CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

1. Strategy for risk management and stakeholder analysis

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - To have a risk management strategy developed.
  - To create an overview of the internal and external stakeholders who are either part of the company or on whom the company depends.
  - To ensure support for the cybersecurity strategy or that stakeholders are informed at an appropriate level.
  - To ensure an effective implementation of the company's cybersecurity strategy.
- **Participants**
  - Carried out by persons with in-depth knowledge of the company's internal and external partners, customers, suppliers, etc.
- **Application**
  - Should be carried out with an appropriate frequency.

Strategy for risk management: Content examples

1. Purpose and scope
2. Governance and roles
3. Risk policy and risk appetite
4. Risk management process
5. Tools and methods
6. Communication
7. Business continuity planning
8. Measurement and improvement

Tasks after the strategy development

- **Identification of stakeholders.**
  - Map the internal and external stakeholders who are important for the success of the strategy.
- **Identify the stakeholders' interests.**
  - Understand what each stakeholder group wants to achieve or protect in relation to cybersecurity.
- **Identify the stakeholders' concerns.**
  - Uncover any reservations, risks, or resistance that stakeholders may have.
- **Develop a plan for how each stakeholder group's interests and concerns should be addressed to gain support for the strategy.**
  - Decide how best to communicate with, involve, and engage the different groups to ensure their support.

Possible stakeholders, interests and concerns

Stakeholders	Interests	Concerns
Management (C-level) and Board of Directors	Strategic overview, risk management, reputation, regulatory compliance, investment decisions	Costs, ROI, complexity, business disruptions
Procurement	Supplier relations, contract management	Supplier resistance, complexity
IT / Cybersecurity teams	Effective implementation, technical security, system stability, threat mitigation, incident response	Resource limitations, lack of management support
Legal & Compliance	Regulatory risk, contract terms	Liability, audit rights
Suppliers	Business continuity Ease of doing business, contract compliance	Costs of compliance
Operations / Logistics	Supply continuity, resilience	Risk of disruptions
Customers / Clients	Protection of personal data, trust, service continuity	Data breaches, lack of transparency, poor handling, data protection
Investors / Shareholders	Risk exposure	Impact on value
Insurance companies	Accurate (cyber) risk assessment, policy compliance	Premium calculation

Other stakeholders, interest, and concerns

Stakeholders	Interests	Concerns
Regulatory bodies & public authorities	National security, law enforcement, economic stability	Public safety
Standardization organizations & industry organizations	Best practices, harmonization	Sector-wide resilience
Society / General public	Data protection, continuity of critical service availability (food, water, etc.)	Public reporting on cybersecurity and maturity, transparent documentation
Media and watchdog organizations	Public accountability	Transparency in incident handling
Cybersecurity forums & information-sharing groups	Threat intelligence sharing	Coordinated response

The list is not exhaustive but is intended as inspiration.

Potential steps for stakeholder support

1. Develop a clear business case

- Quantify risks (e.g., costs of supply chain disruptions, downtime, loss of customers).
- Highlight regulatory and commercial consequences (e.g., NIS2, GDPR).
- Emphasize competitive advantages: trust, resilience, access to contracts.

2. Tailor the message

- Executive management: Highlight financial and reputational risks, legal liability, and alignment with ESG/CSR.
- Procurement: Focus on efficiency, supplier assessment, and contract simplification.
- IT: Show how the strategy integrates with existing controls and architecture.
- Suppliers: Offer support and phased compliance models to ease implementation.
- Etc.

3. Stakeholder workshops and co-creation

- Hold workshops to gather input from all (relevant) stakeholders.
- Test the strategy with a smaller group of suppliers to assess feasibility and make adjustments.