CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

Risk reduction when entering into supplier or other third-party relationships

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

- At identificere, vurdere og reducere cybersikkerheds- og digitale forsyningskæderisici på forhånd, før der etableres tillid, adgang, datadeling eller operationel afhængighed.

Participants

- Data and IT managers, legal/compliance functions, and product and service owners.

Application

- Used prior to entering into formal relationships with suppliers, customers, partners, or other third parties.

Approach

The considerations in the remainder of this document may be used by companies in the following ways prior to entering into formal relationships with suppliers, customers, partners, or other third parties:

- As an assessment tool in early-stage dialogue and in connection with tendering and proposal processes (Request for Proposals – RFP).
- To adapt questionnaires and contractual clauses based on the actual level of risk.
- To determine escalation levels, compensating controls, or potential rejection.
- To distinguish between acceptable and unacceptable residual risk.

Note: Not all requirements will necessarily be relevant, and companies should therefore select the requirements that are applicable in the specific context.

Covered aspects

1. Business context and the criticality of the relationship.
2. Data exposure and information sensitivity.
3. Access and connectivity model.
4. The supplier’s cybersecurity maturity and practices.
5. Incident history, detection, and preparedness/response capability.
6. Dependencies and transparency in the supply chain.
7. Regulatory and legal considerations.
8. Assurance, documentation, and transparency.
9. Contractual readiness.
10. Expectations regarding change and duration.
11. Cultural and collaborative indicators.

Business context and the criticality of the relationship

Considerations

- Which business processes, services, or products will this collaboration support?
- How critical is the relationship to the core business, security, or revenue generation?
- What impact would supplier failure, compromise, or operational disruption have?
- Is the relationship operational, strategic, tactical, or product-based?
- Is this a one-time collaboration or a long-term dependency?

Data exposure and information sensitivity

Considerations

- What types of data will be accessed, processed, stored, or transmitted (e.g. personal data, confidential business information, intellectual property, credentials, keys, or operational data)?
- Will data leave your company's controlled environment?
- Are there requirements relating to data residency or data sovereignty?
- Is data shared one-way, bidirectionally, or aggregated across customers?
- What data segregation mechanisms have been established (particularly relevant for SaaS and MSP providers)?

Access and connectivity model

Considerations

- What types of access will the third party have (e.g., network, application, or application programming interface (API) access)?
- Will the third party have administrative or privileged access?
- Is the access persistent or time-limited?
- Are integrations direct, indirect, or handled through intermediaries?
- How are identities created, authenticated, and revoked?
- Can access technically be restricted according to the principle of least privilege?
- Are remote access tools, service accounts, or automation involved?

The supplier's cybersecurity maturity and practices

Considerations

- Is there a defined governance structure for information security?
- Are roles and responsibilities within cybersecurity clearly defined?
- Are security policies documented and reviewed periodically?
- Is there a secure development lifecycle (for software and service providers)?
- Are vulnerability management and patching processes established?
- How is employee security awareness managed?
- Are subcontractors subject to equivalent security requirements?

Incident history, detection, and preparedness/response capability

Considerations

- Has the company experienced any significant security incidents?
- How were incidents detected, managed, and remediated?
- Is there a documented incident response preparedness plan?
- Are customers/partners notified within defined timeframes?
- Is there coordination between technical, legal, and communications teams?
- Are tabletop exercises or simulations conducted?

Dependencies and transparency in the supply chain

Considerations

- Who are the critical subcontractors, cloud providers, or technology partners?
- Are upstream dependencies disclosed and reviewed periodically?
- Are software components and libraries registered and tracked (e.g., Software Bill of Materials (SBOM))?
- Have measures been established to prevent counterfeit or grey-market components?
- What assumptions form the basis for trust in suppliers?

Regulatory and legal considerations

Considerations

- Which laws and regulations apply (e.g., data protection, sector-specific regulation)?
- In which jurisdictions will data be processed or accessed?
- Are there geopolitical risks or risks related to sanctions?
- Do obligations regarding access for law enforcement agencies or public authorities apply?
- Are regulatory reporting obligations aligned between the parties?

Assurance, documentation, and transparency

Considerations

- What security documentation can be provided (certifications, reports, statements)?
- Is independent assurance available (e.g., third-party audits)?
- How current and relevant is the documentation?
- Can the company support audits or assessments as needed?
- Is transparency ongoing, or is it limited to onboarding?

Contractual readiness

Considerations

- Can security requirements be enforced contractually?
- Are responsibilities and obligations clearly allocated between the parties?
- Are incident notification deadlines realistic and aligned?
- Are change management and the use of subcontractors addressed?
- Are requirements relating to exit, termination, and the return or deletion of data feasible?
- Are liability, limitations of liability, and indemnification aligned with the exposure to cyber risks?

Change and duration expectations

Considerations

- How will significant changes be identified and assessed (e.g., new services, architectural changes, mergers and acquisitions)?
- How often should reassessment take place?
- Are triggers for reapproval or escalation defined?
- Is there a clear exit strategy if the risk becomes unacceptable?

Cultural and collaborative indicators

Considerations

- How transparent and responsive is the company during due diligence?
- Is security regarded as a shared responsibility or as a barrier?
- Is security regarded as a cost or an investment?
- Are issues and risks presented defensively or constructively?
- Is there a willingness to pursue continuous improvement over time?