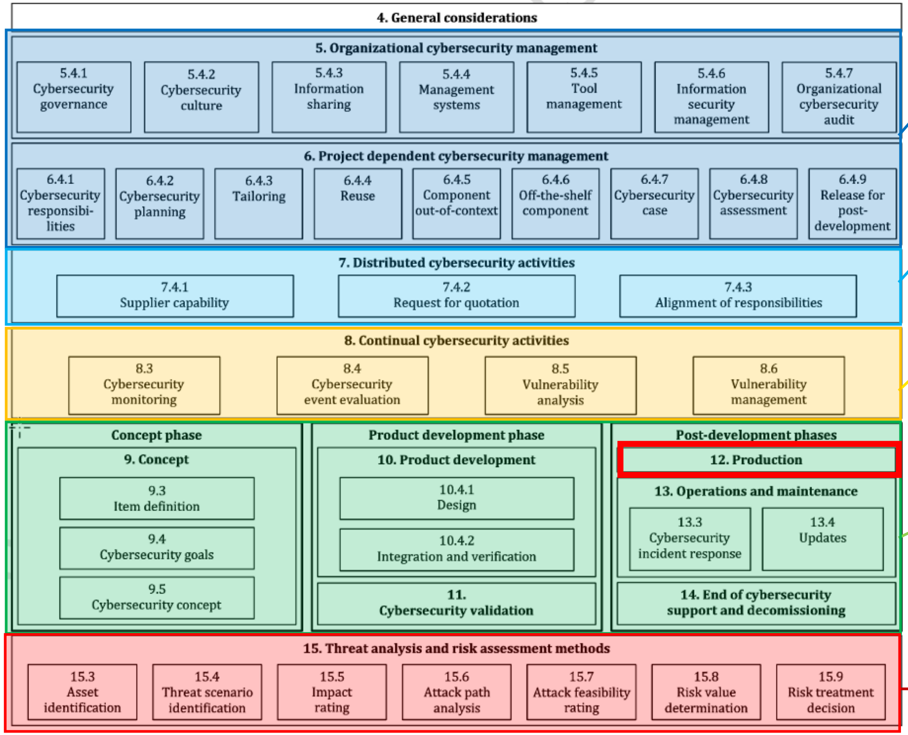
Clause 12:

Production

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
- 9. Concept
  - 9.3 Item definition
  - 9.4 Cybersecurity goals
  - 9.5 Cybersecurity concept

Product development phase
- 10. Product development
  - 10.4.1 Design
  - 10.4.2 Integration and verification
- 11. Cybersecurity validation

Post-development phases
- 12. Production
- 13. Operations and maintenance
  - 13.3 Cybersecurity incident response
  - 13.4 Updates
- 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 12: Production

DEKRA DIGITAL

Definitions

Component: part of an item which is ideally separated by logically and separable

Cybersecurity control: measure that is modifying risk

Cybersecurity goal : concept level cybersecurity requirement associated with one or more threat scenarios

Cybersecurity risk : effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact

Risk management : coordinated activities to direct and control an organization with regard to risk

Vulnerability analysis: systematic identification and evaluation of vulnerabilities

Clause 12: Production

DEKRA DIGITAL

General

- Production covers the manufacturing and assembly of an item or component
- Apply the cybersecurity requirements in post-development phase
- Ensuring cybersecurity controls in place for an item or component post development
- Prevent the introduction of vulnerabilities during production
- CS production control plan can be a part of entire production plan

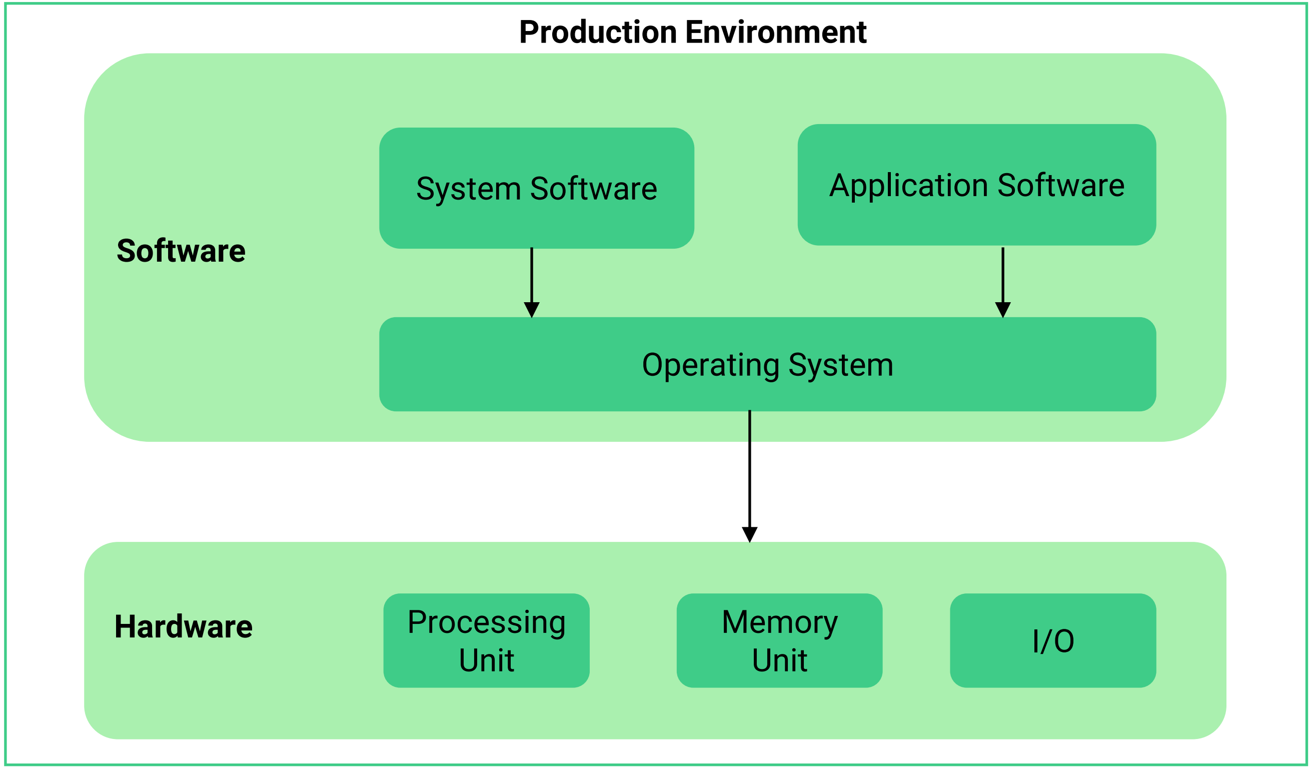
Clause 12: Production

Production establishment

CS requirements for production	• Established during concept phase • E.g. : disabling debug interfaces, erase memory, ...
Necessary installation procedures	• E.g. : How to get privilege access to disable debug mode • How to disable privilege access
Description of protection measures to prevent alteration	• Physical access protections, access control and encryption, ...
Verification of CS requirements for production	• Verification, validation, inspection, configuration and calibration tests, integrity checks

Clause 12: Production

Production establishment



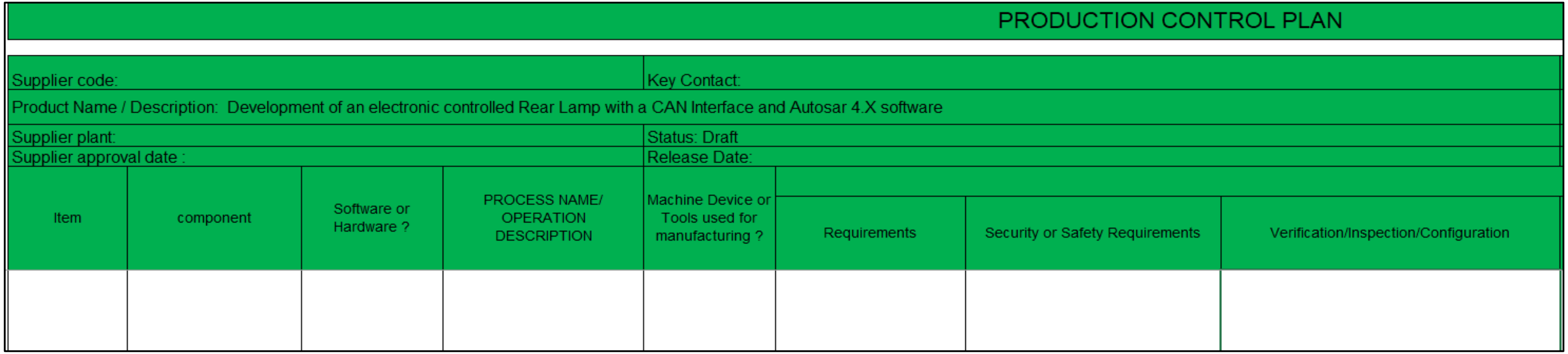
Clause 12: Production

Production control plan (PCP)

- PCP is a document that contains detailed information regarding items that are in production such as:
  - Item characteristics
  - Listed cybersecurity requirements and controls for post-development
    - test methods for validation
  - Production tools and equipment
  - Process controls
  - Tests
  - Measurement system analysis (if applicable)
  - Reaction plans and troubleshoot
  - Inspection planning
  - Etc.,
- PCP will ensure the cybersecurity requirements for post-development for an item or component are applied and cannot be exploited during production

Clause 12: Production

Production control plan (PCP)



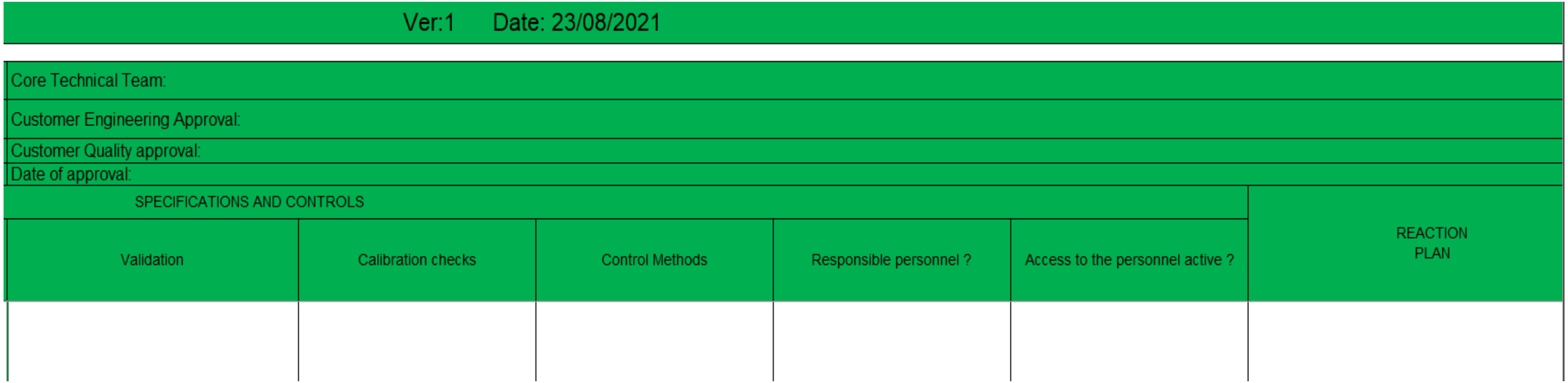
PRODUCTION CONTROL PLAN							
Supplier code:				Key Contact:			
Product Name / Description: Development of an electronic controlled Rear Lamp with a CAN Interface and Autosar 4.X software							
Supplier plant:				Status: Draft			
Supplier approval date :				Release Date:			
Item	component	Software or Hardware ?	PROCESS NAME/ OPERATION DESCRIPTION	Machine Device or Tools used for manufacturing ?	Requirements	Security or Safety Requirements	Verification/Inspection/Configuration

Template continued in the next slide…

Note: please refer the PCP example document for better understanding

Clause 12: Production

Production control plan (PCP)



Ver:1 Date: 23/08/2021					
Core Technical Team:					
Customer Engineering Approval:					
Customer Quality approval:					
Date of approval:					
SPECIFICATIONS AND CONTROLS					REACTION PLAN
Validation	Calibration checks	Control Methods	Responsible personnel ?	Access to the personnel active ?	

Note: please refer the PCP example document for better understanding

Clause 12: Production

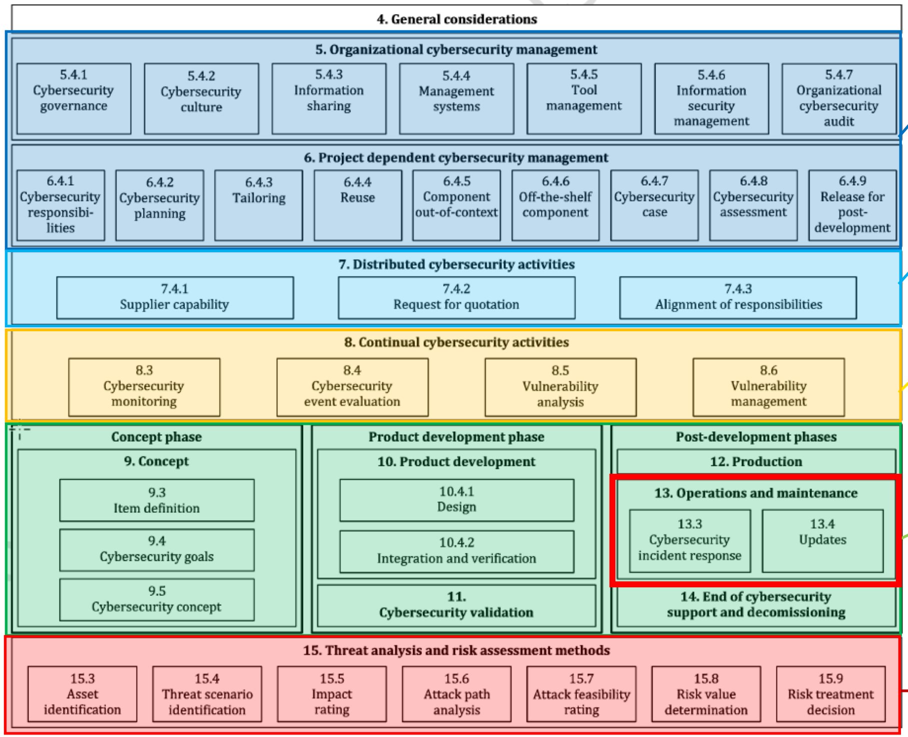
Summary of work products

- [WP-12-01] Production control plan

Clause 13:

Operations & maintenance

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 responsibilities

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

9. Concept

9.3 Item definition

9.4 Cybersecurity goals

9.5 Cybersecurity concept

Product development phase

10. Product development

10.4.1 Design

10.4.2 Integration and verification

11. Cybersecurity validation

Post-development phases

12. Production

13. Operations and maintenance

13.3 Cybersecurity incident response

13.4 Updates

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 13: Operations & maintenance

General

- This clause is all about cybersecurity incident response and management of post-development phases such as production, postproduction
- If an organization responds to the cybersecurity event, it becomes a cybersecurity incident. If not, it will be handled as a change management
- Incident management requires a process and a response team that follows this process
- Any updates or modification made to an item, or a component post-development brings in a lot of changes which in turn may lead to a cybersecurity event

Clause 13: Operations & maintenance

DEKRA DIGITAL

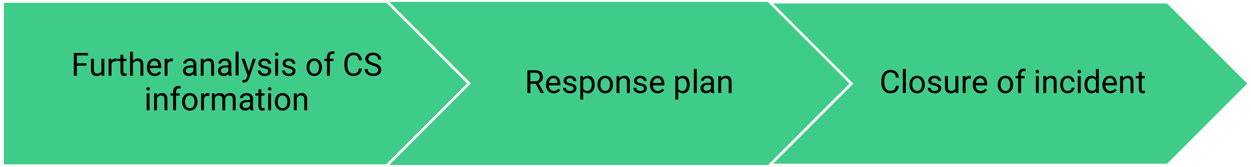
Objectives

- To handle cybersecurity events that become a cybersecurity incident by determining and implementing remediation actions for the incidents
- Cybersecurity event assessment to be done before considering it as an incident
- Vulnerability analysis and management which caused the cybersecurity incident
- To preserve cybersecurity during and after updates to items or components post-production until the end of cybersecurity support
- Cybersecurity incident response plan in order to tackle the incidents

Clause 13: Operations & maintenance

Cybersecurity incident response

- Incidents are cybersecurity information that may need a change of SW or HW through updates or maintenance.
- Only applicable in post-development phase as changes during development can follow the change management processes
- Triggered by continuous monitoring activities, the cybersecurity incident must define processes to follow closely.
- The incident response will follow the following steps



Further analysis of CS information

Response plan

Closure of incident

Clause 13: Operations & maintenance

Cybersecurity incident response: Further analysis of CS information

- Analysis of the CS Event assessment resulting from Continuous Monitoring activities
  - Risk determination
  - Evaluation of risk treatment options
  - Evaluation of new CS goals
  - Estimation of duration

Clause 13: Operations & maintenance

Cybersecurity incident response: Response plan

- Remediation actions and security controls to be implemented
- Establishing a communication plan with the involved parties (communication teams, marketing, quality management, legal department, development teams, etc.)
- Assignment of the tasks to responsible persons, teams, etc.
- Create a method to measure the progress done in the incident response

Clause 13: Operations & maintenance

Cybersecurity incident response: Closure of incident

- Define criteria for closure of the incident (verification and validation activities)
- As a supplier, further testing might be done by OEMs
- Integration to update packages has to be agreed with OEMs
- If applicable, an updated TARA has to be provided to prove that:
  - The update is not covering the vulnerabilities to be fixed
  - The changes in HW and/or SW didn't introduce new vulnerabilities

Clause 13: Operations & maintenance

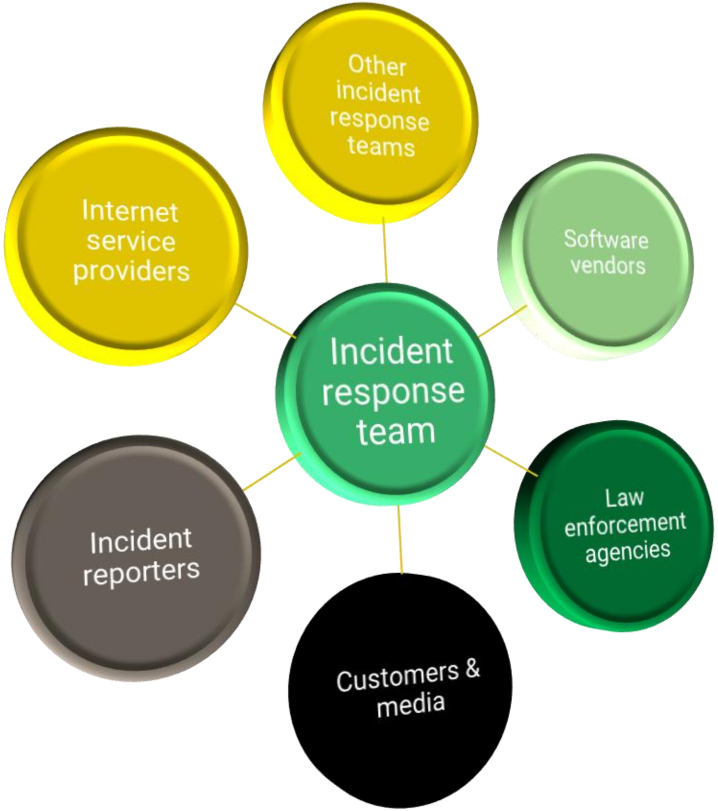
Cybersecurity incident response team

- A dedicated cybersecurity incident response team is required to handle the incidents as needed
- Group of experts that assess, document, and respond to cyber incidents (security breaches)
- Work towards quick recovery and avoid future incidents
- The incident response team shall consist of
  - **IR manager**: Prioritize incidents, allocate resources and expertise, create an action plan
  - **Threat researchers**: Provide threat intelligence, monitor threat agents, understand new threats
  - **Security analysts**: Conduct security assessments, perform security audits, analyze security breaches
- Communication within and across the team should be confidential
- Relevant information should be swiftly shared across various departments in the organization

Clause 13: Operations & maintenance

Cybersecurity incident response – Information sharing

- Outside parties and interest groups are informed whenever necessary
- The communication should be bidirectional
- Incident response teams should discuss with management and establish information-sharing procedures
- All contacts and information shared outside the organization are documented and evidenced



Clause 13: Operations & maintenance

Cybersecurity incident response

- For each cybersecurity incident, a cybersecurity incident response plan shall be created

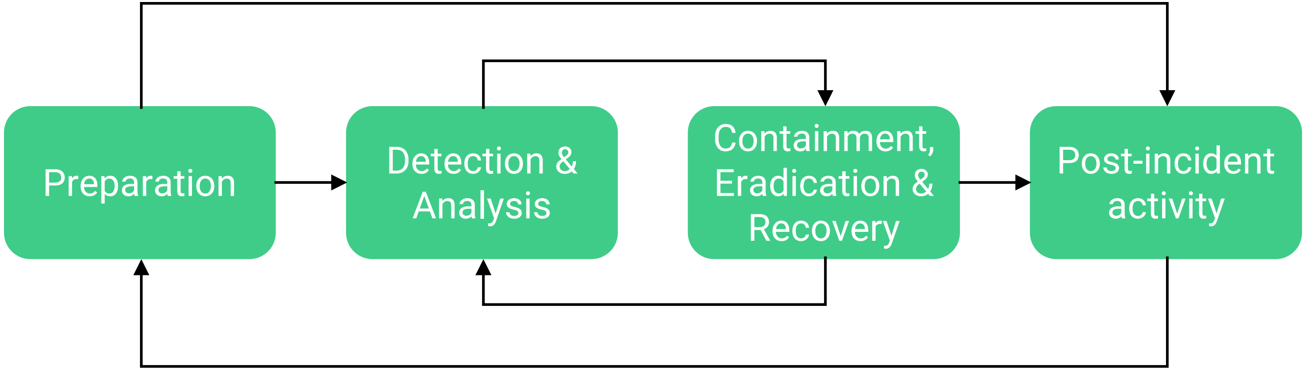
Cybersecurity incident response plan	
Remediation actions	• Actions for the incident are determined based on the vulnerability analysis
Communication plan	• List of internal and external stakeholders such as legal, marketing, purchasing, customers relation etc.. • Product, development, quality teams are involved as needed
Responsible personnel	• Experts (Technical, business) to identify and analyze the incident • Senior authorities in decision making • Organizational level staff for having the process
Cybersecurity incident details	• Incident definition • Affected items and components along with vulnerabilities • Evidence such as data logs, black box information etc. • If available end user complaints
Progress tracking	• In order to know the percentage of recovery or incident is resolved
Incident closure and actions	• Incident closure definition to end the response once resolved • Post incident closure, actions such as legal activities, learning, findings etc. to be addressed as required

Clause 13: Operations & maintenance

DEKRA DIGITAL

What is incident responses lifecycle?

- Incident response lifecycle is the organisation’s step-by-step framework for identifying and reacting to a cyber incident



Clause 13: Operations & maintenance

Preparation

- It is the first and foremost step when an organisation aims to limit the number of incidents
  - Prepare to handle incidents and prevent incidents
  - Security controls and measures are implemented based on risk assessment
- The tools and resources to be used during incident handling should be made available such as,
  - Contact information of the members within and outside the organisation
  - Incident reporting mechanism
  - Issue tracking system
  - War room (at least in case of an incident)
  - Secure storage facility

Clause 13: Operations & maintenance

Preparation

Other incident handling resources that should be made available are,

- List of all commonly used ports and interfaces
- Documentation of intrusion detection controls, and antivirus programs used
- Asset inventory and list of critical assets
- Architectural designs, UML diagrams etc.
- Current baselines of the device under evaluation
- Access to clean software

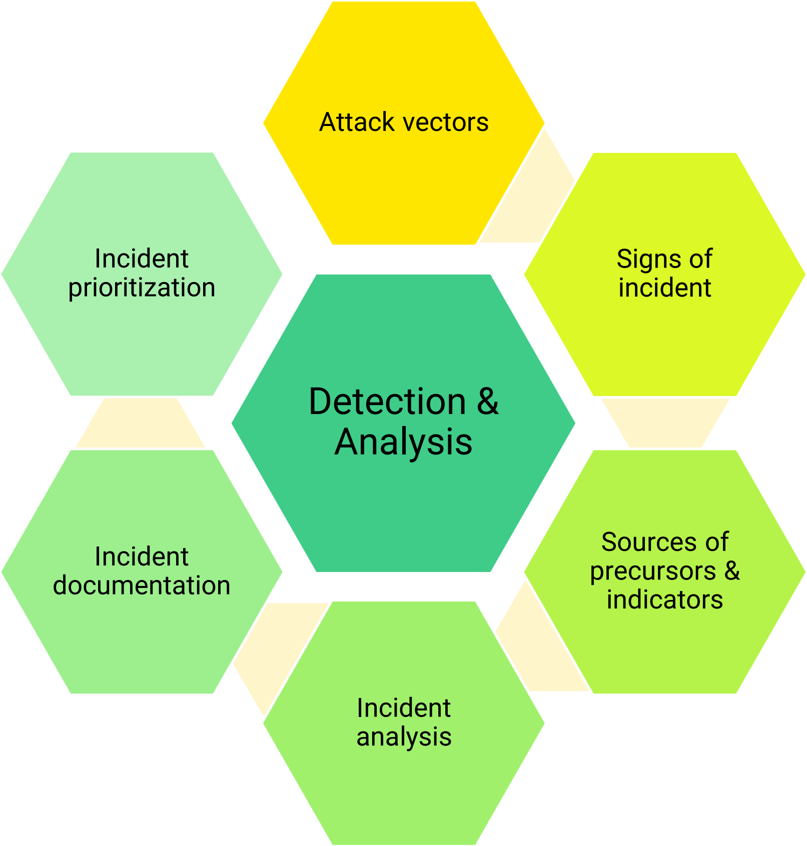
Note: It is advisable to create a 'jump kit', which is a portable case with materials necessary for an investigation

Clause 13: Operations & maintenance

DEKRA DIGITAL

Detection & analysis

- The security breaches and cybersecurity incidents are identified and detected
- The mitigation steps are determined and implemented based on the severity of the incident



Clause 13: Operations & maintenance

Detection & analysis: Attack vector

Attack vector is a method or pathway through which an attacker gains access to the system

- Incident response strategies for well-known attack vectors should be clearly established
- Removable media, improper usage, authenticating mechanisms, wireless networks etc. are some most used attack vectors

Signs of an incident

Accurate detection of possible intrusions is the most challenging part of incident response. Signs of an incident can be classified as:

- Precursor -> an incident may occur in the future
- Indicator -> an incident is occurring or occurred

Clause 13: Operations & maintenance

Detection & analysis: Sources of Precursors and Indicators

Some of the sources to identify precursors and indicators are:

- Intrusion Detection and Prevention Systems (IDPS)
- Antivirus and anti-spam software
- Third party monitoring services
- Public information on new vulnerabilities and exploits
- System and network logs
- People within the organization (developers, security analysts, testing teams etc.)
- People from other organizations (research firms, white hat hackers, other CSIRTs etc.)

Clause 13: Operations & maintenance

Detection & analysis: Incident analysis

Incident analysis is a process of identifying what happened, examining how it happened, and determining solutions to prevent future incidents. The incident response team should work quickly to analyze and validate each incident.

Some of the recommendations to make incident analysis easier and effective,

- **Profile networks and systems:** Profiling is measuring the characteristics of expected activity so changes to it can be identified easily (e.g., deriving checksums of critical files)
- **Understand normal behavior:** networks, systems, and applications are studied to understand the normal behavior that any abnormalities can be identified
- **Create a log retention policy:** Incident information may be stored in different places (IDPS, firewalls, event logs, etc.). Maintaining a log retention policy that specifies how long the data is stored will be helpful to understand similar attacks

Clause 13: Operations & maintenance

Detection & analysis: Incident analysis (cont.)

- **Perform event correlation:** Information about the intrusion may be stored in different logs, and each log may contain different data. Hence, correlating information from different sources is important to determine if an incident occurred.
- **Maintain and use knowledge base information:** the knowledge base should contain all information necessary for quick referencing. Information such as previous incidents and the measures taken, IDPS alerts, logs etc. are stored in the knowledge base
- **Run packet sniffers:** necessary information about the incidents occurring in the network could be easily gathered using packet sniffers. They can be configured to record data traffic that matches certain criteria
- **Data filtering**: filter out insignificant categories of indicators. This may pose a risk as a new malicious activity may not fall under the significant category
- **Internet:** monitor hacker websites and forums (e.g. hacker chatter)

Clause 13: Operations & maintenance

DEKRA DIGITAL

Detection & analysis: Incident documentation

- If the incident response team suspects an incident has occurred, all facts regarding the incident should be recorded
- Documenting system events and observed changes leads to an efficient and systematic approach to solve the issue
- All documents and files regarding the incident should be stored in an issue tracking system where all the steps taken to solve the incident are tracked
- The information to be stored are incident status, indicators, related incidents, actions taken, impact assessment, comments by incident handlers, evidence gathered during the investigation, etc.

Clause 13: Operations & maintenance

Detection & analysis: Incident prioritization

- Prioritizing of handling of incidents is a critical decision during incident handling
- Incident handling should be prioritized based on

  a. Functional impact of the incident
     - How the incident affects the existing functionality is assessed
     - Apart from current impacts, assess impacts that may occur if an incident is not resolved quickly

  b. Information impact of the incident
     - Impacts due to loss of confidentiality, integrity and availability of information are assessed

  c. Recoverability from the incident
     - The type of incident and assets/resources affected determine the recoverability

Clause 13: Operations & maintenance

Detection & analysis: Incident prioritization

The recoverability can be determined from the following table (source: NIST SP 800-61)

Category	Definition
Regular	Time to recovery could be predicted with available resources
Supplemented	Time to recovery predictable using additional resources
Extended	Time to recovery unpredictable, additional resources and outside hep needed
Not recoverable	Recovery from incident not possible, launch investigation

Clause 13: Operations & maintenance

DEKRA DIGITAL

Containment, Eradication & Recovery

- Containment is necessary before an incident creates more damage and should be done at an early stage of incident handling
- Pre-defined strategies and procedures for containment should be established
- Containment strategies include disconnecting systems from the network, curtailing certain functionalities, sending notifications to affected systems, sandboxing, etc.
- Acceptable level of risks should be pre-determined by the organization
- Containment strategy can be decided based on potential damage, the time required to resolve, the effectiveness of the strategy, etc.
- Evidence on the attack and the attacker should be gathered to help with legal proceedings and a detailed log should be maintained

Clause 13: Operations & maintenance

Containment, Eradication & Recovery

- During incident handling, the attacking hosts are identified
- Common activities performed to identify attacking hosts are, using incident databases, tracing the attacker’s IP address, monitoring possible attacker communication channels etc.
- Identify all affected systems to perform remediation
- Normal operation of the systems is restored, and vulnerabilities are mitigated to prevent similar incidents
- The eradication and recovery strategies used are analyzed again to identify residual risks and other hidden vulnerabilities and weaknesses

Clause 13: Operations & maintenance

DEKRA DIGITAL

Post-incident activity

- The incident response teams conduct a formal meeting to discuss the lessons learned
- Share information on improved technology and security controls used to resolve such incidents
- Conduct reviews
- Additional tools and resources necessary to detect and remediate future incidents are identified
- The knowledge learned and best practices to be adopted should be transferred to the relevant teams

Clause 13: Operations & maintenance

Updates

- Updates for an item or component on the vehicle level are made based on the cybersecurity incident plan if required
- Updates should follow the process defined for the product development
- The updates are considered for an item based on the cybersecurity requirements for post-development
- Rollback strategy for both software and hardware should be in place if in case the item must go back to its previous version
- Any update required on the initial phases of the item or component development are monitored using change management (Clause 5)

Clause 13: Operations & maintenance

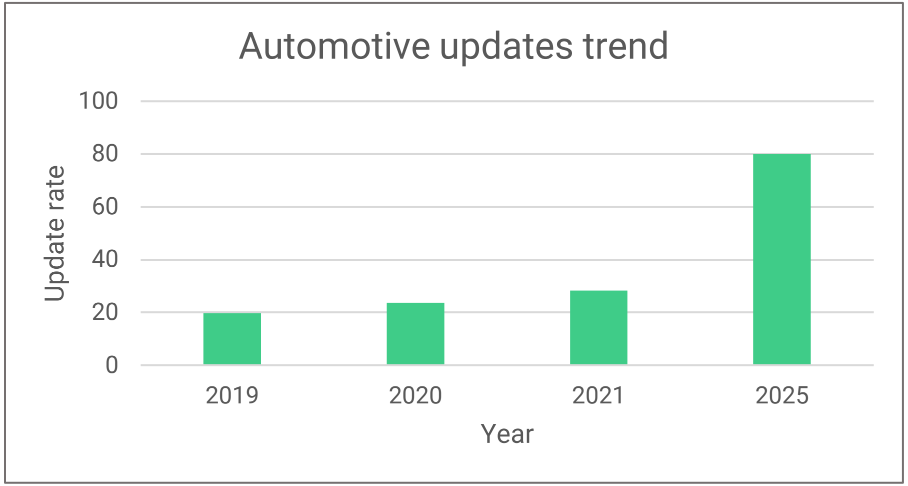
Updates

- Update management will be necessary according to UNECE WP29 R156
- ISO 24089 is in preparation to establish more requirements on Software updates
- ISO 21434 states that updates must follow the same development cycle as the original code. This means :
  - Changes must be analyzed and their impact on the achieved CS must be considered
  - They should follow the same development process, with TARA and vulnerability analysis performed at the same steps
  - They should have verification and validation specifications and reports

Clause 13: Operations & maintenance

Updates

- Automotive updates configurations have maintained a fast-growing trend for the past few years



Reference: Global and China Automotive OTA Industry Report, 2021.

The number of software updates will continue to increase thanks to electronic cars and autonomous driving functions

Clause 13: Operations & maintenance

Updates

- Updates performed in an item or component, can also imply the update of technical documentation or user manuals.
- Maintain a clear process in the organization to perform software update engineering.
  - Create a process template
  - Define the technical rules that should be fulfilled
  - Define the methods and tools used, including their configuration and all relevant documentation
  - Provide the resources required
  - Ensure that the road vehicle can restore the system to its previous version in case of a failed or interrupted update
  - Ensure the road vehicle has enough power to complete the software update
  - Review the lessons learned from previous software update activities performed. Collect and document any new finding
  - Define a process to evaluate the adequacy and safety of the current software update processes implemented. The vehicle user shall be informed before the update is executed and also about the success of the update process

Clause 13: Operations & maintenance

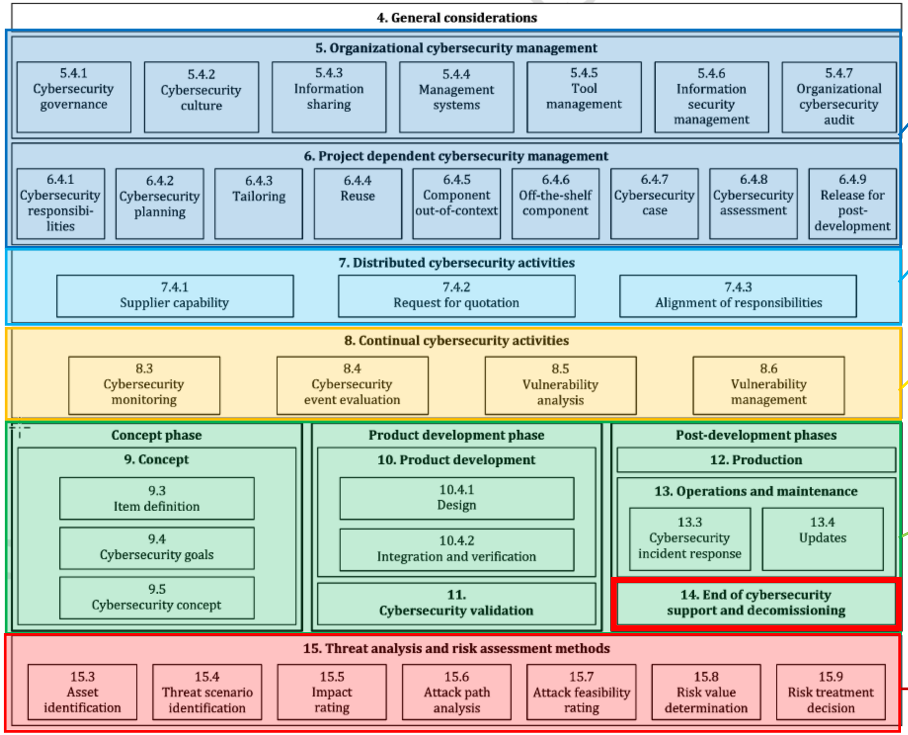
Summary of work products

- [WP-13-01] Cybersecurity incident response plan

Clause 14:

End of cybersecurity support and decommissioning

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 responsibilities
- 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
- 9. Concept
  - 9.3 Item definition
  - 9.4 Cybersecurity goals
  - 9.5 Cybersecurity concept

Product development phase
- 10. Product development
  - 10.4.1 Design
  - 10.4.2 Integration and verification
- 11. Cybersecurity validation

Post-development phases
- 12. Production
- 13. Operations and maintenance
  - 13.3 Cybersecurity incident response
  - 13.4 Updates
- 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

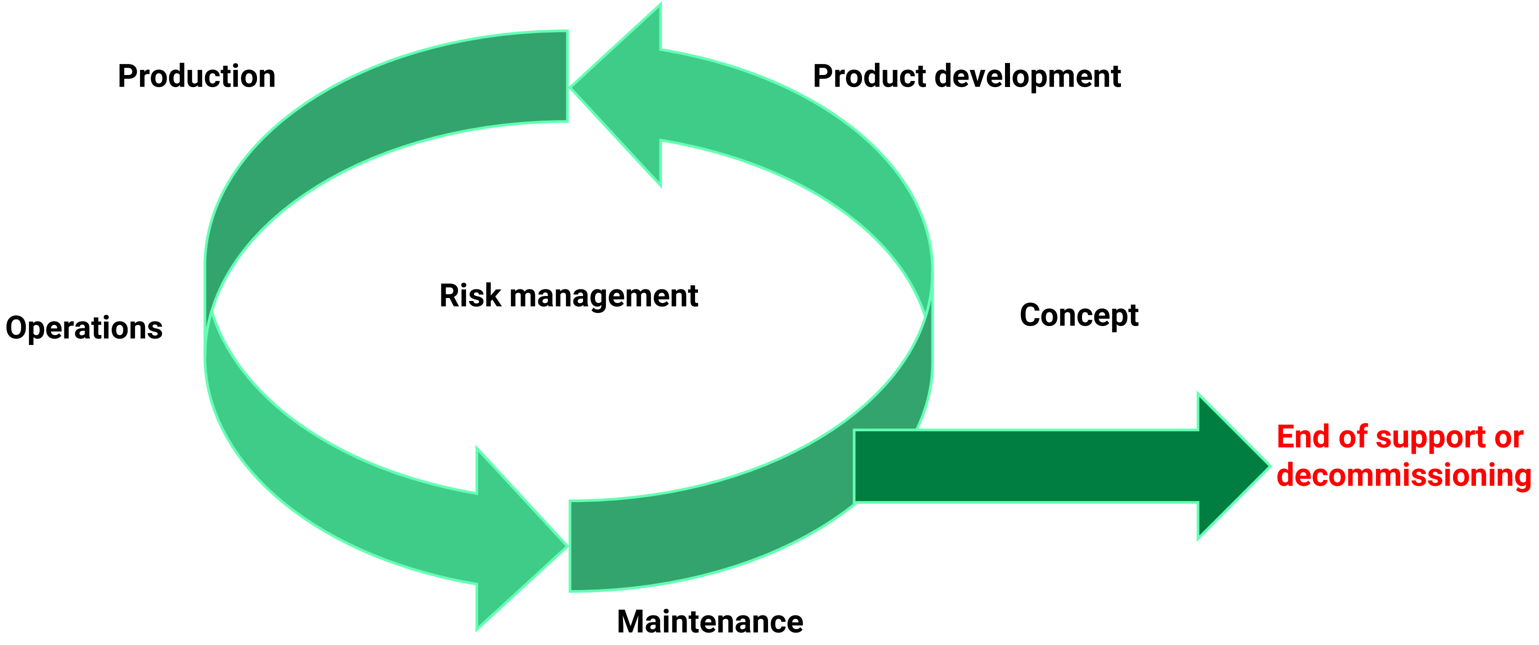
- Describes the steps to perform a robust risk analysis on the system
- Complex process to be performed multiple times and for multiple assets

Clause 14: End of cybersecurity support and decommissioning

General

- The last phase of the product lifecycle and cybersecurity activities
- End of CS support would refer to the end of CS activities, and decommissioning refers to the end of the product lifecycle
- End of support or decommissioning of an item (or component) shall be considered in the early phases of the lifecycle such as concept and development
- Procedures and processes for ending support and decommissioning are different
- Cybersecurity implications post ending support or decommissioning shall be treated separately

Clause 14: End of cybersecurity support and decommissioning



Clause 14: End of cybersecurity support and decommissioning

End of support

- End of support means, any form of service support for an item or component concerning bug fixing, modification, improvement, etc. will no longer be available
- A procedure such as an agreement document will be created to establish and communicate the end of support for an item or component's life cycle
- Communication could be handled between supplier and customer based on the mutual agreement and contractual requirements
- Even after the end of support, the item or component could still function as it's intended to
- Procedure and process could include:
  - Complete handover of technical documents, intellectual property, and support
  - document the supplier's failures and shortcomings
  - review the contract and the termination provisions
  - consider an exit plan that will minimize the potential for disruption

Clause 14: End of cybersecurity support and decommissioning

Decommissioning

- Decommissioning is a generic process term to remove product or service from active status
- Decommissioning is different from end of cybersecurity support with respect to execution
- When decommissioning is to take place, the following can be considered:
  - Decommission planning and approval
  - Create a communication plan
  - Involve and inform the required touchpoints (stakeholders)
  - Consider financial aspects if applicable
  - Archived data removed
  - Any user related personal data to be removed
  - Service updates and access to be removed
  - Etc.

Clause 14: End of cybersecurity support and decommissioning

Summary of work products

- [WP-14-01] Procedures to communicate the end of cybersecurity support

DEKRA

DEKRA DIGITAL

Thank you for your attention