report
Conduct audit result follow-up
NG
Review the audit completion
OK
Complete Cybersecurity audit

Detailed activity

[Description in detail]

- Cybersecurity Auditor shall determine auditee according to PA 7-7
- Cybersecurity Auditor shall establish contact with auditee (Cybersecurity Project Manager and Tier2 Supplier)
- Cybersecurity Auditor shall mutually agree on audit scope and schedule with Cybersecurity Project Manager and Tier2 Supplier
- Cybersecurity Auditor distributes cybersecurity audit plan
- Cybersecurity Auditor requests audit related materials
- Cybersecurity Project Manager prepares the documented information for audit.
- Tier2 Supplier prepares the documented information for audit.
- Cybersecurity Auditor should conduct audit activities such as conducting opening meeting, communicating during audit, reviewing documented information, collecting and verifying information, interviewing Tier2 Supplier and generating audit findings
- Cybersecurity Auditor shares the audit findings with the auditee and mutual agreement on the audit findings shall be conducted
- Cybersecurity Auditor determines audit conclusion and conduct close meeting with the auditee.
- Cybersecurity Auditor distributes cybersecurity audit report.
- Tier2 Supplier shall review the audit report and resolve action items and deliver them to LGe
- The Cybersecurity Auditor reviews whether any action items have been completed.

Inputs

- CSMS Standard
- Assessment report
- CIA between LGE and 3rd party supplier
- Tier2 self-checklist result

Outputs

- Cybersecurity audit plan
- Cybersecurity audit report
- Cybersecurity corrective action report

Related standard

- ISO/SAE 21434 – First edition:2021
- ISO 19011:2018
- IATF 16949
- ISO 9001
- ISO 26262

Exit criteria [Cybersecurity Auditor] After the audit is completed, a audit report should be issued that reflects the audit findings.

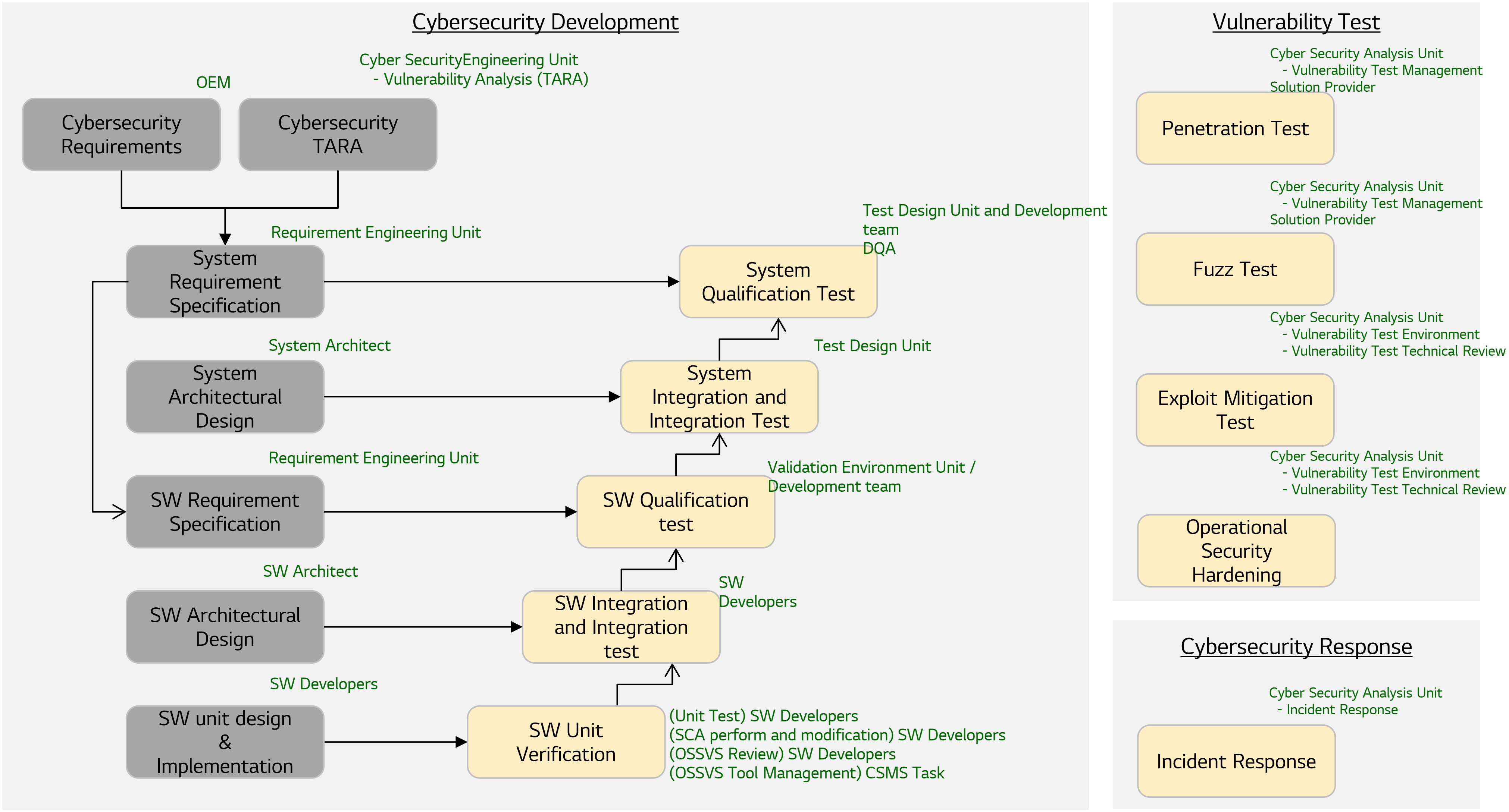
M If you do not perform any mandatory process, you should have a reasonable rationale.

G 1. Cybersecurity Product Development Role & Responsibility

Guidelines

◆ Each test manager shall be agreed with OEM about the test plan.

◆ Role guidelines



Cybersecurity Development

OEM

Cyber SecurityEngineering Unit
- Vulnerability Analysis (TARA)

Cybersecurity Requirements

Cybersecurity TARA

Requirement Engineering Unit

System Requirement Specification

Test Design Unit and Development team
DQA

System Qualification Test

System Architect

System Architectural Design

Test Design Unit

System Integration and Integration Test

Requirement Engineering Unit

SW Requirement Specification

Validation Environment Unit / Development team

SW Qualification test

SW Architect

SW Architectural Design

SW Developers

SW Integration and Integration test

SW Developers

SW unit design & Implementation

SW Unit Verification

(Unit Test) SW Developers
(SCA perform and modification) SW Developers
(OSSVS Review) SW Developers
(OSSVS Tool Management) CSMS Task

Vulnerability Test

Cyber Security Analysis Unit
- Vulnerability Test Management
Solution Provider

Penetration Test

Cyber Security Analysis Unit
- Vulnerability Test Management
Solution Provider

Fuzz Test

Cyber Security Analysis Unit
- Vulnerability Test Environment
- Vulnerability Test Technical Review

Exploit Mitigation Test

Cyber Security Analysis Unit
- Vulnerability Test Environment
- Vulnerability Test Technical Review

Operational Security Hardening

Cybersecurity Response

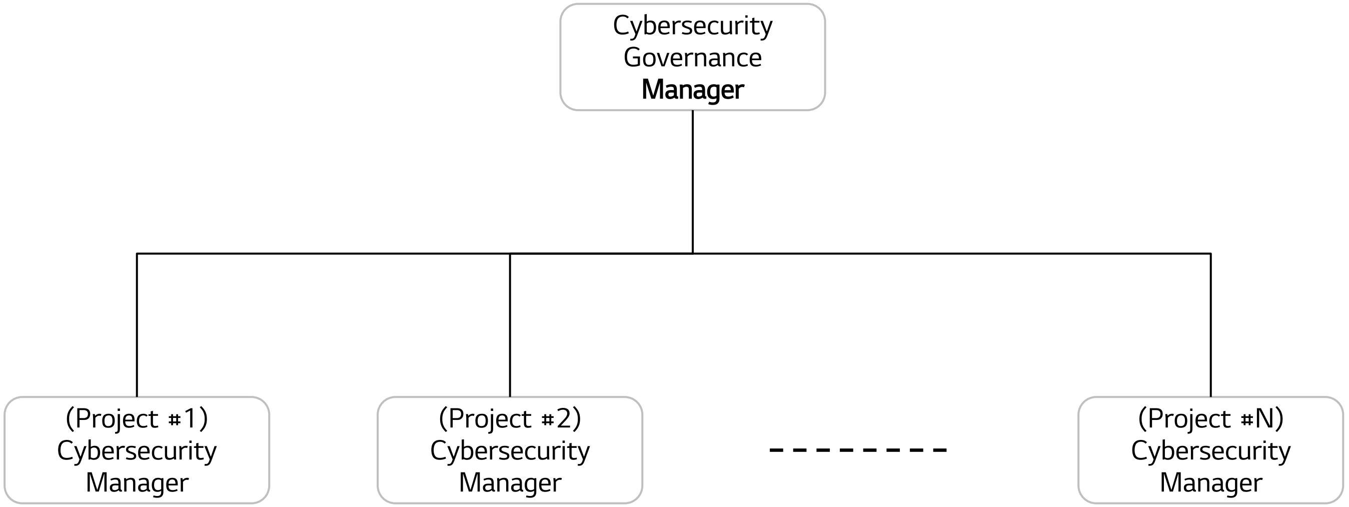
Cyber Security Analysis Unit
- Incident Response

Incident Response

2. Cybersecurity Governance Manager and Cybersecurity Manager Roles

◆ For in compliance with the Global Cybersecurity Regulation, the Cybersecurity Manager shall manage the cybersecurity plan and communicate with OEM.

◆ Role guidelines



Cybersecurity Governance **Manager**

(Project #1) Cybersecurity Manager

(Project #2) Cybersecurity Manager

(Project #N) Cybersecurity Manager

Role	Activity guide
Cybersecurity Governance Manager	Cybersecurity Manager shall manage the cybersecurity activities for all projects in compliance with the Cybersecurity Regulations(UNECE WP.29, ISO/SAE 21434, and etc.). Cybersecurity Manager shall distribute the overall cybersecurity plan, organization-specific rules, and processes to Cybersecurity Manager. - enable the implementation of the requirements of Cybersecurity Regulations; and - support the execution of the corresponding activities. Cybersecurity Manager shall ensure the persons within the organization that are involved in cybersecurity have the competencies and awareness to fulfill their responsibilities.
Cybersecurity Manager	Cybersecurity Manager shall manage the cybersecurity activities for the project in compliance with the CSMS standard. - Review activities based on the Cybersecurity Plan to share them with OEM. - If received any request to improve activity in compliance with OEM cybersecurity regulation, Project Cybersecurity Manage needs to clarify the request by OEM and request it to PL. - After complete to improve it, Cybersecurity Manager review improved activity and work-product and submit or present it to OEM. Cybersecurity Manager establishes and updates the Cybersecurity Plan[1] during the project development. - Project Cybersecurity items(requirements, design, and test) must be included in the general SW Development Process and they shall be shared with related stakeholders. Cybersecurity Manager performs the meeting with OEM at the time agreed with OEM and presents the status of the cybersecurity to OEM.

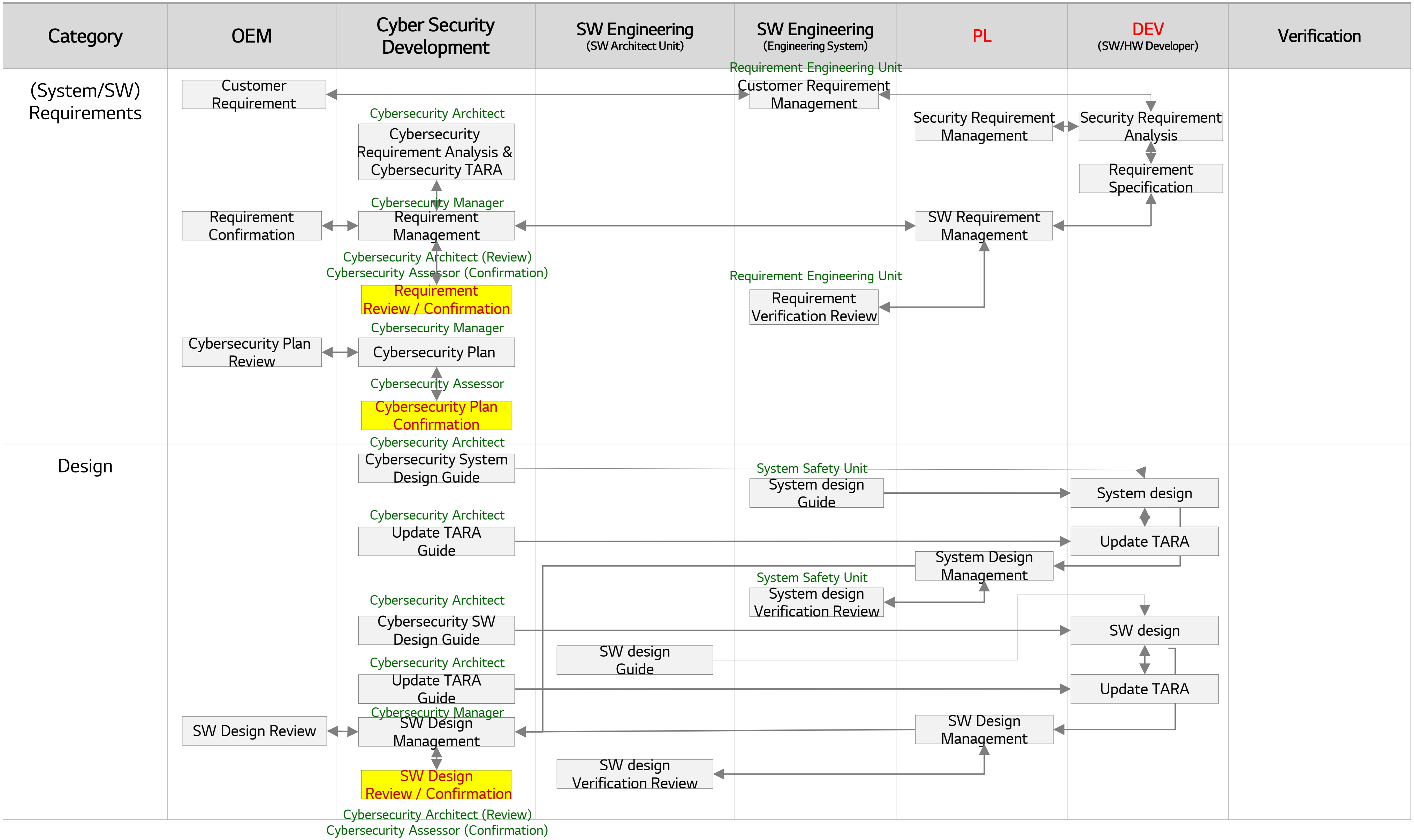
[1] The Cybersecurity Plan can be included in the Project Management Plan.

G 3. Cybersecurity Development Detail Activities (1/2)

Guidelines

Activities

Confirmation (Assessment)



Category

OEM

Cyber Security Development

SW Engineering (SW Architect Unit)

SW Engineering (Engineering System)

PL

DEV (SW/HW Developer)

Verification

(System/SW) Requirements

Customer Requirement

Requirement Engineering Unit

Customer Requirement Management

Cybersecurity Architect

Cybersecurity Requirement Analysis & Cybersecurity TARA

Security Requirement Management

Security Requirement Analysis

Requirement Specification

Requirement Confirmation

Cybersecurity Manager

Requirement Management

SW Requirement Management

Cybersecurity Architect (Review)

Cybersecurity Assessor (Confirmation)

Requirement Review / Confirmation

Requirement Engineering Unit

Requirement Verification Review

Cybersecurity Plan Review

Cybersecurity Manager

Cybersecurity Plan

Cybersecurity Assessor

Cybersecurity Plan Confirmation

Design

Cybersecurity Architect

Cybersecurity System Design Guide

System Safety Unit

System design Guide

System design

Cybersecurity Architect

Update TARA Guide

Update TARA

System Design Management

System Safety Unit

System design Verification Review

Cybersecurity Architect

Cybersecurity SW Design Guide

SW design

SW design Guide

Cybersecurity Architect

Update TARA Guide

Update TARA

SW Design Review

Cybersecurity Manager

SW Design Management

SW Design Management

SW design Verification Review

SW Design Review / Confirmation

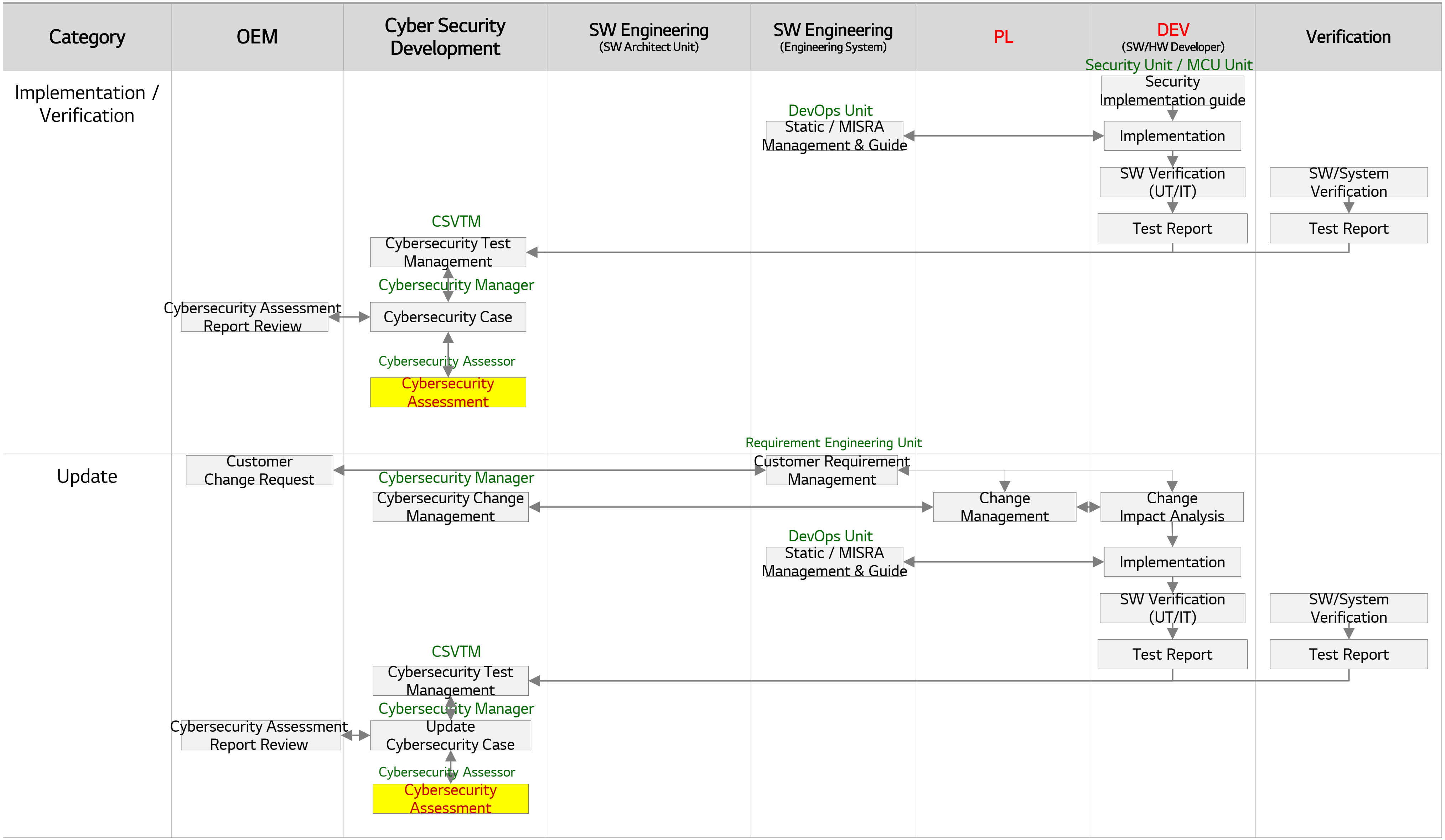
Cybersecurity Architect (Review)

Cybersecurity Assessor (Confirmation)

G 3. Cybersecurity Development Detail Activities (2/2)

Guidelines

Activities	Confirmation (Assessment)



Category	OEM	Cyber Security Development	SW Engineering (SW Architect Unit)	SW Engineering (Engineering System)	PL	DEV (SW/HW Developer)	Verification
Implementation / Verification	Cybersecurity Assessment Report Review	CSVTM Cybersecurity Test Management Cybersecurity Manager Cybersecurity Case Cybersecurity Assessor Cybersecurity Assessment		DevOps Unit Static / MISRA Management & Guide		Security Unit / MCU Unit Security Implementation guide Implementation SW Verification (UT/IT) Test Report	SW/System Verification Test Report
Update	Customer Change Request Cybersecurity Assessment Report Review	Cybersecurity Manager Cybersecurity Change Management CSVTM Cybersecurity Test Management Cybersecurity Manager Update Cybersecurity Case Cybersecurity Assessor Cybersecurity Assessment		Requirement Engineering Unit Customer Requirement Management DevOps Unit Static / MISRA Management & Guide	Change Management	Change Impact Analysis Implementation SW Verification (UT/IT) Test Report	SW/System Verification Test Report

G 4. Management of cybersecurity issues (1/4)

❑ Classification of Cybersecurity issues

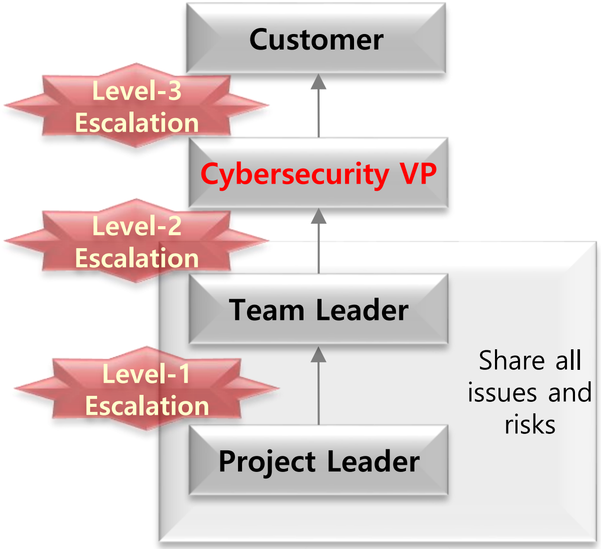
- Cybersecurity issues can be categorized into General Cybersecurity Issues and General/Emergency Cybersecurity Incident issues. The three types of issues have different escalation mechanisms.

Type of Issues	Description
General Cybersecurity issues	Issues that reported during product development.
General Cybersecurity incident issues	Issues that reported from Threat Monitoring Source listed at http://collab.lge.com/main/x/MIfMUQ General Cybersecurity Incident issues do not meet the Emergency Cybersecurity Incident Issue criteria.
Emergency Cybersecurity incident issues	Issues that reported from Threat Monitoring Source listed at http://collab.lge.com/main/x/MIfMUQ Ex) In case, a CVSS Severity Critical (Score 9.0-10.0) or higher vulnerability or a vulnerability affecting your product is disclosed in the media.

G 4. Management of cybersecurity issues (2/4)

Guidelines

❑ General Cybersecurity issues



Level	Report to	Escalation Criteria	Escalation Method
Level-3	Customer	Unresolved issues for Over 4 weeks since reported.	Conference Call / Email and recorded at VLM for each project.
Level-2	Cybersecurity VP	Unresolved issues for Over 3 weeks since reported.	
Level-1	Team Leader	Unresolved issues for over 1 week since reported.	

- General issues including Cybersecurity issues follow the escalation mechanism described at the Project Monitoring and Control Plan in PMP document for each projects.
- If an issue is not resolved(there is no analysis result or patch) until a certain period of time after it is opened to the person in charge, it is escalated and the issue level rises.

G 4. Management of cybersecurity issues (3/4)

❑ General Cybersecurity incident issues

- For General Cybersecurity incident issues, Escalation mechanism is as follow.

<table>
<tr><th>Level</th><th colspan="2">Key Members</th><th>Due Time</th></tr>
<tr><td>Level 4</td><td colspan="2">Customer</td><td>4 weeks</td></tr>
<tr><td>Level 3</td><td colspan="2">Cyber Security VP</td><td>3 weeks</td></tr>
<tr><td rowspan="2">Level 2</td><td>Before SOP</td><td>After SOP</td><td rowspan="2">2 weeks</td></tr>
<tr><td>PL / SW PL
HW PL
Cybersecurity Management Unit Leader</td><td>Cybersecurity Management Unit Leader</td></tr>
<tr><td>Level 1</td><td colspan="2">Cybersecurity Analysis Unit Leader</td><td>1 week</td></tr>
</table>

- **Issues corresponding to General Cybersecurity Incidents follow the Incident Response Management Process.**
  Incident Response Management Process- http://collab.lge.com/main/x/Ys1PWg
- **General Cybersecurity Incident issues do not meet the Emergency Cybersecurity Incident Issue criteria.**
- **When spreading an incident issue, for projects under development, the escalation mechanism follows the Before SOP at level 2.**

4. Management of cybersecurity issues (4/4)

❑ **Emergency Cybersecurity incident issues**

- For Emergency Cybersecurity incident issues, Escalation mechanism is as follow.

<table>
<tr><th>Level</th><th colspan="2">Key Members</th><th>Due Time</th></tr>
<tr><td>Level 4</td><td colspan="2">Customer</td><td>7 Working days</td></tr>
<tr><td>Level 3</td><td colspan="2">Cyber Security VP</td><td>5 Working days</td></tr>
<tr><td rowspan="2">Level 2</td><td>Before SOP</td><td>After SOP</td><td rowspan="2">2 Working days</td></tr>
<tr><td>PL / SW PL
HW PL
Cybersecurity Management Unit Leader</td><td>Cybersecurity Management Unit Leader</td></tr>
<tr><td>Level 1</td><td colspan="2">Cybersecurity Analysis Unit Leader</td><td>1 Working day</td></tr>
</table>

- Issues corresponding to Emergency Cybersecurity Incidents follow the Incident Response Management Process.
  Incident Response Management Process- http://collab.lge.com/main/x/Ys1PWg
- Before SOP, General/Emergency Cybersecurity incident issues are handled by the General Cybersecurity incident issue mechanism.
- As a result of the initial analysis of the Emergency Cybersecurity Incidents issue, if the vulnerability caused by LGE developed function the TARA is performed.
  Incident response & TARA- http://collab.lge.com/main/x/9Ceogg
- Emergency cybersecurity incident issues are recorded at VLM
  - http://vlm.lge.com/issue/projects/CSIM/

G 5. Cybersecurity Requirement and Documentation Management

❑ Requirement Management

- All project development requirements, including cyber security requirements for LGE's projects, are managed using codeBeamer.
  For the description of codeBeamer, refer to the following page. http://collab.lge.com/main/x/L3GIlg
- For a project that does not use codeBeamer, a separate space such as project development collab and vlm can be used.
- Only members with access rights of a specific project can view Requirement of the project, and the access rights are managed by the administrator of the project development team.

❑ Documentation Management

- For guidelines and templates for cyber security activities required during product development, refer to the following page.
  http://collab.lge.com/main/x/fW1-Sg
- The project-dependent cybersecurity document created using the template is stored in the project team's repository. This can be a collab or VLM, and the specific details follow the project team's guide.
- The access rights of these documents are managed by the administrator of the project development team.

A 1. Tailoring Guide

◆ Objective of 'Tailoring Guide'

This guide is for defining project process that is appropriate for each project characteristics based on the 'VS C는 standard Process' and organization standard process.

Tailoring scope and methods shall be described and applied.

※ Follow the customer specific process if there was an agreement to use it.

◆ Tailoring Procedure

1) Analyze Project Information

- Analyze project information to derive project characteristics and identify areas for tailoring.
- Check if 'activity / work product' based tailoring is required.

2) Review tailoring result

- Share and discuss tailoring scope and items with CSMS Task.
- Create and share mutually consulted review results.
- If necessary, share the review results to supervising manager and get approval.

3) Request 'Process Improvement' (if required)

- If 'Process Improvement' is required, create an issue using the 'Process Improvement request system'. (click to system)