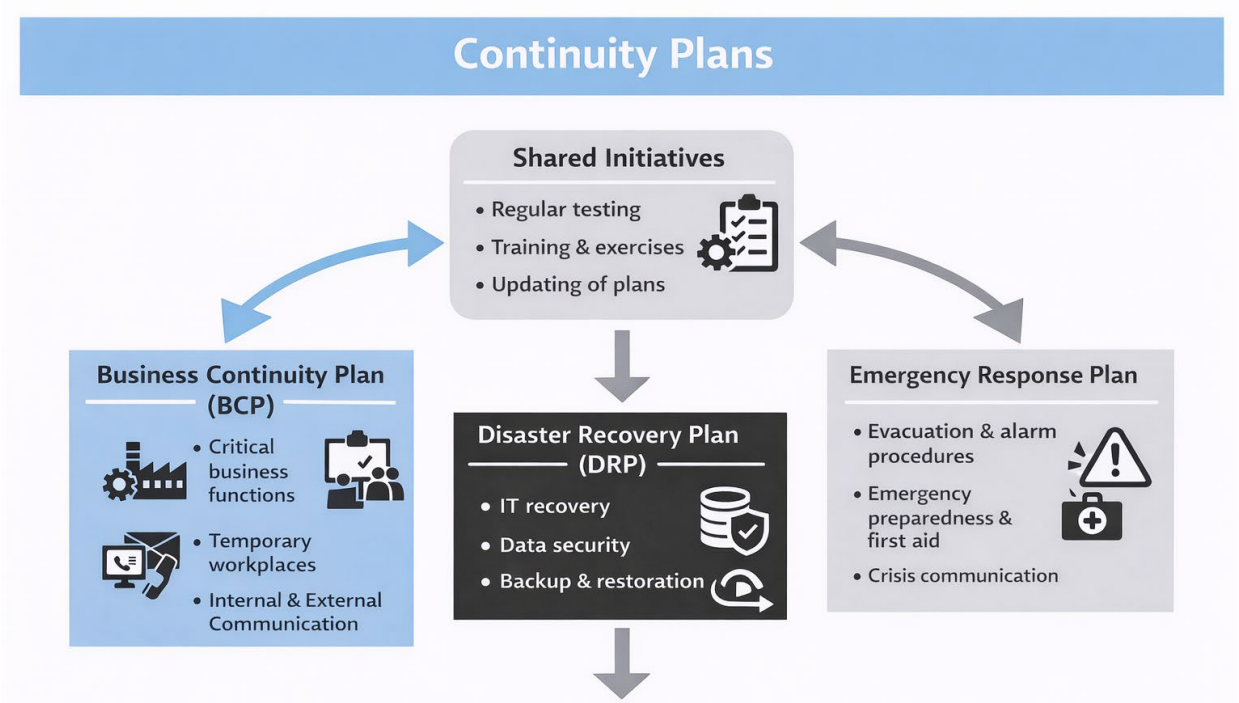
Continuity Plans



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

Continuity Plan

→A business continuity plan is a **strategic plan** that a company develops to ensure that its critical business functions can continue *during* and *after* a crisis or major disruption.

→The purpose is to minimize disruption, reduce financial losses, and protect the organization's reputation.

The Continuity Plan (example of structure)

1. Document Information.
2. Purpose and Scope.
3. Critical Business Functions.
4. Risk Assessment.
5. Strategies and Solutions.
6. Roles and Responsibilities.
7. Communication Plan.
8. Training and Testing.
9. Maintenance.
10. Attachments.

1. Document Information

→Version:
→Date:
→Author(s):
→Approved by:

2. Purpose and Scope

→Brief description of why the plan exists.
→Indicate which parts of the business or systems the plan covers.

Example

Purpose:

The purpose of this continuity plan is to ensure that the company can maintain critical production and delivery processes during unforeseen events, minimize financial losses and protect employees, customers and partners. The plan must enable rapid response, restore operations and make informed decisions in the event of disruptions such as machine breakdowns, IT failures, supplier problems or external crises.

Scope:

The plan covers the parts of the company and systems that are critical for continuous production and delivery, including the production department (machines, production lines, warehouse and raw material supply), IT and management systems (ERP, production management systems, back-office IT), operational technology (OT), supply chain and logistics (critical suppliers and transport channels), employees and key functions (roles and responsibilities in the event of incidents, including security and communication). The plan also includes procedures for internal and external communication, as well as guidelines for evaluation and updating after incidents.

3. Critical Business Functions

Function	Description	Criticality (H, M, L)	Responsible

Note: H = High, M = Medium, L = Low

Critical Business Functions (examples

Function	Description	Criticality (H, M, L)	Responsible
ERP	Daily operation of order processing, inventory management and finances	High	IT-Manager
Production	Manufacturing of core products	High	Production Manager
IT-infrastructure	Operation of networks, servers and cloud services	High	IT-Manager
Supplier Management	Contact and coordination with key suppliers	High	Purchasing Manager
Backup & Data Recovery	Securing critical data and enabling recovery	High	IT-Manager
Security and Access Control	Internal and external communication during crises	Medium	Communication Manager

Note: H = High, M = Medium, L = Low

4. Risk Assessment

Risk	Probability	Consequence	Priority	Mitigation Strategy

Risk Assessment (examples)

Risk	Probability	Consequence	Priority	Mitigation Strategy
Cyberattack	Medium	High	High	Antivirus and firewall on all systems Regular software updates
Power failure	Medium	High	High	Backup generator, emergency plan for outages, UPS for critical machines
Supplier failure	Medium	High	High	Identify critical suppliers and alternative suppliers Maintain buffer stocks of key materials
Machine breakdown	Medium	High	High	Regular maintenance, spare parts inventory, contract with service provider
IT system breakdown (ERP, production management)	Medium	High	High	Daily backup, cloud solution, server redundancy, IT support agreement
Transport problems / delays	Medium	Medium	Medium	Alternative transport, multiple suppliers, buffer stocks

5. Strategies and Solutions

→In a business continuity plan, **strategies** and **solutions** are the concrete actions the company can use to maintain operations during and after a crisis.

→List in a table:

- → Risk/challenge.
- → Strategy/solution.
- → Responsibility.

Strategies and Solutions (examples)

Area	Risk/Challenge	Strategy/Solution	Responsible
IT	IT system breakdown (ERP, production management)	Daily backup for both local and cloud solution Redundant server / failover system IT support agreement with external supplier	IT-Manager
IT	Cyber attack / ransomware	Antivirus, firewall and updated software Employee security training (phishing awareness) Incident response plan Isolated backup systems	IT-Manager
Production	Machine breakdown	Preventive maintenance plan Spare parts warehouse for critical components Contract with service provider with fast response time	Production Manager
Production	Power failure	Backup generator / emergency power UPS for critical machines Plan for priority production during power outage	Production Manager
The Supply Chain	Supplier failure	Alternative supplier ready Buffer stock of critical raw materials Ongoing assessment of suppliers' capacity and finances	Supply Chain Manager
The Supply Chain	Transport problems	Multiple transport options / carriers Optimized warehouse strategy Just-in-case warehouse of finished goods	Supply Chain Manager

6. Roles and Responsibilities

Role	Areas of responsibility	Contact information

Roles and Responsibilities (examples)

Role	Areas of responsibility	Contact information
Responsible for IT	Securing IT operations, backup, cyber security, system recovery,	Name: Maria Nielsen Telephone: +45 2345 XXXX E-mail: mn@example.com
Production Manager	Production operations, handling machine breakdowns, safety in production areas.	Name: Lars Petersen Telephone: +45 3456 XXXX E-mail: lp@example.com
Responsible for Communication	Internal and external communication, contact with customers, suppliers and media.	Name: Sofie Larsen Telephone: +45 6789 XXXX E-mail: sl@example.com
Crisis Management Staff Leader	Overall responsibility for crisis management, decisions and coordination.	Name: Jens Hansen Telephone: +45 1234 XXXX Email: jh@example.com
Financial manager	Liquidity, payments, wages, economic consequences of the crisis.	Name: Christina Holm Telephone: +45 8901 XXXX E-mail: ch@example.com
HR-Manager	Managing staff, disease outbreaks, loss of key employees, working from home	Name: Peter Jensen Telephone: +45 5678 XXXX E-mail: pj@example.com

7. Communication Plan

Target Group	Communication Channel	Responsible	Key Message	Timing

Communication Plan (example)

Target Group	Communication Channel	Responsible	Key Message	Timing
Employees	E-mail, telephone, intranet, SMS	HR-Manager	- Crisis message: What happened? - Instructions: What employees should do - Updates on operations and safety	Immediately after a crisis occurs and ongoing update
Customers	E-mail, telephone, social medias, website	Responsible for Communication	- Inform about any delay or production stoppage - Expected resumption time - Contact person for questions	No later than 4 hours after the incident, update as needed
Suppliers	E-mail, telephone	Logistical Manager / Purchasing Manager	- Supply chain status and any changes - Prioritization of deliveries - Contact person for coordination	Immediately after an incident and in the event of changes in the delivery plan
Authorities	E-mail, telephone	Crisis Management Staff Leader / Responsible for Communication	- Statutory reporting if applicable - Any safety or environmental incident	As soon as necessary according to legislation or regulatory requirements

8. Training and Test

Exercise/ Test	Purpose	Participants	Frequency	Responsible	Comments/ follow-up

Training and Test (examples)

Exercise/ Test	Purpose	Participants	Frequency	Responsible	Comments/ follow-up
Evaluation exercise	Testing of escape routes and alarms	All employees	Annually	Security Officer	Log time, evacuation efficiency
IT crash simulation	Backup and restore testing	IT, production, crisis staff	Twice a year	IT-Manager	Note errors and solutions
Supplier failure exercise	Testing alternative supplier plan	Logistics, purchasing, production	Annually	Logistics Manager	Evaluate delivery management
Cyberattack simulation	Training in IT security and incident response	All IT users	Annually	IT-Manager	Record employee feedback and learning

9. Maintenance

→**1. Regular update of the plan**
- → Revise the BCP at least once a year, or after major changes in the company (e.g., new production, new IT systems and new suppliers).
- → Update contact information for crisis staff, employees, suppliers and authorities.
- → Adjust roles and responsibilities when personnel changes

→**2. Risk assessment update**
- → Review the risk list for new threats (e.g., new cyber threats, supply chain changes, climate change).
- → Update the likelihood, impact and priority of existing risks.
- → Add new risks relevant to production.

→**3. Evaluation of strategies and solutions**
- → Review past crisis situations and tests/exercises.
- → Update strategies and emergency procedures based on experience.
- → Check if backup systems, emergency generators and alternative locations are still working.

9. Maintenance (continued)

→**4. Training and exercises**
- → Plan the next round of training and testing for employees and crisis staff.
- → Ensure that new employees are introduced to the continuity plan.
- → Document all exercises and results for follow-up.

→**5. Documentation and versioning**
- → Keep track of version number, date of update, and responsible person.
- → Archive old versions for traceability.
- → Ensure that all relevant employees have access to the latest version, both digitally and physically.

10. Attachments (examples)

→Forms.
→Contact lists.
→Process maps.
→Alternative locations.
→IT backup procedures.