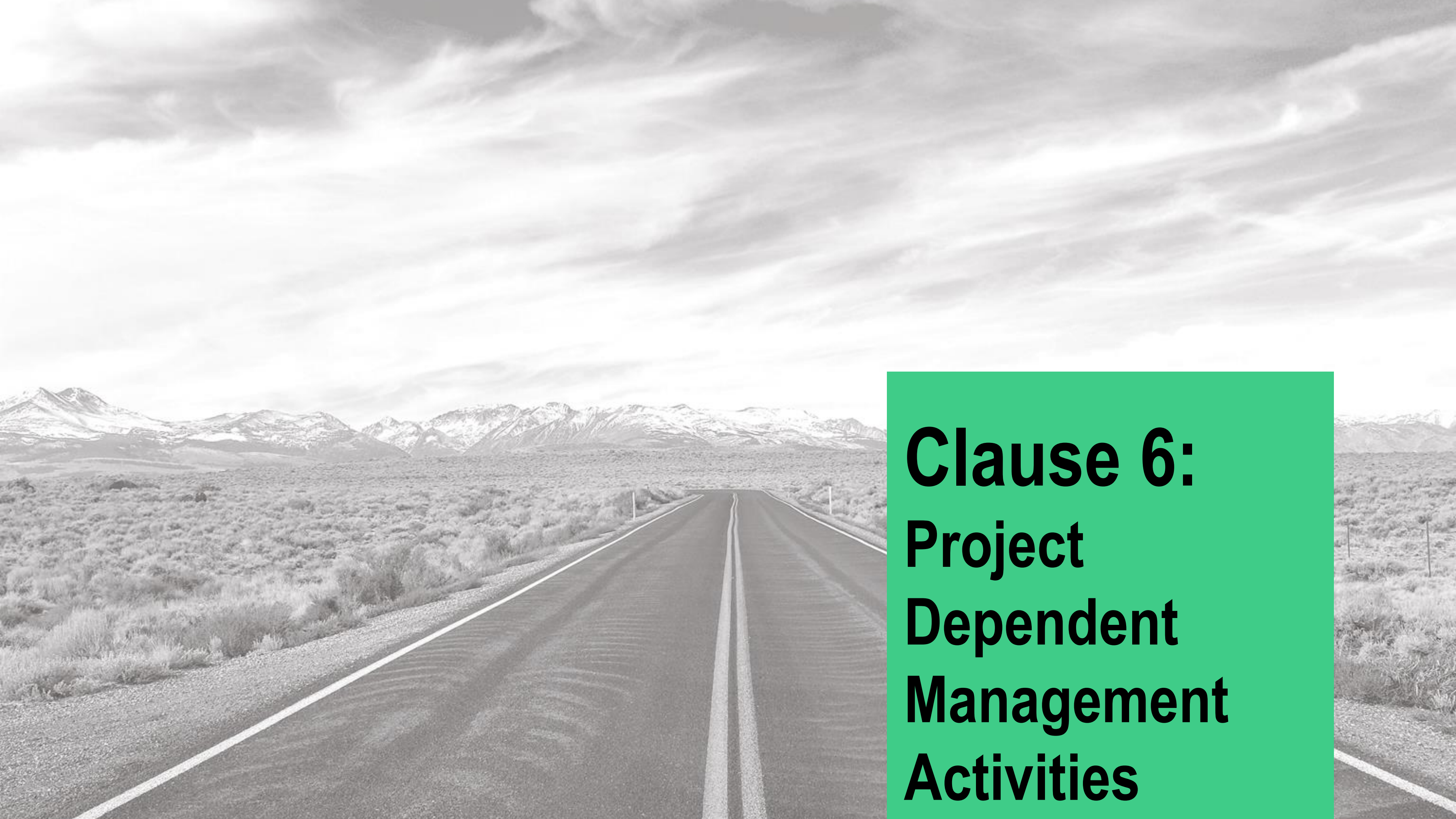
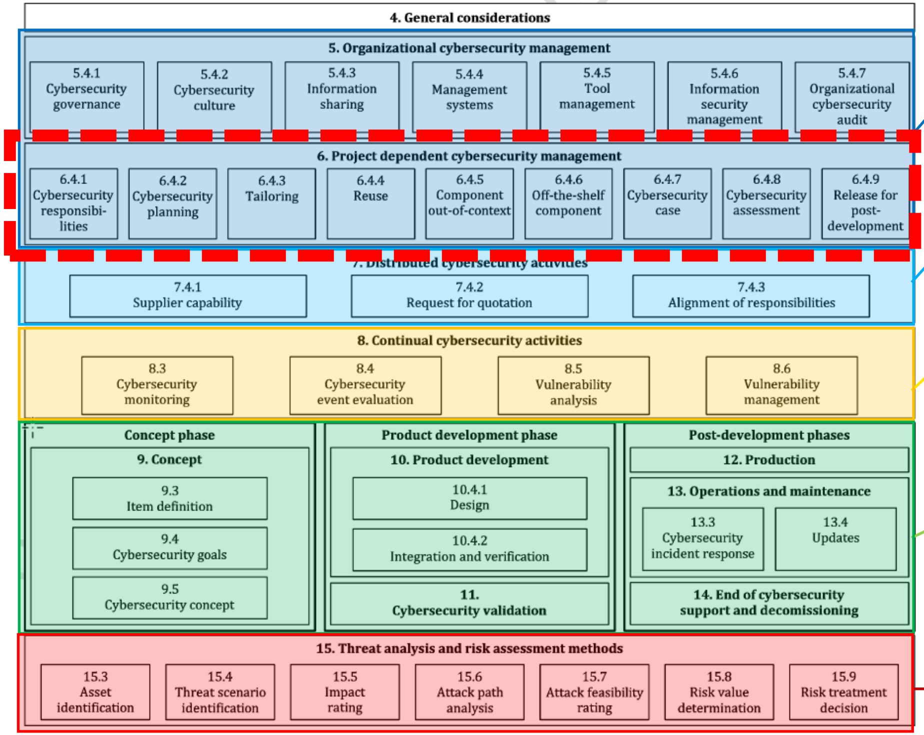


Clause 6: Project Dependent Management Activities

Structure of ISO 21434



4. General considerations

5. Organizational cybersecurity management

5.4.1 Cybersecurity governance	5.4.2 Cybersecurity culture	5.4.3 Information sharing	5.4.4 Management systems	5.4.5 Tool management	5.4.6 Information security management	5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management

6.4.1 Cybersecurity responsibi-lities	6.4.2 Cybersecurity planning	6.4.3 Tailoring	6.4.4 Reuse	6.4.5 Component out-of-context	6.4.6 Off-the-shelf component	6.4.7 Cybersecurity case	6.4.8 Cybersecurity assessment	6.4.9 Release for post-development

7. Distributed cybersecurity activities

7.4.1 Supplier capability	7.4.2 Request for quotation	7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring	8.4 Cybersecurity event evaluation	8.5 Vulnerability analysis	8.6 Vulnerability management

Concept phase	Product development phase	Post-development phases
9. Concept	10. Product development	12. Production
9.3 Item definition	10.4.1 Design	13. Operations and maintenance
9.4 Cybersecurity goals	10.4.2 Integration and verification	13.3 Cybersecurity incident response 13.4 Updates
9.5 Cybersecurity concept	11. Cybersecurity validation	14. End of cybersecurity support and decomissioning

15. Threat analysis and risk assessment methods

15.3 Asset identification	15.4 Threat scenario identification	15.5 Impact rating	15.6 Attack path analysis	15.7 Attack feasibility rating	15.8 Risk value determination	15.9 Risk treatment decision

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..

Continual 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 of 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

Clause 6: Project Dependent Management Activities

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: 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. (example: microcontroller)

Off-the-shelf: Component “ready to use” that doesn’t need modification. It might not have been developed in accordance with this document. (example: 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.

Clause 6: Project Dependent Management Activities

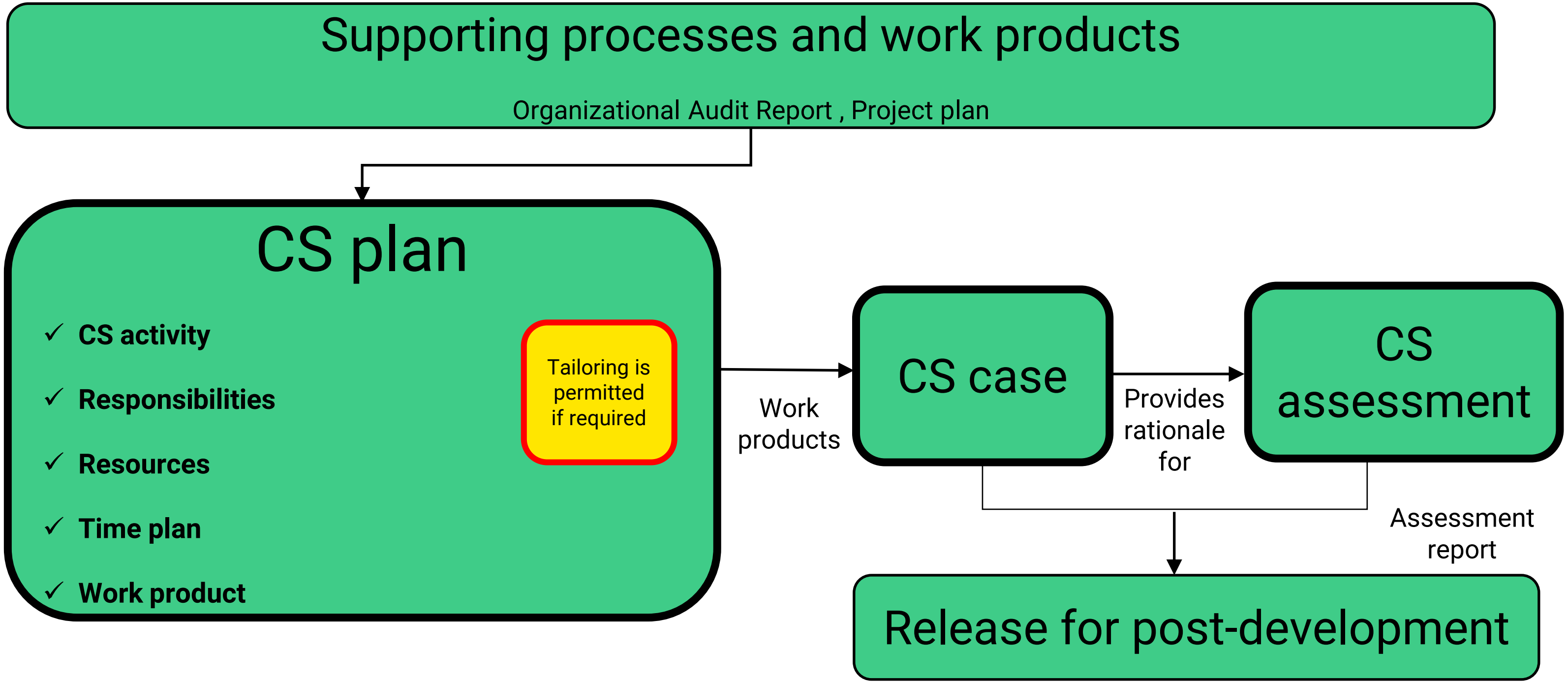


Figure. 1 Blueprint of clause 6: Project dependant cybersecurity management

Clause 6: Project Dependent Management Activities

Project dependent management activities

This section covers the planning of cybersecurity activities, with a focus on requirements for managing cybersecurity development activities for specific projects. It also applies to cases where tailoring is possible.

Objectives

- 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

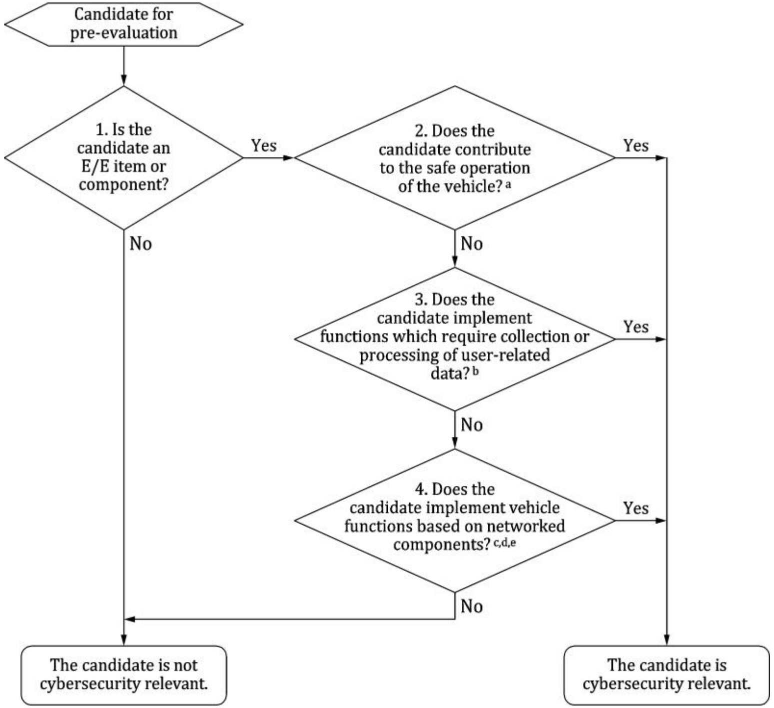
Clause 6: Project Dependent Management Activities

CS plan

The cybersecurity plan is a document describing the activities which will be performed to fulfill the requirements of the ISO 21434.

Key requirements(1)

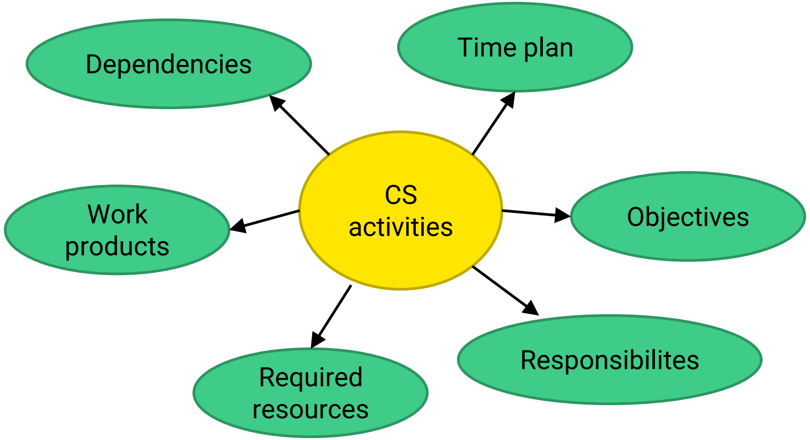
- The item or component should be analyzed to determine cybersecurity activities
  - Item is checked to see if it is relevant to CS; if not, it is omitted from the planning
  - If the item is relevant, additional checks are performed, to see if it is reused, newly developed, or tailored


Candidate for pre-evaluation
1. Is the candidate an E/E item or component?
Yes
No
2. Does the candidate contribute to the safe operation of the vehicle? a
Yes
No
3. Does the candidate implement functions which require collection or processing of user-related data? b
Yes
No
4. Does the candidate implement vehicle functions based on networked components? c,d,e
Yes
No
The candidate is not cybersecurity relevant.
The candidate is cybersecurity relevant.

Clause 6: Project Dependent Management Activities

Key requirements(2)

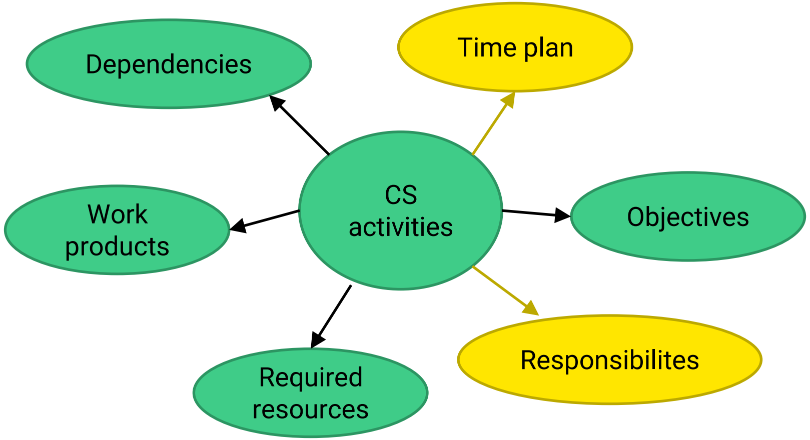
- CS plan must specify activities required for CS during each phase of the product lifecycle
- CS plan should be included in the project plan or highlighted separately
- When performing a change activity, the plan must be updated
  - For example, change in the plan due to new vulnerabilities discovered in the concept phase



Clause 6: Project Dependent Management Activities

Key requirements(3)

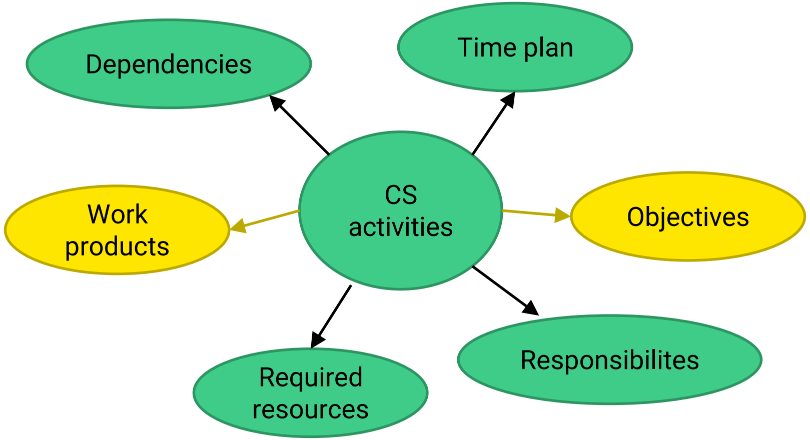
- Responsibilities for the project’s CS activities must be assigned and communicated
  - There should be someone in charge of coordinating the project's CS activities
  - Other roles in the project that perform CS activities should be addressed
  - Responsibilities for maintaining and tracking CS activities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



Clause 6: Project Dependent Management Activities

Key requirements(4)

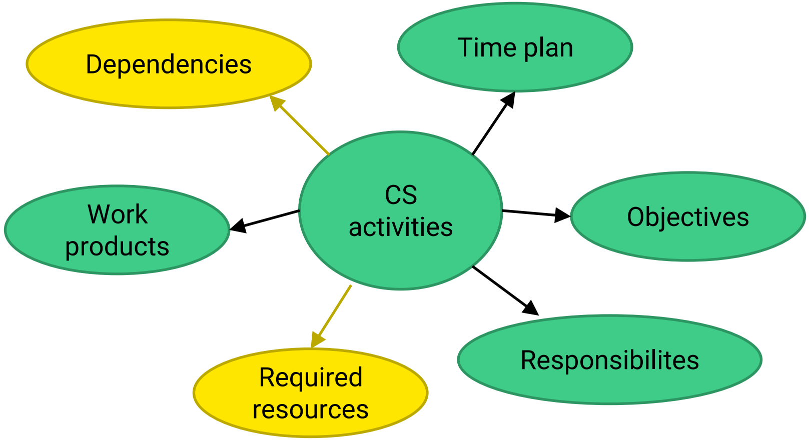
- Determination of CS objective for each phase of the product lifecycle
  - Process for creation of CS objectives
  - Clear objectives for all the CS activities should be defined
- Determination and assignment of work products resulting from each CS activity
  - Work products must be maintained and updated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



Clause 6: Project Dependent Management Activities

Key Requirements(5)

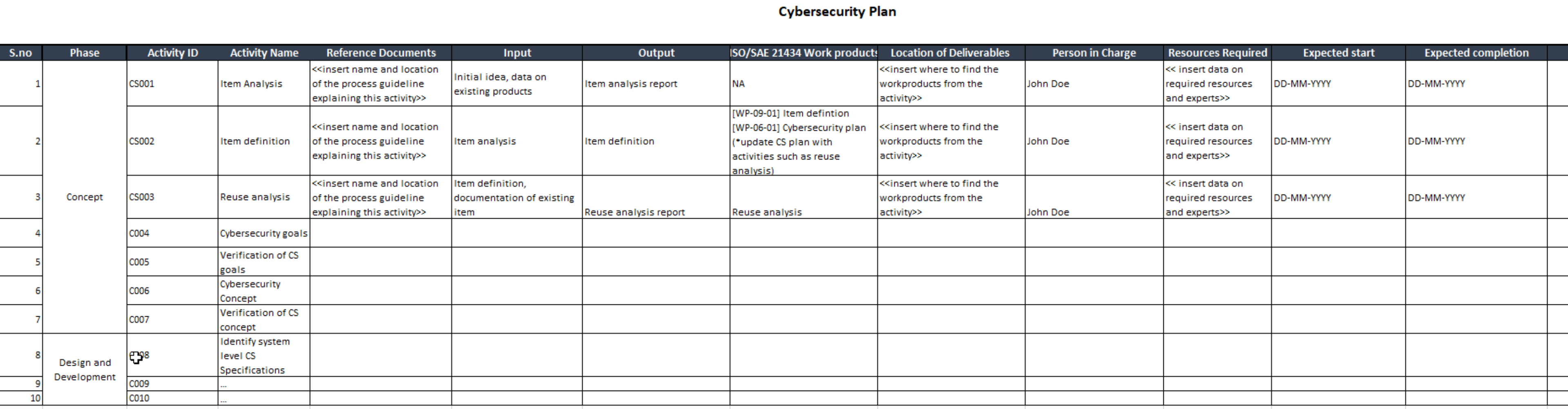
- Resource allocation for performing CS activities should be specified
  - For example, proper infrastructure, training, software tools, skilled staff etc.
- Determination of dependencies with other activities should be clearly stated in the plan
  - For example, dependencies between safety and security



Clause 6: Project Dependent Management Activities

DEKRA DIGITAL

Generic example of a 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 defintion [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	[illegible]8	Identify system level CS Specifications									
9		C009	...									
10		C010	...									

Clause 6: Project Dependent Management Activities

Tailoring

Tailoring means adopting various processes or standards instead of ISO 21434 when performing cybersecurity activities.

Key requirement

- Tailoring is permitted if it is explained, and it should be 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 component off-the-shelf component
  - Different approaches for risk assessment

Clause 6: Project Dependent Management Activities

DEKRA DIGITAL

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

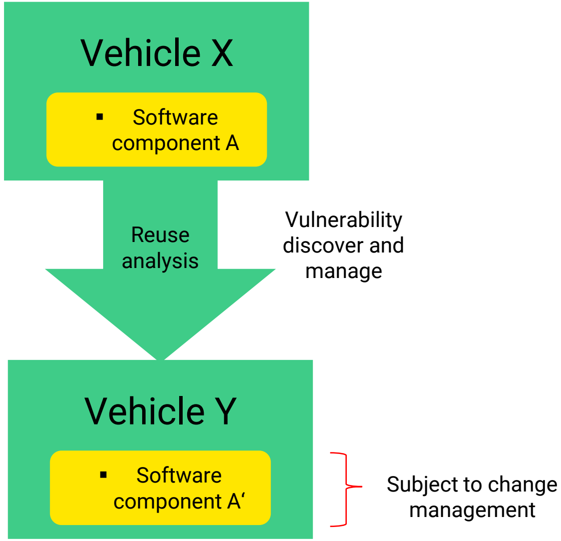


Figure. 3 Reuse analysis example

Clause 6: Project Dependent Management Activities

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.

Example: Microcontrollers

Key requirement

- 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

Clause 6: Project Dependent Management Activities

Off-the-shelf component

An off-the-shelf component is one that is not developed for a specific customer or application. It is ready a 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 21434.

Key requirements

- CS related information should be collected when using an off-the-shelf-component to determine:
  - If it is a suitable application
  - Documents provided are sufficient and
  - Can comply with CS requirements according to ISO 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 21434

Clause 6: Project Dependent Management Activities

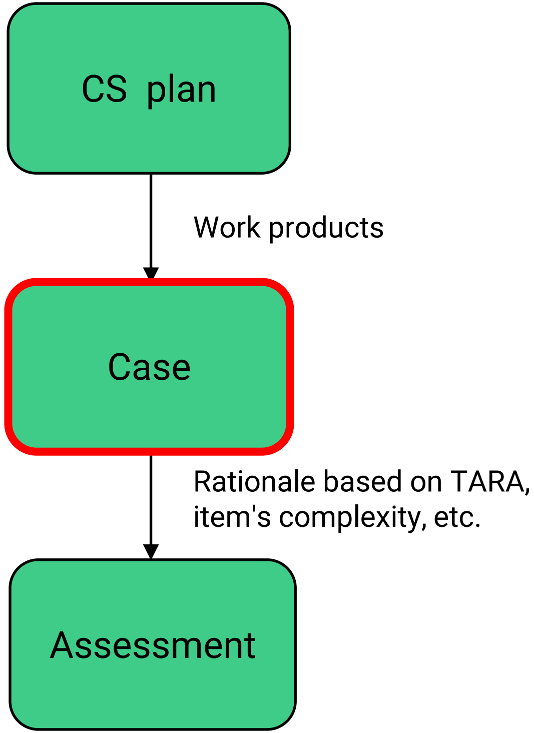
DEKRA DIGITAL

CS case

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

Key requirements

- CS case must be prepared to present an argument for the item's or component's cybersecurity, backed up with work product
    - Work products from the cybersecurity plan are gathered in the cybersecurity case
    - In case of distributed development, the item's overall argument should be supplemented by all the partners involved



Is the content of the cybersecurity case limited to work products as defined in the ISO 21434?

Clause 6: Project Dependent Management Activities

CS assessment

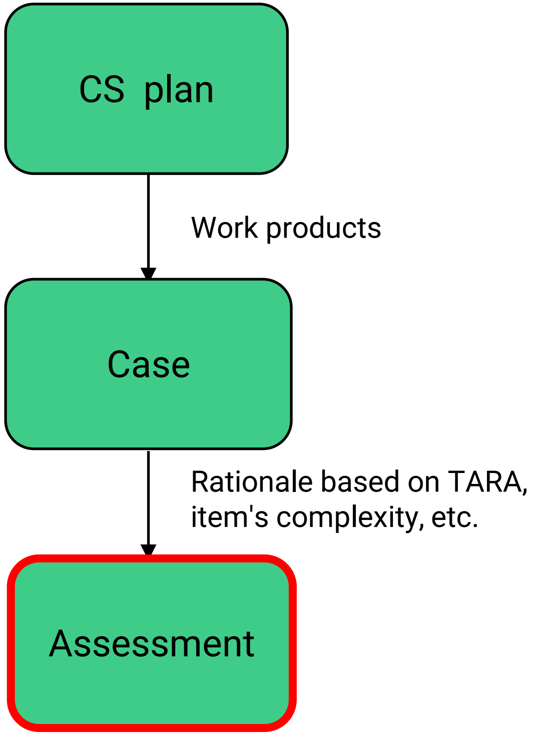
The CS assessment is carried out in the context of a project. It identifies the degree to which the ISO 21434 objectives are met.

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(1)

- 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
  - Rationale should be provided



Clause 6: Project Dependent Management Activities

Key requirements(2)

- Item’s or component's cybersecurity should be evaluated based on:
  - Evidence provided (all work products)
- Based on the evidence, the confidence of achieved security is judged
- An independent party or person should conduct the assessment
  - Example, a person from the quality department or a different team
- The assessment is subject to change management
- The report should offer recommendations for acceptance or rejection of the item's or component's cybersecurity

Clause 6: Project Dependent Management Activities

DEKRA DIGITAL

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**

Clause 6: Project Dependent Management Activities

DEKRA DIGITAL

Summary of 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