DEKRA

DEKRA DIGITAL

Training ISO/SAE 21434

Organizational Management Activities

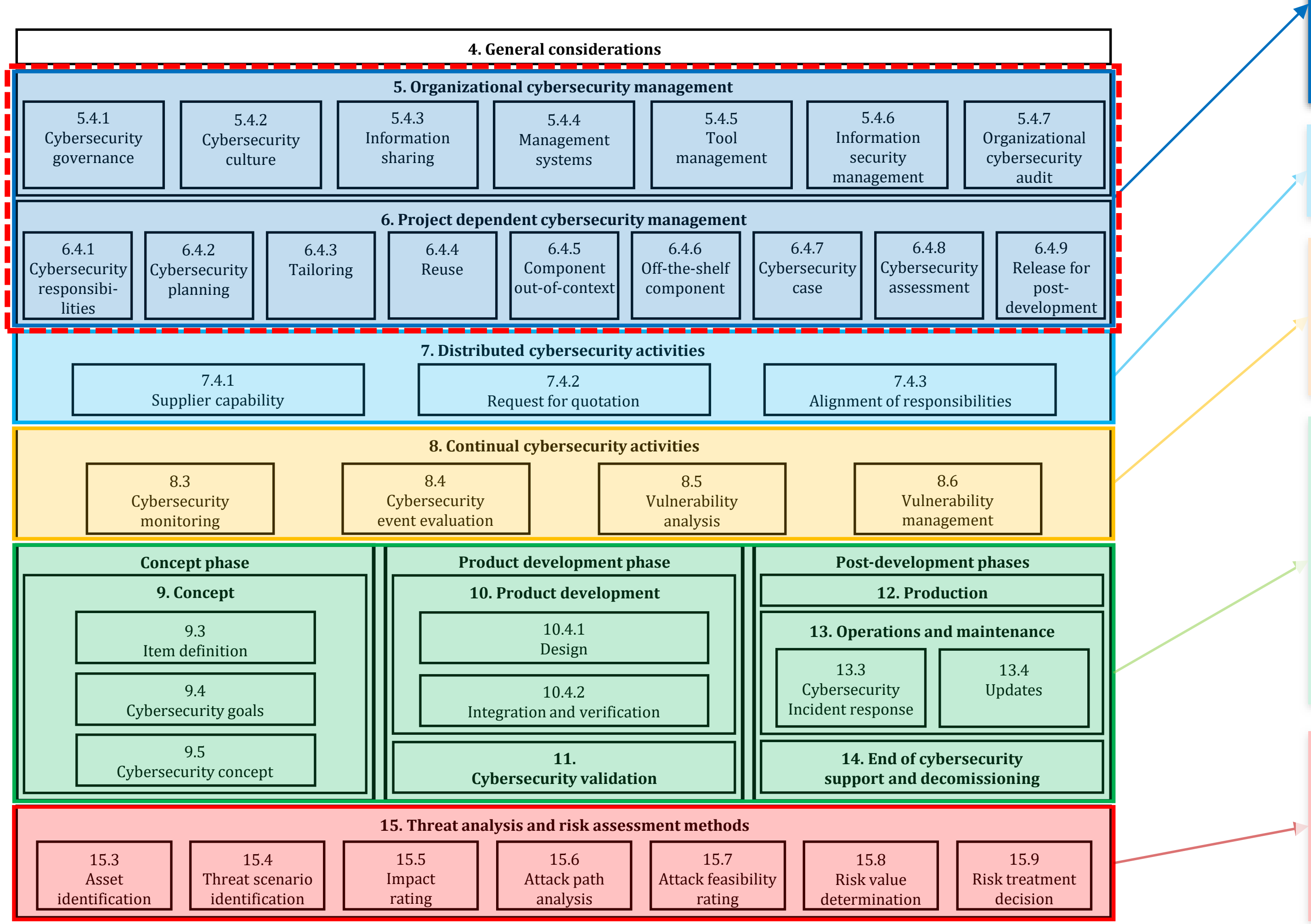
DEKRA

CONTENT

1. Introduction
2. Cybersecurity Governance
3. Cybersecurity Culture
4. Information Sharing and Information Security
5. Quality Management
6. Tool Management
7. Organizational CS Audit
8. Summary

1. INTRODUCTION

Structure of ISO/SAE 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.

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

What is Organizational Cybersecurity Management?

- Managing the risk of road vehicles and protecting their components and interfaces throughout the product lifecycle is the goal of organizational cybersecurity management
- Each phase has its own set of requirements and goals, which rely on continuous risk management throughout the lifecycle
  - Concept phase
  - Product development phase
  - Production, operation, and maintenance phase
- If the management system is effectively implemented, it will assist in lowering the risk both at the organizational and product level

Objectives

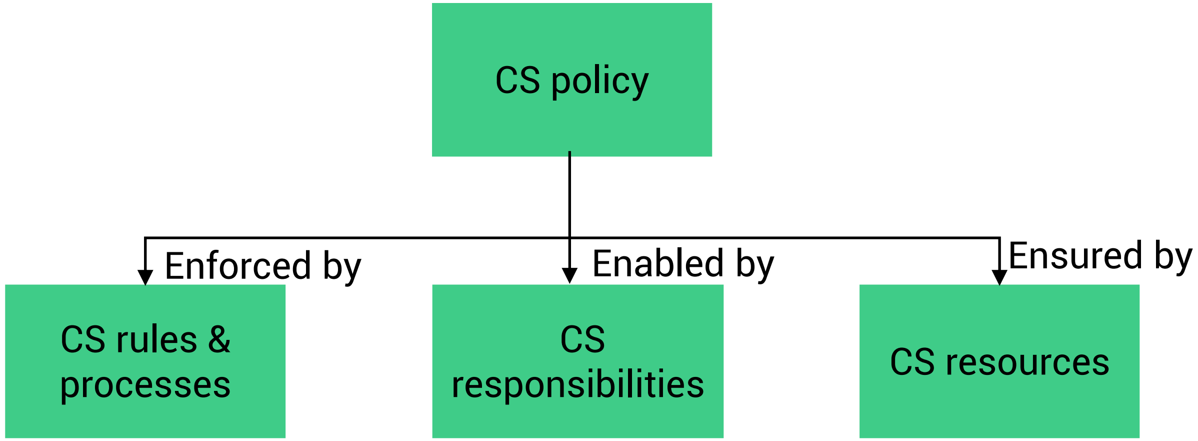
- Define organization-specific rules, policies, and processes for CS activities
- Assignment and communication of roles and responsibilities
- Support CS implementation which includes:
  - Resource allocation
  - Management of interactions between cybersecurity processes
- Establish and maintain a CS culture
  - To manage competence and awareness management
  - To apply continuous improvement
- Institute and maintain management systems
  - Quality management to support CS maintenance
  - Tool management to ensure the security of the tools used for CS activities
- Perform CS audit within the organization

2. CYBERSECURITY GOVERNANCE

Cybersecurity Governance

CS governance explains the policies and processes which determine how organizations identify, prevent, and respond to cyber incidents

- Policies help employees in understanding their role in protecting the organization's assets
- CS policy enforces the rules and processes that enable security engineering
- CS policy ensures resources to implement cybersecurity risk mitigation measures and to train cybersecurity personnel
- CS policy is enabled by communicating roles and responsibilities to corresponding authorities



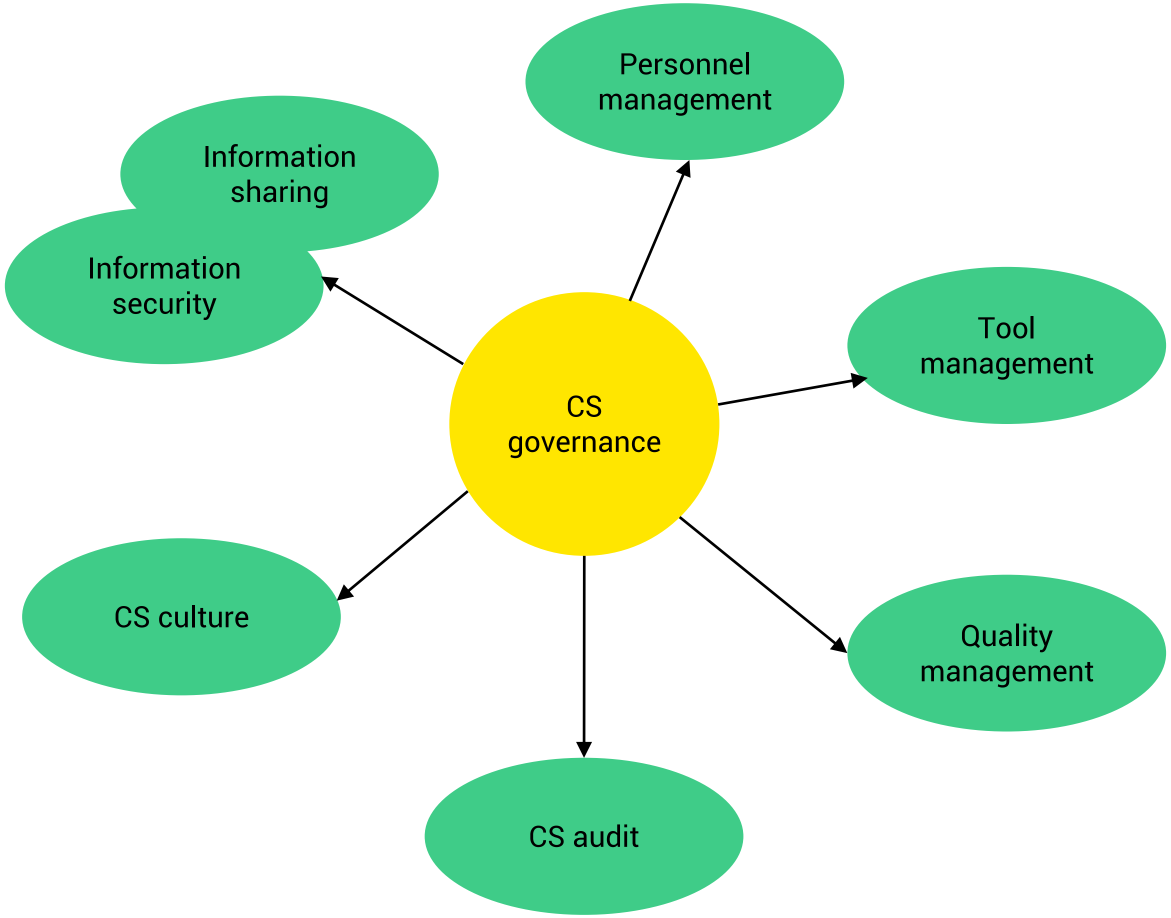
Key Requirements I - Cybersecurity Governance

Organizations should develop a company-wide policy that includes:

- Acknowledgement of risk related to road vehicles
- Top management commitment is required to reduce those risks

Organizations should define CS rules and processes

- E.g., rules for handling sensitive data, process definition for reporting incidents



Key Requirements II - Cybersecurity Governance

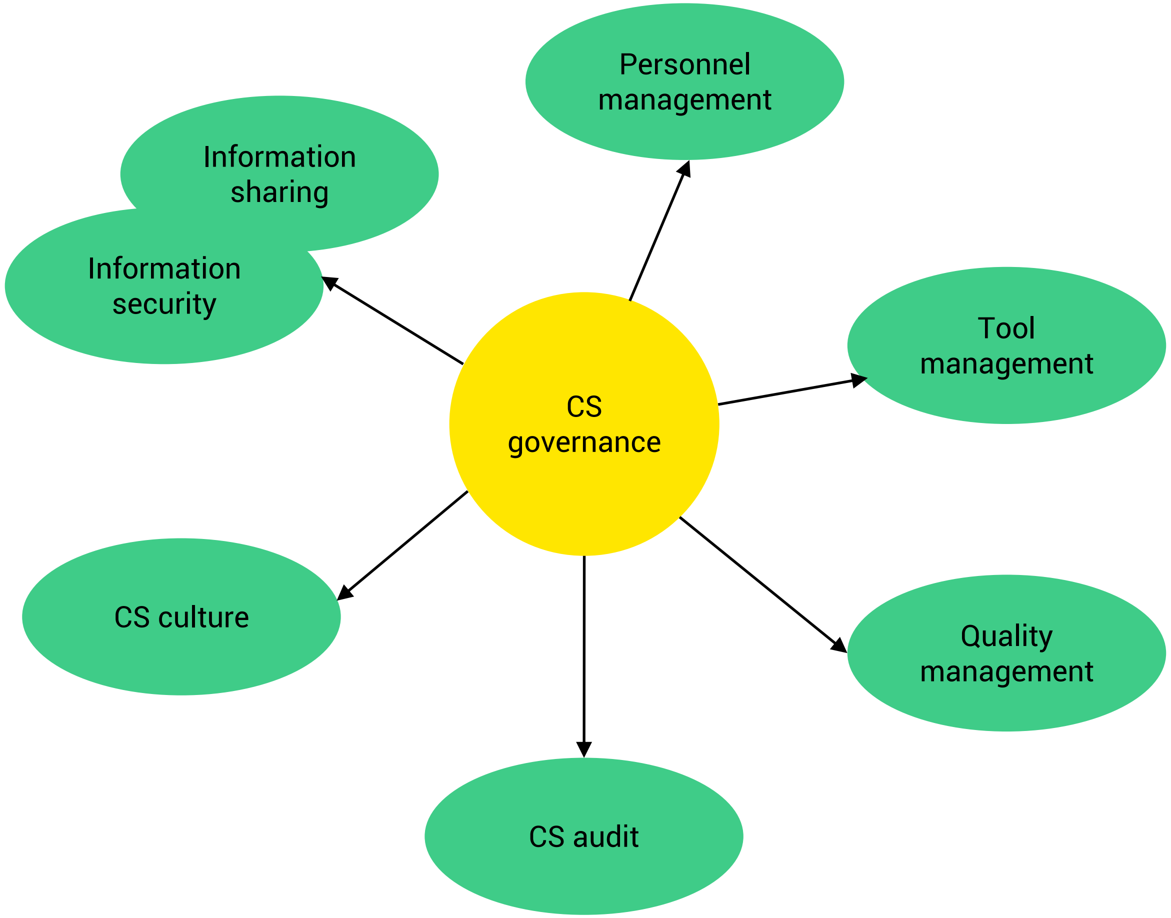
Assign and communicate responsibilities (including project level)

- E.g., assign responsibility according to the RASIC approach

Allocate resources to address CS activities

- Budget, tools, personnel, IT infrastructure, guidelines, etc.

CS-related disciplines should be identified which are related to other disciplines (safety, backend, IT security, etc.)



3. CYBERSECURITY CULTURE

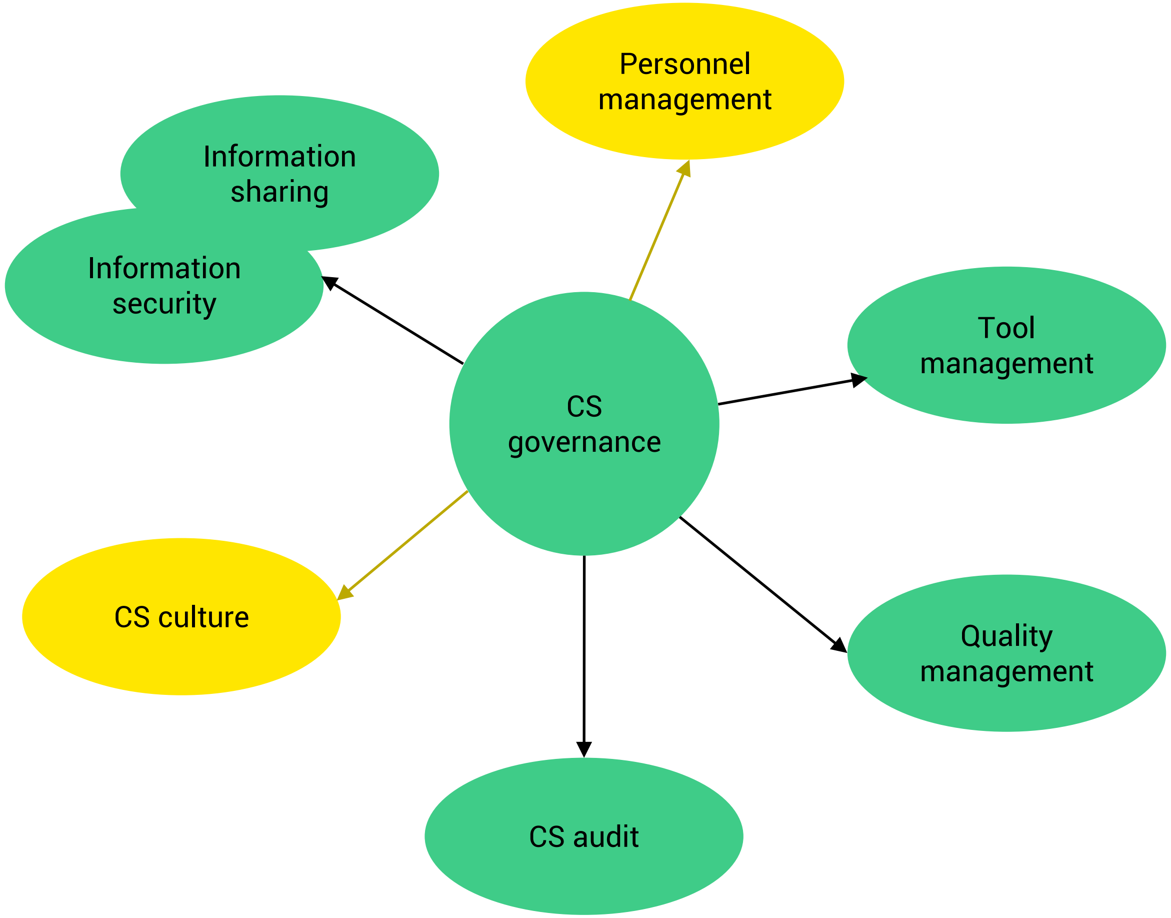
Cybersecurity Culture

CS culture

is about incorporating security considerations into an employee's job, their behavior and embedding them in their day-to-day actions

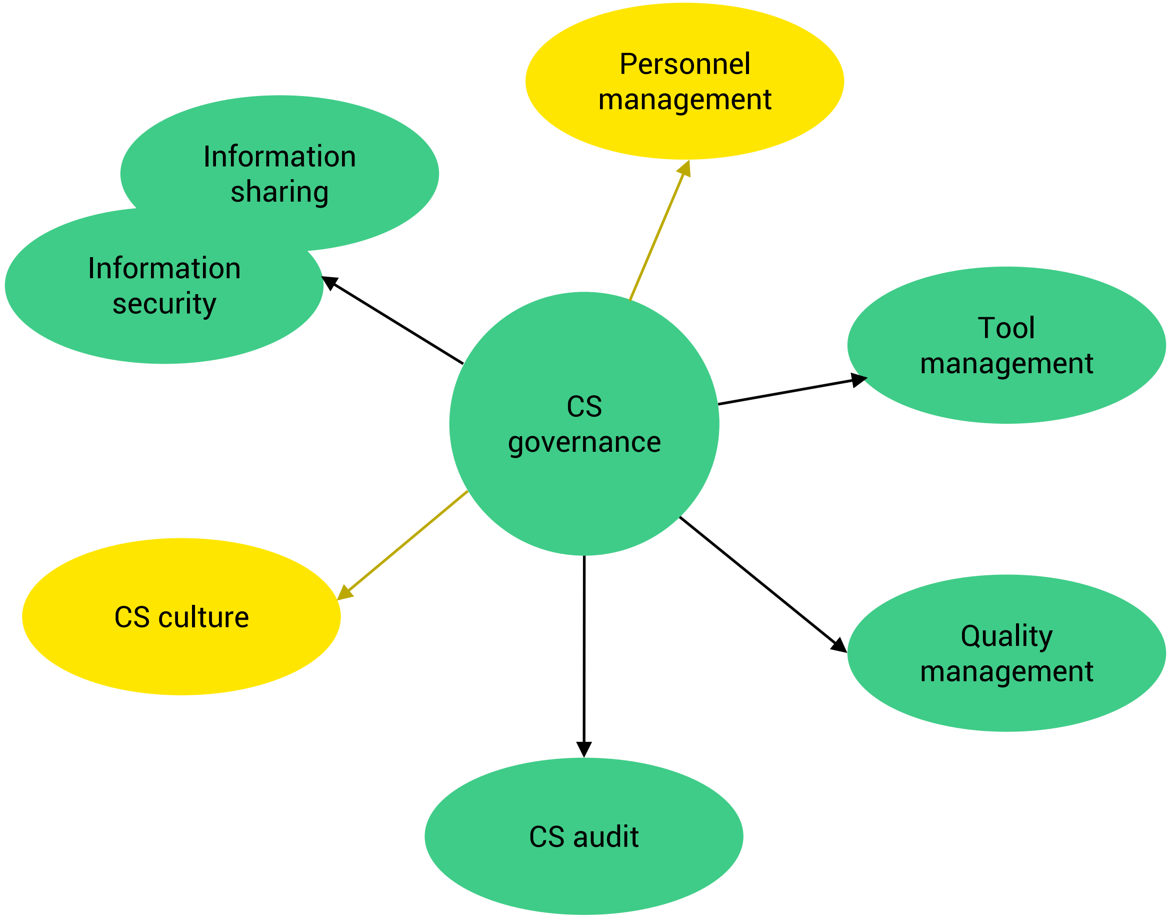
Personnel management

needs CS relevant responsibilities for activities (e.g., risk management, development, incident response, …) well educated CS staff, diversity in different dimensions



Key Requirements - Cybersecurity Culture

- The organization should promote and sustain a strong CS culture
- The organization must ensure that those who are given CS-related roles and responsibilities have the necessary skills and knowledge to carry them out
- Organization must establish and maintain continuous improvement processes for all CS activities
  - For example, learning from previous cybersecurity incidents



Examples of Good Cybersecurity Culture

- Accountability for CS-related decisions is traceable
- CS and safety have the highest priorities regarding design and development decisions
- Effective achievement of CS is encouraged (rewards/punishment)
- Proactive attitude towards CS (monitoring, early vulnerability analysis, and risk assessments, incident response processes defined)
- Resources are planned and allocated
- Intellectual diversity is valued
- Continuous improvement is sought in all processes
- Processes are well-defined, traceable, and controlled

4. INFORMATION SHARING AND INFORMATION SECURITY

DEKRA

Information Sharing and Information Security

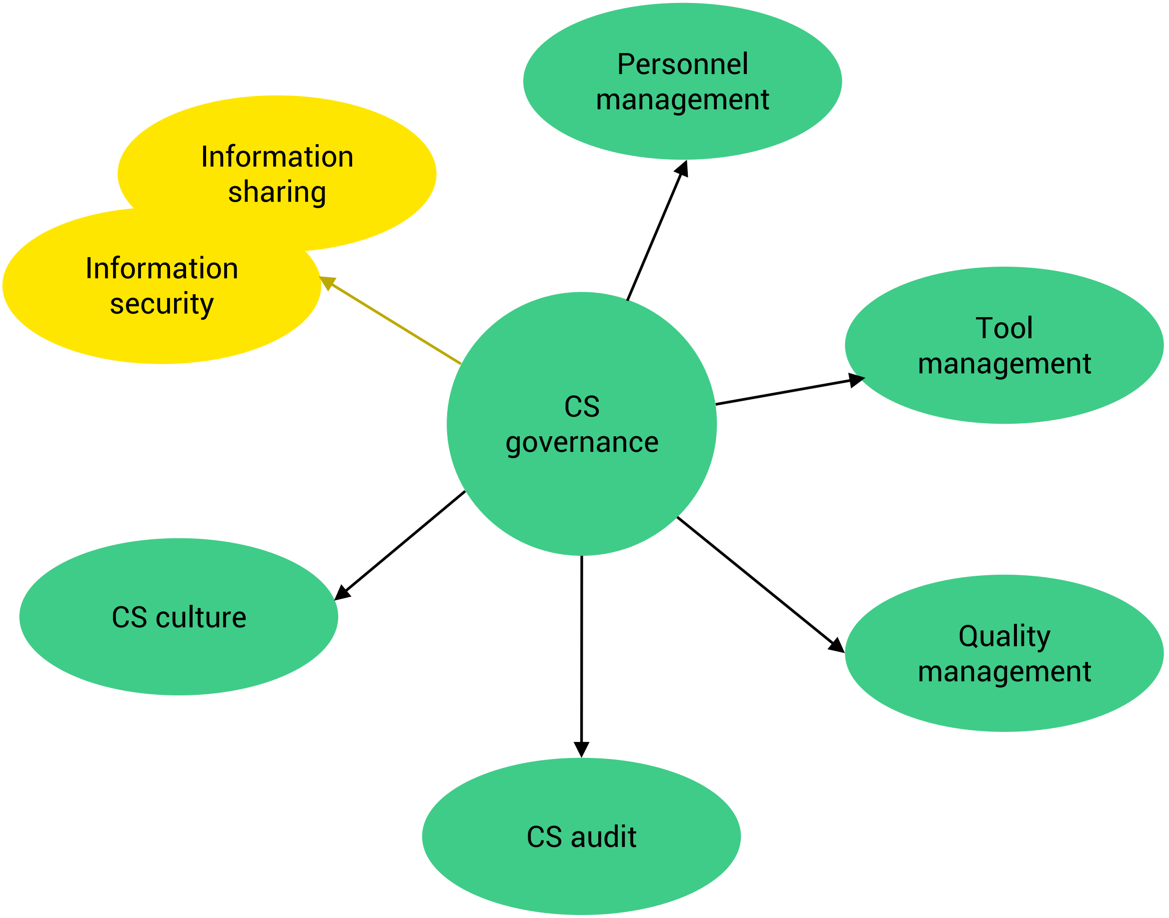
Information sharing

Defines the rules and processes to share cybersecurity relevant information

Information security

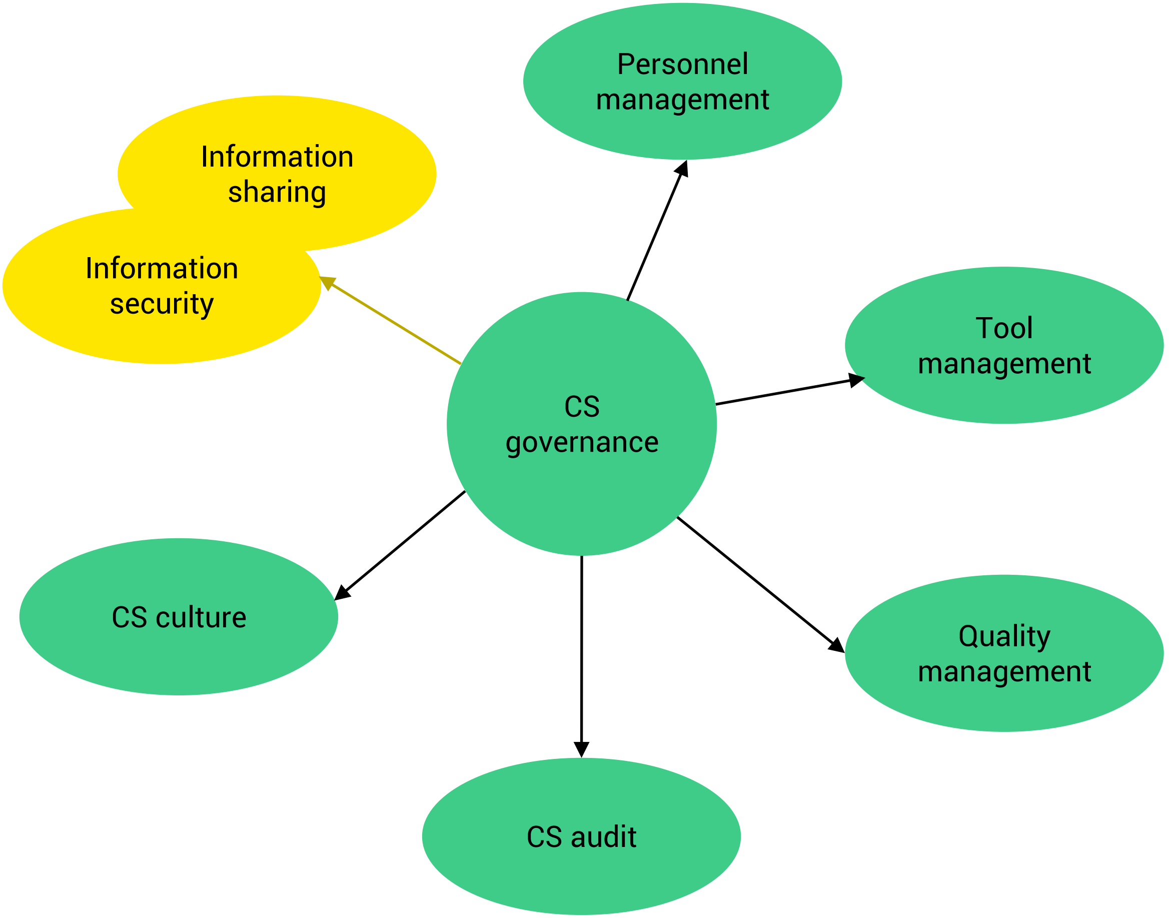
Manages the confidentiality, availability, and integrity of assets

The goal of the above 2 activities is to have complete control of CS relevant information and workflows



Key Requirements - Information Sharing and Information Security

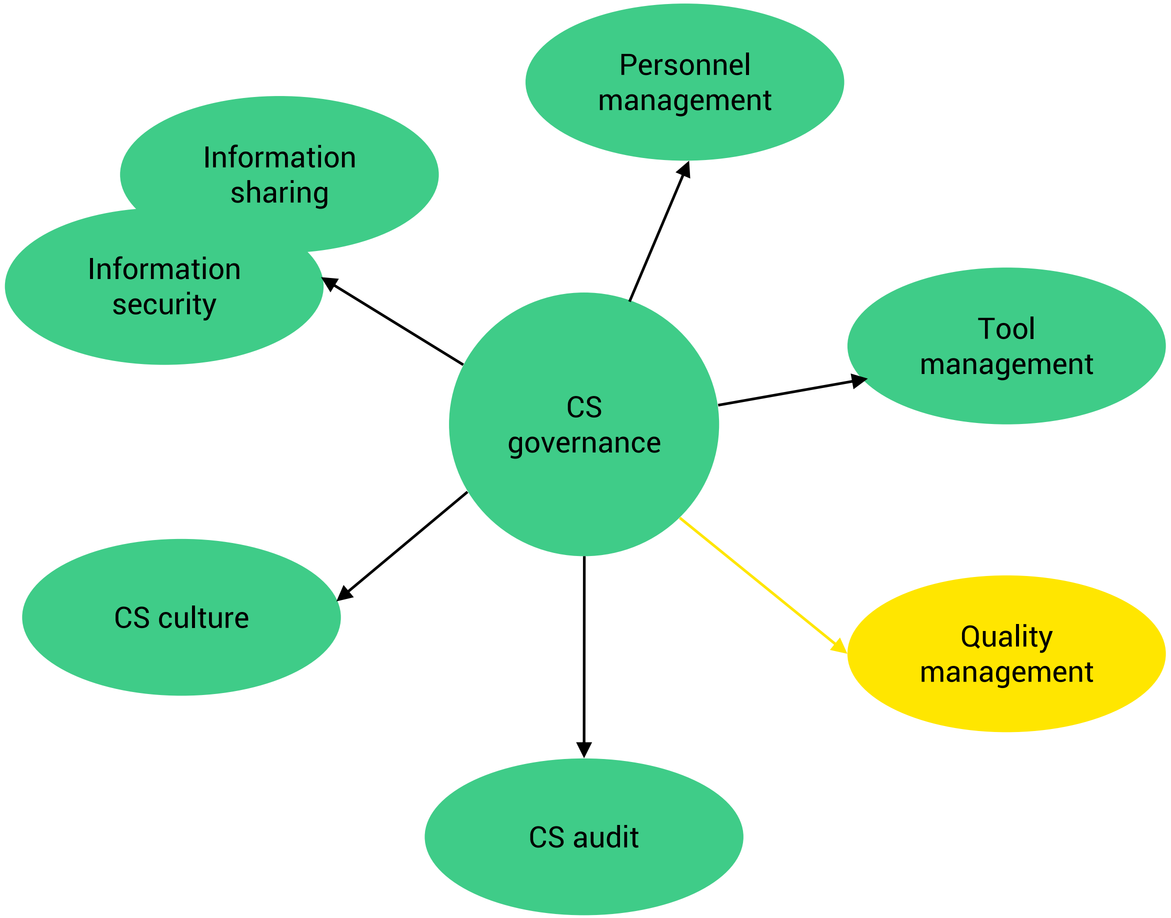
- Information security management systems should be used to manage the work products achieved from all the requirements
  - For example, work products saved on a secured file server
- Organization must define the conditions under which cybersecurity-related information sharing is required, permitted, and prohibited
  - Categorization of information (public/internal/classified)



5. QUALITY MANAGEMENT

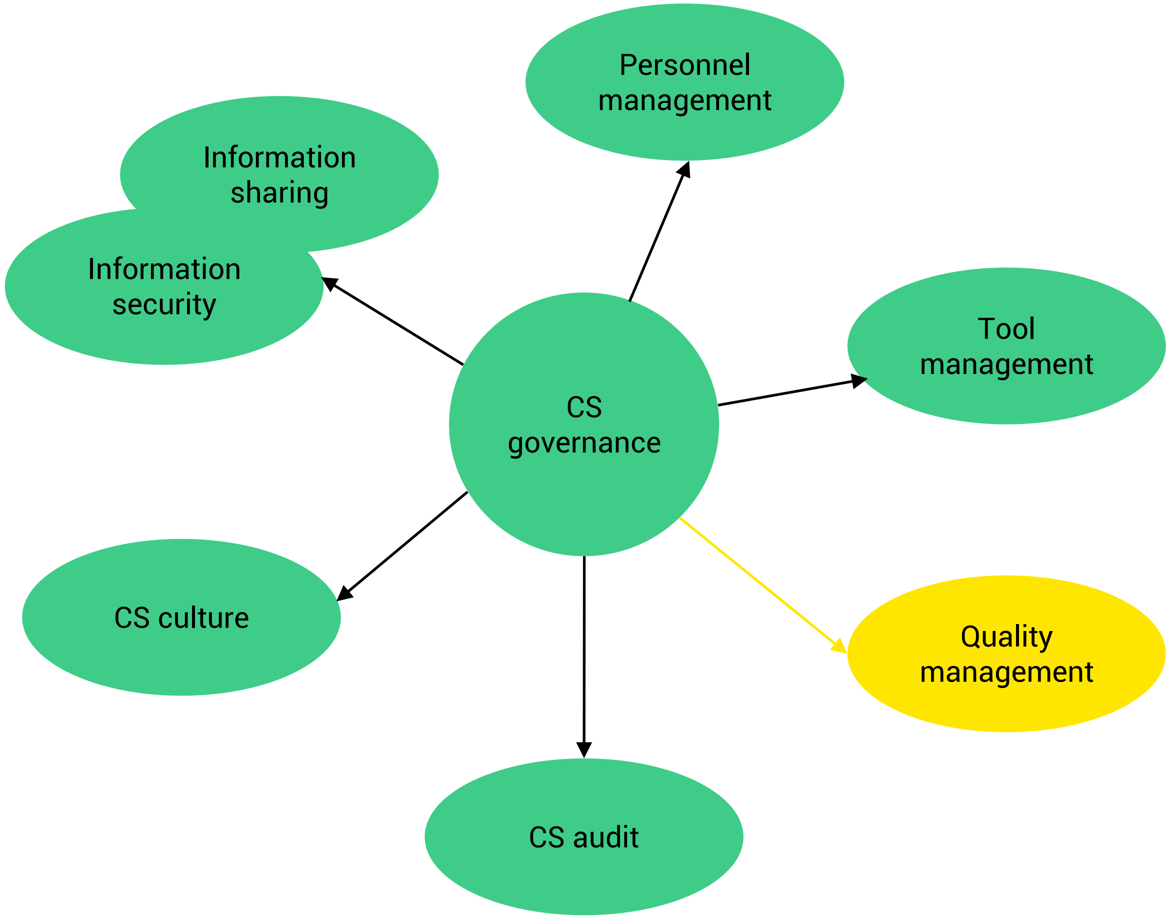
Quality Management

To achieve security engineering goals, a quality management system is defined which states that processes, methods, and responsibilities should be documented for meeting quality policies and objectives



Key Requirements - Quality Management

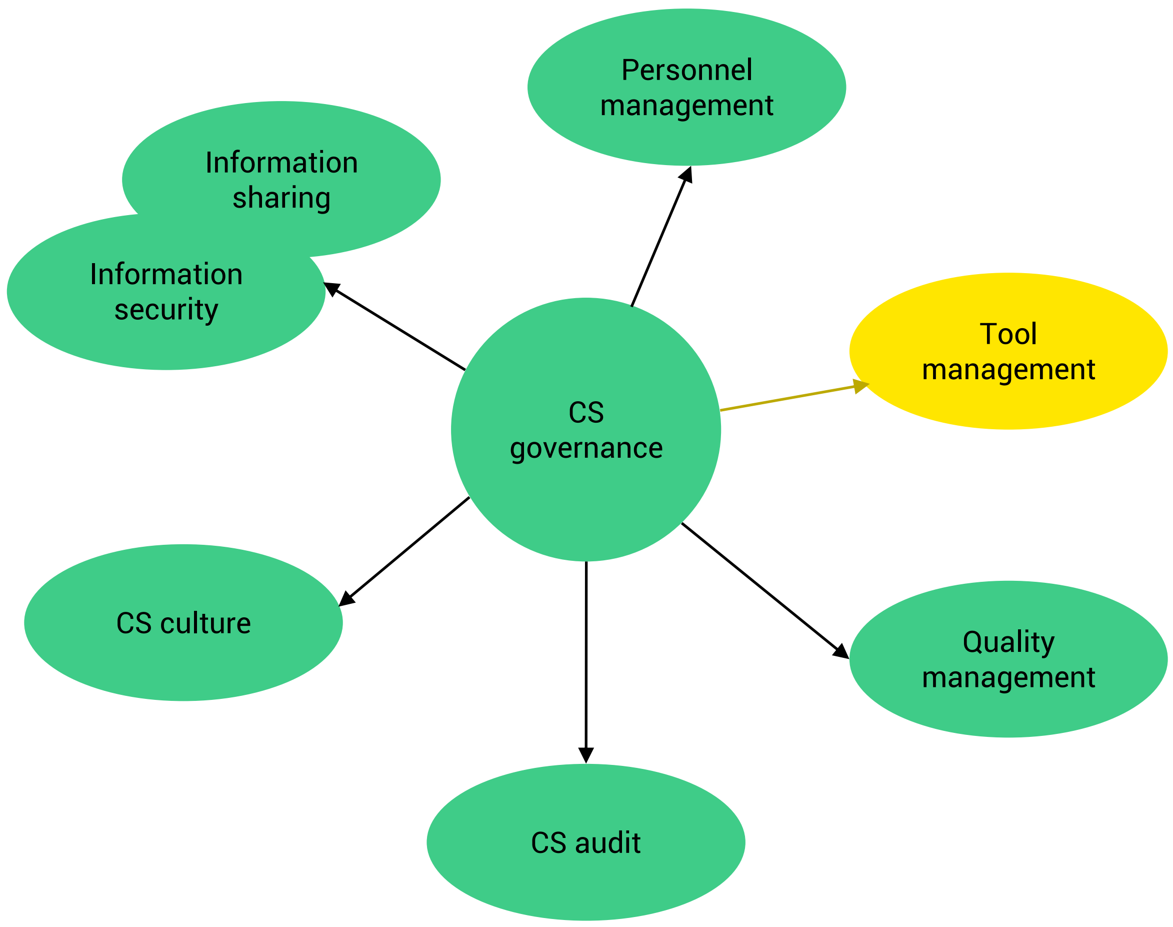
- Quality management system ideally based on existing standards (i.e., IATF 16949, TISAX, …)
- It should define rules and processes for
  - document management,
  - change management,
  - configuration management,
  - and requirement management



6. TOOL MANAGEMENT

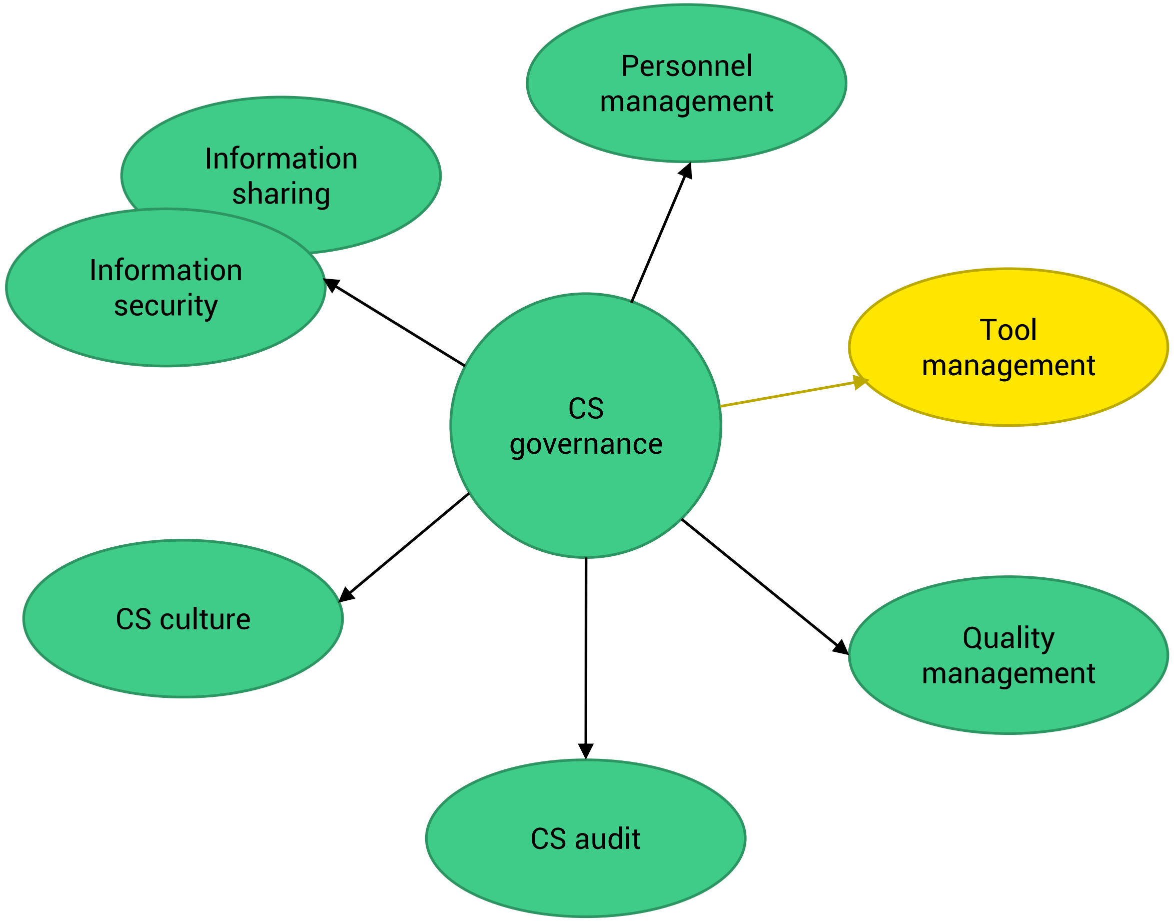
Tool Management

Managing the tools which are used during the production lifecycle that could affect the cybersecurity of an item or component



Key Requirements - Tool Management

- Tools that can affect an item or component's cybersecurity must be controlled throughout the product lifecycle
  - By creating a list of tools that includes the tool's name, the purpose of usage in the project, version number, etc.
  - E.g., Tools for performing TARA, software integration tools, code generation tools, etc.
  - Secure delivery of the tool, such as the process for granting and rescinding access rights
  - Tool related incidents should be recorded and reported

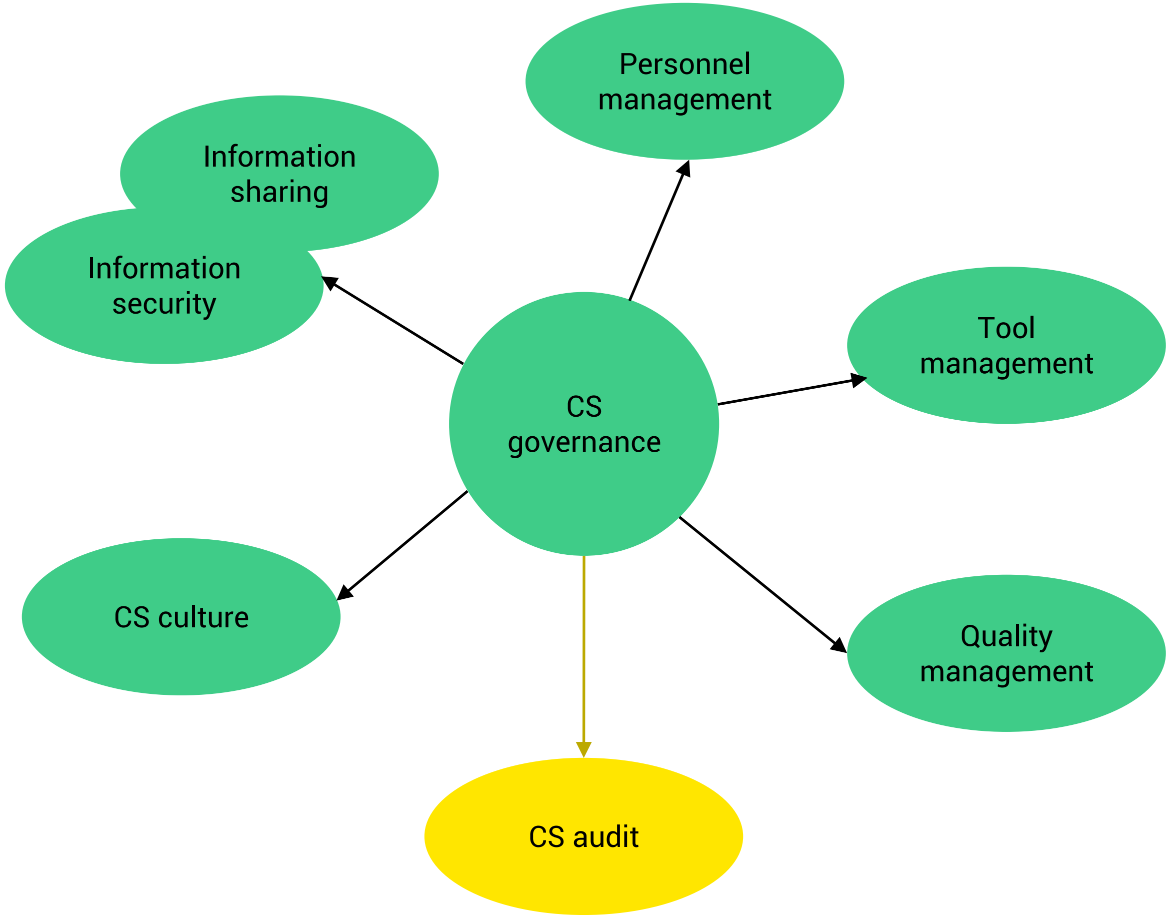


7. ORGANIZATIONAL CS AUDIT

Organizational CS Audit

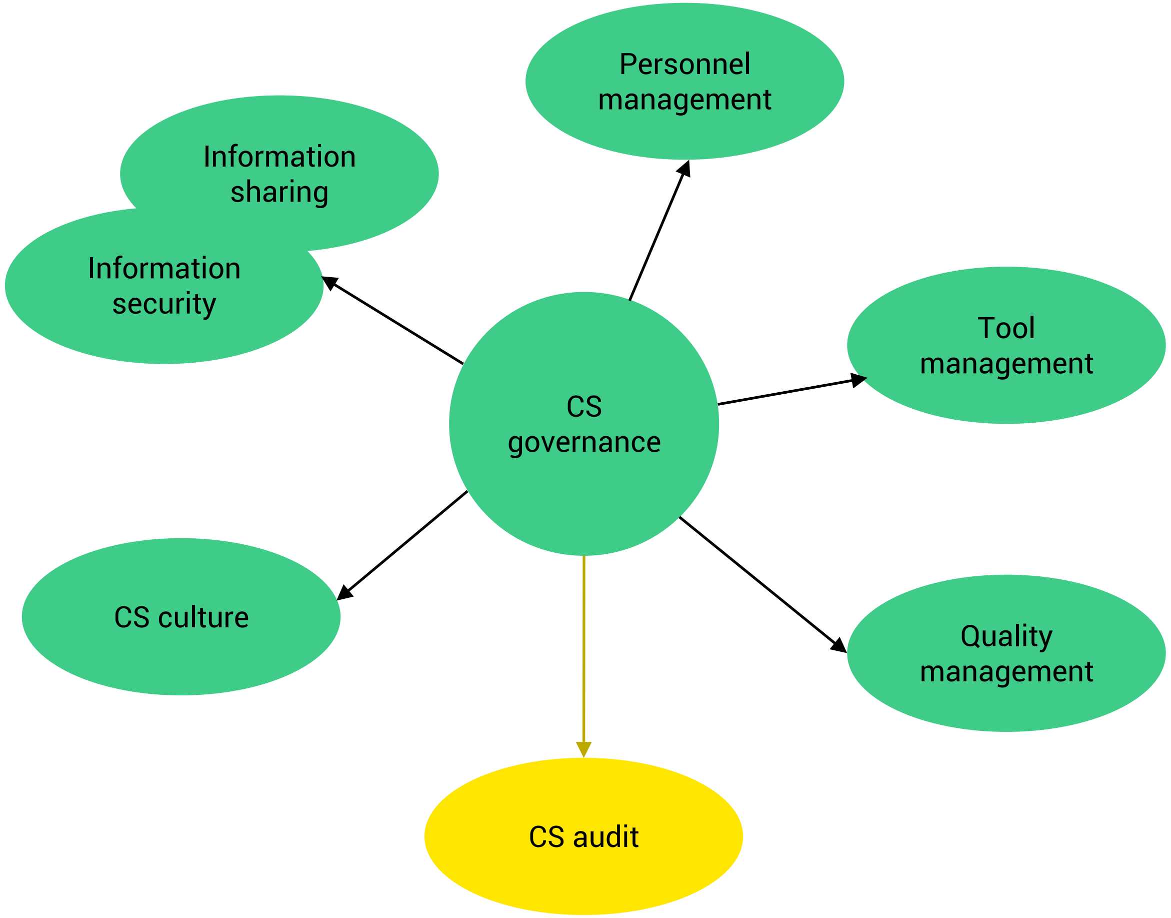
A CS audit examines an organization's CS activities in a systematic and independent manner

An audit verifies that security controls, policies, and procedures are in place and functioning properly



Key Requirements - Organizational CS Audit

- An independent CS audit must be performed to determine whether the organizational processes meet the objectives of this document
  - CS audit can be combined with quality management audit or functional safety audit because they are performed regularly
  - Auditors (independent) can be either internal or external to the organization
  - A periodic audit can be performed to ensure organizational processes remain appropriate for cybersecurity



8. SUMMARY

Summary

Key Takeaways

- Organizations must maintain all the documents relevant to CS activities
- This clause gives us the requirements for enabling CS engineering
- Clear roles and responsibilities should be communicated
- All CS activities are subject to continuous improvement

Work Products

- [WP-05-01] Cybersecurity policy, rules, and processes
- [WP-05-02] Evidence of competence management, awareness management, and continuous improvement
- [WP-05-03] Evidence of the organization's management systems
- [WP-05-04] Evidence of tool management
- [WP-05-05] Organizational cybersecurity audit 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

ORGANIZATIONAL MANAGEMENT ACTIVITIES

Thank you!