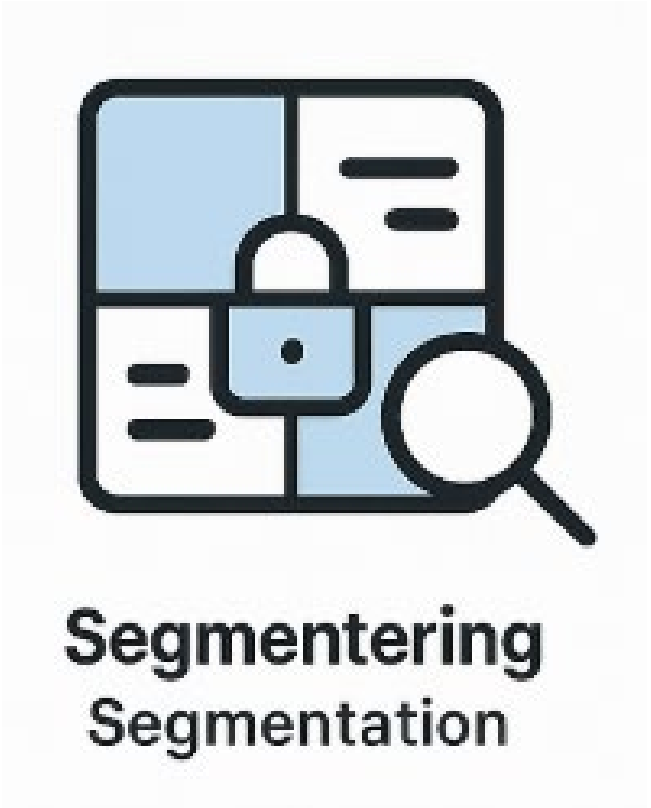
4. Prioritization of suppliers



www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - Suppliers can pose a direct cybersecurity risk. Therefore, it is important to assess which suppliers should have a prioritized focus regarding cybersecurity measures.
- **Participants**
  - Ansvarlige for leverandører/sourcing og IT.
- **Application**
  - Part of the work of segmenting suppliers, which typically takes place annually.

Introduction

- Traditionally, the company will categorize suppliers based on their relative value and supply risk
- Se an example here
- In relation to cybersecurity, however, the company should also include this element in its considerations during supplier evaluations.

Approach (1/2)

- Extract a list of the company's active suppliers.
- Start by focusing on the direct suppliers (suppliers of raw materials, components, etc. for the products).
- Assess each supplier based on the supplier's cybersecurity profile:
  - This may include access to sensitive data, system integration, security certifications, history of data breaches/vulnerabilities, geopolitical risk, dependency in case of system compromise, etc.
- Use a weighting and scoring model.

Approach (2/2)

- Categorize into e.g., High, Medium, and Low risk.
- Develop an action plan per group e.g.,:
  - High: Audit, contractual requirements, inspection visits
  - Medium: Annual self-assessments, possibly audits.
  - Low: Minimal monitoring.
- Implement, follow up, and adjust over time.
- Annual assessments and exit strategies.

Examples of cybersecurity

Criterion	Low risks (1)	Medium risks (3)	High risks (5)
Access to sensitive data	No personal data	Non-sensitive data	Sensitive data
Technical integration	No integration	Limited integration	Full access
Security certification	ISO 27000/NIS2 or similar	Self-assessment	No documentation
Previous security incidents	No history	Minor incident	Known breach/poor response
Supplier's maturity	High cyber maturity	Medium cyber maturity	Low cyber maturity
Geopolitical/supplier risk	The supplier is located in a low-risk country	LevThe supplier is located in a medium-risk country	The supplier is located in a high-risk country
Etc.	xx	xx	

Example of cybersecurity including weights

Criterion	Weight	Example score (1 low risk, 5 = high risk)
Access to sensitive data	30%	5
Technical integration	25%	4
Security certifications	15%	3
Previous security incidents	15%	2
Supplier's cyber maturity	10%	2
Geopolitical/supplier risk	5%	3
Etc.	xx	xx

For the example: = (0.3x5) + (0.25x4) + (0.15x3) + (0.15x2) + (0.1x2) + (0.05x3) = **3.6**

Since the supplier tends towards medium/medium-high risk, it should be monitored and possibly undergo an audit.