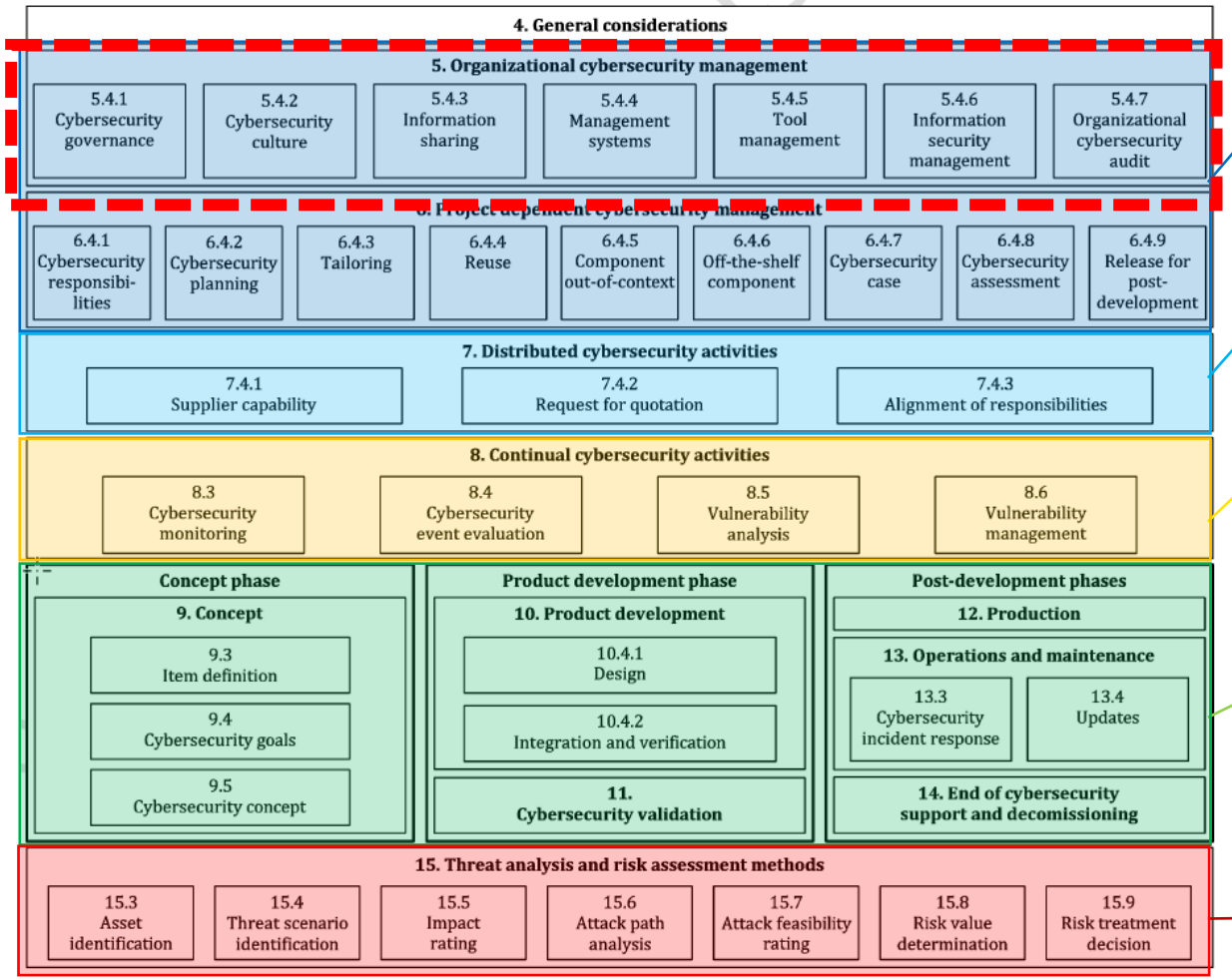
Clause 5: Organizational Management Activities

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..

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 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 5: Organizational Cybersecurity Management

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

Clause 5: Organizational Cybersecurity Management

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

Clause 5: Organizational Cybersecurity Management

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. The policy is imposed by enforcing the rules and processes that enable security engineering.
- CS policy is ensured by securing resources to implement cybersecurity risk mitigation measures and by training cybersecurity personnel
- CS policy is enabled by communicating roles and responsibilities to corresponding authorities

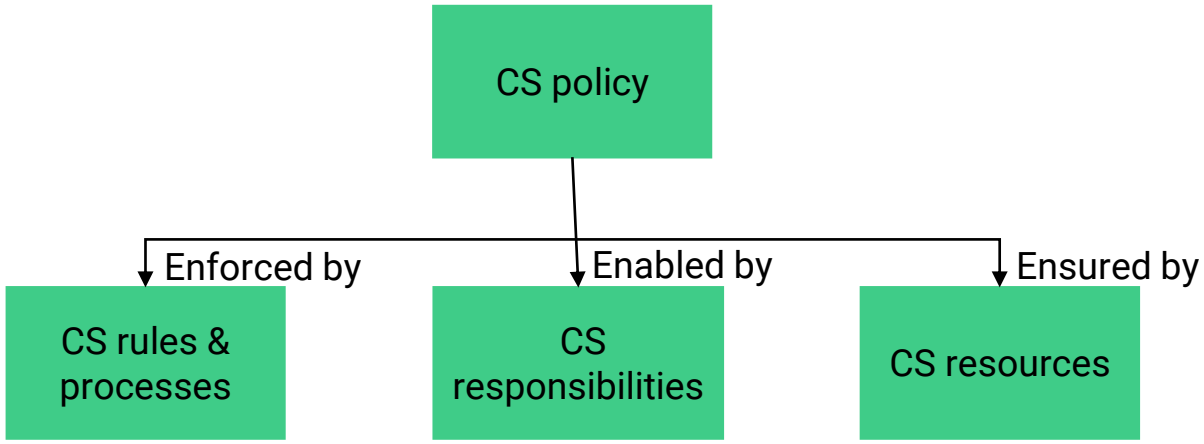
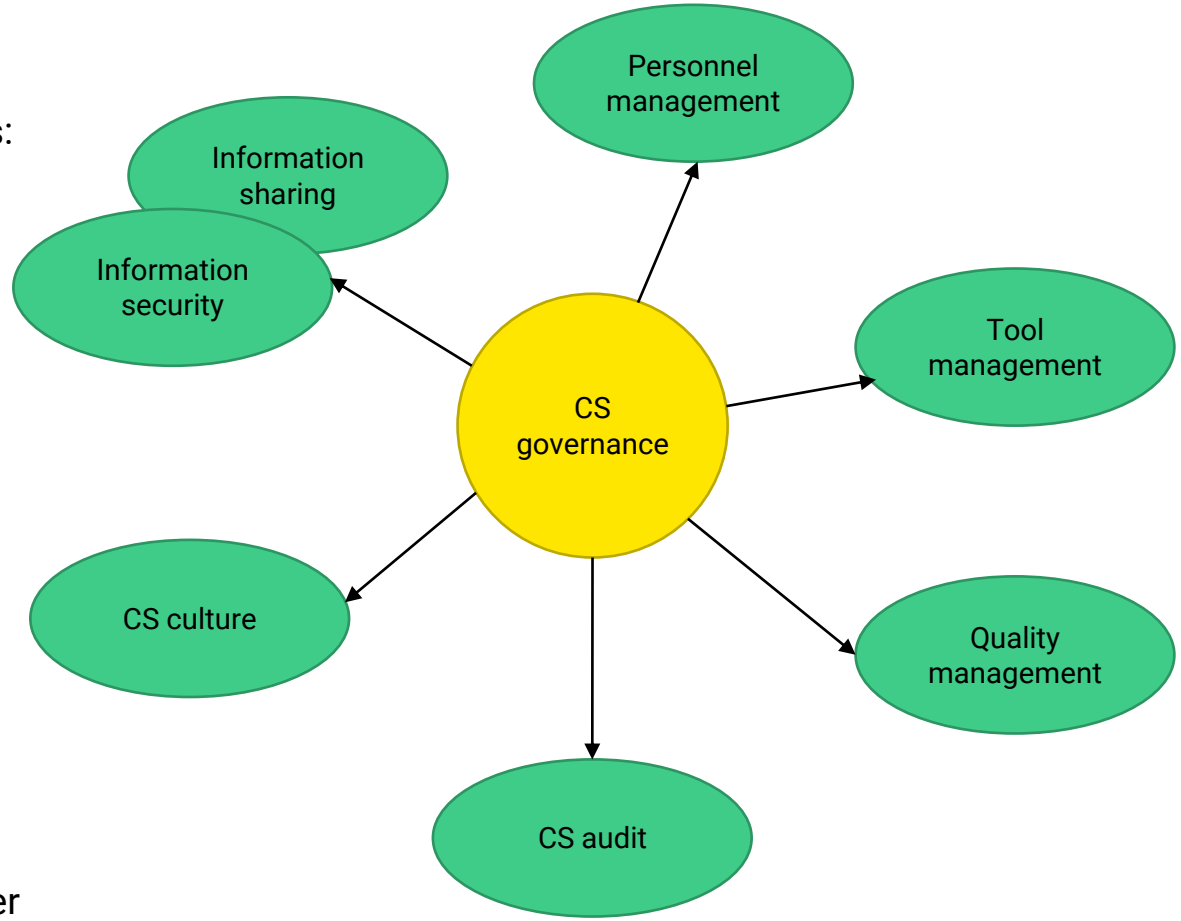


Figure 1- Cybersecurity governance according to ISO 21434

Clause 5: Organizational Cybersecurity Management

Key requirements

- Organization 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
  - For example, rules for handling sensitive data, process definition for reporting incidents
- 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.)

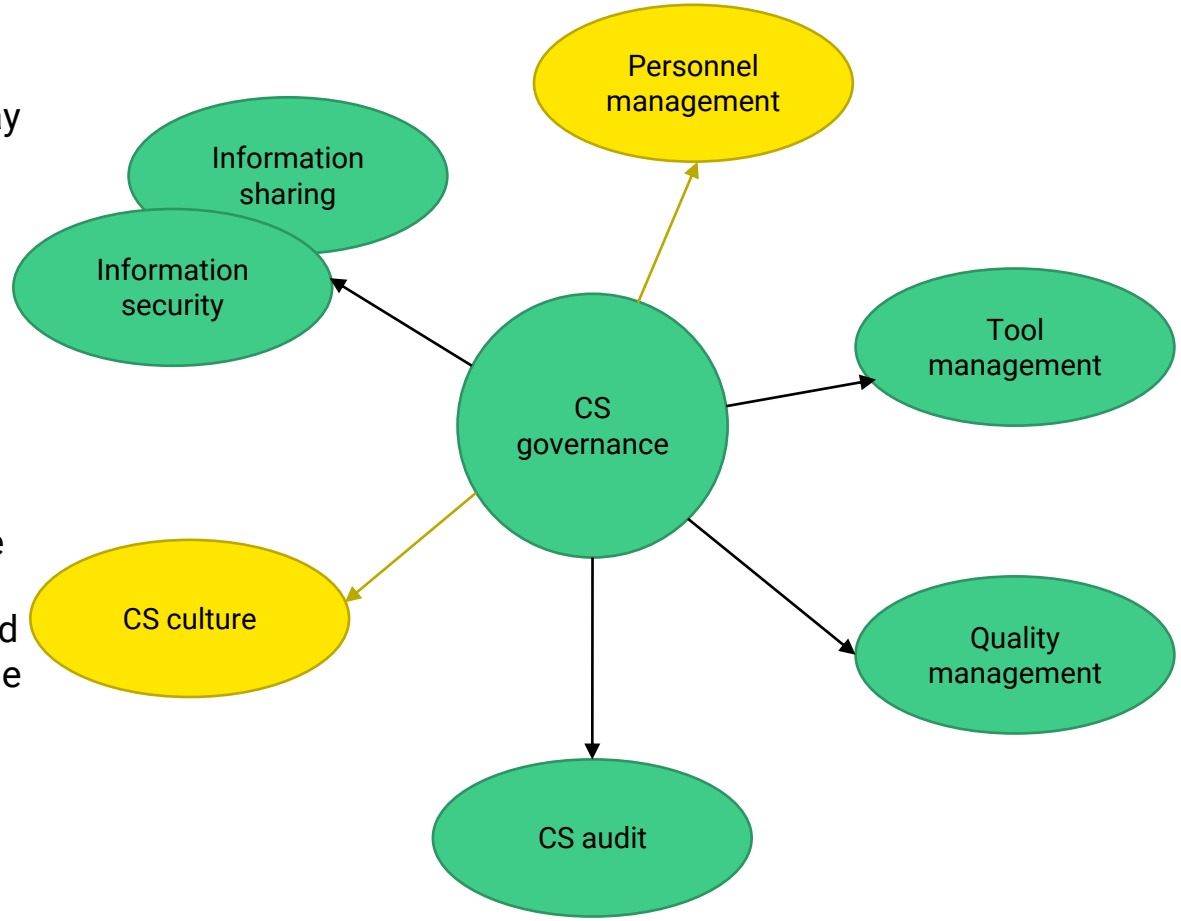


Clause 5: Organizational Cybersecurity Management

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. The success of adherence to CS policy, which is the primary success factor for CS governance, is defined by CS culture.

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



Key requirements

- 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 cyber incidents

Clause 5: Organizational Cybersecurity Management

Examples of a cybersecurity culture practices :

- 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

Clause 5: Organizational Cybersecurity Management

Information sharing and information security

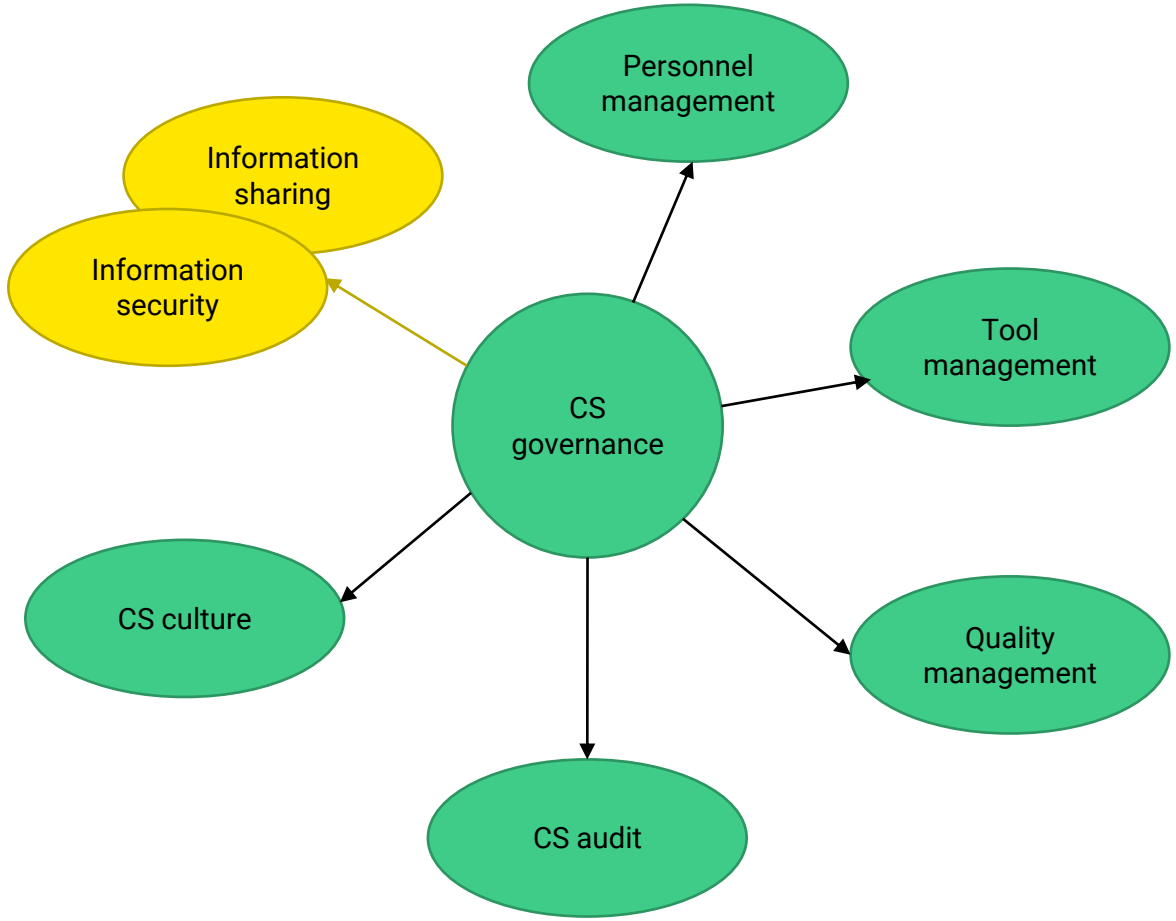
Information sharing: Defines the rules and processes to share cybersecurity relevant information

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 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)



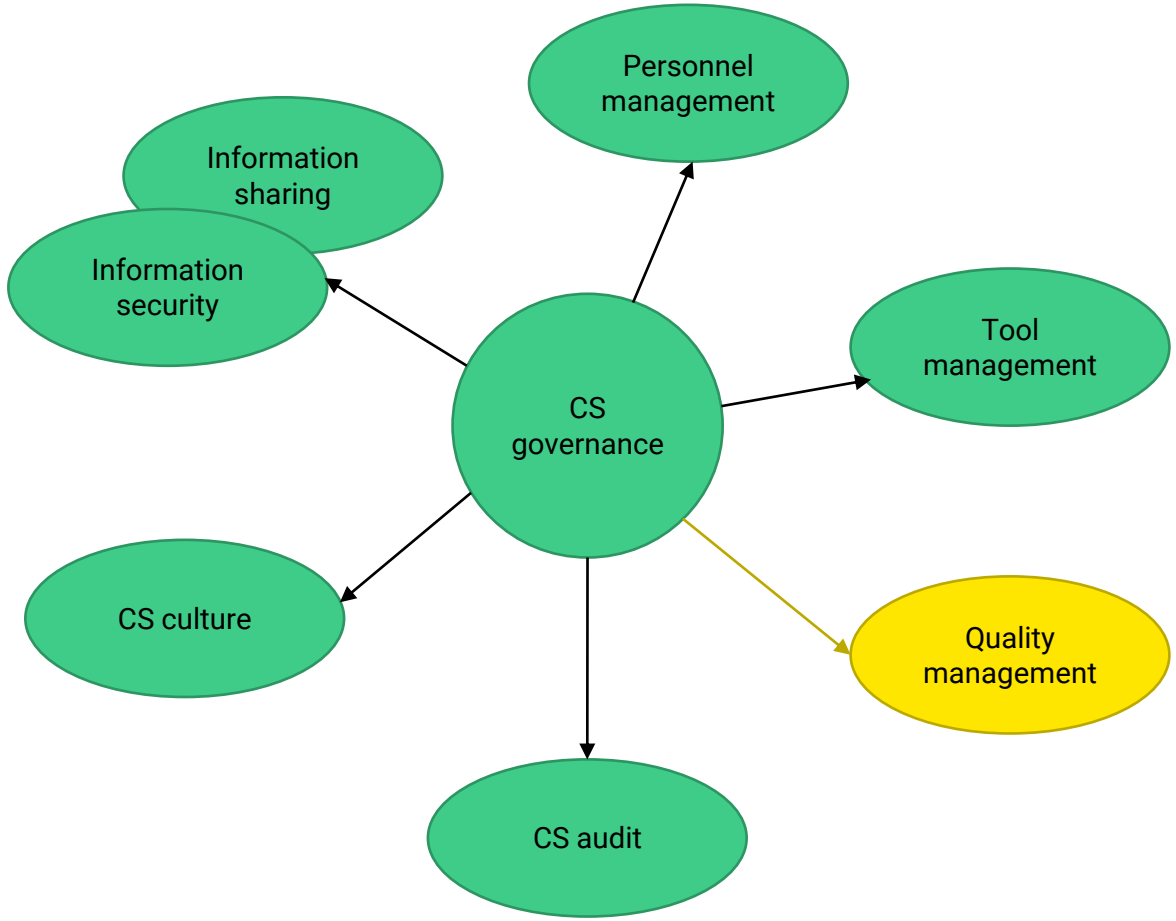
Clause 5: Organizational Cybersecurity Management

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 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



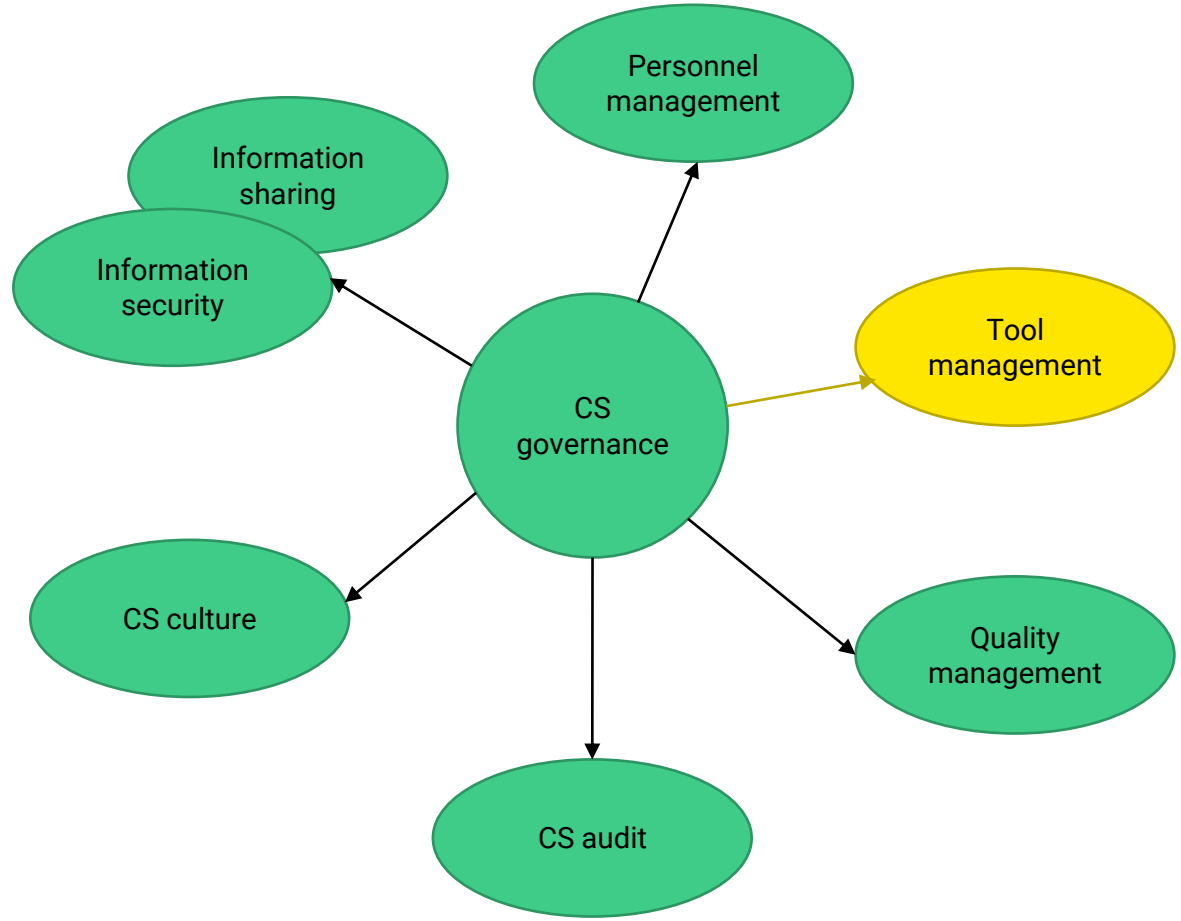
Clause 5: Organizational Cybersecurity Management

Tool management

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

Key requirements

- 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



Clause 5: Organizational Cybersecurity Management

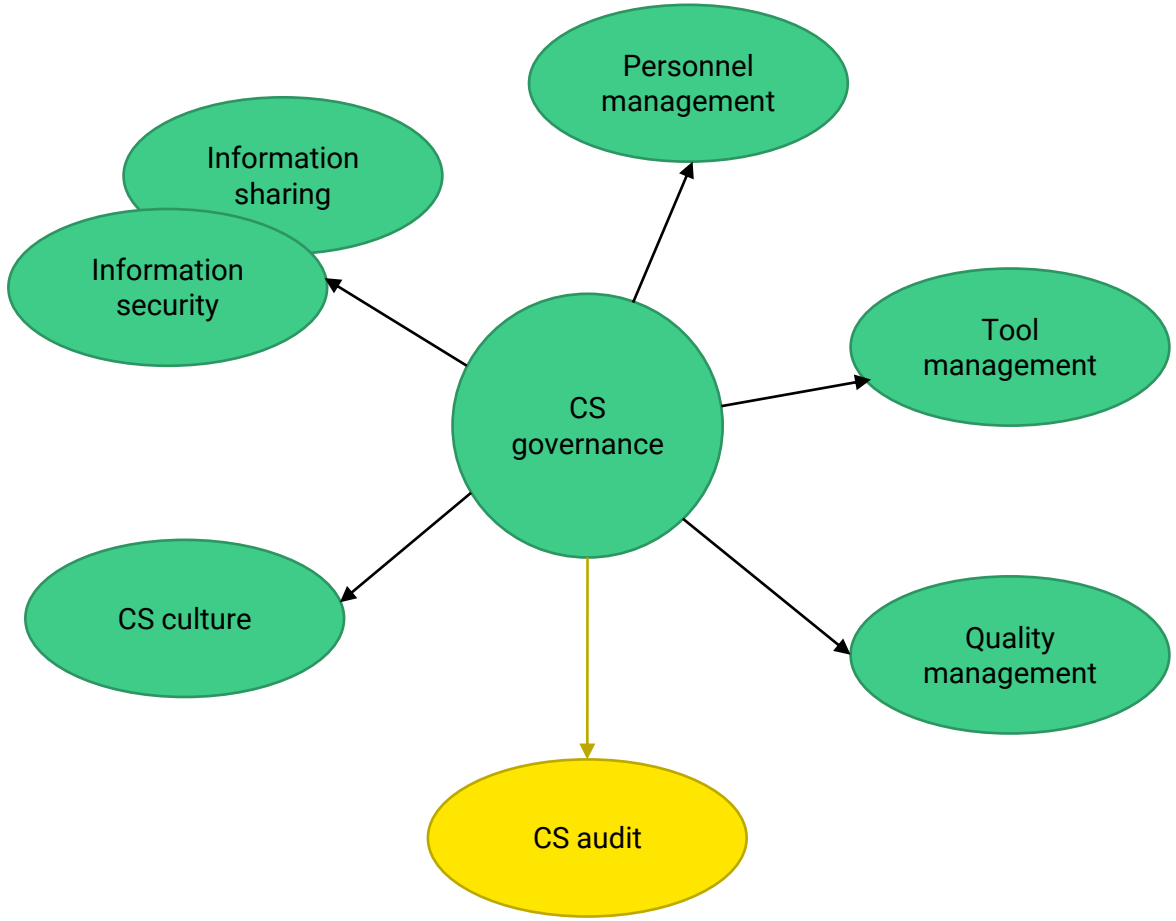
Organizational CS audit

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

- 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 on a regular basis
  - 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



Clause 5: Organizational Cybersecurity Management

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

Summary of 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