9. Integration of supply chain cybersecurity through the product and service life-cycle

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - To ensure that products and services are protected against cyberattacks throughout their entire lifecycle.
- **Participants**
  - Management, IT, procurement, and other relevant functions.
- **Application**
  - Continuius monitoring.

Life-cycle and cybersecurity practice

Life-cycle phase	Focus	Cybersecurity practices	Date	Responsibility	Status
Development					
Introduction					
Growth					
Mature					
Decline					

Examples of content elements

Certain practices may fall within different phases

Life-cycle phase	Focus	Cybersecurity practices
Development	Security by Design -– ensure architecture from the start.	• Threat modeling • Secure coding standard • Penetration testing of prototypes • Secure development pipeline
Introduction	Hardening and compliance – avoid security flaws at launch.	• “Hardening” of systems and networks • Patch management strategy • Compliance with relevant standards (ISO 27001, NIST, NIS2, GDPR) • Incident response plan
Growth	Scalable security – protect growing infrastructure and data.	• Continuous monitoring and incident handling • Automated threat detection • Access control and identity & access management • Data protection (encryption, data loss prevention)
Mature	Optimization and compliance improvement – maintain a high level of security.	• Regular audits and security reviews • Updated penetration tests • Supply chain security • User security training
Decline	Secure phase-out – protect data and avoid residual vulnerabilities.	• Secure data deletion • Decommissioning of systems and servers • Removal of access rights • Communication about end-of-life risks