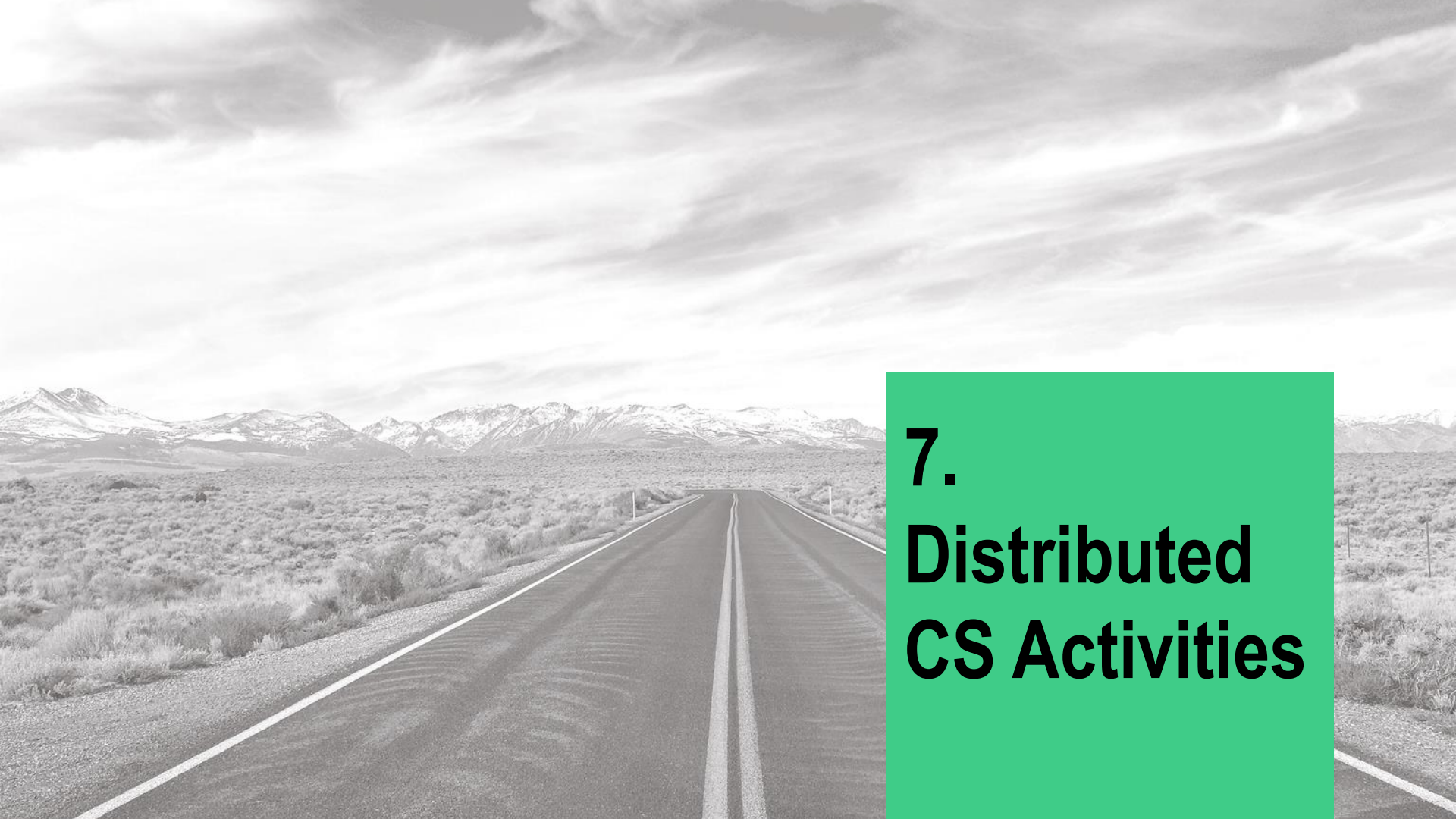
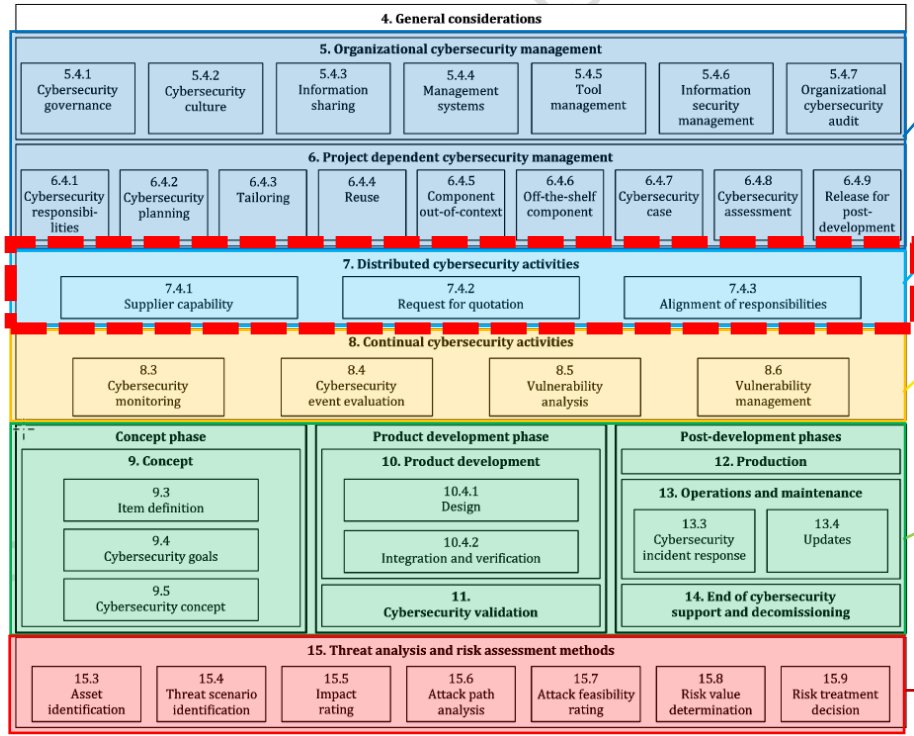


7. Distributed CS Activities

Structure of ISO 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..

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 7: Distributed CS Activities

What are distributed cybersecurity activities?

- To drive the overall business, security measures need to be implemented not only by the OEM, but also by the supply chain, which includes business partners (also companies within the OEM group) involved in the entire product lifecycle.
  - When any cyber attack on business partners happens, there is fear that the organization's information may be compromised
  - As a result, comprehensive distributed cybersecurity measures are required to protect the organization and its business partners from cyber attacks and to collaborate on the development of a secure product

Objectives

- Manage distributed cybersecurity activities
- Define interactions, responsibilities, and dependencies of customers and suppliers for CS activities

Clause 7: Distributed CS Activities

Supplier capability

Supplier capability evaluation is a formal process that assesses a potential supplier's capacity to conform to ISO 21434 or based on the earlier application of another national or international cybersecurity engineering standard.

Key requirements

- Establish processes for evaluation
- Check prior adoption of cybersecurity standards by suppliers
- Suppliers can provide supporting information to demonstrate their capabilities
  - CS assessment report, quality management report
    - E.g., ISO 21434 CSMS Certification, VDA ACSMS, etc.
  - Evidence of vulnerability management
  - Continuous CS activities, risk management practices, etc.

Clause 7: Distributed CS Activities

Request for quotation

A request for quotation is a business process in which a customer entity request a quote from a potential supplier for a specific project, task or service.

Key requirements

- A request for quotation should include:
  - Formal request to follow ISO 21434 standard if applicable
  - CS requirements for which the supplier is quoting
    - Example, requirements related to information sharing
  - Supplier's CS responsibilities

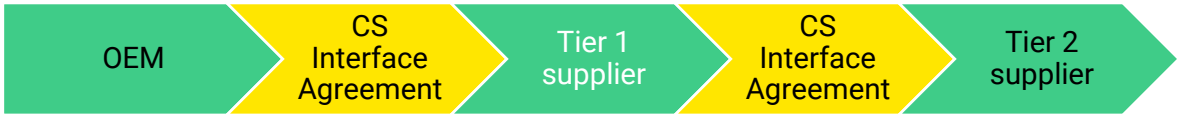
Clause 7: Distributed CS Activities

Cybersecurity Interface Agreement (CIA)

The Cybersecurity Interface Agreement (CIA) is an important document that ensures the successful planning and execution of distributed cybersecurity activities. It is intended to be a record of what each party is expected to complete and should specify the exact means of completion.

How CIA is communicated is of importance to avoid communication gaps among different organizations participating in a distributed development

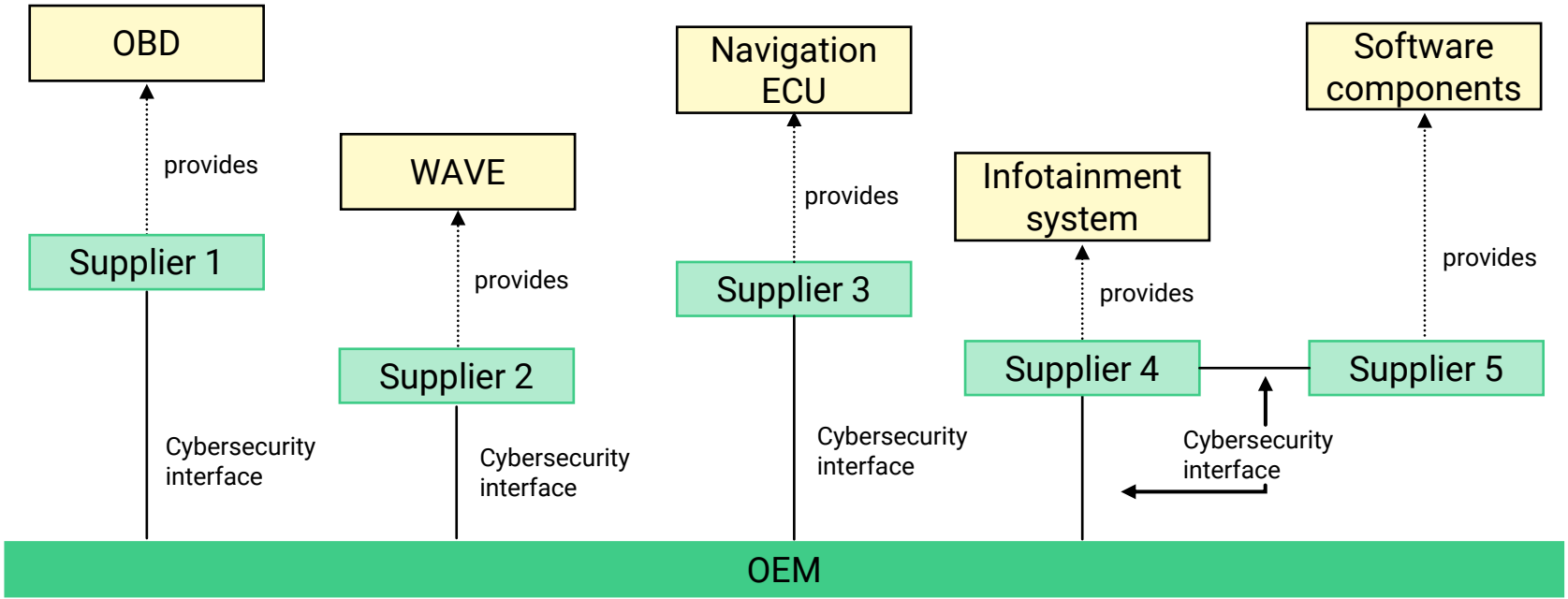
- Example, RASIC table



Clause 7: Distributed CS Activities

DEKRA DIGITAL

Example



Clause 7: Distributed CS Activities

DEKRA DIGITAL

Table. 1: Example of RASIC table for distributed CS activities

Phase	WP	Doc Ref.	Supplier					Customer					Level of confidentiality	Comments
			R	A	S	I	C	R	A	S	I	C		
Concept	Item definition							X						
	TARA					X		X						
	CS concept					X	X	X						
	Concept verification				X			X						
Analysis	Vulnerability analysis		X	X							X			

R: Responsible, A: Approve, S: Support, I: Inform, C: Consult

Clause 7: Distributed CS Activities

Key requirements

- CS activities performed by customers and suppliers should be specified in the CIA
  - The CIA shall include:
    - Points of contact regarding cybersecurity at both the ends
    - Identification of CS activities to be performed by both the parties
    - Process definition in case of a cybersecurity issue
    - Target milestones regarding cybersecurity activities
    - Resolving conflicts and incidents through mutual agreement
    - Responsibility sharing
    - Definition of the end of cybersecurity support

Clause 7: Distributed CS Activities

DEKRA DIGITAL

Summary of work products

- [WP-07-01] Cybersecurity interface agreement