11. Gross list of vulnerabilities

Purpose, participants and application

- **Purpose**
    - Helping participants identify a maximum of 10 vulnerabilities, which they believe the company's supply chains are most exposed to.
- **Participants**
    - To be used by the individual employees and by the team.
- **Application**
    - To be used in phase 2 and 3.

Vulnerabilities

- Vulnerabilities are understood as the factors that make the company sensitive/exposed to disruptions in the company's supply chains.
- 75 vulnerabilities divided into 7 general topics:
  1. Finance
  2. Customers/demand
  3. Processes/organization
  4. Systems/data
  5. Purchasing/sourcing
  6. Supply chain end-to-end
  7. Environment

Vulnerabilities: Finance

- 1.1 Asset turnover
- 1.2 Access to liquidity
- 1.3 High level of net working capital
- 1.4 Low cash flow
- 1.5 Other

Vulnerabilities: Customers/demand

- 2.1 Unpredictability of demand
- 2.2 Lack of sale
- 2.3 Product development pipeline
- 2.4 Insufficient sales pipeline
- 2.5 Customers frequently make changes in orders
- 2.6 Customer dependency
- 2.7 Insufficient product assortment
- 2.8 Too large assortment
- 2.9 Product liability/compensation
- 2.10 Brand image
- 2.11 Time to market challenges
- 2.12 Time pressure
- 2.13 Unprofitable customers
- 2.14 Lack of market focus
- 2.15 Too low transport capacity
- 2.16 Other

Vulnerabilities: Processes/organization

- 3.1 Too low production capacity
- 3.2 Reliability of equipment’s
- 3.3 Manufacturing does not take place at the right locations
- 3.4 Undocumented processes
- 3.5 A too high operational focus
- 3.6 Lack of cross-functional collaboration (silo-culture)
- 3.7 Lack of human resources
- 3.8 Lack of competencies
- 3.9 Too much tacit knowledge
- 3.10 Too high staff turnover
- 3.11 Too dependent on key persons
- 3.12 Lack of financial resources
- 3.13 Quality
- 3.14 Lack of maintenance
- 3.15 Insufficient foundation of production (master data)
- 3.16 Other

Vulnerabilities: Systems/data

- 4.1 Insufficient systems
- 4.2 Lack of IT security
- 4.3 Lack of Quality Management
- 4.4 Too low data quality
- 4.5 Too low data accessibility
- 4.6 Too few/wrong KPI’s
- 4.7 Conflicting KPI’s
- 4.8 Insufficient use of systems
- 4.9 Other

Vulnerabilities: Purchasing/sourcing

- 5.1 Too low supplier capacity
- 5.2 Lack of accessibility of raw materials and supplies
- 5.3 Too low supplier reliability
- 5.4 Dependency of Supplier Relations
- 5.5 Lack of access to supplier competencies
- 5.6 Too little focus on new suppliers
- 5.7 Supplier bankruptcy
- 5.8 Requirements for product purity
- 5.9 Other

Vulnerabilities: Supply chain end-to-end

- 6.1 Lack of transparency
- 6.2 Price pressures from customers/suppliers
- 6.3 Too high/low growth
- 6.4 Import and export restrictions/channels
- 6.5 Too high complexity
- 6.6 Other

Vulnerabilities: Environment

- 7.1 Geopolitical disruptions
- 7.2 Fluctuations in prices and exchange rates
- 7.3 Terrorism/sabotage
- 7.4 Espionage/theft
- 7.5 Cyber-attack
- 7.6 Competitors innovation
- 7.7 Social/demographic/cultural changes
- 7.8 Requirements for CSR/sustainability/ESG/UN SDG's
- 7.9 Political regulatory changes
- 7.10 Stakeholders/NGO's
- 7.11 Disruptions
- 7.12 Unclear/lack of IPR
- 7.13 Strikes
- 7.14 Other