

IT Beredskabsplan - Analysefasen

Frem for at udarbejde beredskabsplaner for alle virksomhedens systemer, med det tidsforbrug og de omkostninger det måtte indebære, identificeres de 3-6 forretningskritiske systemer, som giver virksomheden sit overskud, sin likviditet, sin kundeloyalitet mv. – opgjort i omkostninger i relation til en tidsakse (f.eks. 4 timer, 1 dag, 3 dage, 1 uge mv.), hvor der ikke er adgang til de pågældende systemer.

De udvalgte systemer analyseres med henblik på en vurdering af, om indsatsen skal gøres forebyggende, eller om den skal lægges i beredskabet. Analysefasen afdækker for hvilke forretningskritiske systemer et beredskab er helt nødvendigt for virksomhedens fortsatte drift og overlevelse ud af en katastrofesituation.

Tidsforløb	Aktivitet
Møde 01. AFDÆKNING	<p>Initiering af : Afdækning af eksisterende planer og dokumentation</p> <p>Formålet er fremfinde og evaluere eksisterende planer og dokumentation for håndtering af IT-systemerne under en kortere eller længerevarende problemløstperiode.</p> <p>Identificere IT systemer, deres fysiske placering, driftsenheders ansvar og kompetencer. Aftale og kontraktforhold i forbindelse med evt. housing eller outsourcing.</p>
Møde 02. ANALYSER	<p>Initiering af : Afdækning af beredskabsbehov</p> <p>Formålet er at identificere virksomhedens forretningsmæssige nøglesystemer. Virksomhedens position i markedet og holdning til IT sikkerhed. Hvordan vurderer forretningsenhederne sårbarheden? Fastlægge tidsskema for acceptable nedetider – og hvor smertegrænsen ligger. Sætte konsekvenskroner på tiderne.</p> <p>Analysemodeller udleveres.</p>
Møde 03. ANALYSER	<p>Opfølgning på Møde 02</p> <p>Fastlæggelse af TOP-x systemer for hvilke der skal udarbejdes beredskabsplaner.</p> <p>Initiering af : Risikovurdering (Afdække mulige sårbarheder og trusler, sandsynlighed for forekomst, frekvens), hvordan gennemføres analysen. Analysemodel leveres.</p> <p>Initiering af : Forudsætninger for beredskabet, samt behovet for forebyggende tiltag (økonomisk/teknisk)</p>

IT Beredskabsplan – Beredskabsplanlægning

En beredskabsplan bygger i høj grad på de forretningsgange og procedurer, som virksomheden i forvejen har (eller bør have !) for installation, vedligeholdelse, betjening mv.

Policy Enforcer styrer processen, strukturen og sikrer at planen omfatter alle nødvendige elementer for at virke. Detailplanlægningen påhviler primært virksomhedens egne medarbejdere.

Beredskabsplanlægningsfasen resulterer i en overordnet plan med alarmeringsvilkår, beslutningsforløb, etablering af beredskabsgrupper med ansvar og opgaver, varslingslister, leverandøraftaler – og meget mere – primært med henblik på at genetablere IT-driften af de forretningskritiske systemer inden for de fastsatte tidskrav. Øvrige afdelingers beredskabsplaner for perioden uden IT adgang ligger uden for dette arbejdes primære sigte, men kan tilvælges.

Tidsforløb	Aktivitet
Møde 04. PLANLÆGN.	Opfølgning på Møde 03. Initiering af : Beredskabsplanens opbygning, indhold og underliggende dokumentation. Initiering af : Beredskabsorganisationen. Hvem indgår i IT-beredskabet, internt/eksternt ? Initiering af : Varsling, varslingsstrin, definitioner, eskaleringsforløb, beredskabsorganisation varslingslister mv. Modeller/eksempler udleveres.
	Første udkast til beredskabsplan udarbejdes
Møde 05. HANDL.PLANER	Opfølgning på Møde 04. Initiering af : Handlingsplaner for beredskabsgrupper, og for TOP-x systemer mv. Sikring af at den nødvendige driftsdokumentation er relevant og ajour.
Møde 06. HANDL.PLANER	Opfølgning på Møde 05. Initiering af : Det tekniske beredskab for TOP-x systemerne, dokumentation og aftaler.
	Det tekniske beredskab evalueres og lægges ind i beredskabsplanen.
Møde 07. HANDL.PLANER	Opfølgning på Møde 06. Initiering af : Det organisatoriske beredskab, dokumentation og aftaler.
	Beredskabsdokumentationen samles og redigeres inden præsentation på møde 08.
Møde 08. EVALUERING	Hele Beredskabsdokumentet evalueres med henblik på justeringer, tilføjelser, ændringer og færdiggørelse. Uddannelse af beredskabsorganisationen planlægges.

IT Beredskabsplan – Uddannelse & test

Uden implementering - uddannelse af medarbejdere og afprøvning af planen – er der ingen plan !

Uddannelse:

Uddannelse kan være informationsmøder for nogle, egentlige kurser for andre, information på virksomhedens Intranet sider, papir på opslagstavlen for andre grupper.

Tidsforløb	Aktivitet
	Kursusmaterialer udarbejdes
Møde 09	Introduktion til Beredskab generelt - og til kundens beredskab og plan specifikt.

Test af beredskabsplanen :

Beredskabsplanen skal afprøves jævnligt, dels for at holde organisationen "fit for fight", men også for at sikre at den rent faktisk virker og lever op til sine krav.

Da det er særdeles kostbart og ofte praktisk umuligt at gennemføre en "full scale" afprøvning, afprøver man i stedet dele af planen – noget som skrivebordsøvelser og andre som "real life".

Tidsforløb	Aktivitet
Møde 10. TEST OPLÆG	Fastlæggelse af beredskabsafprøvning: En række forskellige testmuligheder forelægges, diskuteres, udvælges og prioriteres. Der planlægges 2 test: Opkaldstest og samlet skrivebordstest. Øvelsesscenarier udarbejdes.
"Møde 11." TEST 01	Opkaldsøvelsen gennemføres efter aftale og rapport udarbejdes. Kort møde hvor resultatet evalueres. Beredskabsplanen justeres eventuelt.
Møde 12. TEST 02	Den store skrivebordsøvelse afvikles med målet at lære at arbejde efter planen, at kende dokumenterne, at holde tider – og meget mere. Fælles evaluering af øvelsen. Forslag til ændringer og justeringer i beredskabsplanen.