CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

0. Comprehensive overview of cybersecurity supply chain risk management tools

www.cyber-smv.dk

Cybersecurity supply chain risk management

- Cybersecurity Supply Chain Risk Management (C-SCRM) is about **identifying**, **assessing**, and **managing** the cyber-related risks that arise through a company's customers, suppliers, and other business partners.
- It is a discipline at the intersection of cybersecurity and supply chain management, as companies are increasingly dependent on complex, global, and digital supply chains.

Purpose, participants and application

- **Purpose**
  - To create an AS-IS picture of perceptions of concrete practice within 10 areas of cybersecurity supply chain risk management.
  - To determine a desired future level for the company (TO-BE).
  - To prioritize focus areas and develop action plans.
- **Participants**
  - Management and key employees.
- **Application**
  - Should be assessed continuously – at periodic intervals, e.g., every quarter.

Approach

- A tool is linked to each of the 10 concrete practices within cybersecurity supply chain risk management (see slide 5).
- If it is the first time working with the tool, select the tools you want to focus on.
- Based on the (necessary) tools that have been used, the company's current position (AS-IS) is assessed for each tool on a scale from 1 (to a very low degree) to 5 (to a very high degree). Write IB (not used) if a tool is not applied. Assessments are marked in the table.
- Next, the company's desired level (TO-BE) is plotted for each tool.
- Then, the measures necessary to move from AS-IS to TO-BE are identified and prioritized.
- Finally, an action plan (see slide 7) is developed for each focus area.

#	Practice	1	2	3	4	5	TO-BE	Gap
1	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.							
2	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.							
3	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.							
4	Suppliers are known and prioritized by criticality.							
5	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.							
6	P Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.							
7	The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.							
8	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.							
9	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.							
10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement							

NU = noy used; 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

Source: National Institute of Standards and Technology (2024), The NIST Cybersecurity Framework (CSF) 2.0, https://doi.org/10.6028/NIST.CSWP.29

Action plans

No	Improvement area	Description	Objectives	Priority	Responsible	Deadline

Action plan for improvement areas

Improvement area	Name of improvement area
Purpose	
Objectives	
Activities	
Responsible	
Investment	
Risks	
Deadline	
Reporting/follow up	