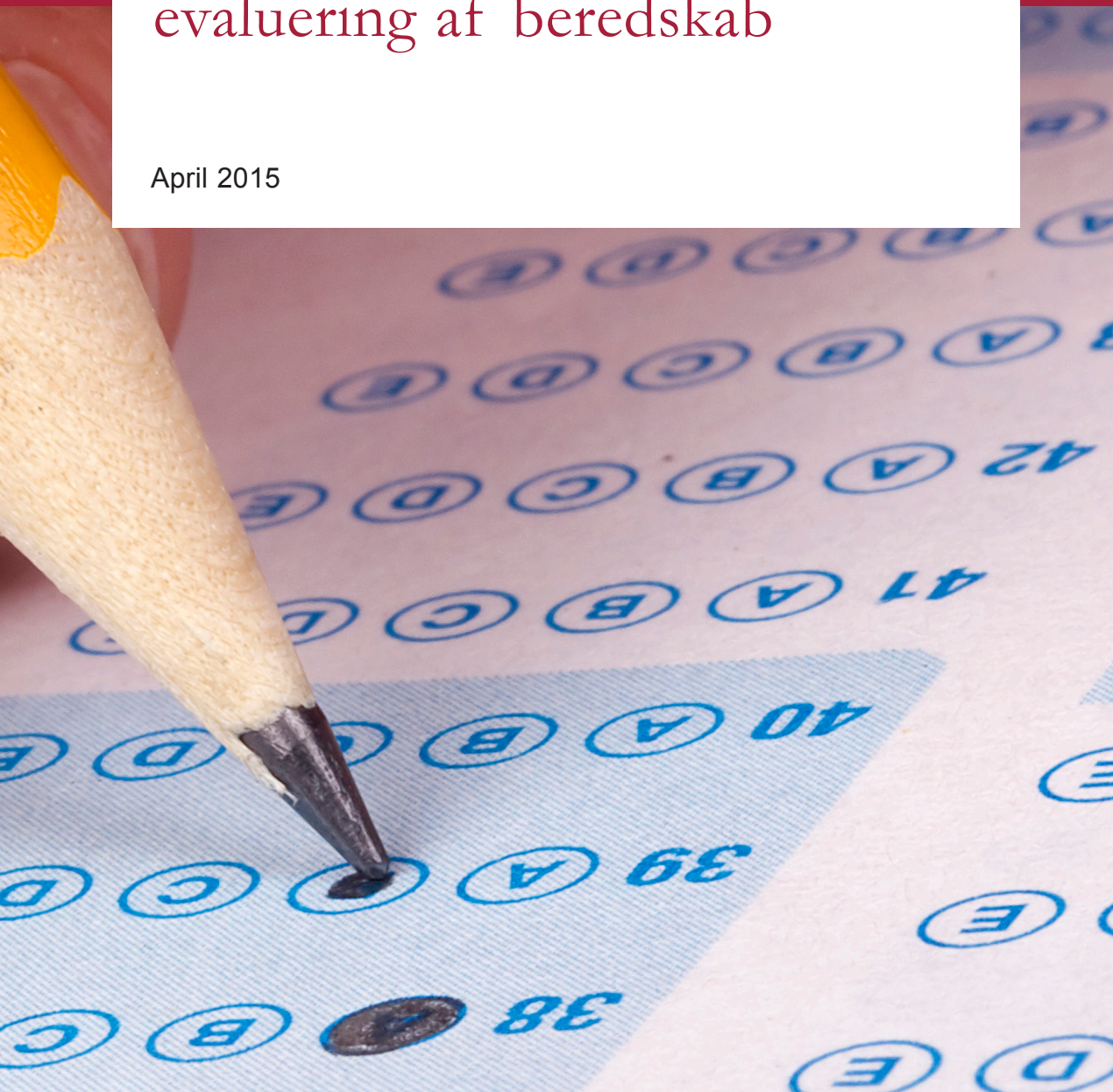
DIGITALISERINGSSTYRELSEN

Vejledning om evaluering af beredskab

April 2015



Vejledning om evaluering af beredskab

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 978-87-93073-13-5

Indhold

Indledning

Evalueringsværktøjet er udviklet for at hjælpe personer, der er ansvarlige for et it-beredskab, til at vurdere og forbedre det. Ved at bruge værktøjet får man en oversigt over de områder, der har behov for forbedringer, for at nå det ønskede niveau (se bilaget til denne vejledning for et billede af oversigten).

Værktøjet ser på beredskabet på otte områder og finder forskellen mellem dét niveau myndigheden ønsker beredskabsplanen skal have på et område – *det ønskede modenhedsniveau* – og en beregning af det aktuelle niveau – *det beregnede modenhedsniveau*.

Modenhedsniveau er en betegnelse, der både indbefatter, om beredskabet tager højde for alle otte områder, og hvor godt området er forankret i organisationen.

Værktøjet er hovedsagligt et dialogværktøj, hvor resultaterne kan bruges til en drøftelse med ledelsen om behovet for fremtidige tiltag for at kunne leve op til organisationens egne (og vigtige interessenters) forventninger til håndteringen af en beredskabssituation. På baggrund af disse drøftelser kan trin-for-trin-guiderne i "Guide til bedre beredskabsstyring" anvendes til at forbedre beredskabet. Guiden findes på Digitaliseringsstyrelsens hjemmeside.

Værktøjet er baseret på den internationale standard ISO27001 med input fra en analyse af it-beredskab og anvendelse af nødprocedurer for kritiske offentlige it-systemer, der blev gennemført i slutningen af 2014.

En vigtig erfaring fra analysen viste, at selve dialogen om modenhed kan give anledning til nye observationer og opmærksomhedspunkter. Det anbefales derfor at planlægge workshops eller interviews med relevante interne og eksterne interessenter. Workshops eller interviews kan både være relevant i forbindelse med fastlæggelsen af det ønskede modenhedsniveau og det beregnede modenhedsniveau, til drøftelsen af forskellen mellem de to niveauer, samt i forbindelse med forbedringen af udvalgte områder.

Opbygning

Selve værktøjet er et Excel-ark, inddelt i en række faneblade.

Fanebladet ***Introduktion*** indeholder en kort beskrivelse af evalueringsværktøjet. Fanebladet ***Inputark*** benyttes til at indtaste det ønskede modenhedsniveau. Fanebladet ***Oversigt*** giver et samlet overblik over forskellen mellem det ønskede og det beregnede modenhedsniveau. Fanebladet ***Definitioner*** indeholder beskrivelse af modenhedsniveauerne. Fanebladet ***Bemærkninger*** indeholder et konsolideret overblik over de bemærkninger, der er noteret i forbindelse med brugen af værktøjet, og som brugeren har beskrevet i arket.

Endvidere er der otte faneblade for hvert af de nedenstående områder inden for beredskabsplanlægning (i bilaget til denne vejledning kan du se et billede af fanebladet for område 3. Organisering, roller og ansvar).

Værktøjet er baseret på ISO27001's definition af beredskab og måler modenhed på følgende otte områder (i værktøjets ark "Inputark" gives en beskrivelse af områderne, der kan ses på næste side i denne vejledning):

1. Samfundsmæssig konsekvens
2. Compliance
3. Organisering, roller og ansvar
4. Vurdering, varsling og mobilisering
5. Kommunikation
6. Styring af leverandører
7. Beredskabsproces
8. Forankring, vedligehold og test af beredskabsplan.

Værktøjet udfyldes ved, at man vurderer modenheden af beredskabet ud fra en række spørgsmål i hvert af de faneblade i værktøjet, der repræsenterer de otte områder. Ud for hvert spørgsmål vurderes modenheden på skala med fem niveauer (modenhedsniveauerne fra evalueringsværktøjet kan ses i bilaget til denne vejledning):

0. = Ikke-eksisterende
1. = Initiel/Ad hoc
2. = Intuitivt
3. = Defineret proces
4. = Styret og målbart

Endvidere kan niveauerne **X** og **N/A bruges**, hvor **X** – "Det har umiddelbart ikke været muligt at finde informationer vedrørende dette", og **N/A** – "Dette område gør sig ikke gældende for beredskabsplanen for systemet".

Det ønskede modenhedsniveau

En organisation med høj modenhed fastlægger det ønskede modenhedsniveau på baggrund af en såkaldt Business Impact Analyse (BIA). Udarbejdelsen af en BIA kan dog være et omfattende analysearbejde. Herunder foreslås derfor en mere simpel metode til at få et bud på det ønskede modenhedsniveau.

Der indsamles oplysninger fra relevante interessenter (eksempelvis system-/serviceansvarlig, driftschef, kontraktansvarlig og eventuelt andre nøglepersoner) om det ønskede modenhedsniveau for hvert af de otte delområder. Interessenterne giver hver deres vurdering af det nødvendige modenhedsniveau ved at udfylde evalueringsværktøjets faneblad **Inputark**. Man kan enten gøre dette sammen med interessenterne eller fremsende et regneark med de to faneblade **Inputark** og **Definitioner**.

Vurderingerne indsamles efterfølgende af den, der er ansvarlig for udarbejdelsen af beredskabet. Man skal beslutte, om interessenterne ønsker at drøfte eventuelle forskelle i deres vurderinger, eller om interessenternes vurderinger skal konsolideres til et gennemsnit for at opnå en samlet vurdering af det ønskede modenhedsniveau, inden vurderingen indtastes i inputarket.

Inputark – det ønskede modenhedsniveau

Område	Beskrivelse	Ønsket modenheds-niveau
1. Samfundsmæssig konsekvens	Området drejer sig om vurderingen af den samlede "samfundsmæssige konsekvens" ved sikkerhedshændelser afspejles i servicemålene for systemet. Den samfundsmæssige konsekvensvurdering indebærer at systemejeren også vurderer i hvilket omfang hændelser, der påvirker eget it-system, vil have afledte konsekvenser på andre områder, fx i andre organisationer eller hos andre myndigheder.	
2. Compliance	Compliance handler om, at organisationen og medarbejderne overholder interne politikker, standarder og eventuelle lovmæssige krav.	
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.	
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?	
5. Kommunikation	Kommunikationsområdet handler om at sikre de rette interne og eksterne kommunikationsveje, herunder kommunikation til kritiske leverandører.	
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.	
7. Beredskabsproces	Hele beredskabsprocessen er en væsentlig del af beredskabsstyringen. Planlægning af processen sikrer at alle vigtige aktiviteter gennemgås i de fire trin i processen; aktivering, håndtering, normalisering og opfølgning.	
8. Forankring, vedligehold og test af beredskabsplan	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).	

Relevant baggrundsviden

Man bør have baggrundsviden om (A) den forretningsmæssig konsekvensvurdering for systemet og (B) erfaringer fra tidligere sikkerhedshændelser og test, til vurderingen af det ønskede modenhedsniveau. Det kan dog overvejes, om der er nogle informationer i denne baggrundsviden, der af sikkerhedsmæssige grunde ikke kan stilles til rådighed for alle eksterne interessenter.

(A) Den forretningsmæssige konsekvensvurdering foretages som en del af organisationens periodiske it-risikostyring og -vurdering, og kan give følgende input til vurdering af det ønskede modenhedsniveau:

1. Hvilke opgaver, som systemet understøtter, er de vigtigste, og hvad ville der ske, hvis de ikke blev løst?
2. Hvilken konsekvens vil det have, eksempelvis i forhold til økonomi og renommé – både for os selv, men også for andre der eventuelt er afhængige af systemet?
3. Er der særlige typer af sikkerhedshændelser, der er meget kritiske? Hvad er eksempelvis grænsen for, hvor lang tid systemet skal være utilgængeligt, før det er kritisk, og er

der tidspunkter (på dagen/måneden/året), hvor det vil være særligt kritisk med utilgængelighed?

(B) Erfaringer fra tidligere driftshændelser og test af beredskabet giver viden, om der eksempelvis opstod uforudsete problemer, eller nogen manglede bestemt information. Desuden giver tilsynsrapporter ofte en rigtig god indsigt i, hvilke områder der bør være fokus på.

Det beregnede modenhedsniveau

I evalueringsværktøjet har hvert af de otte områder et faneblad med en række kontrolspørgsmål. For hvert spørgsmål vurderes organisationens modenhedsniveau ud fra de definitioner, der fremgår af fanen **Definitioner** (kan også ses i bilaget til denne vejledning).

Eksempel:

Herunder er kontrolspørgsmål 3,5 (spørgsmål 5 i ark 3) fremhævet

Kontrol #	Kontrolbeskrivelse	Niveau	Bemærkninger
3,1	I hvor høj grad er beredskabsstyring forankret hos den øverste ledelse i organisationen?		
3,2	I hvilket omfang er det overordnede ansvar for beredskabsorganiseringen forankret?		
3,3	Beredskabsorganisation, roller og ansvar og forankring af disse. Stedfortrædere, forankring af tværgående snitflader, dokumentation etc. Vurdering af modenhed vedr. processerne omkring definering og forankring af organisering, roller og ansvar .		
3,4	I hvilket omfang har ledelsen allokeret fornødne ressourcer og kompetencer til beredskabsplaner og planlægning?		
3,5	I hvilket omfang er roller og ansvar i beredskabsorganisationen identificeret og forankret hos de ansvarlige og deres stedfortrædere?		
3,6			
3,7			
3,8	I hvor høj grad bliver organisationens tilgang til styring af it-beredskabsplan og dens gennemførelse (dvs. kontrol, politikker, processer og procedurer for it-beredskab) revideret i planlagte intervaller, eller når væsentlige ændringer i systemet, beredskabet og organisationen gennemføres?		
3.9	I hvilket omfang bliver aftaler med tredjeparter, der involverer behandling, kommunikation eller vedligehold af beredskabsplanen, gennemgået?		

Vurderingen:
I organisationen, der udfylder skemaet, er relevante personer helt klar over, hvem der skal gøre hvad i en beredskabssituation, og hvem der kan træde til, hvis én af personerne er væk. Rutinerne er dog noget, man er blevet enige om i e-mails og på møder efter længere tids samarbejde med leverandøren.

Derfor er der valgt modenhedsniveauet 2 ”**Intuitivt**”.
(Det skal bemærkes, at det ikke er unormalt at have et modenhedsniveau på 1-2.)

Afslutning

Når evalueringsværktøjet er udfyldt, kan forskelles mellem det ønskede modenhedsniveau og det beregnede modenhedsniveau ses i fanen **Oversigt.**

Til hvert spørgsmål er knyttet et tekstfelt, ”Bemærkninger”. Her kan det eksempelvis noteres, hvordan modenhedsniveauet skal hæves eller årsagen til, at det skal forblive, som det er. Alle indtastede bemærkninger samles i fanen **Bemærkninger**. Ligeledes bliver kontrolspørgsmål, der bliver besvaret med X, samlet i **Bemærkninger.**

Indholdet i de to faner **Oversigt** og **Bemærkninger** er herefter nemme at kopiere fra arket og bruge til afrapportering.

Bilag

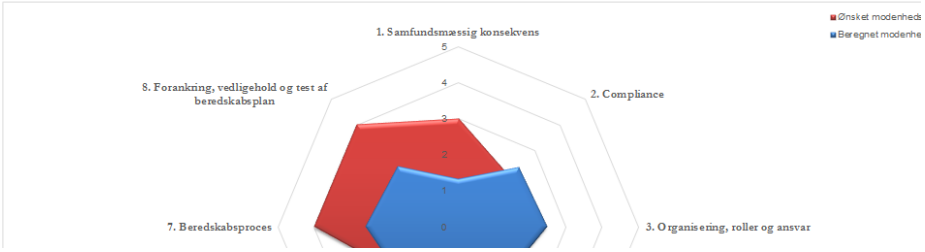
Modenhedsniveau

Definitioner på valgmuligheder ved kategorisering af modenhedsniveau		
N/A	**Not applicable**	Emnet er ikke anvendeligt i forhold til det pågældende system.
X	**Ved ikke**	Der er ikke viden om, hvorvidt dette er indført, og i hvor høj grad dette er indført
0	**Ikke-eksisterende**	Organisationen har ikke erkendt, at der er et behov, der skal løses. Der eksisterer ikke genkendelige aktiviteter eller processer.
1	**Initiel/Ad hoc**	Der er beviser for, at organisationen løser opgaver inden for området. Der er dog ingen standardiserede processer. Opgaver på området løses ad hoc, og tilgangen er ofte afhængig af den udførende person eller den pågældende sag.
2	**Intuitivt**	I organisationen følger de udførende personer normalt de samme processer for opgaveløsningen på området. Der findes dog ingen formel uddannelse eller kommunikation af processerne, og ansvar er overladt til den enkelte. Der er en høj grad af tillid til viden hos enkeltpersoner og derfor sandsynlige fejl.
3	**Defineret proces**	Processerne er standardiseret og dokumenteret og kommunikeres gennem uddannelse. Personer, der udfører opgaver på området, er pålagt at følge processerne. Det er dog usandsynligt, at det opdages eller vægtes højt, hvis processerne ikke følges. Processerne er udarbejdet ved at nedskrive eksisterende praksis.
4	**Styret og målbart**	Ledelsen overvåger og måler på, om processerne overholdes, og om de er effektive. Processerne forbedres løbende baseret på disse resultater. Automatisering og værktøjer anvendes i et begrænset og/eller fragmenteret omfang.

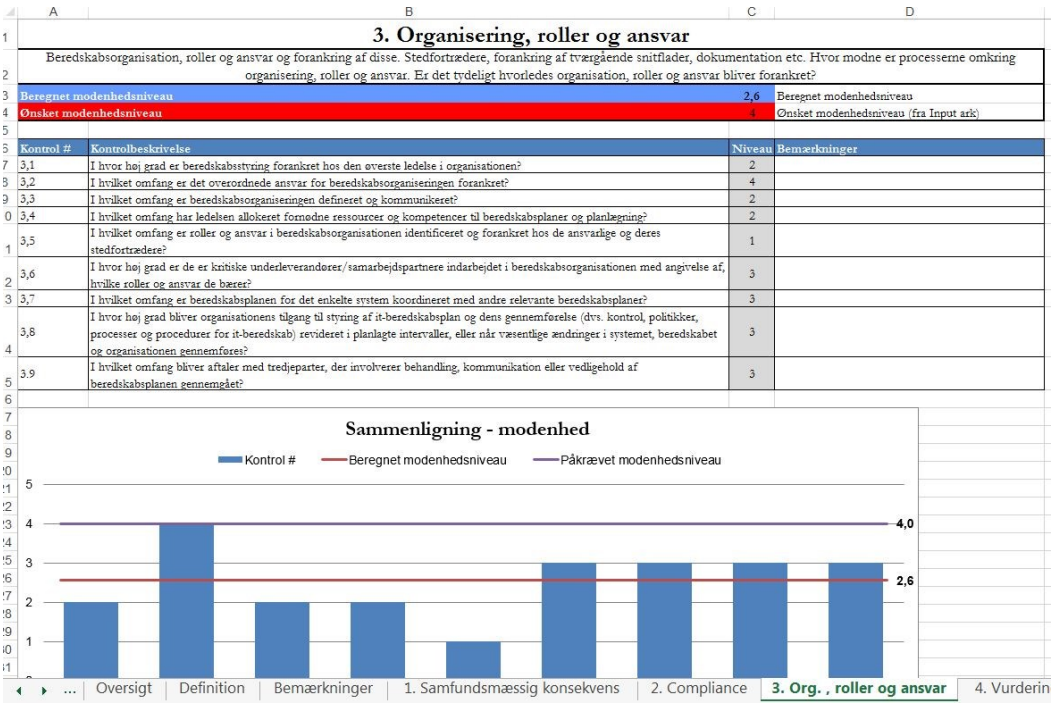
Oversigtsbillede

Område	Beskrivelse	Beregnet modenhedsniveau	Ønsket modenhedsniveau
1. Samfundsmæssig konsekvens	Gennemførelse af forretningsmæssig konsekvensvurdering og fastlæggelse af krav og servicemål.	1,3	3
2. Compliance	Interne politikker, standarder og compliance-krav og eventuelle lovmæssige krav.	2,3	2
3. Organisering, roller og ansvar	Beredskabsorganisation, roller og ansvar og forankring af disse. Stedfortrædere, forankring af tværgående snitflader, dokumentation etc.	2,4	2
4. Vurdering, varsling og mobilisering	Definition af driftshændelser, vurdering og varsling af disse. Eskaleringsprocesser og varslingsmodeller og dokumentation heraf.	1,9	2
5. Kommunikation	Interne samt eksterne kommunikationsveje, kommunikation til kritiske leverandører, awareness-aktiviteter.	3,0	4
6. Styring af leverandører	Styring, vurdering og identificering af eksterne og kritiske leverandører.	2,2	2
7. Beredskabsproces	Aktivering, håndtering, normalisering og opfølgning.	2,6	4
8. Forankring, vedligehold og test af beredskabsplan	Test, afprøvning og vedligeholdelse af beredskabsplanen. Herunder uddannelse og træning af væsentlige interessenter.	2,4	4

Samlede bemærkninger fra selvevalueringsværktøjet:	Oversigt over de noterede bemærkning til de forskellige områder kan findes her



Fanebladsbillede



	A	B	C	D
1		**3. Organisering, roller og ansvar**		
2		Beredskabsorganisation, roller og ansvar og forankring af disse. Stedfortrædere, forankring af tværgående snitflader, dokumentation etc. Hvor modne er processerne omkring organisering, roller og ansvar. Er det tydeligt hvorledes organisation, roller og ansvar bliver forankret?		
3		**Beregnet modenhedsniveau**	2,6	Beregnet modenhedsniveau
4		**Ønsket modenhedsniveau**	4	Ønsket modenhedsniveau (fra Input ark)
5				
6	**Kontrol #**	**Kontrolbeskrivelse**	**Niveau**	**Bemærkninger**
7	3,1	I hvor høj grad er beredskabsstyring forankret hos den øverste ledelse i organisationen?	2	
8	3,2	I hvilket omfang er det overordnede ansvar for beredskabsorganiseringen forankret?	4	
9	3,3	I hvilket omfang er beredskabsorganiseringen defineret og kommunikeret?	2	
10	3,4	I hvilket omfang har ledelsen allokeret fornødne ressourcer og kompetencer til beredskabsplaner og planlægning?	2	
11	3,5	I hvilket omfang er roller og ansvar i beredskabsorganisationen identificeret og forankret hos de ansvarlige og deres stedfortrædere?	1	
12	3,6	I hvor høj grad er de er kritiske underleverandører/samarbejdspartnere indarbejdet i beredskabsorganisationen med angivelse af, hvilke roller og ansvar de bærer?	3	
13	3,7	I hvilket omfang er beredskabsplanen for det enkelte system koordineret med andre relevante beredskabsplaner?	3	
14	3,8	I hvor høj grad bliver organisationens tilgang til styring af it-beredskabsplan og dens gennemførelse (dvs. kontrol, politikker, processer og procedurer for it-beredskab) revideret i planlagte intervaller, eller når væsentlige ændringer i systemet, beredskabet og organisationen gennemføres?	3	
15	3.9	I hvilket omfang bliver aftaler med tredjeparter, der involverer behandling, kommunikation eller vedligehold af beredskabsplanen gennemgået?	3	
16