6a. Cybersecurity due diligence towards new customers

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - When performing cybersecurity-related due diligence, the goal is to assess how well the given customer 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 customer – consciously or unconsciously – may expose your organization to cyber risks.
- **Participants**
  - Sales and customer audit team.
- **Application**
  - In new customer engagements.

Theme 1/8

Generic due diligence procedure for new customer relationships

A general procedure should at a minimum cover the following themes:

Theme 1: Customer risk profiling

- Business type and risk level: Is the customer active in a high-risk industry (e.g., finance, healthcare, defense, or other critical sectors)?
- Data sensitivity: What types of data will be exchanged or stored on behalf of the customer?
- Extent of interaction: Will the customer have deep system integration (e.g., through some form of integration or direct access), or only user-level access?
- Jurisdiction and legislation: Are there regulatory or compliance considerations (e.g., GDPR or other local data protection laws)?

Theme 2/8

Theme 2: Access and integration requirements

- Which systems will the customer have access to? (Internal applications, databases, etc.?)
- How will access to the systems be managed?
  - User management and access rights?
  - Integration with existing identity and access management systems?
  - Role-based access control: Granting access based on the user's role and responsibility?
- Segmentation and isolation: Measures to prevent risks across customers.
- Authentication:
  - Must the customer use multi-factor authentication (MFA)?
  - Is a VPN connection required?

Theme 3/8

Theme 3: The customer’s cybersecurity maturity

For customers requiring integration beyond a simple login, the following should be checked:

- Basic cybersecurity policies:
  - Are there documented policies for information security, access management, incident handling, etc.?
- Third-party risks:
  - Does the customer use vendors or subcontractors that your organization must also be able to trust?
  - Is there a process for assessing and monitoring these third parties?
- Security status and history:
  - Has the customer previously been exposed to security breaches or public incidents?
  - How have they handled past incidents, and what improvements have been implemented?

Theme 4/8

Theme 4: Contractual protections

- Data processing clauses:
  - Who owns the data?
  - What happens if the data is compromised?
  - Are there clear rules for data storage, transfer, and deletion?
- Acceptable use policies:
  - How may the customer use your systems and services?
  - Are there restrictions on automated access, data mining, or redistribution?
- Liability limitations:
  - Limit your exposure if the customer is compromised and it affects your organization.
  - Are maximum compensation amounts defined?
- Termination rights:
  - Does the contract allow termination of the cooperation in the event of cybersecurity breaches or violations of security policies?

Theme 5/8

Theme 5: Monitoring and ongoing controls

- Continuous monitoring:
  - Setup of alerts and notifications for suspicious behavior from customer accounts.
  - Use of automated systems to detect irregularities in real-time.
- Regular reviews:
  - Particularly important for large accounts or customers with a high-risk profile.
  - Periodic evaluation of access rights and security policies.
- Logging and auditing:
  - Ensuring that all customer activities on the platform are logged in a secure and traceable manner.
  - Possibility to conduct audits when needed or in the event of incidents

Theme 6/8

Theme 6: Insurance and financial risk

- Cyber insurance:
  - Should either you or the customer have cyber insurance, depending on the sensitivity and risk profile of the service?
  - Is there a requirement for documentation of active insurance coverage?
- Compensation clauses:
  - Determination of financial liability if a security breach occurs as a result of the customer’s actions or negligence.
  - Clear rules for compensation and cost coverage in the event of loss or damage.

Theme 7/8

Theme 7: Compliance and regulatory obligations

- If data processing is regulated by, for example, GDPR, HIPAA (Health Insurance Portability and Accountability Act), Sarbanes-Oxley Act (SOX), or similar, the following should be ensured:
  - Correct data processing agreements: There must be signed agreements that clearly define roles and responsibilities regarding data processing.
  - Required security certifications: The customer (or you yourself) must have relevant certifications in place – or be in the process of obtaining them – such as ISO 27001 or equivalent.

Theme 8/8

Theme 8: Expectations for notification of security breaches

- Agree on clear timelines for notification if one of the parties discovers a security incident that may affect the other party.
  - How quickly must notification be given? (e.g., within 24 or 72 hours).
- What should the notification include?
  - Description of the incident?
  - Which data or systems are affected?
  - Measures that have been taken or are planned?
- How should the notification be made?
  - Via email, phone, secure portal, or other?
- Who should receive the notification?
  - Named contacts or roles at both parties?

Warning flags – when the customer poses a potential risk

It should be considered a warning if:

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