DIGITALISERINGSSTYRELSEN

Guide til bedre beredskabsstyring

April 2015

Guide til bedre beredskabsstyring

Udgivet april 2015

Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen
kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
Digitaliseringsstyrelsens hjemmeside
www.digst.dk.

Foto Colourbox

Elektronisk publikation
ISBN 978-87-93073-12-8

Indhold

Baggrund

Formålet med denne guide er at give gode råd til, hvordan en organisation kan forbedre sit it-beredskab. Guiden er målrettet systemejere eller andre, der har ansvaret for løbende at vedligeholde og forbedre beredskabet for et system.

Guiden relaterer sig til beredskaber, der kan bruges ved hændelser, hvor de almindelige driftsprocesser ikke er tilstrækkelige eller er sat ud af spil. Formålet med et beredskab er at opretholde eller retablere et acceptabelt niveau for drift i en nødsituation. Ifølge ISO27001 skal der udarbejdes en beredskabsplan for de it-systemer, som risikovurderingen har vist er mest kritiske for myndighedens opgavevaretagelse.

Mange organisationer har allerede it-beredskabsplaner for kritiske systemer, men planer har en tendens til at sande til, hvis de ikke bliver testet jævnligt, eller hvis der sker udskiftning af nøglepersoner på området. Samtidig kan ændringer i omgivelsernes krav og forventninger medføre behov for løbende at tilpasse og forbedre beredskabet.

Guiden er udviklet med afsæt i PwC's globale framework for Business Continuity Management og tager udgangspunkt i ISO2700X-standarderne. Fokus er især på balancen mellem den enkelte offentlige myndigheds risikoprofil kontra de særlige konsekvenser, som kommer ved et brud på integritet eller tilgængelighed af et kritisk system.

Indledning

Ud over denne guide er der udviklet et evalueringsværktøj, som kan bruges til at fastslå, hvor det vil være fornuftigt at forbedre sin beredskabsstyring.

Vejledning i brugen af evalueringsværktøjet findes på Digitaliseringsstyrelsens hjemmeside.

Når evalueringen er gennemført, vil der formentlig være identificeret områder, der kræver forbed-ringer inden for et eller flere af de nedenstående styringsområder:

1. Vurdering af den samfundsmæssige konsekvens
2. Compliance
3. Organisering, roller og ansvarsfordeling
4. Varsling, vurdering og mobilisering
5. Kommunikation internt og på tværs af myndigheder og samarbejdspartnere
6. Styring af leverandører
7. Beredskabsprocessen, herunder løbende risikovurdering af kritiske it-systemer og ensartet tilgang til it-beredskabsstyring
8. Forankring, vedligehold og test af beredskabsplan.

Når man har besluttet, hvilke områder man vil forbedre, giver denne guide praktiske anvisninger til at foretage forbedringerne ved hjælp af en trinvis guide for hvert område.

1. Vurdering af samfundsmæssig konsekvens

Vurderingen af konsekvenser ved sikkerhedshændelser (utilgængelighed, brud på fortrolighed eller udfordringer med datas integritet) danner grundlag for en lang række beslutninger i forbindelse med beredskabsstyringen.

Den systemansvarlige skal overveje den samlede "samfundsmæssige konsekvens" ved sikkerhedshændelser – i hvilket omfang hændelser, der påvirker eget it-system, vil have afledte konsekvenser på andre områder, fx i andre organisationer eller hos andre myndigheder. En afledt konsekvens kan gøre sig gældende på mange forskellige niveauer. Fx vil sikkerhedshændelser i større offentlige it-infrastrukturkomponenter som CPR eller NemID have store afledte konsekvenser.

Med mindre it-systemet udelukkende understøtter interne arbejdsopgaver, er det nødvendigt at tage højde for afledte konsekvenser i konsekvensvurderingen. På den måde kan man tage de rette beslutninger i sit beredskab og sikre det nødvendige input fra relevante eksterne interessenter, fx til intern kommunikation og på tværs af myndigheder og samarbejdspartnere.

Vurdering af afledte konsekvenser

Det kan være vanskeligt for den driftsansvarlige myndighed selv at vurdere de afledte konsekvenser, især hvis der ikke findes en opdateret kortlægning af, hvilke processer og services systemet i de enkelte myndigheder understøtter. I den situation kan eksterne og interne interessenter levere et datagrundlag til konsekvensvurderingen.

Det anbefales, at der også indhentes input fra ledelsen, fx på kontorchefniveau, for at kvalificere vurderingen af forretningsmæssige konsekvenser og sikre den tværorganisatoriske forankring.

Trin 1 – Indsamling af information

Konsekvensvurderingen kan være skriftlig. Det vil desuden ofte være nødvendigt at følge op med en workshop for at skabe en fælles forståelse og afstemme forventninger i forhold til den eksisterende status på beredskabet, fx aftalte servicekrav til systemet, eksisterende kommunikationskanaler og koordinering.

Trin 2 – Fælles begrebsramme

Det er en forudsætning, at der arbejdes med et fælles begrebsapparat på tværs af organisationen, herunder at man har samme opfattelse af konsekvenser. Digitaliseringsstyrelsens vejledning giver eksempler på konsekvenstyper og -niveauer.

Trin 3 – Dokumentering

Resultaterne fra workshoppen dokumenteres. Nedenstående figur 1 er et eksempel på kategorisering af konsekvenser ved utilgængelighed, hvor konsekvensniveauet er angivet med 1, 2, 3 og 4.

Skabelon til konsekvensvurdering

Område		Konsekvensniveau				
Proces	**Aktivitet**	**4 timer**	**4-8 timer**	**2 dage**	**Under 1 uge**	**Mere end 1 uge**
Pasansøgning	Ike muligt at bestille nyt pas	1	1	2	3	4
Boligstøtte	Beregning af boligstøtte ikke tilgængelige	1	1	1	2	2

Konsekvensniveau	
Uvæsentlig	1
Generende	2
Kritisk	3
Uacceptabel	4

Ligeledes er nedenstående et eksempel på et skema til brug for vurdering af konsekvensniveau ved brud på fortrolighed eller manglende integritet.

	Område	Antal borgere	Konsekvens-niveau
Integritet	Borgerdata ikke korrekte	Få borgere	2
	Borgerdata bliver ikke opdateret	Alle borgere	2
Fortrolighed	Borgerdata kan ses af andre borgere	To borgere kan se hinandens data	3
	CPR-numre matcher ikke borgeren	Alle borgere	3
	Der er blevet lækket flere cpr-numre	Uafklaret	4

Trin 4 – Workshop – udarbejdelse af handlingsplan

På baggrund af konsekvensvurderingen af de afledte konsekvenser skabes en ny fælles forståelse og forventningsafstemning af, hvordan beredskabssituationer skal håndteres på tværs af de involverede parter.

Det fastlægges, hvilke tekniske eller forretningsmæssige nødprocedurer systemejeren har implementeret, og om de afledte konsekvenser har givet anledning til en opdatering af nødprocedurerne – især i de tilfælde, hvor de afledte konsekvenser er kritiske eller uacceptable.

Med denne information kan de eksterne interessenter, der er afhængige af systemet, vurdere, i hvilket omfang de har behov for at ændre i deres egne nødprocedurer.

Trin 5 – Opdater eksisterende beredskab

Følgende områder i beredskabsplanen opdateres ud fra den nye viden om afledte konsekvenser, nødprocedurer og behov:

3. Organisering, roller og ansvarsfordeling
4. Varsling, vurdering og mobilisering
5. Kommunikation eksternt og på tværs af myndigheder og samarbejdspartnere
6. Styring af leverandører
7. Beredskabsprocessen, herunder løbende risikovurdering af kritiske it-systemer og ensartet tilgang til it-beredskabsstyring
8. Forankring, vedligehold og test af beredskabsplan.

For flere af områderne vil det formentlig være nødvendigt at koordinere med beredskabsplanlægningen i de afhængige organisationer.

Trin 6 – Opfølgning

ISO27001 foreskriver etablering af en proces, hvor konsekvensvurderinger foretages med faste mellemrum samt i forbindelse med større ændringer i it-systemet, organisationen eller anvendelsen (fx stor tilgang af brugere) mv.

2. Compliance

Compliance handler om overholdelsen af interne politikker, standarder og eventuelle lovmæssige krav. Hele det statslige område[1] arbejder med samme standard for informationssikkerhed (ISO27001). Der er til standarden udviklet flere vejledninger[2].

It-beredskabsplaner kan være meget forskellige både i form og indhold og stadig overholde de foreskrevne standarder.

Trin 1 – Identificering af politikker, standarder og eventuelle lovmæssige krav

ISO27001 er den standard, der skal overholdes af statslige institutioner. Selvom der ikke er tale om en statslig institution, vil man ved brug af standarden få adgang til et begrebsapparat og en forståelse af informationssikkerhed, der kan bruges på tværs af den offentlige sektor.

Trin 2 – Uddannelse og træning

For at sikre overholdelse af alle relevante politikker, standarder og lovmæssige krav er det nødvendigt for nøglemedarbejdere at blive oplært i, hvilken indflydelse disse har på medarbejdernes daglige arbejde. Afsnit 8 i denne guide handler om dette.

Trin 3 – Audit og review

Den, der har ledelsesansvaret for beredskabet, bør sikre, at der er regelmæssige audit- og review-sessioner, der sikrer compliance. Dette betyder, at der periodisk skal ske en gennemgang af kravene til compliance og sikres, at disse overholdes. Ofte er eksterne og interne bedømmere afgørende for at vurdere overholdelsen af lovgivningen eller standarder, men dette er dog ikke gældende for alle myndigheder. Sådanne audits og reviews skal foregå i bestemte intervaller – minimum årligt – og være forankret hos ledelsen.

[1] ISO27001 anvendes også i store dele af de kommunale og regionale områder.

[2] Se eventuelt http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Vejledninger-om-sikkerhedsarbejdet.

3. Organisering, roller og ansvar

Dette område handler om, at alle medarbejdere er klar over, hvad de skal gøre i en beredskabssituation – og at det er indøvet. Hertil kommer udpegning af stedfortrædere og sikring af, at ansvaret for tværgående områder er afklaret og dokumenteret.

Trin 1 – Identificering af organisation, roller og ansvar

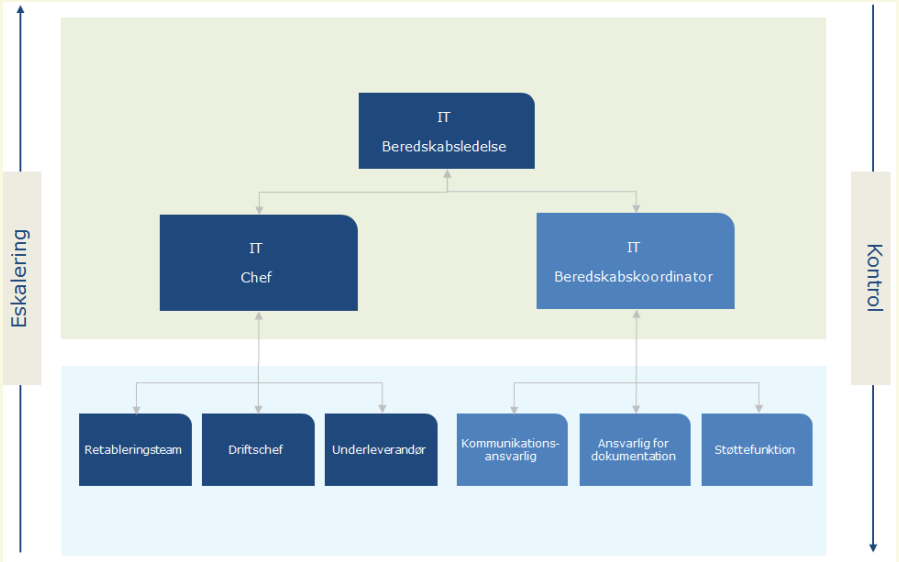
Beredskabsstyring er et ledelsesansvar og skal derfor forankres i ledelsen. Ledelsen skal fastsætte det ønskede beredskabsniveau (via en konsekvensvurdering) og forholde sig til de risici, der måtte være. Ledelsen skal derfor tage stilling til beredskabets organisering, herunder ressourceallokering, roller, ansvar, politikker og løbende opfølgning.

Følgende fire roller med tilhørende ansvarsområder skal som minimum være defineret. For hver rolle udpeges den medarbejder, der skal udfylde rollen og en stedfortræder for denne medarbejder.

- **It-beredskabsledelse** – Øverste myndighed. Varetager væsentlige beslutninger vedrørende håndtering af beredskabsmæssige situationer.
- **It-beredskabskoordinator** – Bistår ledelsen i koordinering og dokumentation.
- **Kommunikationsansvarlig** – Ansvarlig for kommunikation med eksterne og interne interessenter.
- **Retableringsansvarlig(e)** – Teknisk personale med faglig viden, som forestår retablering i henhold til aftalte procedurer og planer. Oftest er disse personer ansat hos leverandøren af løsningen, mens den løsningsansvarlige er fra den systemansvarlige myndighed.

Beredskabsorganisering kan se ud som vist i figuren på næste side.

Beredskabsorganisering



Trin 2 – Forankring og kommunikation af organisation, roller og ansvar

Den fornødne ressourceallokering til oplæring af medarbejderne i beredskabet er ledelsens ansvar. En måde at oplære på kan være ved at teste beredskabsplanen. Endvidere er det vigtigt at sikre, at de udpegede medarbejdere har de nødvendige beslutningskompetencer.

Kommunikation af beredskabsstyring og dets organisering, ansvar og roller skal foregå således, at alle interessenter er informerede – dette gælder især eksterne interessenter og samarbejdspartnere. Kommunikationen kan eksempelvis foregå via nyhedsbreve eller informationsmøder.

4. Vurdering, varsling og mobilisering

Varsling, vurdering og mobilisering drejer sig om definition, vurdering og varsling af hændelser, ved at afklare spørgsmål som: Hvad kendetegner en beredskabshændelse? Hvem kan aktivere beredskabet? Hvilken proces følges for at aktivere beredskabet? Hvilke eskaleringsprocesser og varslingsmodeller benyttes?

Typisk har it-beredskaberne fokus på håndtering af utilgængelighed. Der kan derfor være behov for at vurdere, i hvilket omfang de samme processer kan bruges ved andre typer hændelser, såsom brud på integritet eller fortrolighed.

Det er nødvendigt, at en myndighed selv tager ansvar for at sikre en optimal varslings- og mobiliseringsproces. Årsagen er, at leverandøren ikke nødvendigvis vurderer konsekvenserne ved hændelser, der ikke er relateret til tilgængelighed, såsom cybercrime-hændelser eller påvirkning af dataintegriteten, på samme måde som en offentlig myndighed. Hertil vil myndigheden skulle sikre sig, at mobiliseringsprocessen internt og ved leverandøren understøtter myndighedens behov for information, fx til at kunne imødekomme henvendelser fra presse, politikere og privatpersoner vedrørende hændelsen.

Trin 1 – Identificering af eksisterende retningslinjer for vurdering, varsling og mobilisering

Interview af egen ledelse og af driftsleverandører er en god metode til at undersøge, om der er den samme opfattelse af de nedskrevne retningslinjer for vurdering, varsling og mobilisering. Et væsentligt fokus er her, om kriterierne for varsling, vurdering og mobilisering er klart definerede, og om det tydeligt fremgår, hvem og hvad der aktiverer beredskabet.

Det er værd at bemærke, at de målepunkter på tilgængelighed, en leverandør anvender, ikke nødvendigvis afspejler slutbrugerens oplevelse af servicens tilgængelighed – fx hvornår en myndighed vil få henvendelser. Der kan derfor være behov for at sikre, at myndigheden kan mobilisere beredskabet ved en leverandør. Eksempelvis kan det være uklart, om en fejl skyldes ét system, der driftes ved én leverandør, eller et andet system, der driftes ved en anden leverandør. Her vil der være behov for at mobilisere beredskabet ved begge leverandører, også selv om den ene leverandørs målepunkter viser, at deres system er tilgængeligt.

Trin 2 – Afstemning af retningslinjer for vurdering, varsling og mobilisering

Vurdering, varsling og mobilisering skal tage udgangspunkt i de forretningsmæssige konsekvenser. Vil en hændelse have store konsekvenser, skal det naturligvis afspejles i de kriterier, der er for vurdering, varsling og mobilisering. Kriterierne skal godkendes af ledelsen, som også skal godkende eventuelle risici, fx forskelle mellem hvor hurtigt myndigheden har behov for information til at udtale sig om en hændelse, og hvor hurtigt en leverandør er forpligtet til at levere informationen.

Ved varsling er det vigtigt at gøre sig klart, hvilke interessenter der skal varsles, og hvilke informationer de skal have. Aftagende myndigheder kan eksempelvis have en interesse i tidshorisont, fejlkilde, midlertidig workaround osv.

Det er vigtigt, at man sikrer, at der er de rette beslutningskompetencer til stede, når rollerne i beredskabet bemandes.

5. Kommunikation

Kommunikation er en af de vigtigste opgaver i forhold til beredskabsledelse, men den korrekte kommunikationsindsats viser sig ofte at være vanskelig – mangelfulde kommunikationsprocesser er ofte kilde til fejl i beredskabsindsatsen.

- I en kritisk situation er det vigtigt at kunne tale åbent og fortroligt – også med leverandører og andre samarbejdspartnere. Det er derfor vigtigt at have etableret grundlaget for dette. Her spiller almindelig tillid og gode personlige relationer ind.

- Det er uhensigtsmæssigt at skulle forholde sig til en ny måde at kommunikere på i en beredskabssituation. Planen for beredskabskommunikationen skal derfor baseres på den måde, der i forvejen kommunikeres i organisationen.

Trin 1 – Eksisterende kommunikationsplan

Som grundlag for det videre arbejde er det en god idé at starte med at indsamle den eksisterende dokumentation om kommunikation i organisationen. Der er en god chance for, at flere kommunikationsprocesser er opstået ad hoc, og derfor kun er kendt af dem, der arbejder med drift af systemet samt de kommunikationsansvarlige i organisationen.

Denne viden kan dokumenteres fx ved hjælp af interviews med de relevante personer. Her kan man spørge ind til kommunikationen i tidligere beredskabssituationer, der eventuelt også er dokumenteret skriftligt i form af e-mails eller andet.

Trin 2 – Identificer målgrupper og kanaler

For at få et retvisende overblik over kommunikationsopgaven skal man afdække målgruppen for herved at kunne fastlægge de rette kommunikationskanaler. Hvem har behov for viden ved hændelser, hvilken information har de behov for, hvordan håndteres information nemmest muligt (både for modtager og afsender)?

Det er hensigtsmæssigt at opdele kommunikationsopgaven i henholdsvis intern og ekstern kommunikation, da det er to meget forskellige kommunikationsopgaver.

- Den interne kommunikation er kommunikation i beredskabsorganisationen, dvs. mellem alle interessenter, der er direkte involveret i beredskabet, fx internt hos den ansvarlige myndighed og mellem myndigheden og driftsleverandøren. Det kan også være væsentligt at have en vis indsigt i kommunikationen internt hos driftsleverandøren.

  Den indbyrdes kommunikation foregår i vid udstrækning via telefon blandt de centrale beslutningstagere i en beredskabssituation. For at sikre denne kommunikationskanal er det en god ide at søge bistand hos Beredskabsstyrelsen for særlig rådgivning om mulighederne for prioriterede numre/telefonkonferencer mv.

- Den eksterne kommunikation er al kommunikation uden for beredskabsorganiseringen til fx andre myndigheder, andre driftsleverandører, pressen mv. Viser det sig i trin 1, at der ikke er faste aftaler for kommunikation, skabes disse i dialog med kommunikationsmedarbejdere eller tilsvarende hos de relevante eksterne interessenter.

Større og kritiske it-systemer vil ofte være afhængige af (fx data fra) it-systemer i andre myndigheder og dermed ofte andre driftsleverandører. Det er derfor en vigtig, at myndigheden gør en indsats for at sikre en formalisering mellem driftsleverandører på tværs af myndigheder.

Det er vigtig at sikre, at kommunikationsindsatsen har fokus på dét slutbrugeren oplever, fx en borger. Afsnit 2 og 5 behandler nogle af forudsætningerne for dette.

Trin 3 – Dokumentation af forskelle og mangler

Efter Trin 1 og 2 afdækkes eventuelle mangler, ligesom eventuelle udfordringer i beredskabskommunikationen kan identificeres.

Trin 4 – Udarbejd kommunikationsindsats

På baggrund af Trin 3 udarbejdes en opdateret kommunikationsindsats, som med fordel kan tage udgangspunkt i hver af de identificerede målgrupper. Man kan fx tage udgangspunkt i tabellen herunder:

Målgruppe og kommunikationsbehov stiller krav til kommunikationskanal

Målgruppe	Formål	Anbefalede krav til kommunikationskanal
Eksterne beslutningstagere, herunder andre myndigheder	Orientering, beslutningsgrundlag	Korrekte modtagere nås. Præcis og hurtig information
Teknikere hos andre leverandører	Orientering, fejlfinding, beslutningsgrundlag	Detaljeret information med mulighed for henvisninger til andre kilder/kanaler
Brugere	Orientering/aflastning af mandskabskrævende kommunikationskanaler (telefonservices)	Hurtig information. Gerne anden kanal end internet, fx i forhold til borgere: talebesked på 1818 og andre telefonservices

Ved på forhånd at udforme (og få godkendt) et antal standardformuleringer og planlægge et presseberedskab vil man hurtigt kunne informere om beredskabssituationen eksternt. I det omfang der er behov for særlig information i situationen, kan den udsendes efterfølgende.

Trin 5 – Opfølgning

Der skal etableres løbende opfølgning på kommunikationsindsatsen. Ved større ændringer i løsningen, i brugermønstre osv., bør en ny konsekvensvurdering (afsnit 2) give anledning til opfølgning på kommunikationsindsatsen.

Det er vigtigt, at man fastlægger en proces for at opdatere beskrivelserne af kommunikationsveje jævnligt, da det er naturligt, at de ændrer sig – fx ved udskiftning af nøglepersoner.

6. Styring af leverandører

Både i forbindelse med håndtering af væsentlige hændelser og egentlige katastrofer har et tæt og godt samarbejde med leverandøren afgørende betydning. Dette samarbejde foregår på flere planer; det daglige driftssamarbejde, det formelle, det kommercielle og kontraktuelle samarbejde. Samarbejdet på alle niveauer har indflydelse på samarbejdet i en beredskabssituation.

I dette afsnit behandles det nærmere, hvordan man kan forbedre sin it-beredskabsstyring i forhold til leverandørstyring.

Trin 1 – Identificer kritiske leverandører

De kritiske leverandører vil typisk blive identificeret gennem arbejdet i de forrige afsnit. Hvis ikke dette er tilfældet, vil interviews med driftschefer, systemansvarlige og tilsvarende kunne identificere de kritiske leverandører.

Trin 2 – Undersøg og analyser modenhed for leverandør

Ved fremsendelse af spørgeskema eller gennem interviews undersøges leverandørens modenhed på de otte områder, der er beskrevet i denne guide. Man kan således med fordel benytte sig af evalueringsværktøjet.

Med udgangspunkt i de indhentede data vurderes det, om leverandørens beredskabsstyring stemmer overens med myndighedens krav, eller om der er uoverensstemmelser, der giver anledning til at udarbejde en handlingsplan for at mindske de relaterede risici.

Trin 3 – Inkluder krav i nye kontrakter

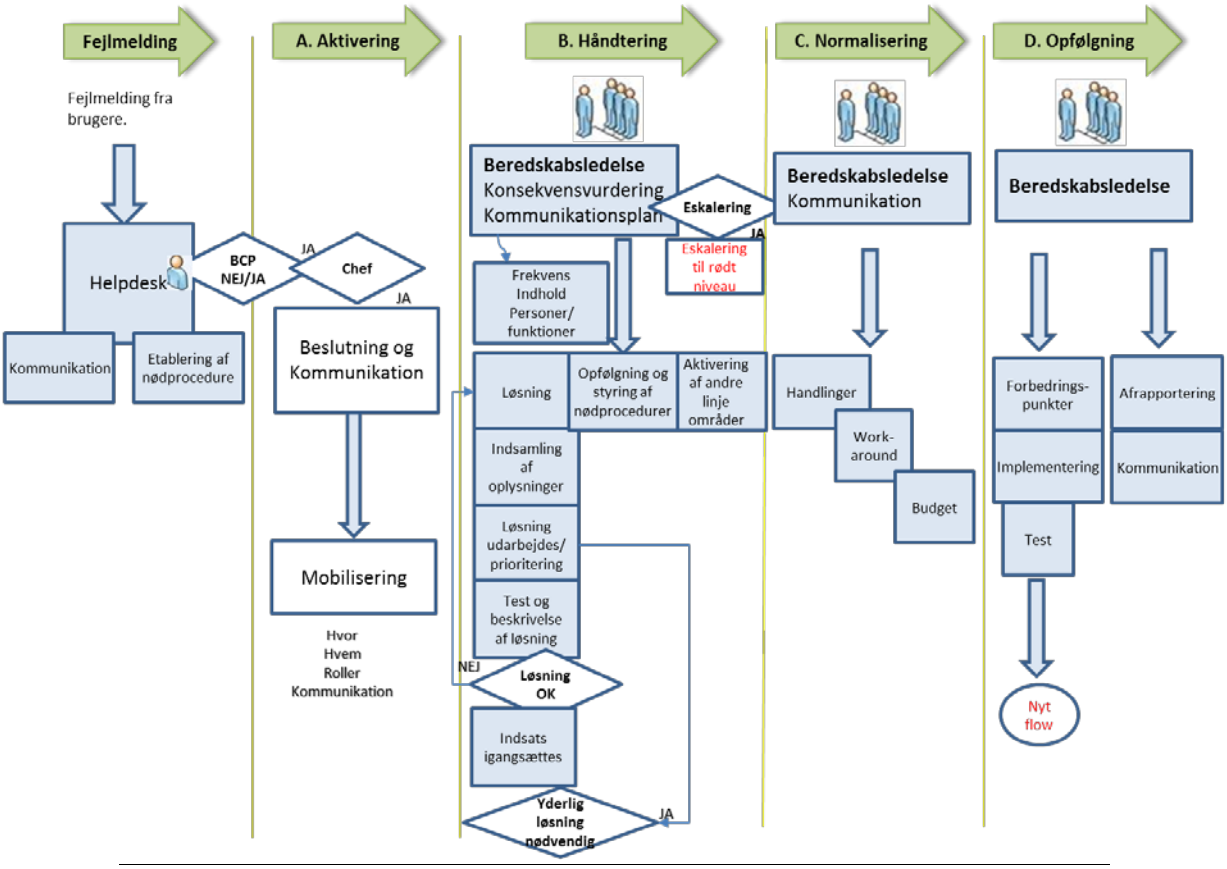
Det skal sikres, at der er fokus på, at myndighedens krav til beredskabsstyring indgår i fremtidige kontrakter med driftsleverandører.

7. Beredskabsproces

Hele beredskabsprocessen er en væsentlig del af beredskabsstyringen. Processen omfatter aktivering, håndtering, normalisering og opfølgning:

- **Aktivering** – Når der er kommet en fejlmelding, underrettes den ansvarlige leder, den planlagte mobilisering foretages, og kommunikationen påbegyndes i det omfang, det er nødvendigt.
- **Håndtering** – Efter aktivering håndteres den pågældende fejlmelding med henblik på at finde brugbare løsninger. Nødprocedurer iværksættes om nødvendigt.
- **Normalisering** – Efter håndtering og etablering af løsninger foretages en normalisering fra beredskab til normal drift. Skyldes hændelsen fejl i systemet, kan det fx være, at man skal beslutte, om man vil rette fejlen eller gøre et midlertidigt workaround permanent. Der vil hertil ofte være økonomiske overvejelser.
- **Opfølgning** – Efter normalisering skal der ske en opfølgning, der sikrer, at eventuelle forbedringspunkter i beredskabet identificeres, og at der foretages en rapportering til interessenter omkring hændelsen. Der er typisk en tendens til at fokusere mest på de to første faser og mindst på to de sidste, hvilket medfører, at gode erfaringer til forbedringer går tabt.

Figuren herunder viser en generisk beredskabsproces.



Trin 1 – Etabler en forståelse af den nuværende beredskabsproces

Undersøg eksisterende processer for beredskab ved at gennemgå dokumentation eller ved at foretage interviews, og afdæk, hvad der sker trin for trin under fejlmelding, aktivering, håndtering, normalisering og opfølgning. Sammenlign organisationens skabelon for it-beredskab[3] og se, om der er behov for at tilpasse de eksisterende processer.

Trin 2 – Rapportering af mangler til ledelsen

Dokumenter erfaringer, og informer ledelsen om dem. Er der behov for forbedringer, skal ledelsen tage stilling til, om den vil afsætte ressourcer til forbedringerne eller acceptere de dokumenterede risici.

Trin 3 – Påbegynd udfyldelse og opdatering af beredskabsskabelon

Opdater og gennemgå beredskabsplanen, hvis ledelsen har besluttet, at der er behov for forbedringer.

Trin 4 – Opfølgning

Opfølgning bør ske på baggrund af nye erfaringer (herunder fra de faste test af beredskabet), ved større ændringer i løsningen eller ved ændringer i brugsmønstre osv. En ny konsekvensvurdering (afsnit 2) vil ligeledes give anledning til opfølgning på beredskabsprocessen.

[3]Hvis denne mangler, har Digitaliseringsstyrelsen publiceret et eksempel her: http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Vejledninger-om-sikkerhedsarbejdet/Beredskabsplanlægning.

8. Forankring, vedligeholdelse og test af beredskabet

Forankring af beredskabsstyringen i hverdagen omfatter test, afprøvning og vedligeholdelse af beredskabsplanen, herunder også uddannelse og træning – både internt og af vigtige samarbejdspartnere (såsom leverandører).

Den bedste metode til forankring er, at der løbende er fokus på beredskabet. Dette kan opnås med enkle initiativer såsom:

- Løbende test af beredskabsplanen. Baseret på erfaringer fra tidligere test kan det være, at det kun er dele af beredskabsplanen, der skal være i fokus i en given test.
- Udvidelse af testomfanget til også at omfatte små hverdagstests, såsom opkald til medarbejdere med en central rolle i it-beredskabet, hvor man kort oplyser, at der er indtruffet en kritisk hændelse, og hvor medarbejderen så kort skal redegøre for, hvilke handlinger der skal iværksættes.
- Sikring af at der foregår rapportering ved test af beredskabsplaner.
- Kommunikation af resultater fra it-beredskabstests til alle interessenter i beredskabsplanlægningen og særligt til ledelsen.

Et eksempel på en enkel test, der ikke kræver omfattende ressourcer, er en skrivebordstest. Denne type test kan også benyttes til uddannelse. Denne test afdækker, hvor godt de eksisterende processer dækker en beredskabssituation, og hvorvidt processerne er praktisk anvendelige, samt hvor godt de involverede (både interne og eksterne) personer er uddannet i beredskabet.

Test af kommunikationsplanen er også enkel og sikrer, at de ansvarlige ved, hvem de skal kontakte og med hvilken type information.

Trin 1: Ønsket niveau for forankring, vedligehold og test af beredskabsplan

Hyppigheden af de faste periodiske test er en ledelsesbeslutning. Det bør dog minimum være hvert halve år ved kritiske it-systemer, samt ved ændringer i organisationen og udskiftning af nøglepersoner i beredskabsplanen.

Relevant input til denne beslutning vil også være et spørgsmål om, hvor godt de involverede personer forventes at kende beredskabsplanen. Et oplagt input er dokumenterede erfaringer fra seneste test af beredskabsplanen.

Trin 2: Etabler en forståelse af det nuværende niveau af forankring, vedligehold og test af beredskabsplan

Undersøg eksisterende politikker og procedurer for forankring, vedligehold og test ved eksempelvis at gennemgå dokumentation og ved at spørge til de involverede personers viden om beredskabsplanen, herunder roller og ansvar. Hertil skal det afklares, om de nødvendige ressourcer og kompetencer er afsat til vedligeholdelse og test af beredskabsplanen, samt om ansvaret for dette er fastlagt og kendt.

Trin 3: Planlæg og integrer med de eksisterende beredskabsplaners forankring, vedligeholdelse og testaktiviteter

Hvis Trin 2 viser, at der er forskel mellem det ønskede niveau og det eksisterende niveau, bør der planlægges nye initiativer for rette op på dette, medmindre ledelsen vil godkende de relaterede risici.

Det er en god ide at sørge for, at resultaterne fra it-beredskabstest mv. kommunikeres til alle interessenter i beredskabsplanlægningen, herunder i særlig grad ledelsen for at sikre den ledelsesmæssige forankring.

Den øverste ansvarlige for beredskabsstyringen skal godkende planer for forankring, vedligeholdelse og test. Det er en god ide at bruge et skema til at holde styr på sin testplanlægning. Herunder vises et eksempel på et testskema.

Planlægning af test

Testskema	Frekvens	Varighed	Beredskabskoordinator	Beredskabsledelse	Driftschef	Reetableringsteam	Kommunikationsansvarlig	Alle medarbejdere	Nyansatte
Forankring af beredskab									
Uddannelse vedrørende beredskabsplan	Årligt	1 time		X	X	X	X		
Uddannelse fra eksterne vedrørende it-beredskab	Årligt	½ dag	X						X
Beredskabsplan									
Gennemgang af it-beredskabsplan	Årligt	2 timer	X	X	X	X			
Test									
Denial of Service angreb	Årligt	2 timer	X	X					
Cyberangreb	Årligt	2 timer	X	X					
Test af kommunikationsplan	Årligt	2 timer	X		X	X	X		
Fuld test	Årligt	2 timer	X	X	X	X	X	X	

Trin 4 – Planlæg og udfør test

Undertrin 1:

Undersøg og fastlæg, hvilke områder der skal testes og hvor ofte. Udover de større test, hvor der fx simuleres et nedbrud i systemet, er det også en god ide at planlægge hyppige små tests, der er med til at sikre forankring af beredskabet blandt de involverede.

Eksempler på tests, der kan benyttes er:

- Skrivebordstest, hvor man forestiller sig, at der foregår en beredskabssituation. En test der ikke har de store omkostninger, men sikrer afprøvning af beredskabet.

- Ansvarstest, hvor man kontakter en eller flere af de ansvarlige i beredskabsplanen for at sikre, at de er bekendte med deres ansvar, og er vidende om, hvad de skal gøre i en beredskabssituation.
- Simulering af delelementer af beredskabsplanen for at teste reaktionstider og handlinger.

Undertrin 2:

Klare mål for testen fastsættes, og et passende testscenarie vælges for at opfylde disse mål.

Målene bør især defineres i forhold til de mangler, der er fundet ved tidligere test eller ved tidligere sikkerhedshændelser. Er det muligt at mobilisere beredskabet inden for en acceptabel tidsramme? Er det muligt, at beslutninger kan blive truffet tids nok til at løse beredskabssituationen?

Undertrin 3:

Beredskabskoordinatoren faciliterer testen, bl.a. ved hjælp af en oversigt over de aftalte tidstolerancer. Efter testen afholdes en kort evalueringssession for at opfange læringspunkter fra de forskellige deltagere i testen.

Undertrin 4:

Der udarbejdes en post-testrapport til at dokumentere de erfaringer og muligheder for forbedringer, som testen har vist. Der udarbejdes herefter en handlingsplan for forbedringsområderne, der bør godkendes af ledelsen.

Trin 5: Opfølgning

Forankring, vedligeholdelse og test af beredskabsplanen skal undersøges og sikres løbende. Periodisk skal der foregå en vurdering af det eksisterende niveau (undertrin 1-4 herover). Eventuelle ændringer i organisation, standarder (afsnit 3) og større ændringer i løsningen medfører ligeledes et behov for opfølgning på området.