CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

Supply chain security practices from a product and service lifecycle perspective

www.cyber-smv.dk

The tool has been developed as part of the project **Cybersecurity and Business Continuity** (www.cyber-smv.dk), supported by the Danish Industry Foundation. Published on May 12, 2026.

Purpose, participants, and application

- **Purpose**
  - Integration of supply chain security practices into cybersecurity and enterprise risk management programs.
  - Monitoring the effectiveness of these practices throughout the entire product and service lifecycle of the technology.
- **Participants**
  - **Internal:** Data and IT managers, legal/compliance functions, and product and service owners.
  - **External:** Suppliers and subcontractors, as well as potentially auditors/reviewers if certification is an objective.
- **Application**
  - Should be carried out on a risk-based and event-driven basis—routinely (e.g., annually, on contract renewal), and when material changes occur (e.g., major updates, incidents, ownership changes, or new critical dependencies).

Approach

Based on the practices in the rest of this document, organizations select the practices that are proportionate to a given supplier's criticality, risk profile, and role.

1. Select relevant lifecycle phases for the supplier (e.g., SaaS provider (Software as a Service) vs. hardware supplier).
2. Apply proportionality based on criticality and risk.
3. Map the selected practices to internal cybersecurity and Enterprise Risk Management (ERM) controls.
4. Monitor developments over time using KPIs/KRIs.

Covered aspects

1. Governance and integration of risks.
2. Concept, design, and requirements phase.
3. Supplier due diligence and selection.
4. Contracting and onboarding.
5. Development, production, and integration.
6. Delivery, implementation, and approval.
7. Operations, maintenance, and support.
8. Phase-out and termination.

Governance and integration of risks

Purpose

- To ensure that supply chain security risks are systematically integrated into the organization's governance, cybersecurity, and risk management.

Practices

- Establishing a supply chain security strategy and aligning it with cybersecurity and Enterprise Risk Management (ERM) objectives.
- Establishing a formal Cybersecurity Supply Chain Risk Management (C-SCRM) policy.
- Defining risk appetite and risk tolerance for supplier-related cyber risks and incorporating supplier risks into the company's risk registers.
- Establishing an explicit link between supplier risks and business impact analysis (BIA).
- Defining and monitoring KPIs/KRIs for supply chain security performance.
- Establishing fixed intervals for reporting to senior management or risk committees.

Concept, design, and requirements phase

Purpose

- To prevent risk by incorporating security requirements at an early stage.

Practices

- Identification of critical suppliers, subcontractors, and service dependencies.
- Mapping of product components and services in relation to business-critical processes.
- Establishment of security requirements for hardware, software, and services, including the definition of trust boundaries and threat models that also encompass suppliers.
- Establishment of privacy and data protection requirements.
- Establishment of secure design reviews that include supply chain threats (e.g., tampering and counterfeit components).

Supplier due diligence and selection

Purpose

- To select suppliers that are capable of meeting the security requirements.

Practices

- Establishment of a risk-based supplier classification (critical, high, medium, low) that includes assessments of financial, operational, legal, and geopolitical risks, as well as the supplier's cybersecurity maturity (policies, controls, certifications).
- Ongoing monitoring of suppliers' certification status (e.g., ISO/IEC 27001, NIS2).
- Establishment and maintenance of an overview of suppliers' incident history and vulnerability management practices.
- Requirements for transparency and disclosure regarding subcontractors, as well as outsourced development and processes.

Contracting and onboarding

Purpose

- Make security obligations enforceable

Practices

- Establishment of contractually enforceable obligations regarding cybersecurity and supply chain security.
- Establishment of contracts with right-to-audit provisions and access to documentation and security attestations.
- Definition of incident notification deadlines and cooperation requirements in contracts.
- Establishment of requirements for notification of significant changes (ownership, subcontractors, architecture).
- Definition of obligations regarding secure termination and deletion of data.
- Establishment of transition and continuity requirements to reduce the risk of vendor lock-in.
- Establishment of controls to enforce approval requirements for the use of subcontractors in critical functions.
- ‘Regular revalidation of contractual security controls.
- Reapproval of suppliers following mergers, acquisitions, or changes in ownership.

Development, production, and integration

Purpose

- To prevent compromise during development and integration.

Practices

- Establishment of secure software development practices, including secure coding standards, peer reviews, automated security testing, and protection of build pipelines and signing keys.
- Implementation of chain-of-custody controls and the use of tamper-evident packaging.
- Establishment of practices for physical security of facilities and background checks of personnel.
- Establishment of controls to prevent gray market or counterfeit components.
- Use and maintenance of a Software Bill of Materials (SBOM).

Delivery, implementation, and approval

Purpose

- To ensure integrity between supplier and customer environments.

Practices

- Verification of the supplier’s hardening and configuration requirements.
- Validation that delivered components correspond to the approved versions.
- Conducting security testing before deployment into production.
- Verification of secure configuration baselines before acceptance of products and services.
- Establishment of approval gates linked to risk acceptance.

Operations, maintenance, and support

Purpose

- To manage evolving supply chain risks over time.

Practices

- Continuous reassessment of supplier risks.
- Monitoring vulnerabilities affecting supplier components.
- Collection of threat intelligence related to the supplier ecosystem.
- Definition of deadlines and responsibilities for patching, including coordination in the event of disclosure of critical vulnerabilities.
- Establishment of integrated incident preparedness and response in collaboration with suppliers.
- Establishment of processes for applying lessons learned to updates of suppliers' risk profiles.

Phase-out and termination

Purpose

- To prevent residual risks after the phase-out of services or products.

Practices

- Establishment of processes for secure shutdown and destruction of data.
- Establishment of processes for revocation of access rights and credentials.
- Conducting a post-termination risk assessment.