

DEKRA DIGITAL

Training ISO/SAE 21434

A black and white photograph of a long, straight road stretching towards snow-capped mountains under a cloudy sky. The road is a two-lane asphalt highway with a double white line down the center and single white lines on the shoulders. The landscape is arid with low-lying shrubs and grasses. In the distance, a range of mountains is visible, with significant snow cover on their peaks and upper slopes. The sky is filled with dramatic, layered clouds.

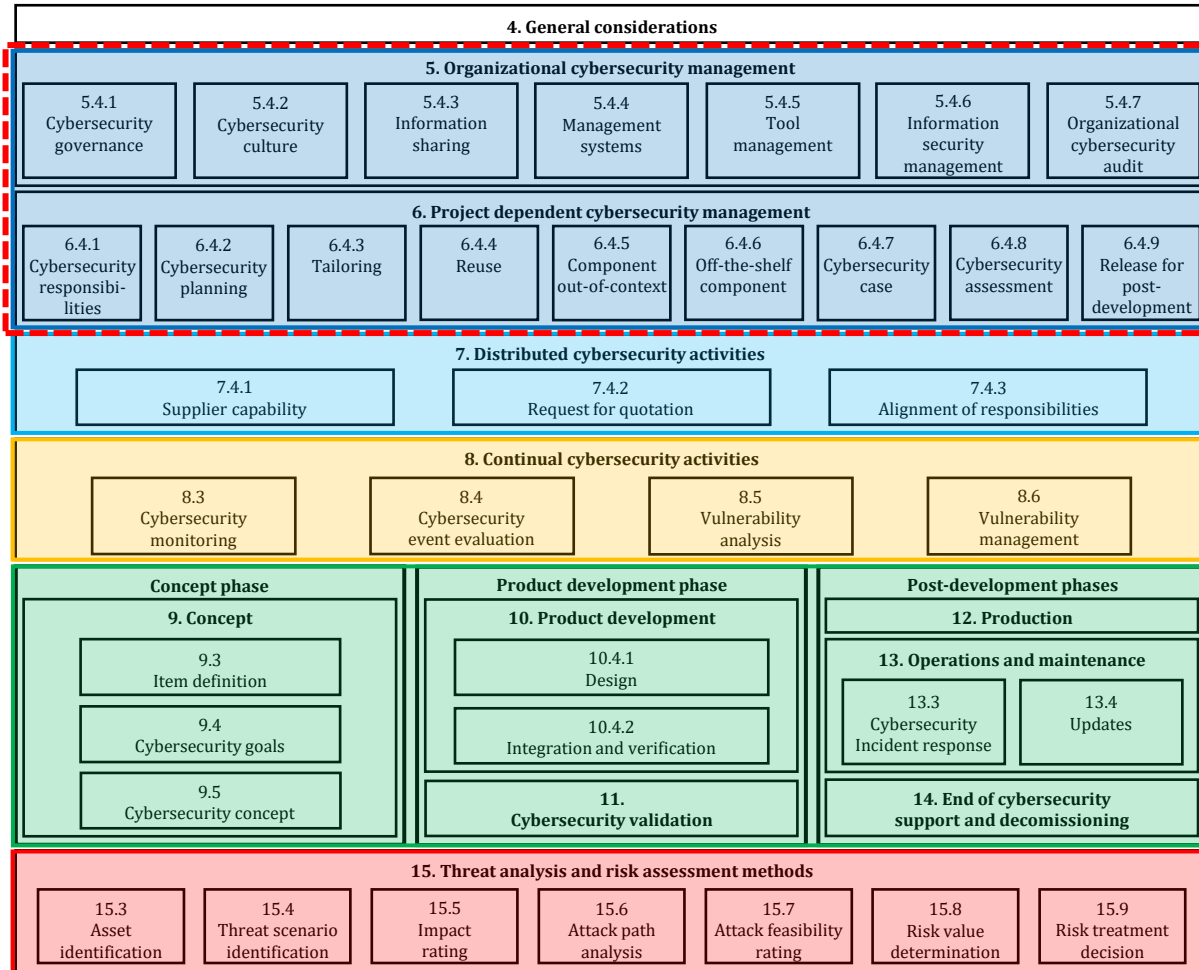
Project Dependent Management Activities

CONTENT

1. **Introduction**
2. **Cybersecurity Plan**
3. **Tailoring**
4. **Reuse**
5. **Component Out-Of-Context**
6. **Component Off-The-Shelf**
7. **Cybersecurity Case**
8. **CS Assessment & Conditions for Release**
9. **Summary**

1. INTRODUCTION

Structure of ISO/SAE 21434



Overall & project specific management processes (similar to ISO 26262)

- Management systems
- Policies
- Preparation for assessment

Distributed CS activities

- Define interfaces between customer, supplier, third parties.

Continuous CS activities

- Requirements for continuous monitoring of CS relevant information
- Framework for analysis and management of vulnerabilities

Concept, development and post-development

- Add-on of CS relevant activities during concept and development
 - Establishment of CS goals and requirements
 - TARA and vulnerability analysis during development
- Consideration of post-development requirements (during or after production, decommissioning ...)
- Definition of post-development processes (production, incident response, update)

TARA (Threat Analysis and Risk Assessment)

- Describes the steps to perform a robust risk analysis on the system
- Complex process to be performed multiple times and for multiple assets

Definitions

Reuse

- Using an existing developed item again for another development, with or without modifications to the item, component, or operational environment.

Out-of-context

- Component which has been developed as a generic component prior to engagement or commercial agreement with the customer
- The supplier can only make assumptions about the context and intended use (i.e., microcontroller).

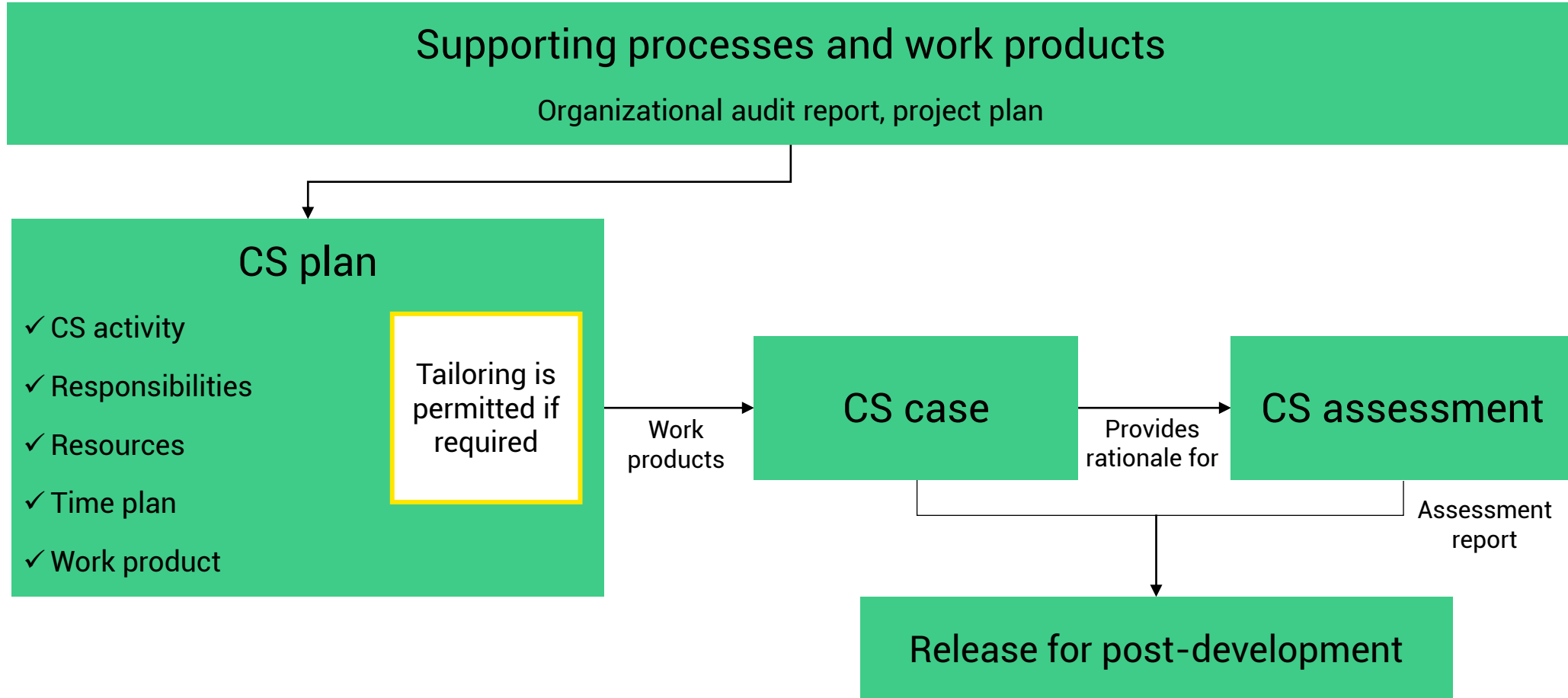
Off-the-shelf

- Component “ready to use” that doesn’t need modification
- It might not have been developed in accordance with this document (i.e., 3rd party library).

Tailoring

- An activity is tailored if it is omitted or performed in a different manner compared to its description in this document

Blueprint



Objectives

This section covers the planning of cybersecurity activities, with a focus on requirements for managing cybersecurity development activities for specific projects (includes possible tailoring)

- Assign responsibilities for cybersecurity activities
- Plan cybersecurity activities
- Create a cybersecurity case that provides the argument for the level of cybersecurity achieved
- If necessary, conduct a cybersecurity assessment
- Decide whether the item or component can be released for post-development

2. CYBERSECURITY PLAN

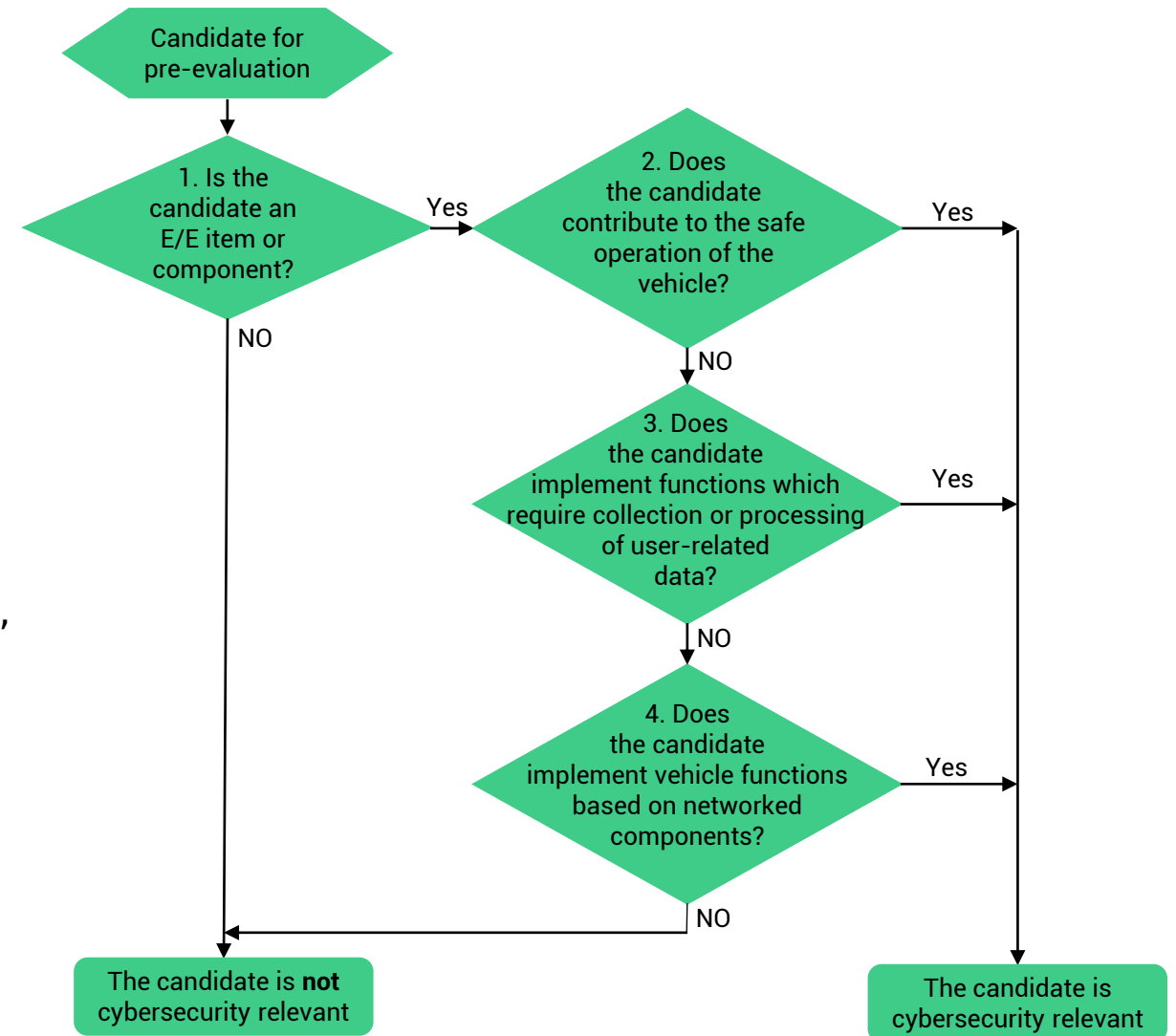
CS Plan

The cybersecurity plan is a document describing the activities which will be performed to fulfil the requirements of the ISO/SAE 21434

Precondition:

The item or component should be analyzed to determine cybersecurity activities

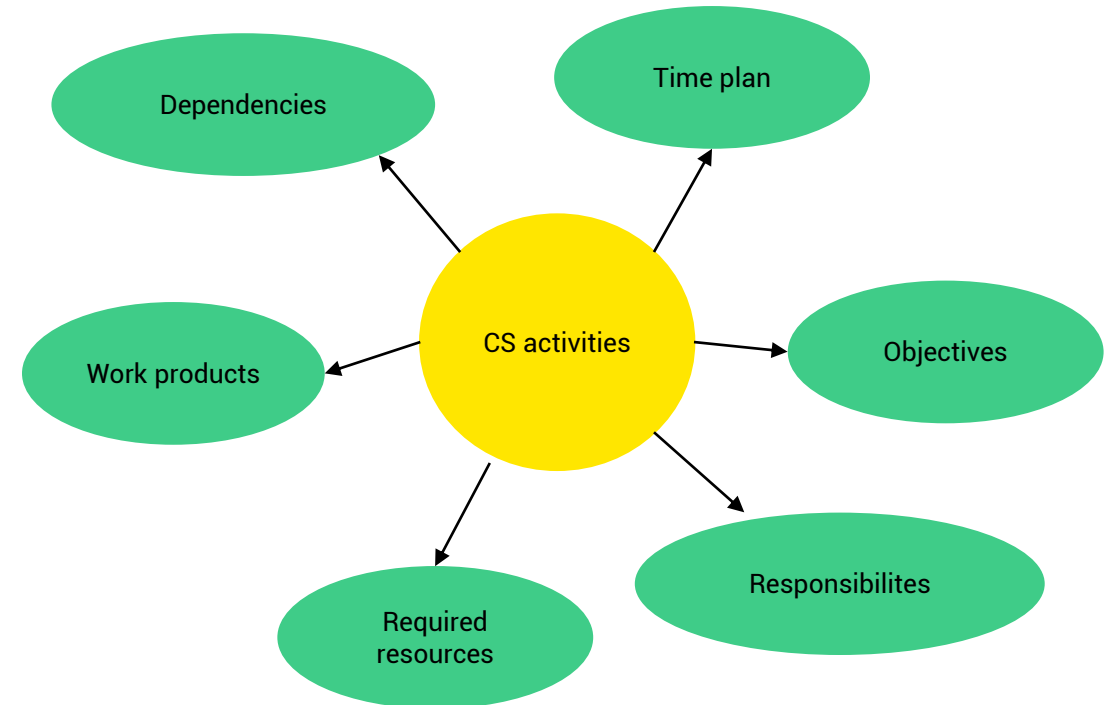
- Item is checked to see if it is relevant to CS; if not, it is omitted from the planning
- If the item is relevant, additional checks are performed, to see if it is reused, newly developed, or tailored



Key Requirements - CS Plan

Key Requirements (1)

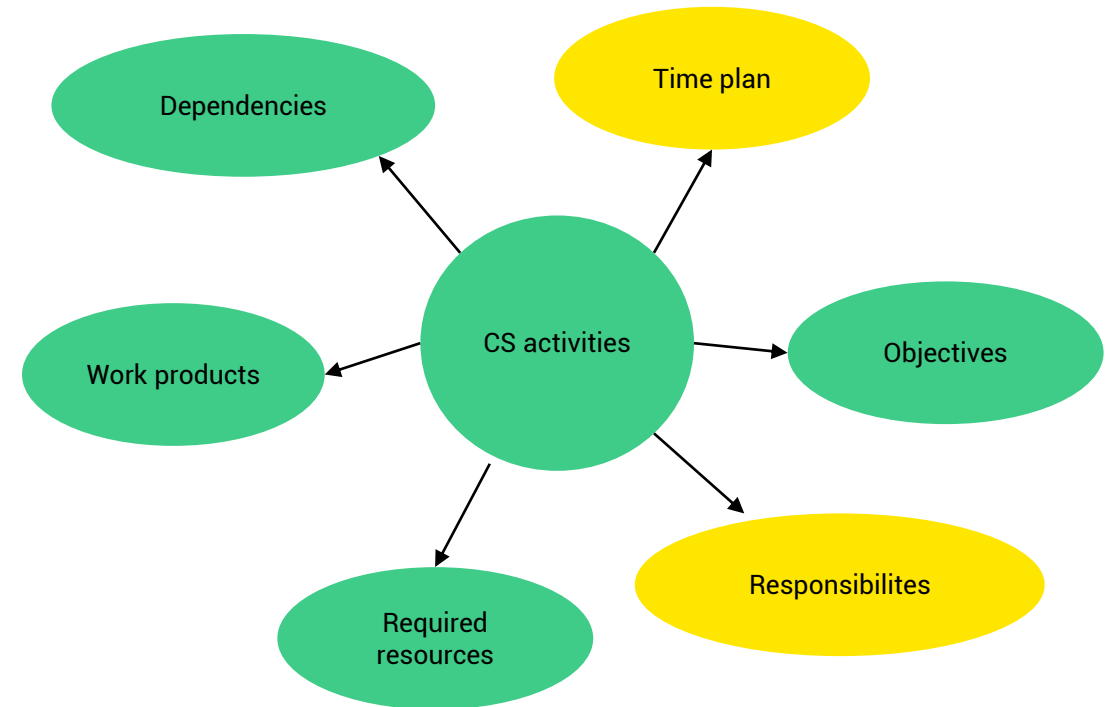
- Determination of CS objective for each phase of the product lifecycle
 - Process for creation of CS objectives
 - Clear objectives for all the CS activities should be defined
- Determination and assignment of work products resulting from each CS activity
 - Work products must be maintained and updated
 - Work products requires configuration, change, requirements and documentation management



Key Requirements - CS Plan

Key Requirements (2)

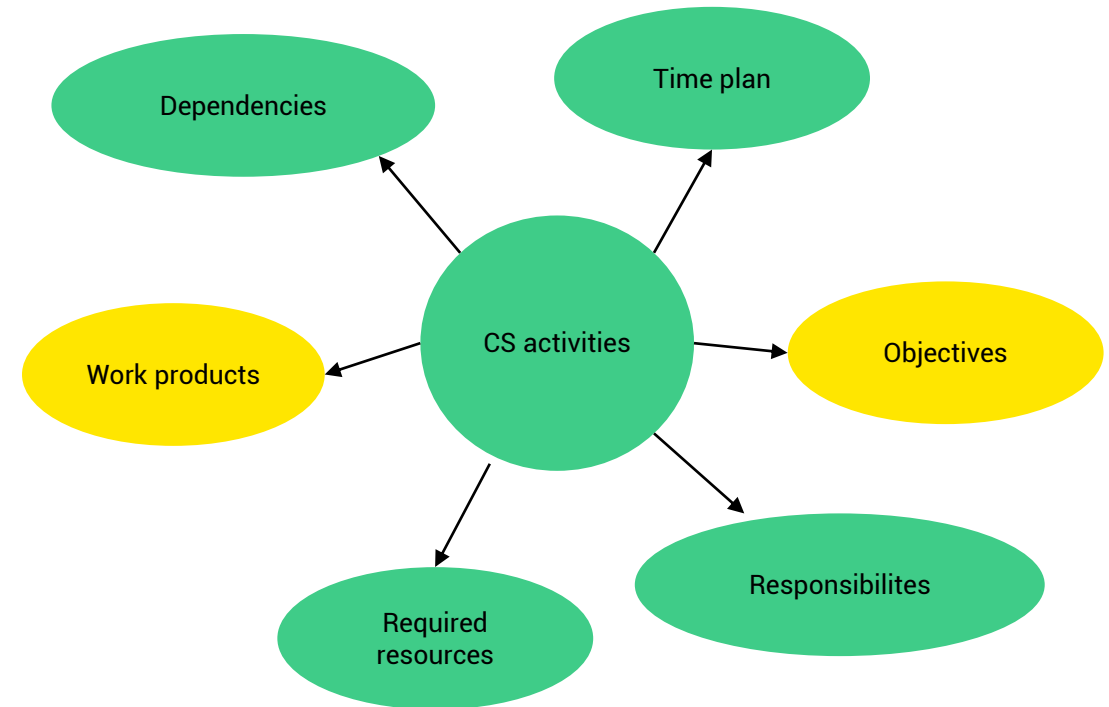
- Responsibilities for the project's CS activities must be assigned and communicated
- There should be someone in charge of coordinating the project's CS activities
- Other roles in the project that perform CS activities should be addressed
- Responsibilities for maintaining and tracking CS activities should be assigned
- The project's start and end dates, as well as milestones, should be determined



Key Requirements - CS Plan

Key Requirements (3)

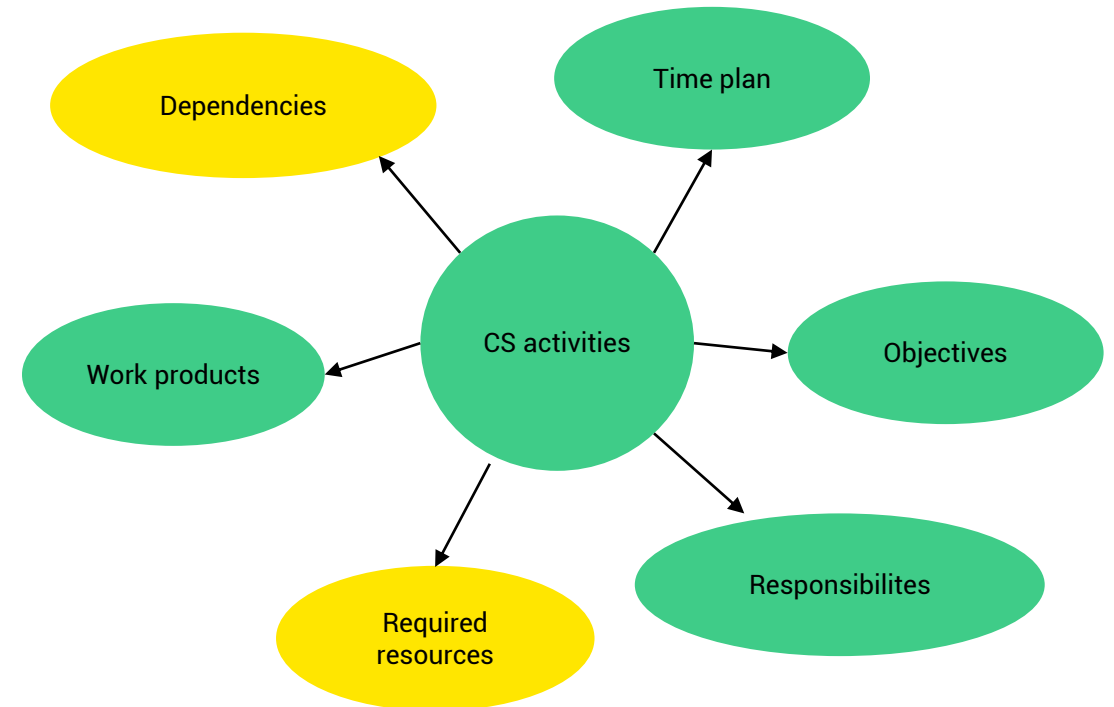
- Determination of CS objective for each phase of the product lifecycle
 - Process for creation of CS objectives
 - Clear objectives for all the CS activities should be defined
- Determination and assignment of work products resulting from each CS activity
 - Work products must be maintained and updated
 - Work products requires configuration, change, requirements and documentation management



Key Requirements - CS Plan

Key Requirements (4)

- Resource allocation for performing CS activities should be specified
 - For example, proper infrastructure, training, software tools, skilled staff etc.
- Determination of dependencies with other activities should be clearly stated in the plan
 - For example, dependencies between safety and security



Excerpt of a Generic Cybersecurity Plan

Cybersecurity Plan

S.no	Phase	Activity ID	Activity Name	Reference Documents	Input	Output	ISO/SAE 21434 Work products	Location of Deliverables	Person in Charge	Resources Required	Expected start	Expected completion	
1	Concept	CS001	Item Analysis	<<insert name and location of the process guideline explaining this activity>>	Initial idea, data on existing products	Item analysis report	NA	<<insert where to find the workproducts from the activity>>	John Doe	<< insert data on required resources and experts>>	DD-MM-YYYY	DD-MM-YYYY	
2		CS002	Item definition	<<insert name and location of the process guideline explaining this activity>>	Item analysis	Item definition	[WP-09-01] Item definition [WP-06-01] Cybersecurity plan (*update CS plan with activities such as reuse analysis)	<<insert where to find the workproducts from the activity>>	John Doe	<< insert data on required resources and experts>>	DD-MM-YYYY	DD-MM-YYYY	
3		CS003	Reuse analysis	<<insert name and location of the process guideline explaining this activity>>	Item definition, documentation of existing item	Reuse analysis report	Reuse analysis	<<insert where to find the workproducts from the activity>>	John Doe	<< insert data on required resources and experts>>	DD-MM-YYYY	DD-MM-YYYY	
4		C004	Cybersecurity goals										
5		C005	Verification of CS goals										
6		C006	Cybersecurity Concept										
7		C007	Verification of CS concept										
8	Design and Development	C008	Identify system level CS Specifications										
9		C009	...										
10		C010	...										

3. TAILORING

Tailoring

- Tailoring means adjusting CS activities or omitting them entirely

Key Requirements - Tailoring

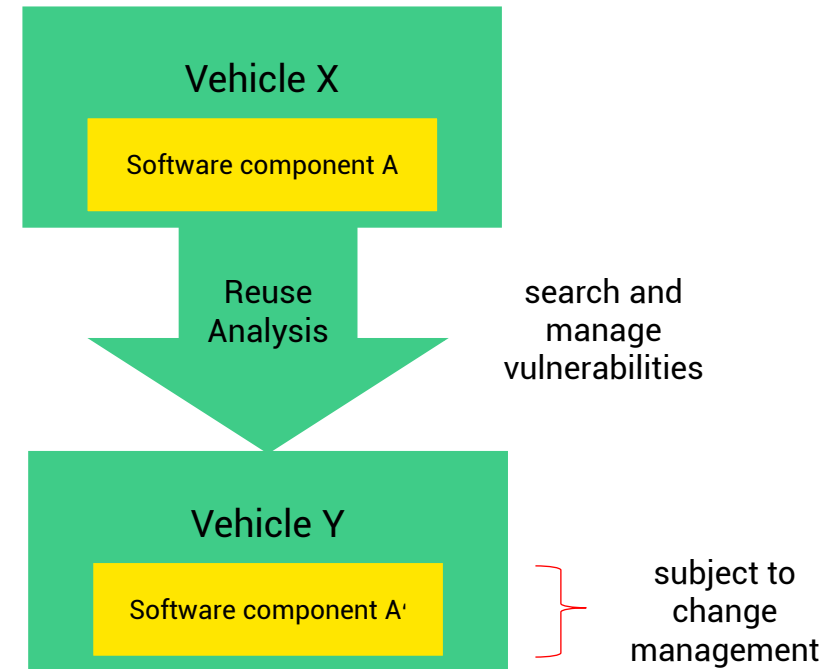
Key Requirements

- Tailoring is permitted if it is explained, justified and outlined in the CS plan
- Examples of when tailoring can be used include:
 - Reuse of item or component
 - When developing components out-of-context based on assumptions
 - Use of an off-the-shelf component
 - Different approaches for risk assessment

4. REUSE

Reuse

- A reuse analysis should be performed on a newly developed item or component
- This includes, modification plan, different use cases with or without modifications
 - Modifications can be related to design, implementation, requirement etc.
 - Identification of modifications
 - CS implications of the modifications
 - Specification of CS activities
- Reuse analysis should also include the evaluation result, which should state whether the specific component meets the CS requirement of the and can be used



5. COMPONENT OUT-OF-CONTEXT

Component Out-Of-Context

- Organizations that develop and manufacture automotive components typically produce generic components for a wide range of applications
- These generic components are based on assumptions about the vehicle's applications
- As a result, these components are referred to as components out of context (i.e., microcontrollers)

Key Requirements - Component Out-Of-Context

- Assumptions for the use and context of the component out of context should be documented
 - Including external interfaces of the component
 - After context definition the CS activities should be performed
- Component out-of-context should be analyzed before integration with other components
 - CS claims and assumptions must be validated before integration

6. COMPONENT OFF-THE-SHELF

Off-The-Shelf Component

- An off-the-shelf component is one that is not developed for a specific customer or application
- It is a ready to use component which does not require any changes to its design or implementation
- This component may not have been developed in accordance with ISO/SAE 21434

Key Requirements - Off-The-Shelf Component

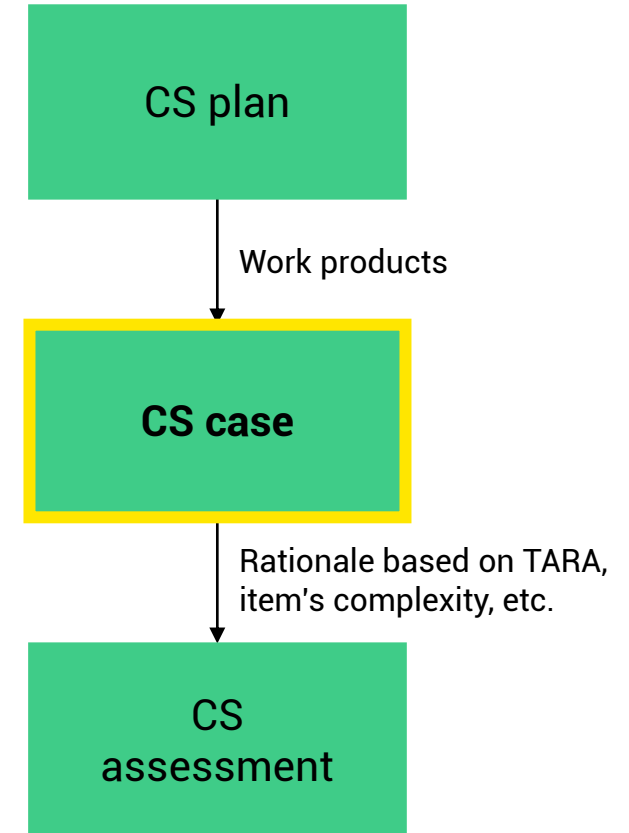
- CS related information should be collected when using an off-the-shelf component to determine the following cases
 - It is a suitable application
 - The documents provided are sufficient and
 - It can comply with CS requirements according to ISO/SAE 21434 or not
- If the component is not allowed for integration after analysis, then CS activities should be identified and performed in accordance with ISO/SAE 21434

7. CYBERSECURITY CASE

Cybersecurity Case

The CS case is a document that gathers all the evidence to demonstrate the achieved level of cybersecurity

- CS case must be prepared to present an argument for the cybersecurity of the item or component, supported by work products
 - Work products from the CS plan are gathered in the CS case
 - In distributed development, the CS case can be a combination of the CS cases of all partners involved

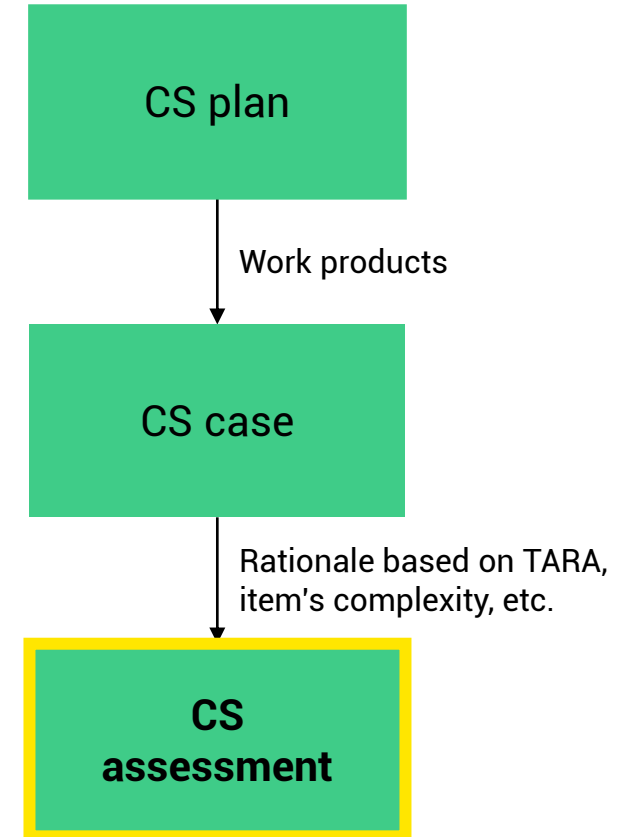


- 
- **How to evaluate the cybersecurity case according to ISO/SAE 21434 requirements?**

8. CS ASSESSMENT AND CONDITIONS FOR RELEASE

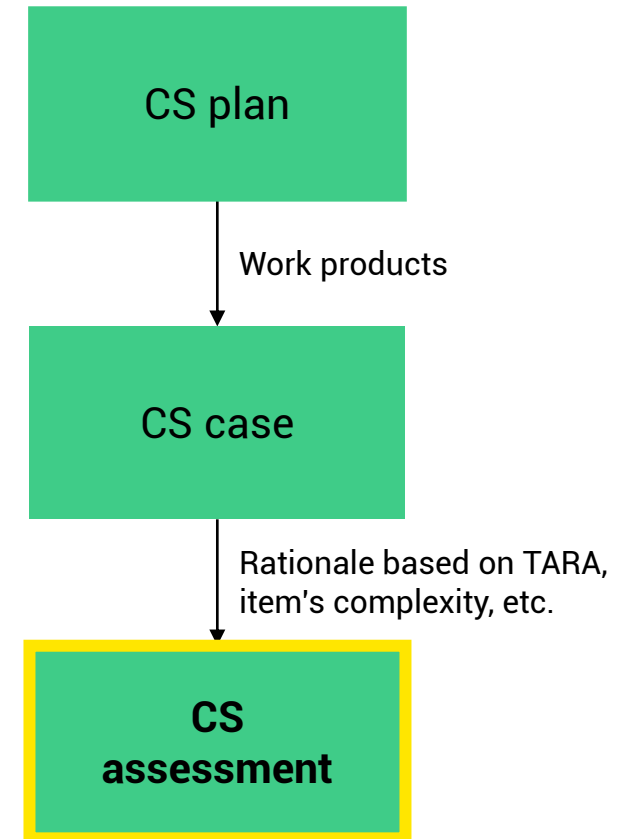
CS Assessment

- The CS assessment is carried out in the context of a project
- It identifies the degree to which the ISO/SAE 21434 objectives are met
- The assessment examines the process implementation in relation to the activities outlined in the CS plan
- To begin the post-development phase, an independent entity's judgment in the CS assessment is required



Key Requirements - CS Assessment

- A decision should be made whether to conduct a CS assessment or not, based on risk assessment or the complexity of an item that is related to CS
 - A rationale should be provided
- Item's or component's cybersecurity should be evaluated based on evidence provided (i.e., work products identified in the CS plan, treatment of CS risks, appropriateness and effectiveness of CS controls)
- Based on the evidence, the level of cybersecurity achieved is judged
- An independent party or person should plan and conduct the CS assessment (i.e., a person from the quality department or a different team)
- The CS assessment is subject to change management
- The report should offer recommendations for acceptance or rejection of the item's or component's cybersecurity



Conditions for Release for Post-Development

Prior to the release	For the release
Cybersecurity case is available	Argument for cybersecurity provided by the cybersecurity case is convincing
Cybersecurity assessment report is available	The cybersecurity case is confirmed by the cybersecurity assessment report
Cybersecurity requirements for post-development are available	The cybersecurity requirements for post-development phases are accepted


9. SUMMARY

Summary

Work Products

- [WP-06-01] Cybersecurity plan
- [WP-06-02] Cybersecurity case
- [WP-06-03] Cybersecurity assessment report
- [WP-06-04] Release for post-development report

Training Overview ISO/SAE 21434



Part 1, Duration: 4hrs	
	Introduction
	Organizational Management Activities
	Project Dependent Management Activities
	Distributed Cybersecurity Activities
Part 2, Duration: 4hrs	
	Threat Analysis and Risk Assessment Methods (TARA)
	CS Related Topics and Case Study
Part 3, Duration: 4hrs	
	Continual Cybersecurity Activities
	Concept
	Product Development
	Cybersecurity Validation
Part 4, Duration: 4hrs	
	Production
	Operations and Maintenance
	End of Cybersecurity Support and Decommissioning
	Final Questions / Knowledge Test (if considered in this training)

* intermediate break to be decided by trainer and participants on an hourly basis

DEKRA DIGITAL

innovating safety

That's all of

PROJECT DEPENDENT MANAGEMENT ACTIVITIES

Thank you!