6b. Cybersecurity due diligence towards new suppliers

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - When conducting cybersecurity-related due diligence, the goal is to assess how well the given supplier manages cyber risks, and whether there are hidden threats or liabilities. The attached procedure helps identify potential cybersecurity risks and liabilities, as well as understand how a supplier – consciously or unconsciously – may expose your organization to cyber risks.
- **Participants**
  - Sourcing/supplier team.
- **Application**
  - When entering into supplier engagements.

Theme 1/10

Theme 1: Security Management and Policies

- Does the supplier have documented information security policies?
- Are they aligned with recognized frameworks (e.g., ISO 27001, NIST, NIS 2)?
- Is there a person at management level responsible for cybersecurity?

Theme 2/10

Theme 2: Data Access and Handling

- Network security – Firewalls, intrusion detection/prevention systems, segmentation, VPNs.
- Is data encrypted during transfer and at rest?
- Do they have endpoint protection (e.g., antivirus, mobile device management)?
- Do they have security policies for cloud solutions?
- Are the principles of least privilege and need-to-know applied for access?

Theme 3/10

Theme 3: Identity and Access Management

- Do they enforce strong authentication methods, such as multi-factor authentication (MFA)?
- Do they have password policies?
- How is the creation and termination of users handled (especially for employees leaving the company)?
- How are privileged accounts managed?

Theme 4/10

Theme 4: Contractual Protections

- Does the agreement include:
  - Clear data protection clauses?
  - Security requirements?
  - Right to audit?
  - Deadlines for breach notifications (e.g., within 24 or 72 hours)?
- Data processing clauses: Who owns the data? What happens if the data is compromised? Are there clear rules for data storage, transfer, and deletion?
- Are there sanctions or remedies in case of a breach?
- Termination rights: What options does the contract provide for terminating the collaboration in case of cybersecurity breaches or violations of security policies?
- Liability limitations: Limit your exposure if the supplier is compromised and it affects your organization. Are maximum compensation amounts defined?

Theme 5/10

Theme 5: Incident Management and Data Breach History

- Do they have a tested incident response plan (IRP) for security incidents?
- What is their history with data breaches?
- Will they inform you immediately if your data is affected?
- Setup of alerts and notifications for suspicious behavior from customer accounts.
- Use of automated systems to detect irregularities in real time.
- Is there periodic evaluation of access rights and security policies?
- Possibility to conduct audits when needed or in the event of incidents.

Theme 6/10

Theme 6: Security Controls and Practices

- Do they perform regular vulnerability scans and patching?
- Have they conducted recent security audits or obtained certifications? (e.g., ISO 27001, etc.)
- Are systems and infrastructure separated for each customer?
- Do they have a backup and recovery plan?

Theme 7/10

Theme 7: Testing and Assessment

- Have they conducted penetration tests or third-party risk assessments – and when?
- Will they accept a security questionnaire or technical audit?
- Are there external public or private security assessments?

Theme 8/10

Theme 8: Risk from subcontractors (sub-contractors/fourth parties)

- Do they outsource any services? If yes, to whom and which ones?
- Do they conduct cybersecurity due diligence on their own suppliers?
- Will you be informed if they change critical service providers?

.

Theme 9/10

Theme 9: Security Awareness and Training

- Do their employees receive regular security awareness training?
- Are phishing simulations or social engineering exercises conducted?
- Is there a policy for reporting security incidents?

.

Theme 10/10

Theme 10: Cyber Insurance and Liability

- Do they have cyber liability insurance?
- Is there a requirement for documentation of active insurance coverage?
- Does the insurance cover third-party claims or only own losses (first-party)?

.

Warning flags – when the supplier poses a potential risk

It should be considered a **warning** if:

- The supplier refuses to accept security clauses in the contract:
  - For example, resistance to data processing agreements, liability limitations, or breach notification.
- The supplier requests exceptions from basic security practices:
  - Example: Wants to avoid the use of multi-factor authentication (MFA).
- The supplier insists on deep system access without oversight:
  - For example, access to backend systems, databases, etc. without logging, control, or restrictions.