



NIS2

D-Mærket



Præsentation af underviser

Majken Prip, Chefkonsulent

D-mærket

Baggrund

Dansk Standard

Københavns Kommunes Koncern it

Udviklings- og forenklingsstyrelsen

Kandidat i Politik og informatik fra RUC

Præsentation af jer

- Hvem er du, og hvor kommer du fra?
- Hvad inspirerer dig ift. Cyber- og informationssikkerhed?
- Hvad ønsker du at få med dig herfra i dag?

Hvad lærte I i sidste?

NIS2 vil øge robustheden i flere virksomheder for at øge samfundets modstanddygtighed inden for cyber- og informationssikkerhed

NIS2 stiller minimumskrav til risikostyring, ledelsens ansvar, rapporteringsforpligtelser og tilsynsbeføjelser og sanktioner

ISO/IEC 27001 er en international ledelsesstandard for informationssikkerhed, der har fokus på ledelsesmæssig forankring, og hvor en række af minimumskravene i NIS2 bliver konkretiseret



Hvad vil I lære i dag?

D-mærket som rammeværk

Kriteriesæt og mapping til NIS2

Hands on på selvevalueringen



MØD D-MÆRKET

D-mærket kort fortalt



Danmarks mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse – og det første i verden til at koble it-sikkerhed og ansvarlig dataanvendelse



Relevant for alle typer og størrelser af virksomheder og offentlige organisationer



Guider virksomheder til, hvad de skal leve op til inden for datasikkerhed, databeskyttelse og dataetik



Lanceret i 2021 af Industriens Fond i samarbejde med Dansk Industri, Dansk Erhverv, SMVdanmark og Forbrugerrådet Tænk



D-mærket er et af tre initiativer i Cybersikkerhedspagten

Hvilken gruppe tilhører virksomheden?

Antallet af kriterier og krav som virksomheden skal leve op til afhænger af virksomhedsgruppen, men alle virksomheder skal som minimum leve op til kriterie 1, 2, 3 og 5.

Kriterier for indplacering i gruppe	Gruppe I	Gruppe II	Gruppe III	Gruppe IV
Antal ansatte	0-9	10-49	50-249	250+
Nettoomsætning (mio. DKK)	0-7,9	8-155,9	156-313	≥ 313
Leverandør af software eller it-tjenester	Nej	Nej	Ja	Ja
Behandler særlige kategorier af personoplysninger (fx helbredsoplysninger, race, sexualitet)	Nej	Ja	Ja	Ja

D-mærkets 8 kriterier

1	KRITERIE 1 Styring og forankring i ledelsen	→
2	KRITERIE 2 Awareness og sikker adfærd	→
3	KRITERIE 3 Teknisk it-sikkerhed	→
4	KRITERIE 4 Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse	→
5	KRITERIE 5 Transparens & kontrol med data	→
6	KRITERIE 6 Privacy & security by design & default	→
7	KRITERIE 7 Pålidelige algoritmer & AI	→
8	KRITERIE 8 Dataetik	→



Styring og forankring

- 1.1 Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse
- 1.2 Overblik over data og systemer
- 1.3 Risikostyring
- 1.4 Politik for it-sikkerhed
- 1.5 It-beredskabsplan
- 1.6 Politikker for ansvarlig dataanvendelse
- 1.7 Udviklingsproces

Awareness og sikker adfærd

- 2.1 Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik
- 2.2 Awareness om og træning i it-sikkerhed
- 2.3 Awareness om og træning i ansvarlig dataanvendelse



Teknisk it-sikkerhed

- 3.1 Netværkssikkerhed og kryptering
- 3.2 Korrekt konfiguration
- 3.3 Beskyttelse af administrative brugerkonti
- 3.4 Beskyttelse mod malware
- 3.5 Kontinuerlig opdatering af software og styresystemer
- 3.6 Beskyttelse mod tab af vigtige og fortrolige data
- 3.7 Overvågning af systemaktivitet gennem logging

Krav til leverandørers it-sikkerhed

- 4.1 Leverandørlivscyklus og risikovurdering
- 4.2 Krav til it-sikkerhed hos leverandører
- 4.3 Krav til ansvarlig databehandling hos leverandører



Transparens & kontrol med data

- 5.1 Information i relation til personoplysninger
- 5.2 Cookies
- 5.3 Kontrol over egne personoplysninger
- 5.4 Lettilgængelig klagevejledning

Security & privacy by design og default

- 6.1 Vurdering
- 6.2 Privacy by design & default
- 6.3 Security by design & default
- 6.4 Implementering igennem udviklingsproces



Pålidelige algoritmer og AI

7.1 Menneskeligt tilsyn og mellemkomst/indgriben og transparens

7.2 Data- og modelkvalitet

7.3 Implementering igennem udviklingsproces

Dataetik

8.1 Dataetik



NIS2 OG D-MÆRKET



Hvis din virksomhed ikke lever op til
D-mærket, så lever I heller ikke op til NIS2

1. Medlemsstaterne sikrer, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med dens gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel.

Anvendelsen af dette stykke berører ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

2. Medlemsstaterne sikrer, at medlemmerne af væsentlige og vigtige enheders ledelsesorganer er forpligtet til at følge kurser, og skal tilskynde væsentlige og vigtige enheder til løbende at tilbyde tilsvarende kurser til deres ansatte, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.

Artikel 20 i [NIS2 direktivet](#)

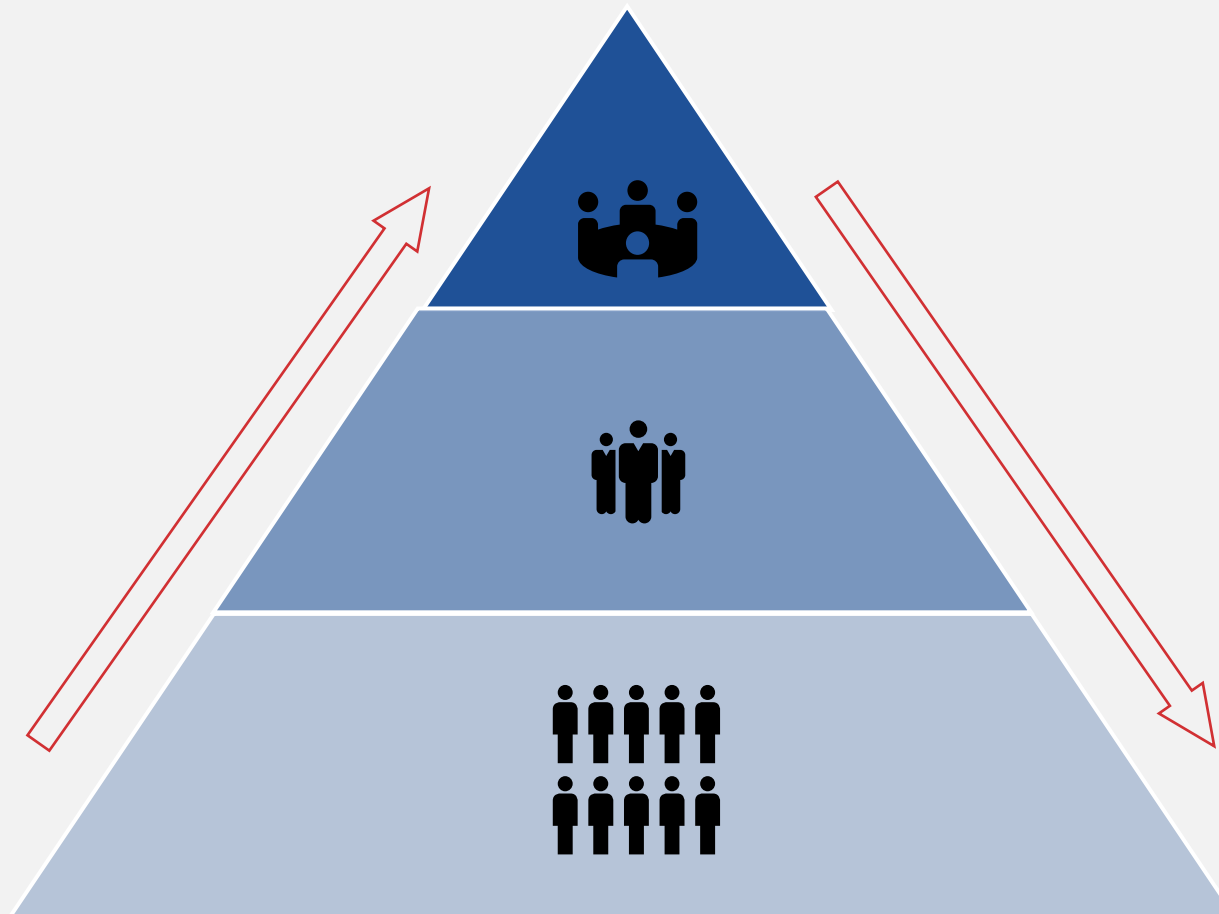


Styring og ledelse

Strategisk niveau:
Sætter mål og strategi for
informationssikkerhed

Taktisk niveau:
monitorere, vedligeholde og
opdatere processer

Operationelt niveau: Driften;
implementering af tekniske
kontroller, awareness,
dokumentation samt
håndtering af hændelser



1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

2. De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

Artikel 21 i [NIS2 direktivet](#)

Risikostyring

NIS2: a) Politikker for risikoanalyse og informationssikkerhed



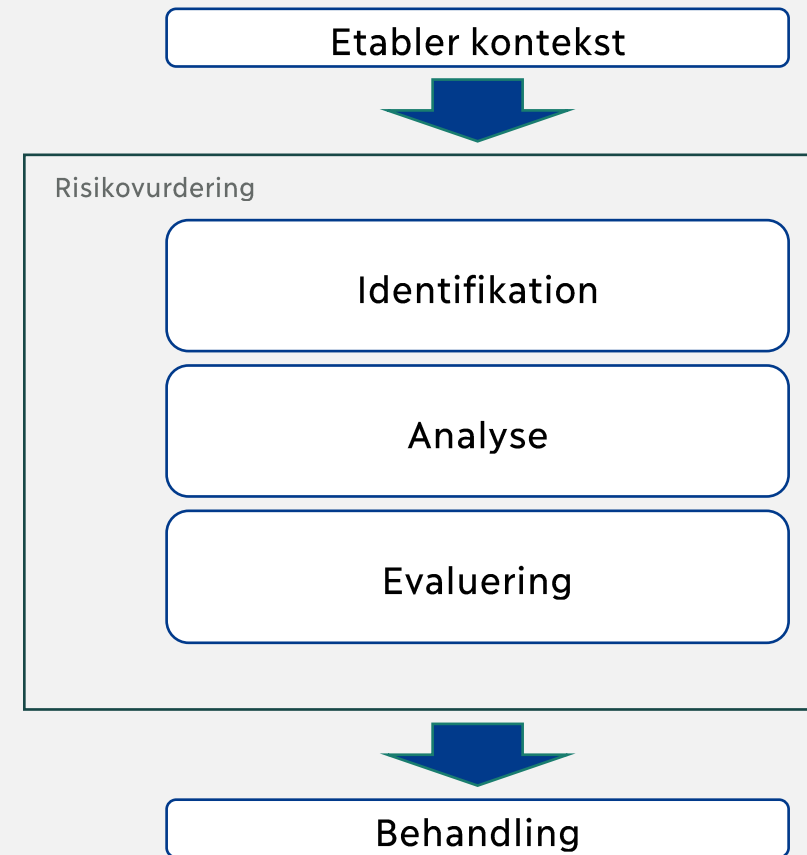
Politik for it-sikkerhed



Overblik over data og systemer



Risikostyring



Afklar målsætninger og metode. Få overblik over data og systemer

Identifikation

Find risikoscenarier på baggrund af overblik

Hacker
kompromitterer
underleverandør, så
forretningskritisk
data er
utilgængeligt



ingen
risikovurdering eller
krav til leverandør

Analyse

Beregn sandsynlighed og konsekvens for risikoscenarier

4. Meget sandsynligt
3. Sandsynligt
2. Ret usandsynligt
1. Meget usandsynligt

4. Meget stor konsekvens
3. Stor konsekvens
2. Lille konsekvens
1. Meget lille konsekvens

Evaluering

Sammenhold risici med acceptkriterier

	SANDSYNLIGHED FOR SCENARIO	Sandsynlighed				
		Meget usandsynligt	Usandsynligt	Muligt	Sandsynligt	Meget sandsynligt
KONSEKVENSS IFT. AKTIV	Meget lille	1	2	3	4	5
	Lille	2	4	6	8	10
	Middel	3	6	9	12	15
	Stor	4	8	12	16	20
	Meget stor	5	10	15	20	25

Risikohåndtering: Undgå, mindsk, acceptér, del



Pause

Hændelser

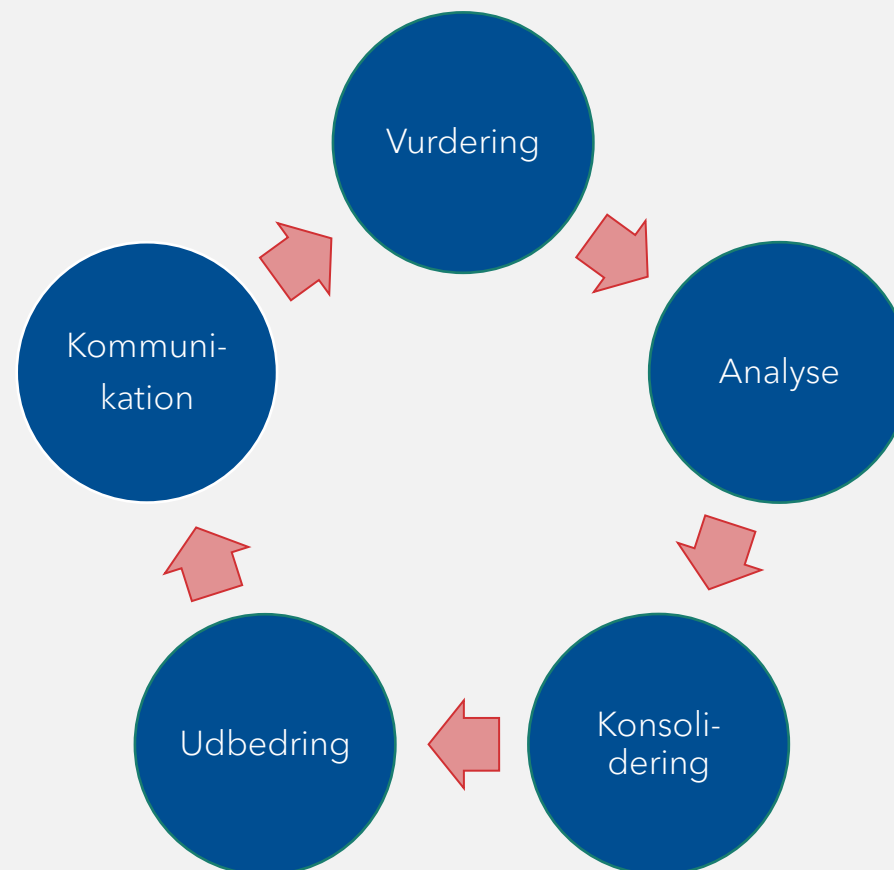
NIS2: b) Håndtering af hændelser



Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse



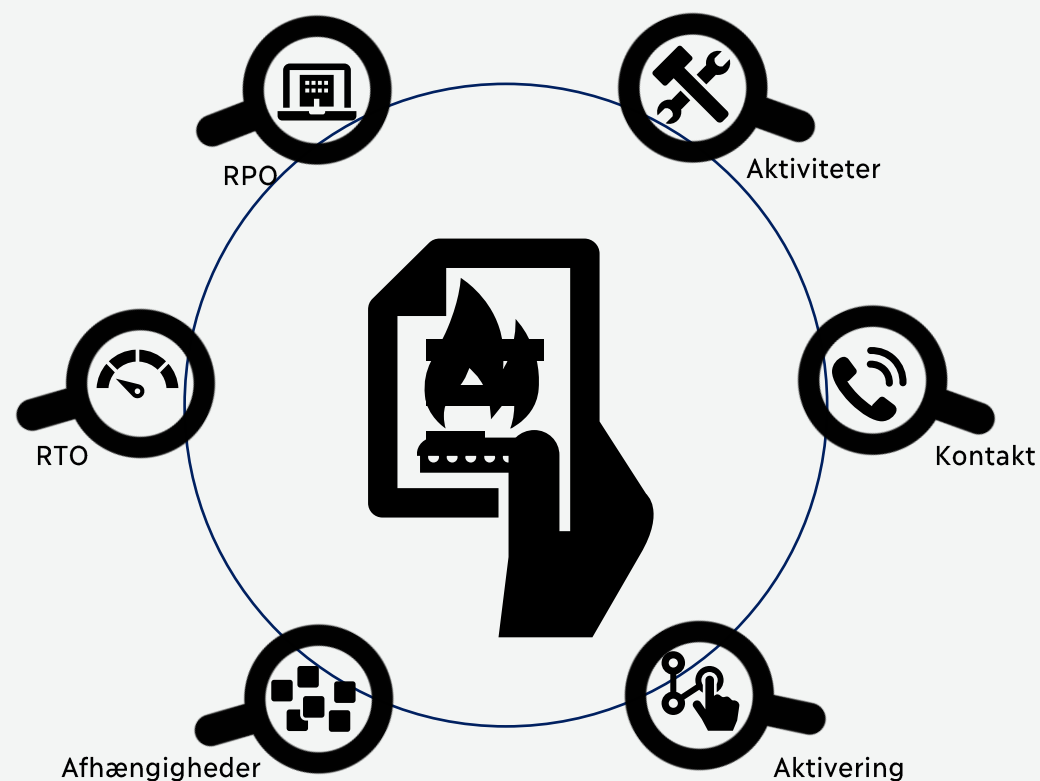
It-beredskabsplan

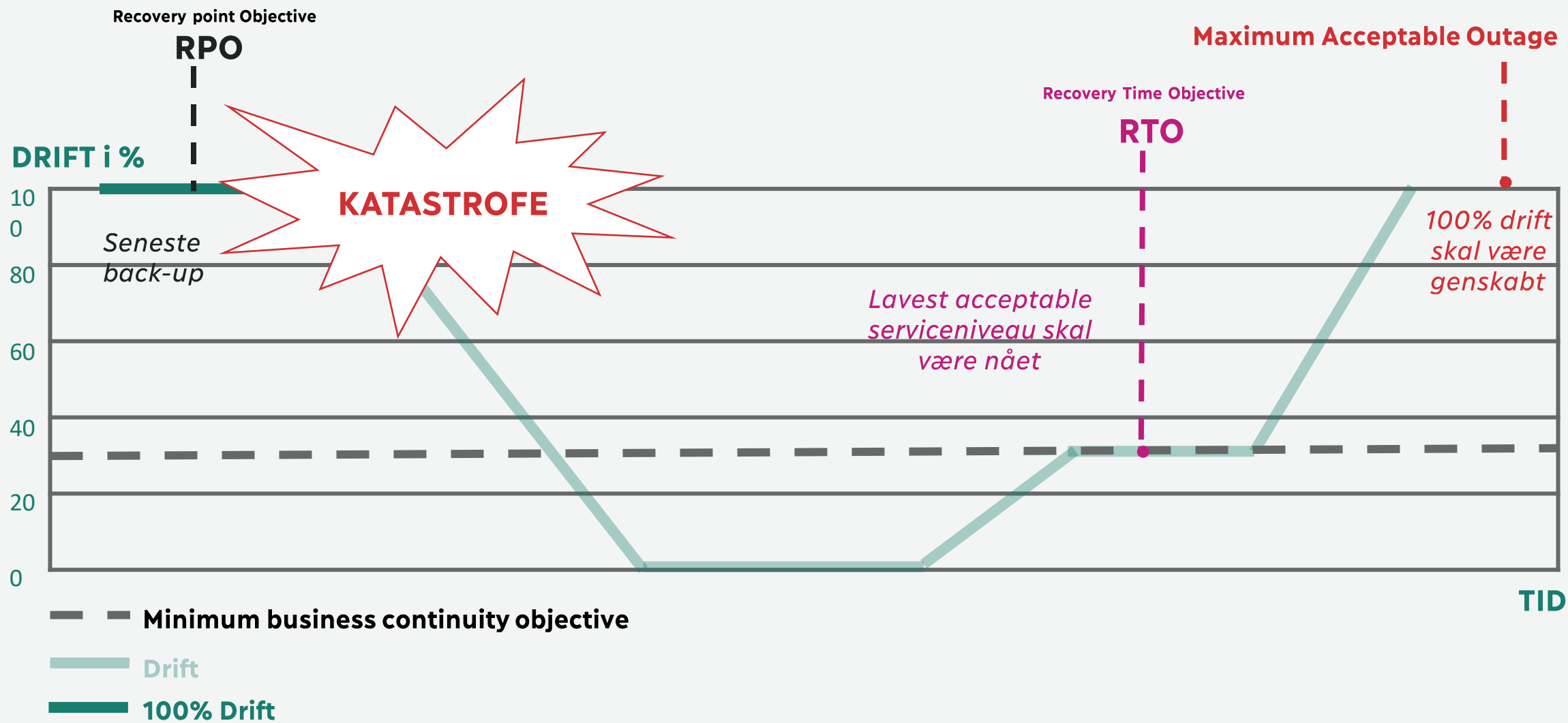


Forretningskontinuitet

NIS2: c) Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring

-  Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse
-  Overblik over data og systemer
-  It-beredskabsplan
-  Beskyttelse mod tab af vigtige og fortrolige data
-  Overvågning af systemaktivitet gennem logning





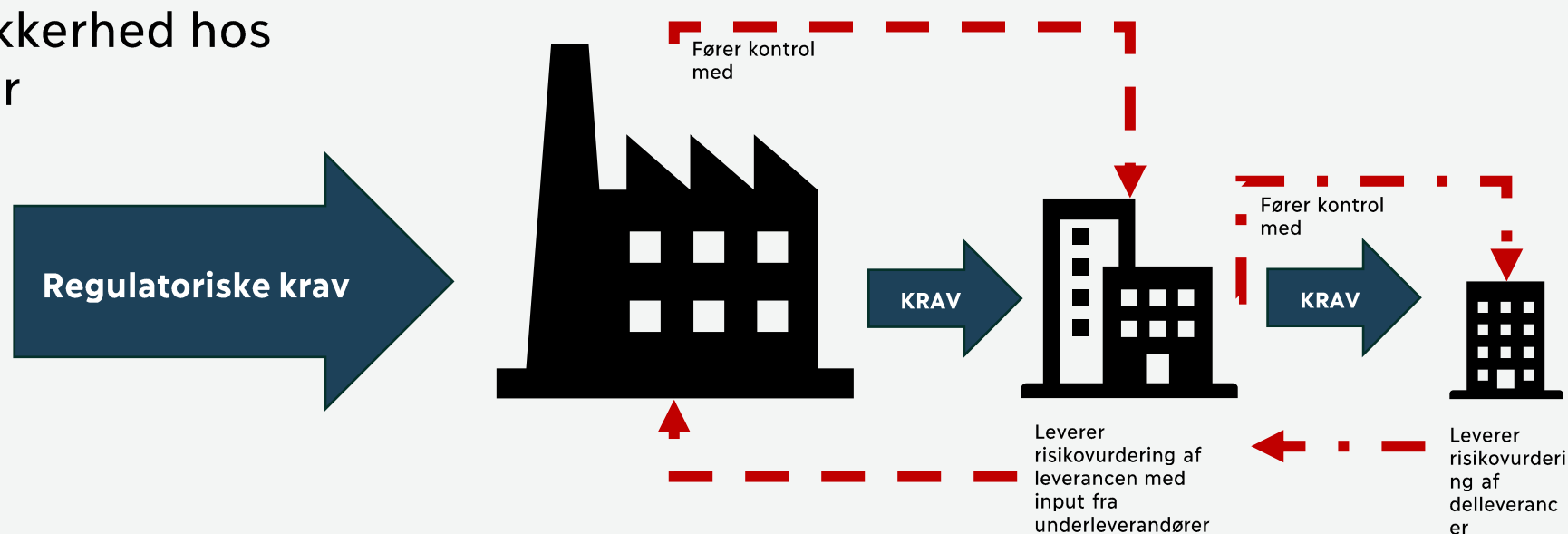
Kilde: Dansk Standard 'Styrk modstandsdygtigheden i jeres virksomhed'

Leverandør- og forsyningskædesikkerhed

NIS2: d) Forsyningskæde-sikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere

 Leverandørlivscyklus og risikovurdering

 Krav til it-sikkerhed hos leverandører



Udvikling og vedligehold af systemer

NIS2: e) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder



Udviklingsproces



Leverandørlivscyklus og risikovurdering



Krav til it-sikkerhed hos leverandører



Kontinuerlig opdatering af software og styresystemer



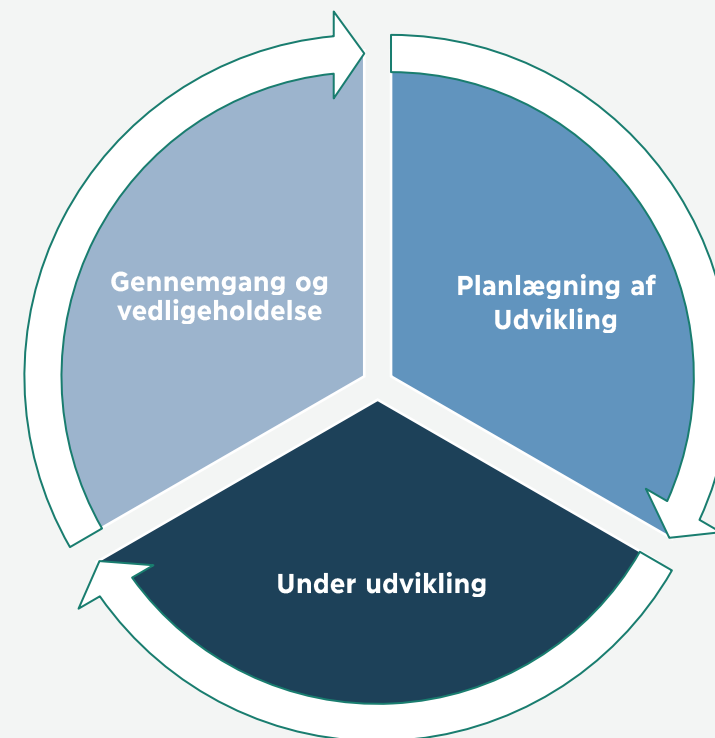
Vurdering



Privacy by design & default



Security by design & default



Effektivitet

NIS2: f) Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici



Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse



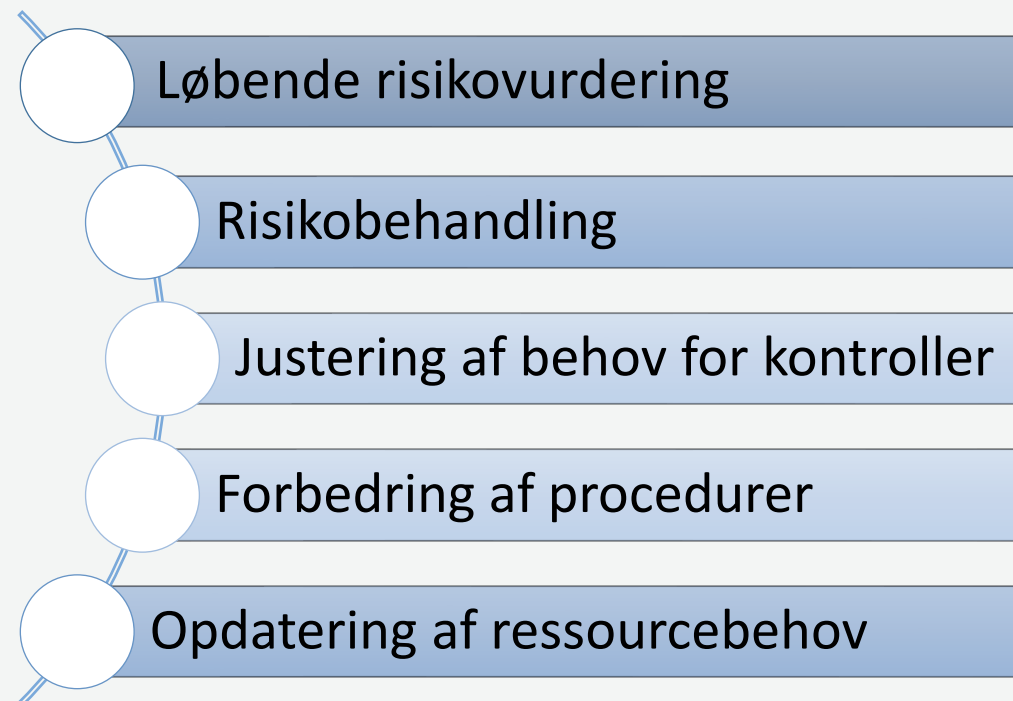
Politik for it-sikkerhed



It-beredskabsplan



Risikostyring



Awareness og træning

NIS2: g) grundlæggende cyberhygiejnepraksisser og cybersikkerheds-uddannelse

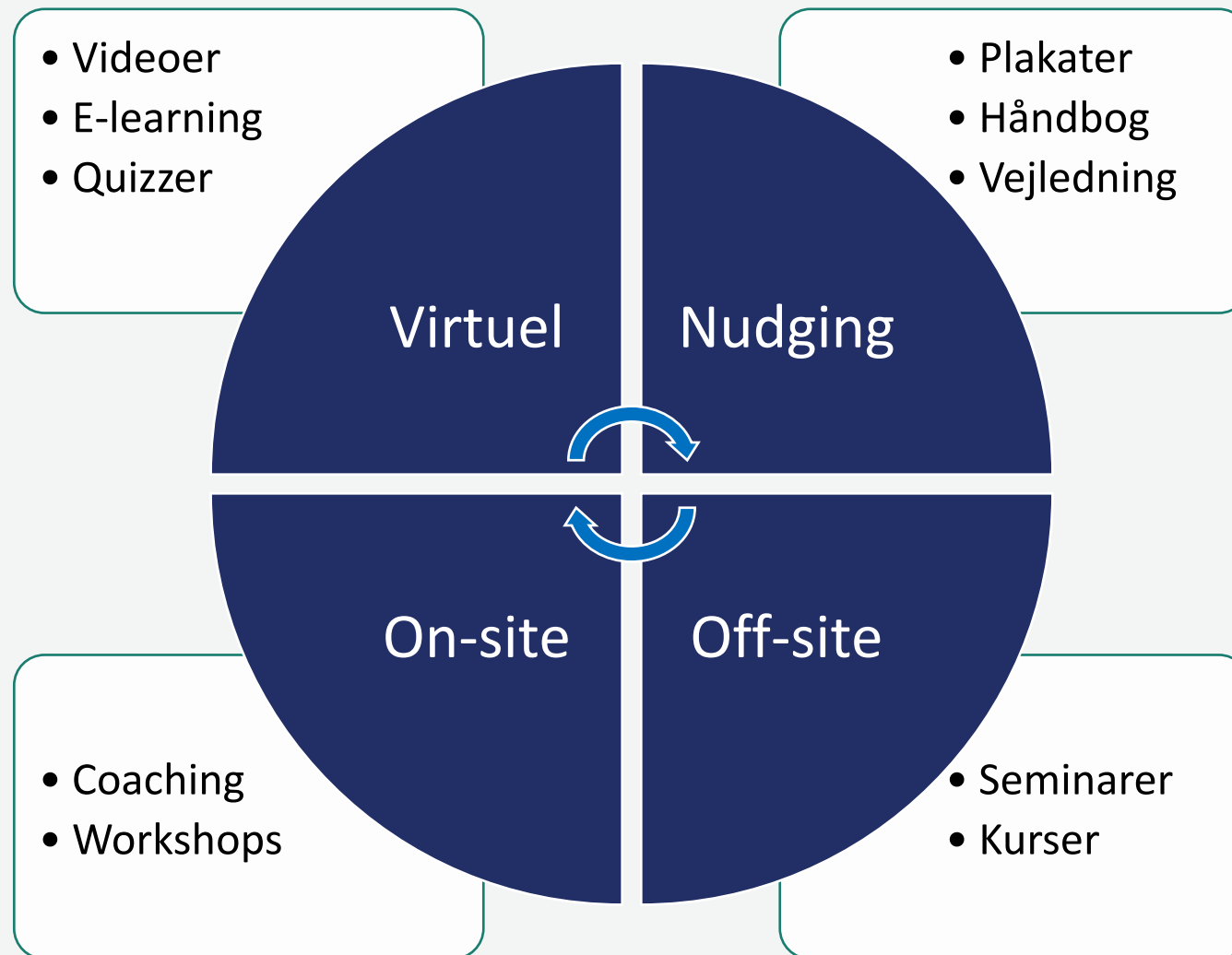


Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik



Awareness om og træning i it-sikkerhed





Kryptering

NIS2: h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering



Politik for it-sikkerhed



Politikker for ansvarlig dataanvendelse



Netværkssikkerhed og kryptering



Vurdering



Privacy by design & default



Security by design & default

Transmission af personoplysninger via e-mail

Generelt



Rettigheder og pligter



Hvad vil det sige at sende e-mails sikkert?



Hvem har ansvaret?



Læs mere



Personale og aktiver

NIS2: i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver



Overblik over data og systemer



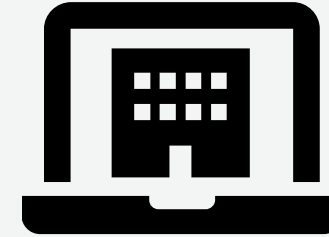
Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik



Awareness om og træning i it-sikkerhed



Beskyttelse af administrative brugerkonti



Autentificering

NIS2: j) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant



Netværkssikkerhed og kryptering



Beskyttelse af administrative brugerkonti



It-beredskabsplan






Selvevaluering



D-mærkets selvevalueringsværktøj



<div> digital tryghed</div> <div>Selvevaluering</div> <div>Status og besvarelse</div>	Selvevaluering Organisation Rapport og mapping Hjælp og vejledning					Majken Majken_Test	
	Navn	Sidste ændring	Status besvarelse	Status efterlevelse	Handler		
	▼ D-mærket kriterier	23/02/2024	I gang	<div><div></div>19%</div>			
	1 Styring og forankring i ledelsen	13/02/2024	I gang	<div><div></div>5%</div>	⋮		
	2 Awareness og sikker adfærd	13/02/2024	I gang	<div><div></div>9%</div>	⋮		
	3 Teknisk it-sikkerhed	23/02/2024	I gang	<div><div></div>38%</div>	⋮		
	4 Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse	23/02/2024	Alle besvaret	<div><div></div>42%</div>	⋮		
	5 Transparens & kontrol med data		Ikke i gang	<div><div></div>0%</div>	⋮		
	6 Privacy & Security by design & default		Ikke i gang	<div><div></div>0%</div>	⋮		
	7 Pålidelige algoritmer & AI	23/02/2024	Alle besvaret	<div><div></div>43%</div>	⋮		
	8 Dataetik	23/02/2024	Alle besvaret	<div><div></div>0%</div>	⋮		



Kilde: <https://digital.d-maerket.dk/>



Overensstemmelse mellem D-mærket og NIS2

Onepager

Kriterier


Mapping værktøj

Selvevaluering

Organisation

Rapport og mapping

Hjælp og vejledning

 Majken
Majken_Test

RAMMEVÆRK

← D-mærket + Mapninger 1

Søg efter krav

Filtrer

Krav

NIS2

Eksportér

1 Styring og forankring i ledelsen

Virksomhedens øverste ledelse tager aktivt ansvar for arbejdet med it-sikkerhed og ansvarlig dataanvendelse. Det er dog ikke nødvendigvis den øverste ledelse, som er udførende på de definerede krav.

> 1.1 Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse

●

> 1.2 Overblik over data og systemer

●

> 1.3 Risikostyring

●

> 1.4 Politik for it-sikkerhed

●

> 1.5 It-beredskabsplan

●

> 1.6 Politikker for ansvarlig dataanvendelse

●

> 1.7 Udviklingsproces

●

2 Awareness og sikker adfærd

Virksomheden skal sikre, at bestyrelsen og den øverste ledelse modtager træning i it-sikkerhed og ansvarlig dataanvendelse. Virksomheden skal yderligere sikre, at ansatte, konsulenter og leverandører løbende og med jævne mellemrum bliver trænet i awareness og handlingskompetencer i relation til it-sikkerhed og ansvarlig dataanvendelse.

> 2.1 Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik

●