5. Cybersecurity in contracts

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - This checklist is intended to ensure that cybersecurity risks are effectively managed through contractual requirements and ongoing follow-up in relationships with suppliers and third parties. The list can be used as a management tool in contract drafting, evaluation, and supplier management.
- **Participants**
  - Responsible for sourcing/suppliers, legal, and finance.
- **Application**
  - In the preparation of contracts and cooperation agreements.

Check list 1/6

1. Preparation and risk-based approach

- □ Has a systematic risk assessment been carried out for each supplier type (based on data access, system integration, geographic location, etc.)?
- □ Are suppliers prioritized based on criticality for business operations, compliance, and information security?
- □ Have supplier profiles with requirement levels been prepared (e.g., level 1 = critical IT operations, level 2 = consulting services, etc.)?
- □ Is cybersecurity included in the early stages of supplier selection (Request for Information/Request for Proposal)?

Check list 2/6

2. Formulation of contractual cybersecurity requirements

- □ Are the cybersecurity requirements specified and written in the main text of the contract or in appendices?
- □ Are there differentiated requirements depending on the supplier’s risk profile?
- □ Do the following topics apply:
  - □ Access restrictions and user rights?
  - □ Encryption of sensitive data (in transit and at rest)Backup and recovery strategies)?
  - □ Secure software development (if relevant)?
  - □ Processing of personal data (GDPR)?
  - □ Use of subcontractors and requirements for?
- □ Are specific standards and frameworks referenced (e.g., ISO 27001, NIS2, NIST, etc.)?

Check list 3/6

3. Right to audit, supervision, and documentation

- □ Does the contract provide the right to auditing and inspection, including both announced and unannounced supervision?
- □ Are there requirements for documentation of security measures, e.g., annual ISAE 3000/3402 statement?
- □ Must the supplier present results from, for example:
  - □ Penetration tests?
  - □ Vulnerability scans?
  - □ Incident response exercises?
- □ Is it stated that lack of documentation constitutes a breach of contract?

Check list 4/6

4. Incident management and responsibility

- □ Are there requirements for incident reporting within a set timeframe (e.g., 24 hours)?
- □ Is a contact structure and communication plan established for security incidents?
- □ Are roles and responsibilities for incident management and investigation clearly defined?
- □ Must the supplier participate in joint incident exercises or test scenarios?
- □ Does the contract include provisions such as:
  - □ Liability for data loss or operational downtime?
  - □ Coverage of legal and regulatory consequences?

Check list 5/6

5. Sanctions and breach of contract

- □ Are there clear sanction mechanisms for breaches of security requirements, e.g.:
  - □ Contractual penalties?
  - □ Suspension of cooperation?
  - □ Termination of the contracts?
- □ Is cybersecurity integrated into Service Level Agreements (SLAs), including:
  - □ Response and remediation times?
  - □ Number of annual incidents?
- □ Are there requirements for financial security or insurance in relation to security breaches?
- □ Have mechanisms been established for follow-up and reaction in case of repeated violations?

Check list 6/6

6. Contract management, follow-up and updating

- □ Is there a process for continuous evaluation of cybersecurity requirements in line with:
  - □ New threats?
  - □ New technologies?
  - □ Changes in the supplier’s services?
- □ Have internal responsibilities for contract follow-up and security monitoring been assigned?
- □ Is cybersecurity included in contract change processes (change appendices, renewals, extensions)?
- □ Is there a centrally maintained overview of which contracts include which cybersecurity requirements?

Special focus areas

□ Has a classification system been introduced, where suppliers with high business criticality receive:
  - □ More and stricter security requirements?
  - □ A higher level of supervision?
  - □ Faster response times?

□ Are the cybersecurity requirements adapted to the supplier’s role (data processor, system integrator, hardware supplier)?

□ Is cybersecurity prioritization included as part of contract negotiation and scoring?