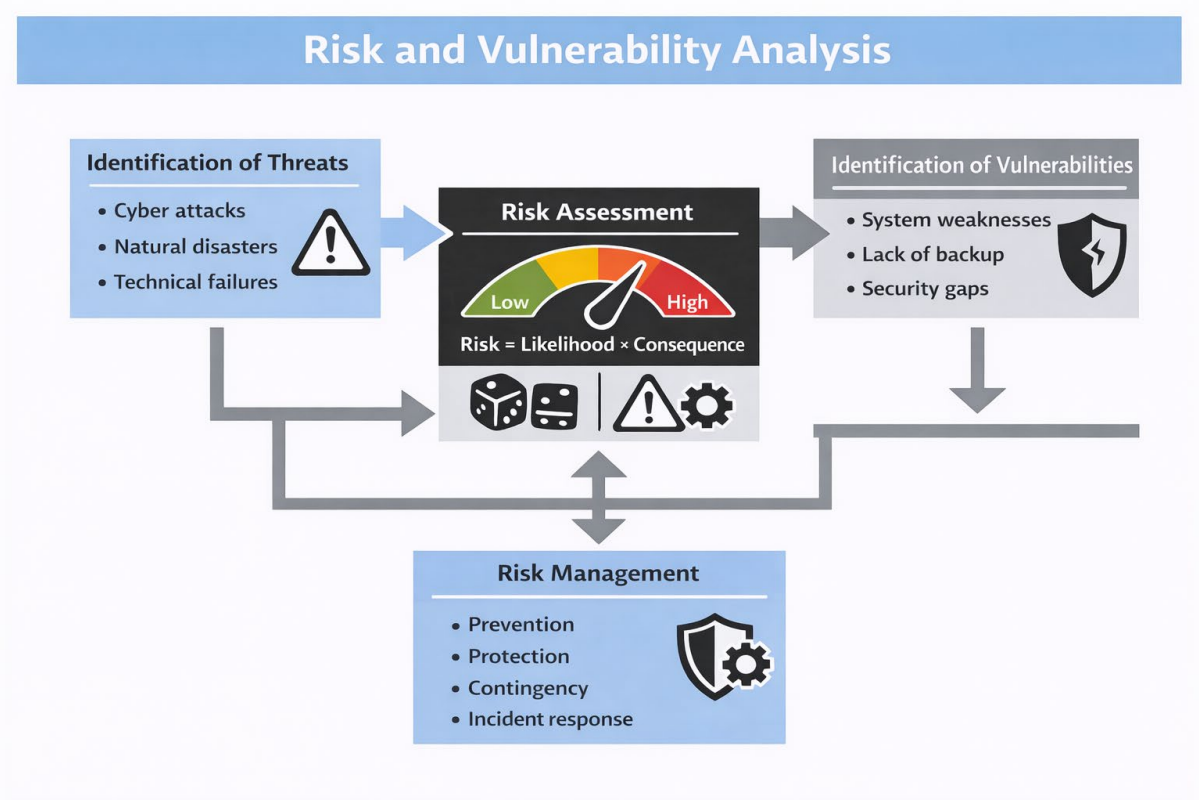
Risk and Vulnerability Analysis



The tool have been provided in connection with the project **Cybersecurity and Business Continuity** (www.cyber-smv.dk), funded by the Danish Industry Foundation. Publication date: 29.12.2025

Procedure

1. **Preparation**
   - → Define purpose and scope: Decide which business areas, processes and IT systems the analysis should cover.
   - → Establish a steering group: Involve management and key people from critical functions (finance, IT, production, sales).
   - → Collect relevant data: Previous incidents, system documentation, supplier information, contracts and security policies.
2. **Identification of Business-Critical Processes and Assets**
   - → Map all business processes and assess which ones are critical to the survival of the business.
   - → Identify associated assets: IT systems, employees, locations, supply chain and suppliers.
   - → Assess dependencies between processes and assets.
3. **Identify Threats and Vulnerabilities**
   - → Threats: Events that can affect the company's operations (e.g. cyberattacks, power outages, fires, natural disasters, pandemics). Vulnerabilities: Weaknesses in the company's processes or systems, e.g. lack of backup, inadequate IT security, dependence on single suppliers and dependence on single customers.
4. **Risk Assessment**
   - → For each combination of threat and vulnerability, assess:
   - → Probability: How likely is it that the event will occur? (Low = 1, Medium = 2, High = 3).
   - → Consequence: What will be the impact on critical processes (financial, operational, reputation)? (Low = 1, Medium = 2, High = 3). Calculate risk, e.g. Risk = Probability × Consequence.

Procedure (continued)

5. **Analysis of Consequences (Business Impact)**
   - → Identify the maximum tolerable downtime for critical processes.
   - → Quantify potential losses (financial, operational, customer satisfaction).
   - → Use the results to determine which processes should be prioritized in continuity plans.
6. **Preparation of Action Plans**
   - → Develop risk management actions: Prevention, protection, preparedness, recovery.
   - → Consider alternative solutions for critical dependencies: backup vendors, temporary locations, redundant IT systems.
7. **Implementation and Training**
   - → Implement action plans and safety measures.
   - → Conduct training and exercises so employees know how to respond in the event of incidents.
8. **Monitoring and Updating**
   - → Monitor risks and vulnerabilities on an ongoing basis.
   - → Update the analysis at least annually or when there are major changes in business processes, technology, or supplier relationships.

The focus should also be on *single points of failure*, which is a vulnerability in a system where a failure here will cause the entire system to stop functioning.