Beredskabsplanlægningsmodel

Template: Beredskabsplanlægningsmodel for Robot-, Drone- og Automationsindustrien udarbejdet ud fra ISO22301 standardens kravelementer og forslag til aktionspunkter.

Contents

1. Formål og anvendelse 2
2. Introduktion til beredskabsplanlægning 2
3. Opbygning af en beredskabsplan 2
   3.1 Identifikation af kritiske funktioner 2
   3.2 Risiko- og impactanalyse (BIA) 3
   3.3 Udvikling af kontinuitetsstrategier 3
   3.4 Roller og ansvar 4
   3.5 Ressourcer og afhængigheder 4
4. Implementering og vedligehold 5
   4.1 Øvelser og test 5
   4.2 Træning og bevidsthed 5
   4.3 Kommunikation og alarmering 6
5. Dokumentation og revision 6
   5.1 Dokumentationskrav 6
   5.2 Revision og opdatering 7
6. Beredskabsplanens anvendelse ved IT-incidents 7
   Før hændelsen (Forberedelse): 8
   Under hændelsen (Respons): 8
   Efter hændelsen (Recovery og læring): 8
7. Anvendelse af PDCA i beredskabsstyring 9

1. Formål og anvendelse

Formålet med denne beredskabsmodel er at understøtte en effektiv planlægning og styring af forretningskritiske funktioner, så virksomheden kan modstå og komme sig efter afbrydelser, herunder it-sikkerhedshændelser. Modellen tager udgangspunkt i ISO 22301-standarden, som fastsætter krav til etablering, implementering, vedligehold og forbedring af et ledelsessystem for forretningskontinuitet.

Denne guide er udviklet til undervisningsbrug og kan benyttes som inspiration ved udarbejdelse af konkrete beredskabsplaner i virksomheder.

2. Introduktion til beredskabsplanlægning

En beredskabsplan sikrer, at virksomheden er i stand til at reagere hurtigt og effektivt på afbrydelser, uanset om de skyldes cyberhændelser, tekniske fejl, leverandørsvigt eller naturkatastrofer.

Centrale principper fra ISO 22301 omfatter:

- Risiko- og konsekvensvurdering (Business Impact Analysis, BIA)
- Etablering af kontinuitetsstrategier og -løsninger
- Klar rollefordeling og ansvar
- Dokumentation, øvelse og vedligehold af planerne

3. Opbygning af en beredskabsplan

3.1 Identifikation af kritiske funktioner

Formålet med dette trin er at identificere de forretningsfunktioner og ressourcer, som er afgørende for virksomhedens evne til at opretholde drift under og efter en afbrydelse. Dette danner grundlag for hele beredskabsplanlægningen.

Fremgangsmåde:

1. *Kortlægning af forretningsprocesser:* Identificér alle centrale processer, beskriv deres formål og output.
2. *Identificér it-systemer og teknologiske afhængigheder:* Notér hvilke systemer, databaser og applikationer der understøtter hver proces.
3. *Vurder kritikalitet:* Hvilke funktioner er nødvendige for minimumsdrift? Hvilke kan midlertidigt undværes?
4. *Dokumentér afhængigheder*: Interne (personale, systemer) og eksterne (leverandører, infrastruktur).

3.2 Risiko- og impactanalyse (BIA)

Dette trin handler om at analysere potentielle trusler og vurdere konsekvenserne af afbrydelser.

Fremgangsmåde:

1. *Identificér trusler:* F.eks. cyberangreb, strømudfald, sygdom blandt nøglepersonale, leverandørsvigt.
2. *Vurder sandsynlighed og konsekvens:* Brug en risikomatrix til at prioritere trusler.
3. *Analyser konsekvenser:*
    - Finansielle: Tabt omsætning, ekstraomkostninger
    - Juridiske: Overtrædelse af kontrakter eller lovgivning
    - Omdømme: Tab af kundetillid, negativ presse
4. Fastlæg tolerancer:
    - RTO (Recovery Time Objective): Hvor hurtigt skal funktionen være genetableret?
    - RPO (Recovery Point Objective): Hvor meget datatab er acceptabelt?

3.3 Udvikling af kontinuitetsstrategier

Her udarbejdes konkrete strategier og planer for at sikre fortsat drift eller hurtig genopretning.

Fremgangsmåde:

1. *Udarbejd scenarier:* F.eks. nedbrud i ERP-system, brand i kontorbygning, ransomware-angreb.

2. *Definér responsplaner:* Hvem gør hvad, hvornår og hvordan?
3. *Genopretningsprocedurer:*
    - It-systemer: Backup, failover, gendannelse
    - Kommunikation: Internt og eksternt
    - Personale: Erstatningsroller, hjemmearbejde, tilkaldeberedskab

3.4 Roller og ansvar

Dette trin handler om at identificere klare roller og placere ansvar for at undgå uklarheder under en hændelse, og sikre effektiv beredskabsstyring.

Fremgangsmåde:

1. Udpeg ansvarlige:
    - For aktivering af beredskabsplanen
    - For løbende opdatering og vedligehold
2. Etabler kriseorganisation:
    - Kriseteam: Beslutningstagere og koordinatorer
    - Kommunikationsteam: Håndtering af intern og ekstern kommunikation
    - Teknisk team: It-genopretning og systemovervågning

3.5 Ressourcer og afhængigheder

For at sikre kontinuitet skal alle nødvendige ressourcer og afhængigheder være identificeret og dokumenteret.

Fremgangsmåde:

1. *Registrér kritiske ressourcer:*
    - Personale og nøglekompetencer
    - Data og dokumentation
    - Udstyr og lokationer
2. Kortlæg eksterne afhængigheder:
    - Leverandører og partnere
    - Tjenesteudbydere (cloud, netværk, logistik)
    - Juridiske og regulatoriske krav

4. Implementering og vedligehold

Når beredskabsplanen er udarbejdet, er det afgørende at sikre, at den fungerer i praksis. Det kræver løbende test, træning, kommunikation og opdatering.

4.1 Øvelser og test

Formålet med dette trin er at sikre, at beredskabsplanen er operationel og effektiv, når den skal bruges.

Fremgangsmåde:

1. *Regelmæssige tests:*
    - Gennemfør planlagte tests mindst én gang årligt eller ved større ændringer i organisationen.
    - Evaluer planens effektivitet og identificér forbedringsområder.

2. *Scenariebaserede øvelser:*
    - Simulér realistiske hændelser (fx cyberangreb, systemnedbrud, brand).
    - Involver relevante teams og ledelse.

3. *Tekniske recovery-tests:*
    - Test backup- og gendannelsesprocedurer.
    - Verificér failover-løsninger og systemers robusthed.

Resultatet herved, vil være en dokumenteret testhistorik og en løbende forbedret beredskabsplan.

4.2 Træning og bevidsthed

Alle medarbejdere skal kende deres rolle i en krisesituation og forstå vigtigheden af hurtig og korrekt reaktion.

Fremgangsmåde:

1. *Uddannelse:*
    - Gennemfør introduktionstræning for nye medarbejdere.
    - Tilbyd regelmæssige opfriskningskurser for nøglepersoner.

2. *Rollespecifik træning:* Træn kriseteam, it-personale og kommunikationsansvarlige i deres specifikke opgaver.
3. *Bevidsthedskampagner:*
    - Brug plakater, intranet, nyhedsbreve og workshops til at fremme beredskabskultur.
    - Fremhæv vigtigheden af hurtig reaktion og korrekt kommunikation.

4.3 Kommunikation og alarmering

Effektiv kommunikation er afgørende under en krise – både internt og eksternt.

Fremgangsmåde:

1. *Etabler kommunikationskanaler:*
    - Interne: Telefonkæder, e-mail, intranet, SMS-varsling
    - Eksterne: Pressemeddelelser, sociale medier, kundeservice
2. *Udarbejd kommunikationsplaner:*
    - Forbered skabeloner til beskeder til kunder, partnere og myndigheder.
    - Definér hvem der må udtale sig, og hvordan information skal godkendes.
3. *Alarmeringsprocedurer:*
    - Fastlæg hvordan og hvornår beredskabsplanen aktiveres.
    - Brug automatiserede systemer til hurtig varsling.

5. Dokumentation og revision

Effektiv beredskabsstyring kræver, at alle aktiviteter dokumenteres systematisk, og at planen løbende revideres og forbedres i takt med ændringer i trusselsbilledet og forretningen.

5.1 Dokumentationskrav

Formålet med dokumentationen er at sikre sporbarhed, gennemsigtighed og tilgængelighed i hele beredskabsarbejdet.

Fremgangsmåde:

1. *Vedligehold en opdateret beredskabsplan:*
    - Planen skal være godkendt af ledelsen og tilgængelig for relevante medarbejdere.
    - Versionér dokumentet og registrér ændringer (ændringslog).
2. Centraliser dokumentationen:

- Opbevar planen og relaterede dokumenter i et sikkert, men tilgængeligt system (f.eks. intranet, dokumentstyringssystem).

3. *Dokumentér øvelser og tests:*
    - Registrér dato, deltagere, scenarie, resultater og læringspunkter.
    - Notér identificerede forbedringsområder og opfølgende handlinger.
4. *Sørg for revisionsspor:* Alle ændringer og beslutninger skal kunne spores tilbage til ansvarlige personer og datoer.

5.2 Revision og opdatering

En beredskabsplan er et levende dokument, der skal tilpasses løbende for at forblive effektiv.

Fremgangsmåde:

1. *Gennemfør regelmæssige reviews:*
    - Minimum én gang årligt eller ved større organisatoriske ændringer (f.eks. nye systemer, flytning, fusioner).
    - Involver relevante interessenter (it, drift, HR, ledelse).
2. Opdatér planen baseret på:
    - Erfaringer fra øvelser og hændelser: Hvad fungerede, og hvad skal forbedres?
    - Ændringer i trusselsbilledet: Nye cybertrusler, geopolitiske forhold, klimarisici.
    - Forretningsændringer: Nye produkter, processer, lokationer eller leverandører.
3. Godkend og kommuniker ændringer:
    - Sikr ledelsens godkendelse af større ændringer.
    - Informér relevante medarbejdere om opdateringer og nye procedurer.

6. Beredskabsplanens anvendelse ved IT-incidents

IT-hændelser kan have alvorlige konsekvenser for forretningen. En effektiv beredskabsplan skal derfor dække hele hændelsesforløbet – fra forberedelse til genopretning og læring.

6.1 Før hændelsen (Forberedelse):

Formålet er at reducere risikoen for hændelser og sikre, at organisationen er klar til at reagere hurtigt og effektivt.

Fremgangsmåde:

1. Identificér kritiske IT- og OT-systemer:
    - Kortlæg systemer, applikationer og data, der er essentielle for forretningsdrift.
    - Vurder afhængigheder og sårbarheder.
2. Etablér backup- og recoveryprocedurer:
    - Implementér regelmæssige og testede backups.
    - Definér RTO og RPO for hvert system.
3. Udvikl incident response team og kommunikationsplaner:
    - Udpeg roller og ansvar i et dedikeret incident response team.
    - Udarbejd kommunikationsplaner for både interne og eksterne interessenter.

6.2 Under hændelsen (Respons):

Når en hændelse opstår, er hurtig og koordineret indsats afgørende for at begrænse skaden.

Fremgangsmåde:

1. Aktivér krisehåndteringsteamet:
    - Følg aktiveringsproceduren i beredskabsplanen.
    - Indkald relevante nøglepersoner.
2. Isolér og inddæm skaden:
    - Afbryd adgang til kompromitterede systemer.
    - Begræns spredning af malware eller datalæk.
3. Iværksæt genopretning og kommunikation:
    - Start gendannelse af systemer i prioriteret rækkefølge.
    - Kommunikér løbende med medarbejdere, ledelse og eksterne parter.

6.3 Efter hændelsen (Recovery og læring):

Når hændelsen er håndteret, skal fokus være på at genskabe normal drift og lære af forløbet.

Fremgangsmåde:

1. Genskab systemer og drift:
    - Verificér integritet og funktionalitet af gendannede systemer.
    - Genoptag normal drift i henhold til forretningsprioriteter.
2. Gennemfør post-incident review:
    - Afhold en evaluering med alle involverede parter.
    - Identificér årsager, styrker og svagheder i responsen.
3. Opdatér planen og rapportér:
    - Justér beredskabsplanen baseret på læring.
    - Rapportér hændelsen til relevante myndigheder og interessenter, hvis påkrævet (kan også være essentielt under hændelsen).

7. Anvendelse af PDCA i beredskabsstyring

PDCA-cyklussen er en systematisk metode til løbende forbedring og styring af processer. I konteksten af beredskabsstyring sikrer den, at beredskabsplanen ikke blot bliver udarbejdet, men også implementeret, testet og forbedret over tid.

7.1 Plan (Planlægning)

Formål: At etablere grundlaget for beredskabsstyring gennem analyse, målsætning og politikker.

Aktiviteter:

- Udfør risiko- og konsekvensanalyser (BIA og risikovurdering)
- Identificér kritiske funktioner og afhængigheder
- Fastlæg mål, politikker og procedurer for forretningskontinuitet
- Udarbejd beredskabsstrategier og -planer

7.2 Do (Udførsel)

Formål: At implementere de planlagte tiltag og sikre organisatorisk forankring.

Aktiviteter:

- Implementér beredskabsplanen og tekniske løsninger
- Gennemfør træning og øvelser for medarbejdere og kriseteams
- Etablér kommunikationskanaler og alarmeringsprocedurer
- Sørg for tilgængelig dokumentation og adgang til planen

7.3 Check (Kontrol)

Formål: At overvåge og evaluere effektiviteten af beredskabsindsatsen.

Aktiviteter:

- Gennemfør test og scenariebaserede øvelser
- Udfør interne audits og evalueringer
- Dokumentér afvigelser, forbedringspunkter og læring
- Overvåg overholdelse af politikker og procedurer

7.4 Act (Forbedring)

Formål: At forbedre beredskabsplanen og styringssystemet baseret på erfaringer og ændringer.

Aktiviteter:

- Opdatér planen efter øvelser, hændelser og reviews
- Tilpas til ændringer i trusselsbilledet eller forretningen
- Implementér forbedringsforslag og korrigerende handlinger
- Sikr ledelsens involvering og godkendelse af ændringer

PDCA-cyklussen er ikke en engangsproces, men en kontinuerlig forbedringsmodel, der sikrer, at beredskabsstyringen forbliver relevant, effektiv og tilpasset virksomhedens behov.