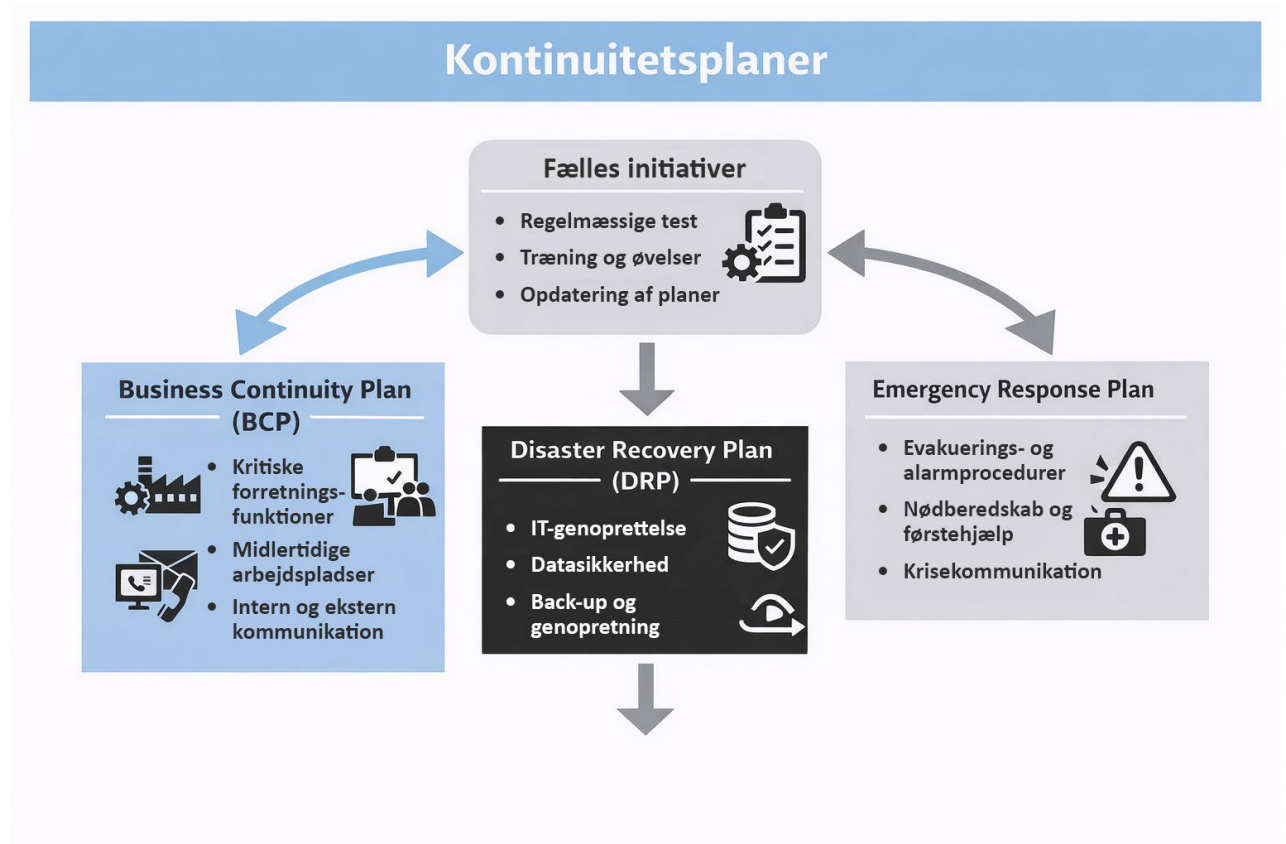


Kontinuitetsplaner



Kontinuitetsplan

- En forretningskontinuitetsplan, er en **strategisk plan**, som en virksomhed udarbejder for at sikre, at dens kritiske forretningsfunktioner kan fortsætte *under* og *efter* en krise eller større forstyrrelse.
- Formålet er at minimere afbrydelser, reducere økonomiske tab og beskytte organisationens omdømme.

Kontinuitetsplanen (eksempel på struktur)

1. Dokumentinformation.
2. Formål og omfang.
3. Kritiske forretningsfunktioner.
4. Risikovurdering.
5. Strategier og løsninger.
6. Roller og ansvar.
7. Kommunikationsplan.
8. Træning og test.
9. Vedligeholdelse.
10. Bilag.

1. Dokumentinformation

- Version:
- Dato:
- Forfatter(e):
- Godkendt af:

2. Formål og omfang

- Kort beskrivelse af, hvorfor planen eksisterer.
- Angiv hvilke dele af virksomheden eller systemer planen dækker.

Eksempel

Formål:

Formålet med denne kontinuitetsplan er at sikre, at virksomheden kan opretholde kritiske produktions- og leveringsprocesser under uforudsete hændelser, minimere økonomiske tab og beskytte medarbejdere, kunder og samarbejdspartnere. Planen skal gøre det muligt hurtigt at reagere, genoprette driften og træffe informerede beslutninger ved afbrydelser såsom maskinnedbrud, IT-svigt, leverandørproblemer eller eksterne kriser.

Omfang:

Planen dækker de dele af virksomheden og systemer, som er kritiske for kontinuerlig produktion og levering, herunder produktionsafdelingen (maskiner, produktionslinjer, lager og råvareforsyning), IT- og styringssystemer (ERP, produktionsstyringssystemer, back-office IT), produktionsteknologi (OT), leverandørkæde og logistik (kritiske leverandører og transportkanaler), medarbejdere og nøglefunktioner (roller og ansvar ved hændelser, herunder sikkerhed og kommunikation). Planen omfatter også procedurer for kommunikation internt og eksternt, samt retningslinjer for evaluering og opdatering efter hændelser.

3. Kritiske forretningsfunktioner

Funktion	Beskrivelse	Kritikalitet (H, M, L)	Ansvarlig

Note: H = høj, M = medium, L = lav

Kritiske forretningsfunktioner (eksempler)

Funktion	Beskrivelse	Kritikalitet (H, M, L)	Ansvarlig
ERP	Daglig drift af ordrebehandling, lagerstyring og økonomi	Høj	IT-chef
Produktion	Fremstilling af kerneprodukter	Høj	Produktionschef
IT-infrastruktur	Drift af netværk, servere og cloud-tjenester	Høj	IT-chef
Leverandørstyring	Kontakt og koordinering med nøgleleverandører	Høj	Indkøbschef
Backup & data recovery	Sikring af kritiske data og mulighed for gendannelse	Høj	IT-chef
Sikkerhed & adgangskontrol	Intern og ekstern kommunikation under kriser	Middel	Kommunikationschef

Note: H = høj, M = medium, L = lav

Risiko	Sandsynlighed	Konsekvens	Prioritet	Mitigationsstrategi

Risikovurdering (eksempel)

Risiko	Sandsynlighed	Konsekvens	Prioritet	Mitigationsstrategi
Cyberangreb	Medium	Høj	Høj	Antivirus og firewall på alle systemer Regelmæssige softwareopdateringer
Strømsvigt	Medium	Høj	Høj	Backup-generator, nødplan for driftstop, UPS til kritiske maskiner
Leverandørsvigt	Medium	Høj	Høj	Identificer kritiske leverandører og alternative leverandører Oprethold bufferlager af nøglematerialer
Maskinnedbrud	Medium	Høj	Høj	Regelmæssig vedligeholdelse, reservedelslager, kontrakt med serviceleverandør
IT-systemnedbrud (ERP, produktionsstyring)	Medium	Høj	Høj	Daglig backup, cloud-løsning, redundans på servere, IT-supportaftale
Transportproblemer / forsinkelser	Medium	Medium	Medium	Alternativ transport, flere leverandører, bufferlagre

5. Strategier og løsninger

- I en forretningskontinuitetsplan er **strategier og løsninger** de konkrete tiltag, virksomheden kan bruge for at opretholde driften under og efter en krise.
- List i en tabel:
 - Risiko/udfordring.
 - Strategi/løsning.
 - Ansvar.

Strategier og løsninger (eksempler)

Område	Risiko/udfordring	Strategi/løsning	Ansvarlig
IT	IT-systemnedbrud (ERP, produktionsstyring)	Daglig backup til både lokal og cloud-løsning Redundant server / failover-system IT-supportaftale med ekstern leverandør	IT-chef
IT	Cyberangreb / ransomware	Antivirus, firewall og opdateret software Træning af medarbejdere i sikkerhed (phishing awareness) Incident response plan Isolerede backup-systemer	IT-chef
Produktion	Maskinnedbrug	Forebyggende vedligeholdelsesplan Reservedelslager for kritiske komponenter Kontrakt med serviceleverandør med hurtig responstid	Produktionschef
Produktion	Strømafbrydelse	Backup-generator / nødstrøm UPS til kritiske maskiner Plan for prioriteret produktion under strømafbrydelse	Produktionschef
Forsyningskæden	Leverandørsvigt	Alternativ leverandør klar Bufferlager af kritiske råvarer Løbende vurdering af leverandørers kapacitet og økonomi	Supply Chain Manager
Forsyningskæden	Transportproblemer	Flere transportmuligheder / transportører Optimeret lagerstrategi Just-in-case lager af færdigvarer	Supply Chain Manager

[illegible]

Roller og ansvar (eksempel)

Rolle	Ansvarsområde	Kontaktinformation
IT-ansvarlig	Sikring af IT-drift, backup, cyber-sikkerhed, gendannelse af systemer	Navn: Maria Nielsen Telefon: +45 2345 XXXX E-mail: mn@eksempel.dk
Produktionschef	Drift af produktion, håndtering af maskinnedbrud, sikkerhed i produktionsområder	Navn: Lars Petersen Telefon: +45 3456 XXXX E-mail: lp@eksempel.dk
Kommunikationsansvarlig	Intern og ekstern kommunikation, kontakt til kunder, leverandører og medier	Navn: Sofie Larsen Telefon: +45 6789 XXXX E-mail: sl@eksempel.dk
Krisestabsleder	Overordnet ansvar for krisehåndtering, beslutninger og koordinering	Navn: Jens Hansen Telefon: +45 1234 XXXX Email: jh@eksempel.dk
Økonomiansvarlig	Likviditet, betalinger, løn, økonomiske konsekvenser af krisen	Navn: Christina Holm Telefon: +45 8901 XXXX E-mail: ch@eksempel.dk
HR-chef	Håndtering af personale, sygdomsudbrud, tab af nøglemedarbejdere, hjemmearbejde	Navn: Peter Jensen Telefon: +45 5678 XXXX E-mail: pj@eksempel.dk

7. Kommunikationsplan

Målgruppe	Kommunikationskanal	Ansvarlig	Nøglebesked	Tidspunkt

Kommunikationsplan (eksempel)

Målgruppe	Kommunikationskanal	Ansvarlig	Nøglebesked	Tidspunkt
Medarbejdere	E-mail, telefon, intranet, SMS	HR-chef	- Krisebesked: Hvad er sket? - Instrukser: Hvad medarbejdere skal gøre - Opdateringer om drift og sikkerhed	Umiddelbart efter krise opstår og løbende opdatering
Kunder	E-mail, telefon, sociale medier, website	Kommunikationsansvarlig	- Informere om eventuel forsinkelse eller produktionsstop - Forventet genoptagelsestid - Kontaktperson ved spørgsmål	Senest 4 timer efter hændelsen, opdatering efter behov
Leverandører	E-mail, telefon	Logistikchef / Indkøbschef	- Status på forsyningskæde og eventuelle ændringer - Prioritering af leverancer - Kontaktperson for koordinering	Umiddelbart efter hændelse og ved ændringer i leveranceplan
Myndigheder	E-mail, telefon	Krisestabsleder / Kommunikationsansvarlig	- Lovpligtig rapportering hvis relevant - Eventuelle sikkerheds- eller miljøhændelse	Så snart det er nødvendigt iht. lovgivning eller tilsynskrav

8. Træning og test

Øvelse/test	Formål	Deltagere	Frekvens	Ansvarlig	Kommentar/ opfølgning

Træning og test (eksempler)

Øvelse/test	Formål	Deltagere	Frekvens	Ansvarlig	Kommentar/ opfølgning
Evaluerings- øvelse	Test af flugtveje og alarm	Alle medarbejdere	Årlig	Sikkerhedsansvarlig	Logfør tid, evakueringseffektivitet
IT-nedbruds- simulering	Test af backup og gendannelse	IT, produktion, krisestab	To gange årligt	IT-ansvarlig	Noter fejl og løsninger
Leverandør- svigt-øvelse	Test af alternativ leverandørplan	Logistik, indkøb, produktion	Årlig	Logistikchef	Evaluer leveringshåndtering
Cyberangreb- simulering	Træning i IT-sikkerhed og incident response	Alle IT-brugere	Årlig	IT-ansvarlig	Registrer medarbejderrespons og læring

9. Vedligeholdelse

1. Regelmæssig opdatering af planen

- Revidér BCP mindst én gang årligt, eller efter større ændringer i virksomheden (f.eks. ny produktion, nye IT-systemer, nye leverandører).
- Opdater kontaktinformationer for krisestab, medarbejdere, leverandører og myndigheder.
- Justér roller og ansvar ved personaleændringer.

2. Opdatering af risikovurdering

- Gennemgå risikolisten for nye trusler (f.eks. nye cybertrusler, ændringer i leverandørkæden, klimaændringer).
- Opdater sandsynlighed, konsekvens og prioritet for eksisterende risici.
- Tilføj nye risici, der er relevante for produktionen.

3. Evaluering af strategier og løsninger

- Gennemgå tidligere krisesituationer og test/øvelser.
- Opdater strategier og nødprocedurer baseret på erfaringer.
- Tjek, om backup-systemer, nødgeneratorer og alternative lokationer stadig fungerer.

9. Vedligeholdelse (fortsat)

4. Træning og øvelser

- Planlæg næste runde af træning og test for medarbejdere og krisestab.
- Sørg for, at nye medarbejdere introduceres til kontinuitetsplanen.
- Dokumentér alle øvelser og resultater for opfølgning.

5. Dokumentation og versionering

- Hold styr på versionsnummer, dato for opdatering og ansvarlig person.
- Arkivér gamle versioner for sporbarhed.
- Sørg for, at alle relevante medarbejdere har adgang til den nyeste version, både digitalt og fysisk.

10. Bilag (eksempler)

- Skemaer.
- Kontaktlister.
- Processkort.
- Alternative lokationer.
- IT-backup-procedurer.