3. Integration of cybersecurity in risk management and improvement processes

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - To ensure that cybersecurity becomes an integrated part of the company's overall risk management.
- **Participants**
  - Responsible for risk management with input from the various functional areas.
- **Application**
  - Integrated part of the general risk management process.

Approach

- List the internal business functions (see examples on slide 4) and indicate to what extent cybersecurity within these areas is integrated into the company's overall risk management and improvement processes.
- Mark from 1 = to a very low degree to 5 = to a very high degree.
- Also indicate what the target should be (TO-BE), after which a gap can be calculated.

Assessment form

Internal business functions	1	2	3	4	5	TO-BE	Gap
Inbound logistics							
Manufacturing							
Distribution							
Product development							
Finance							
External business functions	**1**	**2**	**3**	**4**	**5**	**TO-BE**	**Gap**
Financial partners							
Public authorities							
Customers							
Suppliers							
Other service partners							

1 = to a very low degree, 2 = to a low degree, 3 = to some degree, 4 = to a high degree, 5 = to a very high degree

Examples of content elements in the categories

Inbound logistics
Procurement
Inbound transportation
Goods receipt incl. inspection
Storage and inventory management
Picking for production

Production / R&D
Product development
Planning
Production
Quality control
Completion reporting

Outbound logistics
Forecast
Sales
Order processing
Picking, packing and shipping
Invoicing

Financial partners
Bank
Payroll service
Insurance
External book keeping
Auditor

Authorities
Tax Authority (SKAT)
Business Authority (VIRK)
Certification
Labour Inspection

Other service partners
Electricity, Water, Heating
GPS
Alarm/monitoring
Service agreements (Equipment))

Action points

- Scores of 4–5 are considered a **high level** of cybersecurity, and only minor or no attention is required.
- A score of 3 indicates **some** cybersecurity, but with room for improvement.
- Scores of 1–2 indicate a **low level** of cybersecurity and require attention and improvements.