7. Cybersecurity register

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - To identify, record, prioritize, assess, respond to, and monitor risks associated with a supplier, its products and services, as well as other third parties throughout the relationship.
- **Participants**
  - Responsible for cybersecurity.
- **Application**
  - When entering into supplier engagements.

Risk register

- Is a list of identified cyber risks and other necessary information.
  - Contains the results of various risk management processes and is often displayed in table or spreadsheet format.
  - A tool for documenting potential risk events and related information.
- Risk events refer to specific or potential cyber incidents that may negatively affect the company.

A risk register should include …

- ❑Identification number for each potential cyber risk event.
- ❑Ranking of each cyber risk event.
- ❑Name of each cyber risk event.
- ❑Description of each cyber risk event.
- ❑Category to which each cyber risk event belongs.
- ❑Root cause of each cyber risk.
- ❑Triggers for each cyber risk; indicators or symptoms of actual cyber risk events.
- ❑Potential responses to each cyber risk.
- ❑Risk owner or the person responsible for each individual cyber risk.
- ❑Likelihood and impact of each cyber risk occurring.
- ❑Status of each cyber risk.

Risk register – an example

No.	Priority	Risk name	Description	Category	Root cause	Triggers	Potential response	Responsible	Probability for incident 1-5 (1 = low)	Impact 1-5 (1 = low)	Status
R44											
R21											
R7											

Risk register

Updating and reporting

- The risk register should be continuously updated with any newly recognized cyber risks.
- Likewise, there should be formal reporting – for example, at monthly management meetings, which could include the following agenda:
  - Causes/sources of overall cyber risk.
  - Key drivers of cyber risk exposure.
  - Information on any cyber risk events.
- It is recommended that, once a potential cyber risk has been addressed, it is retained in the register so that the register can serve as documentation of progress.