CYBERSIKKERHED FOR BESTYRELSER og VIRKSOMHEDSLEDERE

RAPPORTERING til BESTYRELSEN

14. November 2022

Kirsten Hede
Bestyrelsesforeningens Center for Cyberkompetencer

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS OPGAVER og ANSVAR

Det vi godt ved...

I kernen af enhver forretningsmæssig beslutning er **styring og afvejning af risici.**

Værdiskabelse rimer i dag på digitalisering – og jo mere digitale virksomheders produkter og infrastruktur er, jo mere **sårbare er de over for cyberangreb.**

Cyberangreb er blandt de største forretningsrisici, virksomheder står overfor, og **koster danske virksomheder på bundlinje, kundeforhold og renommé.**

Det er derfor vigtigt **at stille skarpt** på cyber- og informationssikkerhed **i bestyrelseslokalet**.

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS OPGAVER og ANSVAR … og LOVGIVNING

Den regulatoriske ramme udgøres primært af NIS-lovgivningen
(samt databeskyttelseslovgivningen)

NIS-lovgivningen i DK
(sektorer)

- Energi
- Finans
- Sundhed
- Søfart
- Tele
- Transport
- Vand
- Digital infrastruktur

9

"Passende og forholdsmæssige tekniske og organisatoriske foranstaltninger" – og hvad så?

NIS-direktivets artikel 14, stk. 1
"passende og forholdsmæssige tekniske og organisatoriske foranstaltninger"

Persondataforordningens artikel 32, stk. 1
"passende tekniske og organisatoriske foranstaltninger"

Lov om finansiel virksomhed, § 71, nr. 4 og 6
(finansielle virksomheder)
"betryggende kontrol- og sikringsforanstaltninger på it-området"

Outsourcingbekendtgørelsen, § 20, stk. 1 og 2, nr. 5
(finansielle virksomheder)
"passende tekniske og organisatoriske foranstaltninger"

Bekendtgørelse 2016-06-01 nr. 567, § 2, stk. 3 (teleudbydere)
"passende foranstaltninger"

Lov 2018-05-08 nr. 441, § 4, stk. 1 (transportområdet)
"passende og forholdsmæssige tekniske og organisatoriske foranstaltninger"

Lov 2018-05-08 nr. 436, § 4, stk. 1 (digital infrastruktur):
"passende og forholdsmæssige tekniske og organisatoriske foranstaltninger"

Lov 2018-05-08 nr. 440, § 4, stk. 1 (sundhedsområdet):
"passende og forholdsmæssige tekniske og organisatoriske foranstaltninger"

www.kromannreumert.com

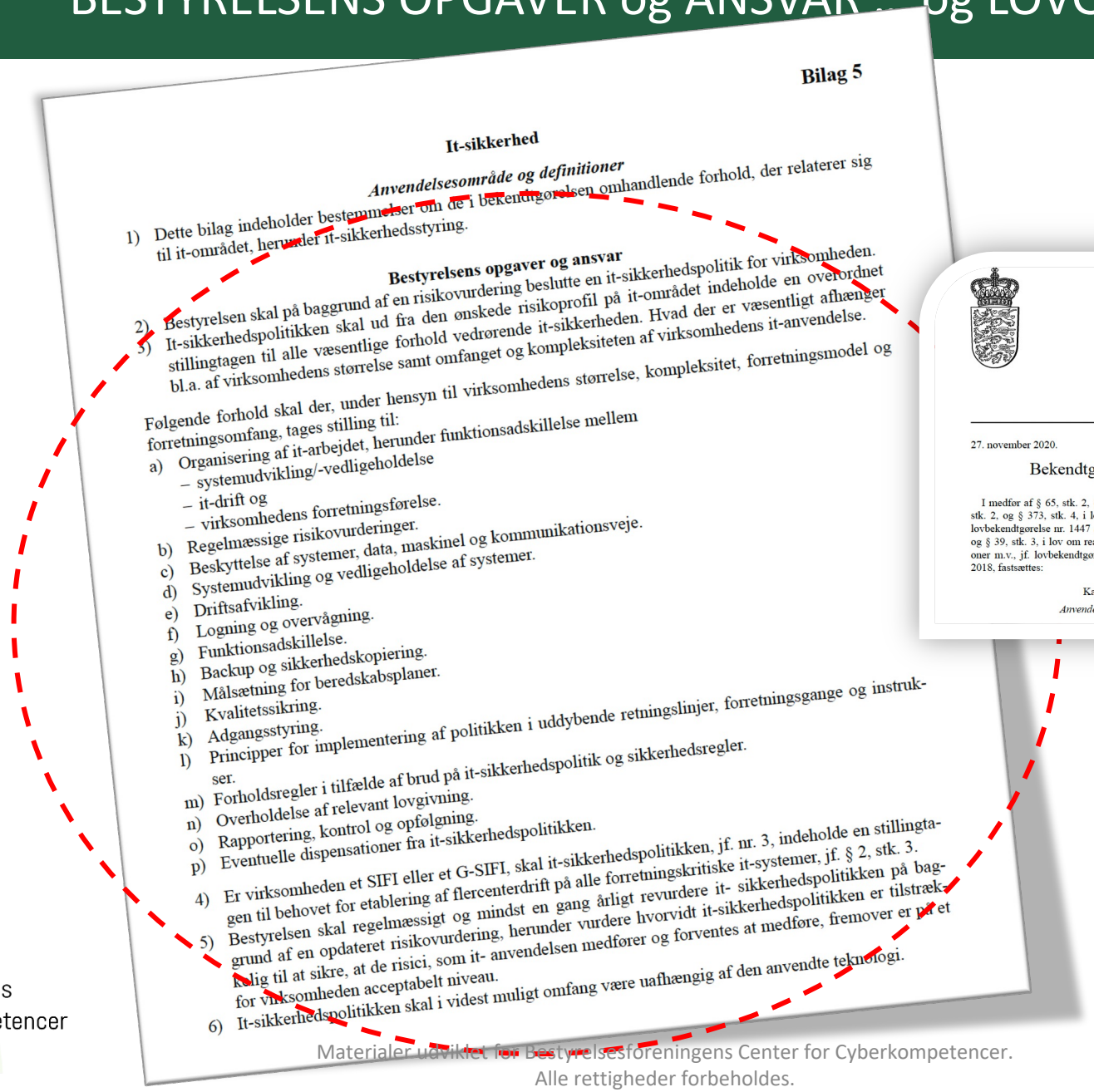
10

Slides fra Kromann Reumert

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS OPGAVER og ANSVAR ... og LOVGIVNING



Bilag 5

It-sikkerhed

Anvendelsesområde og definitioner

1) Dette bilag indeholder bestemmelser om de i bekendtgørelsen omhandlende forhold, der relaterer sig til it-området, herunder it-sikkerhedsstyring.

Bestyrelsens opgaver og ansvar

2) Bestyrelsen skal på baggrund af en risikovurdering beslutte en it-sikkerhedspolitik for virksomheden.
3) It-sikkerhedspolitikken skal ud fra den ønskede risikoprofil på it-området indeholde en overordnet stillingtagen til alle væsentlige forhold vedrørende it-sikkerheden. Hvad der er væsentligt afhænger bl.a. af virksomhedens størrelse samt omfanget og kompleksiteten af virksomhedens it-anvendelse.

Følgende forhold skal der, under hensyn til virksomhedens størrelse, kompleksitet, forretningsmodel og forretningsomfang, tages stilling til:

a) Organisering af it-arbejdet, herunder funktionsadskillelse mellem
   – systemudvikling/-vedligeholdelse
   – it-drift og
   – virksomhedens forretningsførelse.
b) Regelmæssige risikovurderinger.
c) Beskyttelse af systemer, data, maskinel og kommunikationsveje.
d) Systemudvikling og vedligeholdelse af systemer.
e) Driftsafvikling.
f) Logning og overvågning.
g) Funktionsadskillelse.
h) Backup og sikkerhedskopiering.
i) Målsætning for beredskabsplaner.
j) Kvalitetssikring.
k) Adgangsstyring.
l) Principper for implementering af politikken i uddybende retningslinjer, forretningsgange og instrukser.
m) Forholdsregler i tilfælde af brud på it-sikkerhedspolitik og sikkerhedsregler.
n) Overholdelse af relevant lovgivning.
o) Rapportering, kontrol og opfølgning.
p) Eventuelle dispensationer fra it-sikkerhedspolitikken.

4) Er virksomheden et SIFI eller et G-SIFI, skal it-sikkerhedspolitikken, jf. nr. 3, indeholde en stillingtagen til behovet for etablering af flercenterdrift på alle forretningskritiske it-systemer, jf. § 2, stk. 3.
5) Bestyrelsen skal regelmæssigt og mindst en gang årligt revurdere it- sikkerhedspolitikken på baggrund af en opdateret risikovurdering, herunder vurdere hvorvidt it-sikkerhedspolitikken på baggrund af en opdateret risikovurdering, herunder vurdere hvorvidt it-sikkerhedspolitikken er tilstrækkelig til at sikre, at de risici, som it- anvendelsen medfører og forventes at medføre, fremover er på et for virksomheden acceptabelt niveau.
6) It-sikkerhedspolitikken skal i videst muligt omfang være uafhængig af den anvendte teknologi.

Lovtidende A

2020 Udgivet den 28. november 2020

27. november 2020. Nr. 1706.

Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl.[1)]

I medfør af § 65, stk. 2, § 70, stk. 7, § 71, stk. 3, § 152, stk. 2, og § 373, stk. 4, i lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 1447 af 11. september 2020, og § 21, og § 39, stk. 3, i lov om realkreditlån og realkreditobligationer m.v., jf. lovbekendtgørelse nr. 1188 af 19. september 2018, fastsættes:

Kapitel 1

Anvendelsesområde

Stk. 4. § 4, stk. 2, nr. 7, § 5, stk. 3, nr. 4 og bilag 8 finder ikke anvendelse for virksomheder omfattet af § 1, stk. 1, nr. 5-7.

Stk. 5. § 5, stk. 3, nr. 5 finder ikke anvendelse for virksomheder omfattet af § 1, stk. 1, nr. 5-6.

§ 2. Bestyrelsen henholdsvis direktionen i de af § 1, stk. 1, omfattede virksomheder skal træffe foranstaltninger, der er tilstrækkelige til, at virksomheden drives betryggende. Bestyrelsen henholdsvis direktionen skal herunder tage

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS OPGAVER og ANSVAR … og NY LOVGIVNING

Hvilke krav stiller NIS2 til din organisation?

NIS2-direktivet stiller både krav til ledelse, risikostyring, forretningskontinuitet og rapportering til myndighederne:

- Ledelsen i jeres organisation skal være bekendte med kravene i direktivet og risikostyringsindsatsen. De får et direkte ansvar for, at cyberrisici bliver identificeret og håndteret samt, at kravene overholdes.
- Øgede krav til risikostyring og robusthed betyder, at din organisation skal risikostyre og implementere både skadesforebyggende og -begrænsende foranstaltninger, der reducerer risici og konsekvenser. Minimumskrav er fx incident management, sikring af cybersikkerhed i forsyningskæder, netværkssikkerhed, adgangskontrol og kryptering.
- Jeres organisation skal forholde sig til, hvordan I vil sikre forretningskontinuiteten i tilfælde af, at I skulle blive ramt af en større cyberhændelse. Dette indebærer eksempelvis genopretning af systemer, nødprocedurer og etablering af en kriseorganisation.
- Jeres organisation skal have etableret processer for, hvordan I vil sikre den korrekte rapportering til myndighederne. Der stilles blandt andet krav til, at større hændelser rapporteres inden for 24 timer.

Bestyrelsesforeningens Center for Cyberkompete

INDUSTRIENS FOND

VEJLEDNING … UDVIKLINGEN ->

December 2019 v. 1.0

- Hjemmearbejde
- Personlig sikkerhed
- Sikker kommunikation

December 2020 v. 2.0

- Insidertrusler
- Bestyrelsesansvar
- Leverandørsikkerhed

December 2021 v. 3.0

- Stategi
  …sammenhænge til forretning
  …sammenhænge til IT organisationens værktøjskasse
- Rapportering
  … risikovurderinger/appetit
  … forankring/opfølgning
- Governance og organisering
  … lines of defence
- Lovgivning – NIS2
  …bestyrelsesansvar 2.0

December 2022 v. 4.0

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

OPBYGNING AF CYBERSTRATEGIEN

Forudsætninger
Cybersikkerhedsstrategien bør overordnet handle om at beskytte virksomhedens *LtO aktiver*.

Den grundlæggende forudsætning for at udarbejde strategien er at have et klart billede af bl.a.:

- Virksomhedens overordnede strategi og forretningsmål,
- Virksomhedens LtO aktiver,
- Virksomhedens organisatoriske og tekniske opbygning og forudsætninger,
- Virksomhedens minimumskrav til cybersikkerhed, og
- Virksomhedens digitale leverandører, outsourcing og samarbejdspartnere.

Risikoforståelse
Bestyrelsen har ansvaret for, at det samlede risikobillede afspejler de relevante cybersikkerhedsrisici.

Ledelsen bør - på tværs af virksomheden – således skabe et fælles sprog og forståelse af:

- **hvad risiko er, og**
- **hvornår en risiko er væsentlig eller uvæsentlig.**

Governance
Bestyrelsen bør rammesætte governance for beskyttelse af det digitale. Dette kan gøres ved grundlæggende at svare på:

- Hvem gør hvad, hvorfor og hvornår?,
- Hvem kontrollerer hvem?, og
- Er der konfliktende interesser / forhold?

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS RISIKOSTYRINGSMODEL for CYBERSIKKERHED

Tema 1 – License to Operate aktiver/aktiviteter LtO

Aktiver og aktiviteter fastsættes ift. strategi/formål/forretningsmodel

Tema 1 - Risikovurdering

Udarbejdes af organisationen på baggrund af LtO aktiver og aktiviteter

Tænkt eksempel = en lufthavn

- Aeronautisk drift
- Transport og parkering
- Toldfri og mad/drikke
- Service/faciliteter

BRUTTO-RISIKO
License to Operate aktiver/aktiviteter (LtO)

- Trusselsbilledet
- IT-infrastruktur
- Procesforandringer
- Opkøb/outsourcing
- XXX

RISIKO-TILTAG (forebyggelse)

NETTO-RISIKO = RISIKOVURDERING

RISIKO-TILTAG (beredskab)

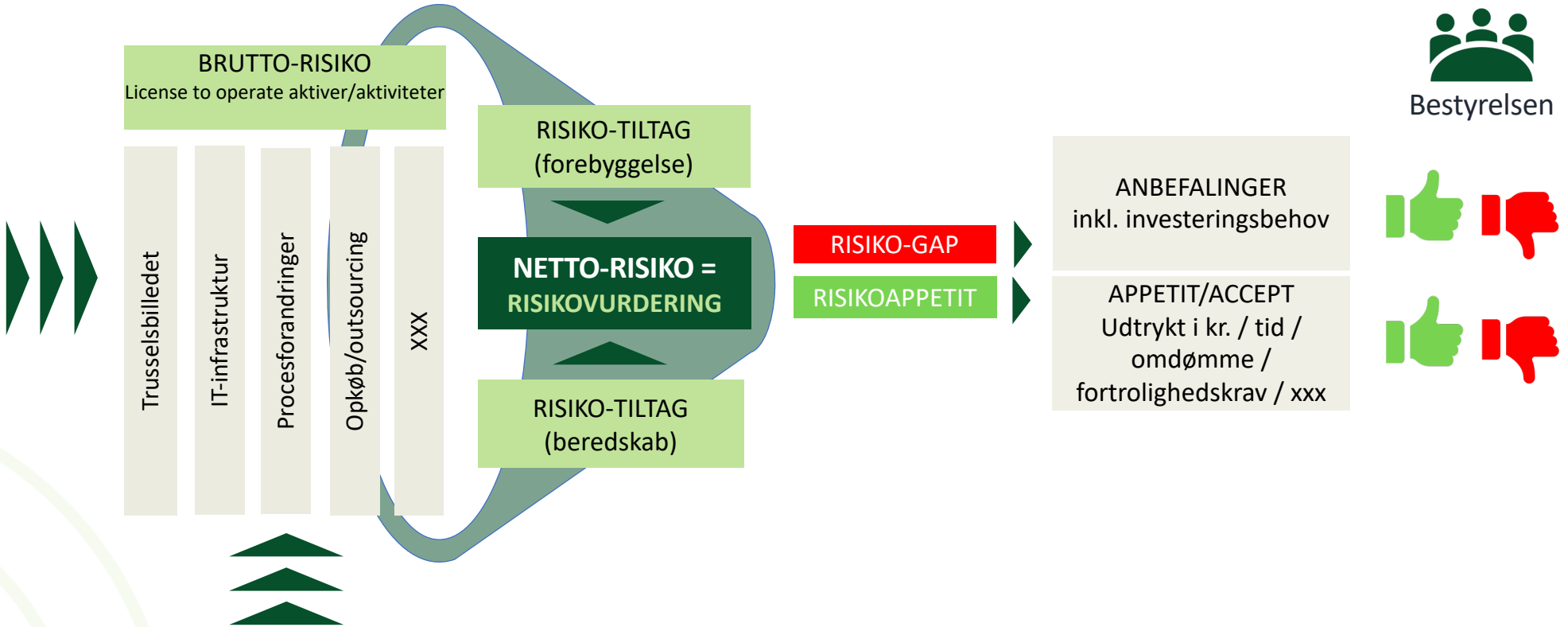
Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS RISIKOSTYRINGSMODEL for CYBERSIKKERHED

Tema 1 - Risikovurdering

Tema 2 - Risikoappetit



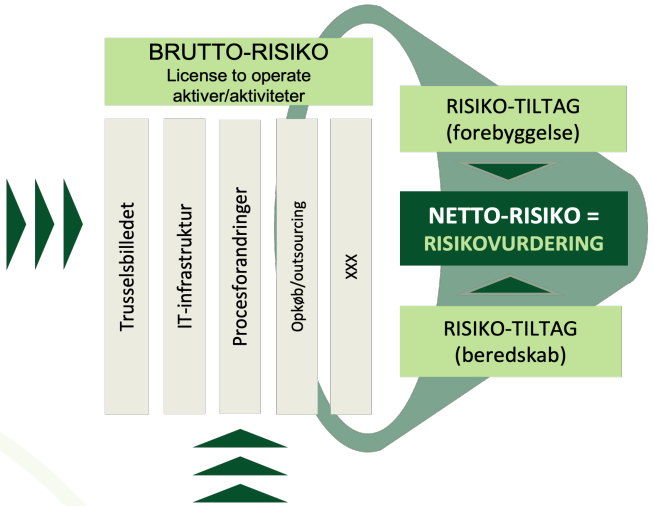
Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS RISIKOSTYRINGSMODEL for CYBERSIKKERHED

Bestyrelse og ledelse

Daglig drift / operations

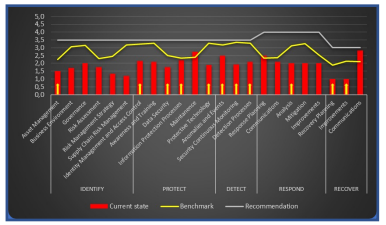


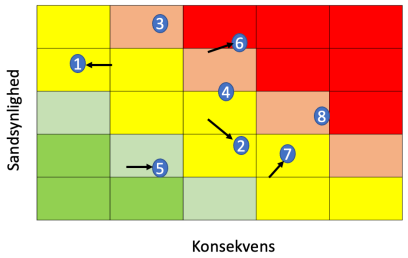
Tema 3
Politikker, processer og beredskab

Tema 4
Rapportering og kontrol

Identificer | Beskyt | Opdag | Håndter | Genopret

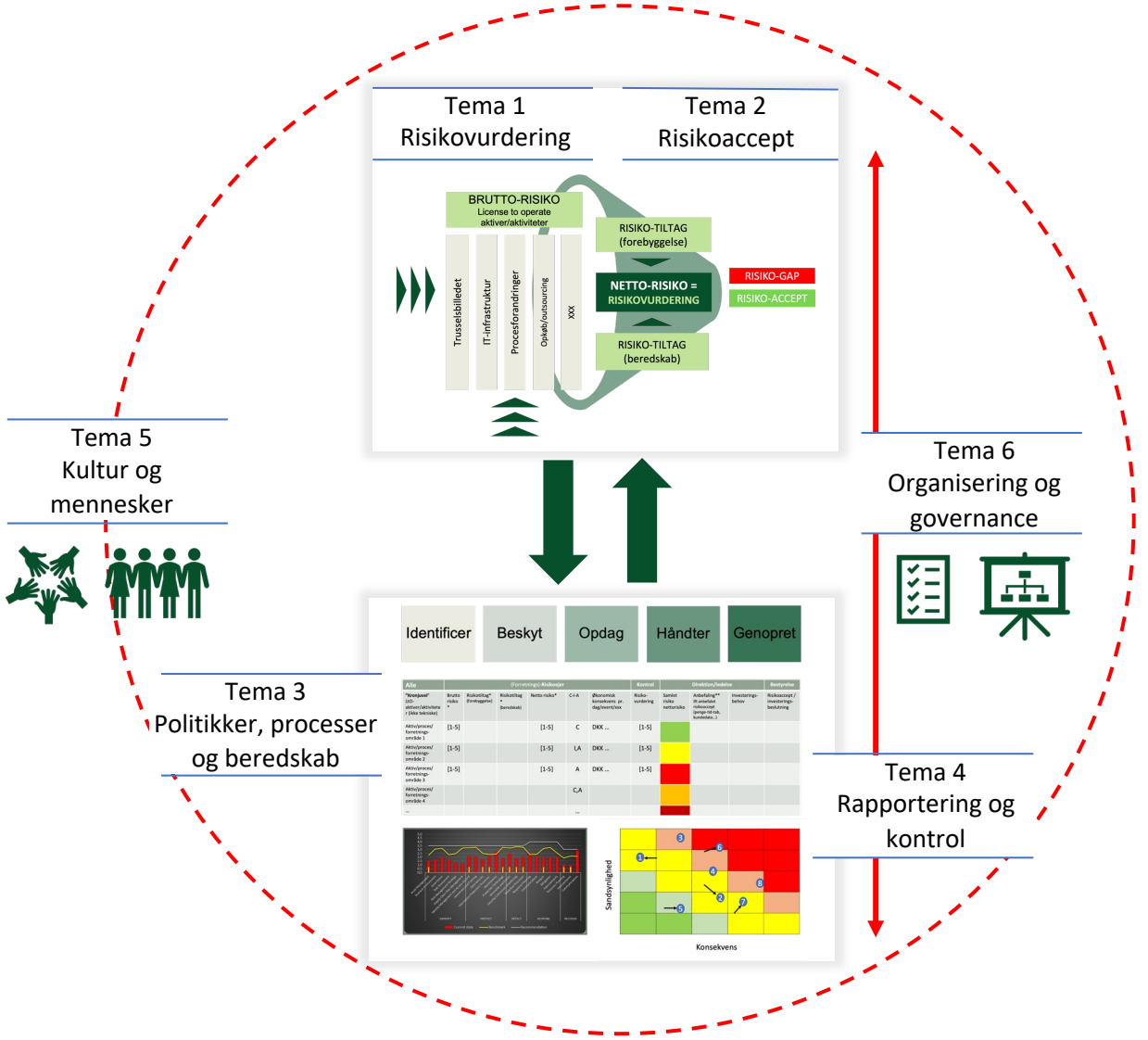
Alle	(Forretnings)-Risikoejer						Kontrol	Direktion/ledelse			Bestyrelse
"Kronjuvel" LtO-aktiver/aktiviteter (ikke tekniske)	Brutto risiko *	Risikotiltag* (forebyggelse)	Risikotiltag * (beredskab)	Netto risiko*	C-I-A	Økonomisk konsekvens pr. dag/event/xxx	Risiko-vurdering	Samlet risiko nettorisiko	Anbefaling** ift anbefalet risikoaccept (penge-tid-tab, kundedata…)	Investerings-behov	Risikoaccept / investerings-beslutning
Aktiv/proces/ forretnings-område 1	[1-5]			[1-5]	C	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 2	[1-5]			[1-5]	I,A	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 3	[1-5]			[1-5]	A	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 4					C,A						
…					…						





Bestyrelsesforeningens
Center for Cyberkompetencer

BESTYRELSENS RISIKOSTYRINGSMODEL for CYBERSIKKERHED



Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING dec. 2022

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

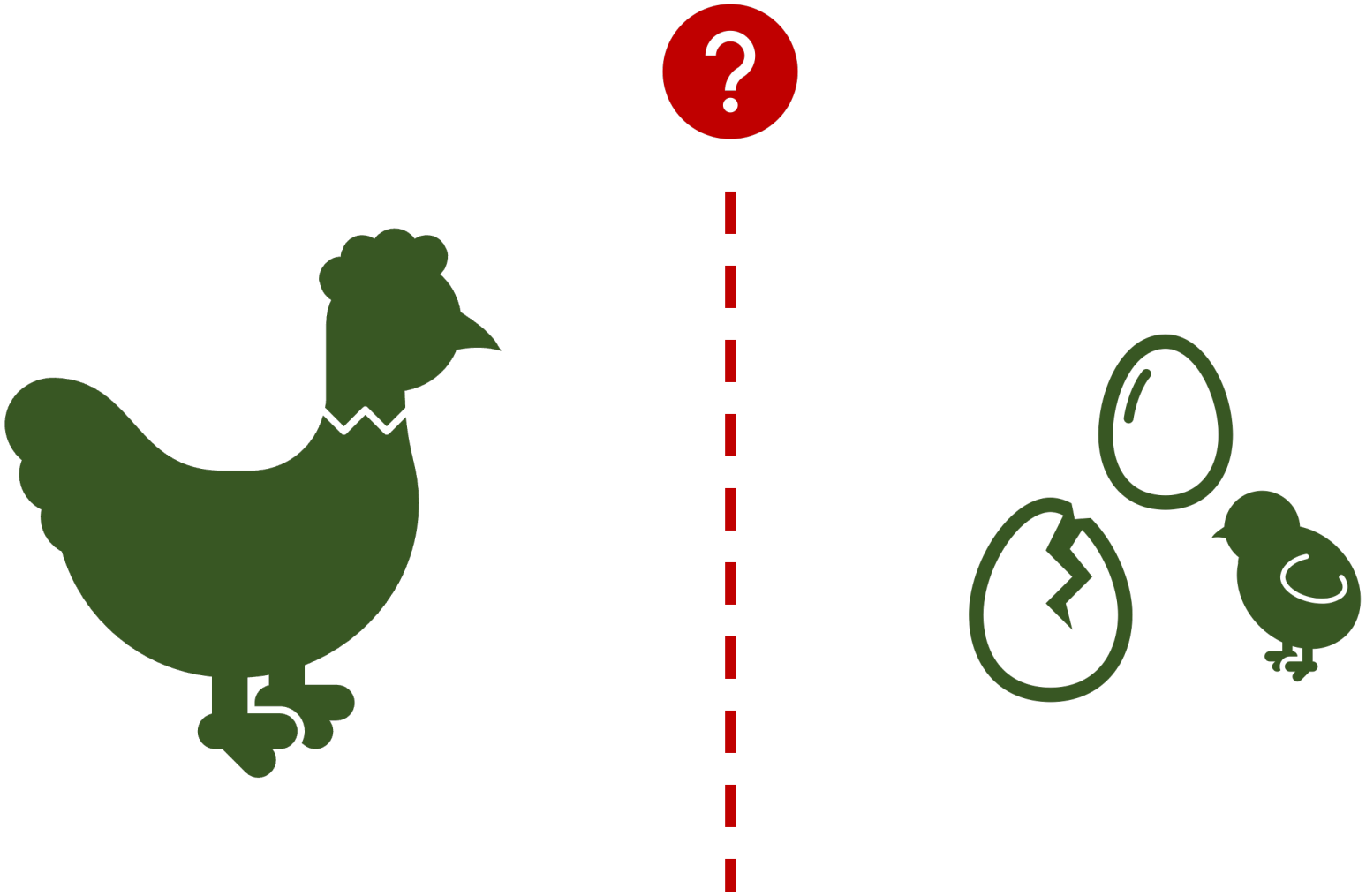
Tema 4. Rapportering *- kontrol og tilsyn*

Det anbefales, at

- bestyrelsen implementerer cybersikkerhed som en **fast del af sit årshjul** og, **på linje med øvrige væsentlige risici**,

- bestyrelsen har **cybersikkerhed på agendaen på hvert møde**, og **modtager relevant rapportering** forud for mødet med bl.a. **aktuelt trusselsbillede, sikkerhedshændelser, resultater af sikkerhedstest, awareness aktiviteter og revisionsgennemgange, samt evt. forslag til supplerende tiltag.**

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING dec.2022



Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

Tema 2 Risikoappetit – *risikoafvejning og risikovillighed*

Centrale spørgsmål:

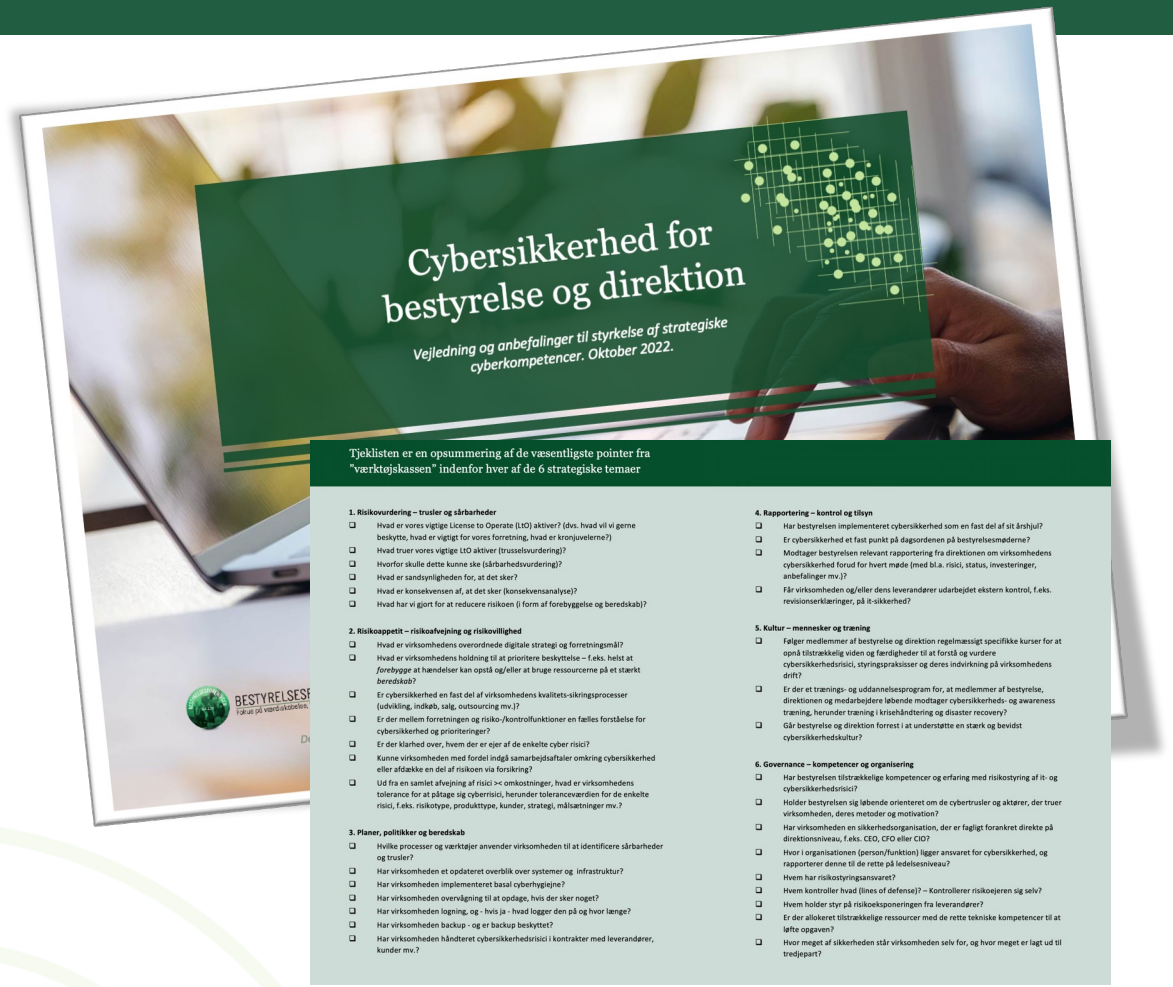
- Hvad er virksomhedens overordnede **digitale strategi og forretningsmål?**
- Hvad er virksomhedens **holdning til at prioritere beskyttelse** – f.eks. helst at **forebygge** at hændelser kan opstå og/eller at bruge ressourcerne på et stærkt **beredskab?**
- Er cybersikkerhed en **fast del af virksomhedens kvalitets-sikringsprocesser** (udvikling, indkøb, salg, outsourcing mv.)?

Tema 2 Risikoappetit – *risikoafvejning og risikovillighed*

Centrale spørgsmål:

- Er der mellem **forretningen og risiko-/kontrolfunktioner en fælles forståelse** for cybersikkerhed og prioriteringer?
- Er der klarhed over, hvem der er **ejer af de enkelte cyber risici**?
- Kunne virksomheden med **fordel indgå samarbejdsaftaler** omkring cybersikkerhed eller **afdække en del af risikoen** via forsikring?
- Ud fra en samlet afvejning af risici >< omkostninger, hvad er virksomhedens **tolerance** for at påtage sig cyberrisici, herunder toleranceværdien for de enkelte risici, f.eks. **risikotype, produkttype, kunder, strategi, målsætninger mv.?**

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING dec.2022



Centrale overvejelser i et bestyrelseslokale

Rapportering
Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed fra direktionen, herunder:

- Aktuel risikostatus (sammenfatning af risikostatus)
- Aktuelt trusselsbillede samt udvikling/trends siden sidst
- Observationer og kommentarer fra revisorer/rådgivere
- Lovgivning og myndighedskrav (og aktuelle/kommende ændringer hertil)
- Resultater fra test af beredskabsplaner og kritiske systemer
- Eventuelle fravigelser fra de af bestyrelsen fastsatte risikotolerancer
- Interne sikkerhedshændelser, herunder hændelser rapporteret til myndighederne
- Eksterne sikkerhedshændelser – fx leverandører og outsourcing partnere
- Projekt status (Status på implementering af sikkerhedstiltag)
- System status, herunder: Væsentligste generelle (tekniske) risikoområder, risiko og kontrol oversigt (tekniske) og heat map status med top X (tekniske) risici
- Status personale / medarbejdere og organisering
- Status på sikkerhedskategorier generelt (NIST)
- Krisehåndtering - ansvar og bemyndigelse
- Begrænsninger og udeladelser
- Anbefalinger til forbedringer og investeringer forbundet hermed
- En inspirationsliste til rapportering er vist i Appendiks 4.

Årshjul

- Har bestyrelsen implementeret cybersikkerhed som en fast del af et årshjul, der sikrer opfølgning og kontrol som en fast del af bestyrelsens arbejde, og sikrer rette rapportering i rette tid?
- Et eksempel på et årshjul med cyberaktiviteter er vist i Appendix 6.
- Kontrol og revision (på sikkerhed)
- Får virksomheden udarbejdet revisorerklæringer i forhold til it sikkerhed, f.eks. ISAE3402 eller ISAE3000?
- Stiller virksomheden krav om, at dets kunder eller leverandører får udarbejdet disse erklæringer?
- Er der opmærksomhedspunkter fra disse rapporter, og hvis ja, en plan for udbedring?

Tilsynsmyndigheder

- Er virksomheden i en branche eller sektor, der kræver løbende dialog og forventningsafstemning med nationale myndigheder (f.eks. virksomheder der leverer kritisk infrastruktur)?
- Har virksomheden en proces for opbevaring og gennemgang af data til brug for eventuelle tilsynsbesøg?

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

Tema 4 Rapportering *- kontrol og tilsyn*

Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed fra direktionen, herunder:

- **Aktuel risikostatus** (sammenfatning af risikostatus)
- Aktuelt trusselsbillede samt udvikling/trends siden sidst
- **Observationer** og kommentarer fra revisorer/rådgivere
- Lovgivning og **myndighedskrav** (og aktuelle/kommende ændringer hertil)
- Resultater fra test af **beredskabsplaner** og kritiske systemer
- Eventuelle fravigelser fra de af bestyrelsen fastsatte risikotolerancer
- Interne **sikkerhedshændelser**, herunder hændelser rapporteret til myndighederne
- Eksterne sikkerhedshændelser – fx leverandører og outsourcing partnere
- **Projekt status** (Status på implementering af sikkerhedstiltag)
- System status, herunder: Væsentligste generelle (tekniske) risikoområder, risiko og kontrol oversigt (tekniske) og heat map status med top X (tekniske) risici
- **Status personale** / medarbejdere og organisering
- **Osv osv … men find vejen i DIN virksomhed= vi har givet nogle ideer!**

BESTYRELSENS RISIKOSTYRINGSMODEL for CYBERSIKKERHED - RAPPORTERING

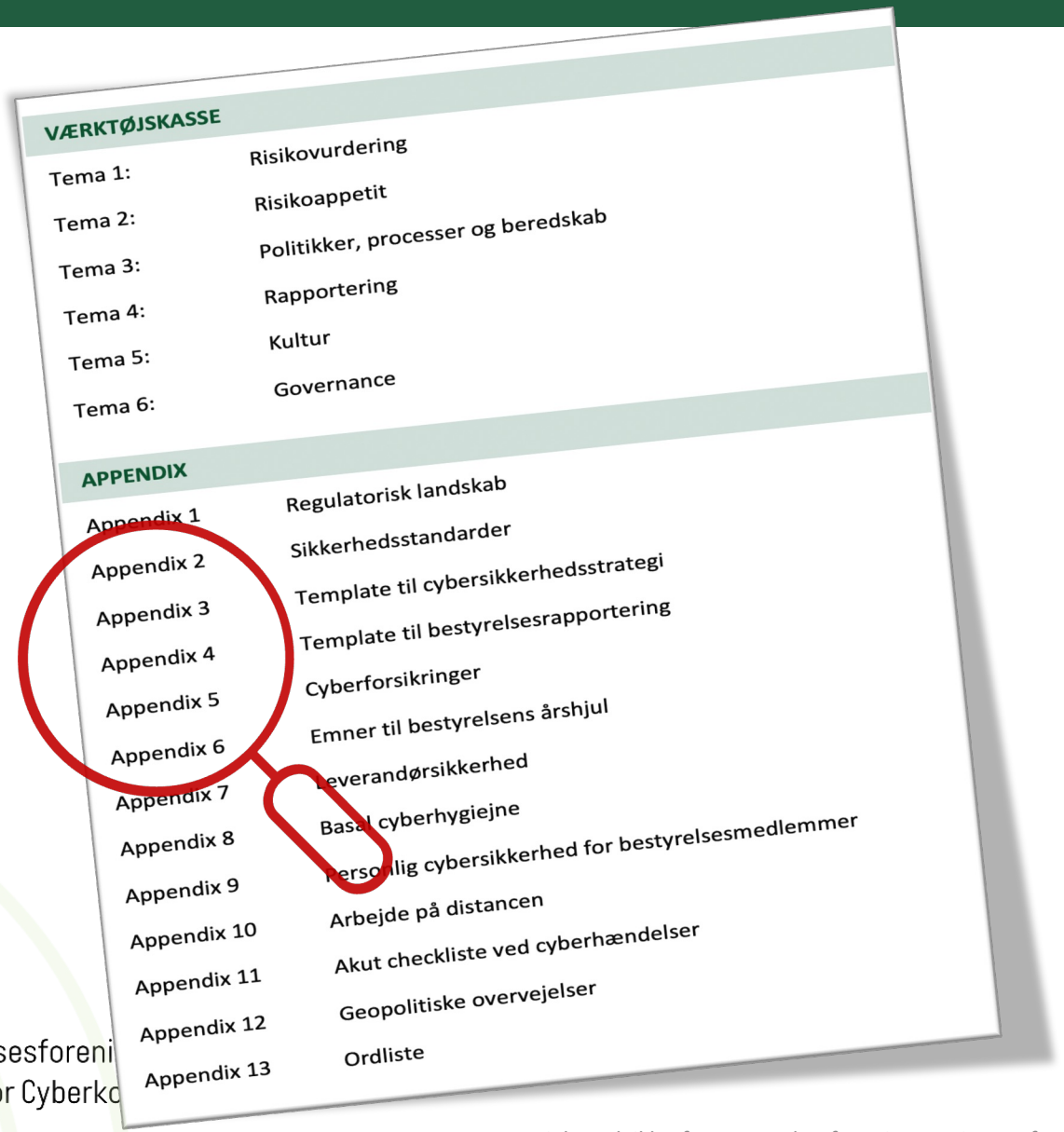
Alle	(Forretnings)-Risikoejer						Kontrol	Direktion/ledelse			Bestyrelse
LtO- aktiver /aktiviteter (ikke tekniske)	**Brutto risiko***	**Risikotiltag*** (forebyggelse)	**Risikotiltag*** (beredskab)	**Netto risiko***	C-I-A	**Økonomisk konsekvens** pr. dag/event/xx	**Risiko-vurdering**	**Samlet risiko nettorisiko**	**Anbefaling**** ift anbefalet risikoaccept (penge-tid-tab, kundedata…)	**Investerings-behov**	**Risikoappetit / investerings-beslutning**
Aktiv/proces/ forretnings-område 1	[1-5]			[1-5]	C	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 2	[1-5]			[1-5]	I,A	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 3	[1-5]			[1-5]	A	DKK …	[1-5]				
Aktiv/proces/ forretnings-område 4					C,A						
…					…						

* = samlet vurdering af tekniske og operationelle elementer, der understøtter (strategiske) "Licence to Operate aktiver/aktiviteter" i forretningen = skal sammenholdes med selskabets strategi – forretningsmål og forretningsmodel
** = evt i forhold til tidligere defineret risikoappetit

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

VEJLEDNING – VÆRKTØJSKASSEN

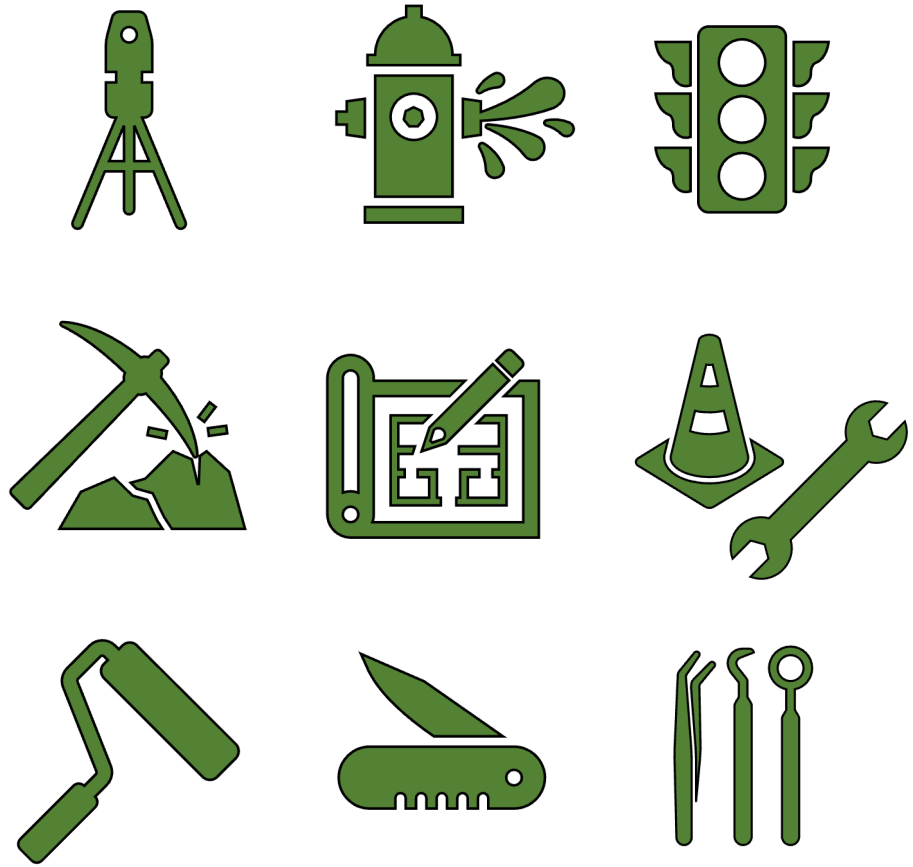


VÆRKTØJSKASSE

Tema 1:	Risikovurdering
Tema 2:	Risikoappetit
Tema 3:	Politikker, processer og beredskab
Tema 4:	Rapportering
Tema 5:	Kultur
Tema 6:	Governance

APPENDIX

Appendix 1	Regulatorisk landskab
Appendix 2	Sikkerhedsstandarder
Appendix 3	Template til cybersikkerhedsstrategi
Appendix 4	Template til bestyrelsesrapportering
Appendix 5	Cyberforsikringer
Appendix 6	Emner til bestyrelsens årshjul
Appendix 7	Leverandørsikkerhed
Appendix 8	Basal cyberhygiejne
Appendix 9	Personlig cybersikkerhed for bestyrelsesmedlemmer
Appendix 10	Arbejde på distancen
Appendix 11	Akut checkliste ved cyberhændelser
Appendix 12	Geopolitiske overvejelser
Appendix 13	Ordliste



Bestyrelsesforeni
Center for Cyberko

INDUSTRIENS FOND

Tema 4. Rapportering *- kontrol og tilsyn*

Den korte version:

- Skab en **fælles forståelse** af (cyber)risici i DIN virksomhed
- Sørg for at sætte cybersikkerhed på **dagsordenen**
- Få en **god debat og spørg** til du har forstået svarene på dine spørgsmål
- Få aftalt hvem, der har **ansvar** for hvad - **inkl. afgrænsninger og "trickers"** i rapporteringen
- Skab en **overskuelig rapportering**, der til stadighed kan danne ramme for en relevant dialog mellem **forretningen, kontrolfunktioner og virksomhedsledelsen**
- Hav – og skab - blik for, at cybersikkerhed er både **komplekst og uforudsigeligt** – der er mange mange **black swans og tailriskevents…**

BESTYRELSESFORENINGEN.DK

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

TAK FOR I DAG

…og lad os sammen styrke cybersikkerheden i Danmark

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND