CYBERSIKKERHED FOR BESTYRELSE og DIREKTION

Why and **How** Board and Management Must Prioritize Cybersecurity

Dubex - 5. September 2024

Kirsten Hede, Projektdirektør
Bestyrelsesforeningens Center for Cyberkompetencer

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSESFORENINGEN – DEN KORTE VERSION

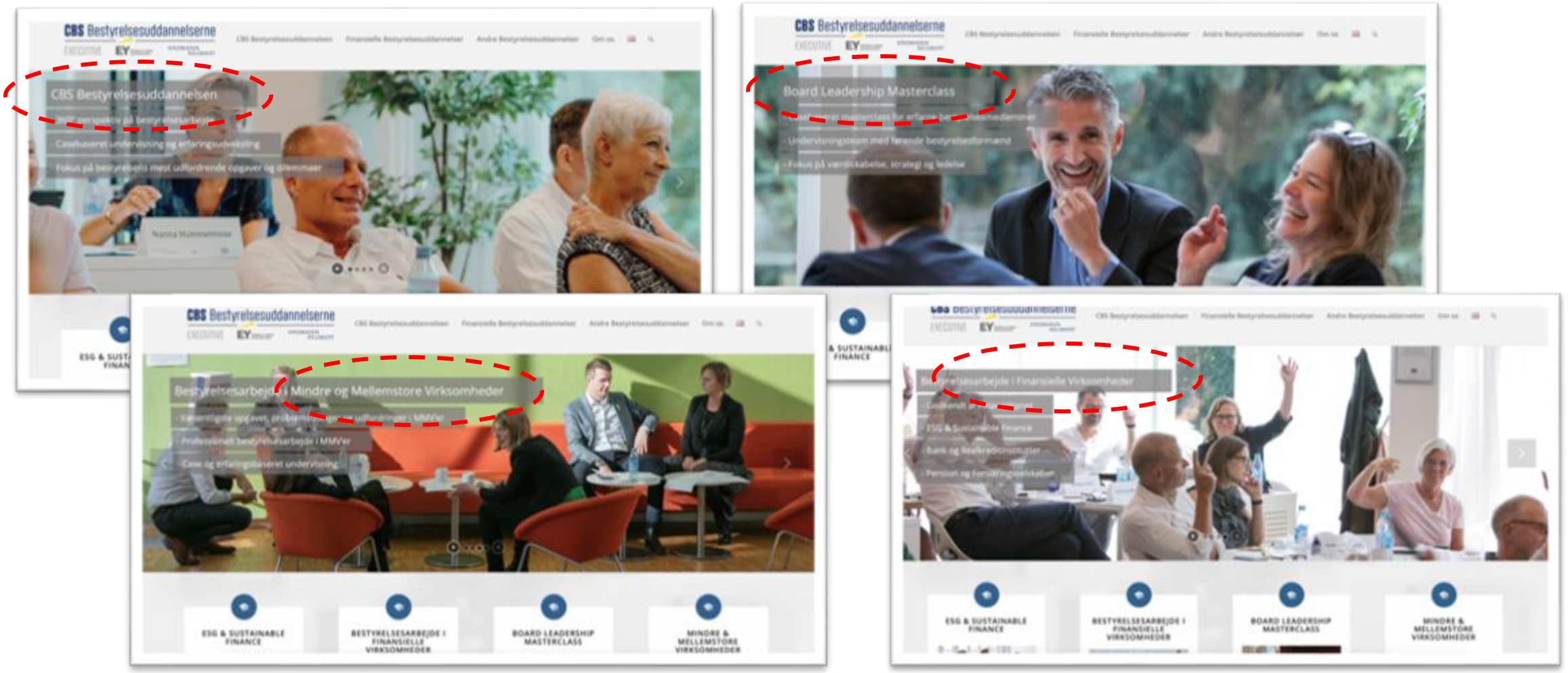
Foreningens formål er på **non-profit** basis at arbejde for en stadig **opkvalificering** af bestyrelsesarbejdet i **danske selskaber, virksomheder, organisationer og institutioner**

Bestyrelsesforeningen blev stiftet den 7. maj 2013 som et tværnationalt projekt af 8 virksomheder, 24 bestyrelsesformænd og 10 professorer.
I dag har foreningen 900 medlemmer heraf 66 medlemsvirksomheder

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

CBS Bestyrelsesuddannelserne – DEN KORTE VERSION



Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

Why and how Board and Management must prioritize Cybersecurity

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS OPGAVER og ANSVAR

Det vi godt ved…

Værdiskabelse … på alle planer og i forhold til alle bundlinjer - rimer i dag på digitalisering. Jo mere digitale virksomheders produkter og infrastruktur er, jo mere **sårbare er de over for cyberangreb.**

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

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

… og det handler ikke kun om IT – men også om **processer, ledelse, governance og ikke mindst mennesker…**

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

BESTYRELSENS OPGAVER og ANSVAR – slides fra konference i BF d. 28.aug 2024

Professor Jan Damsgaard / CBS

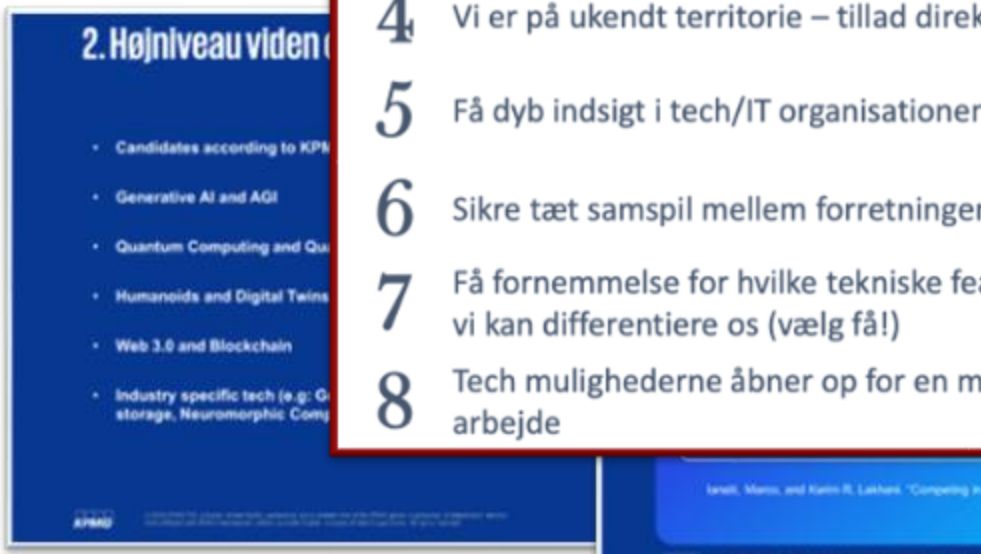
Bent Dalager / KPMG new Tech

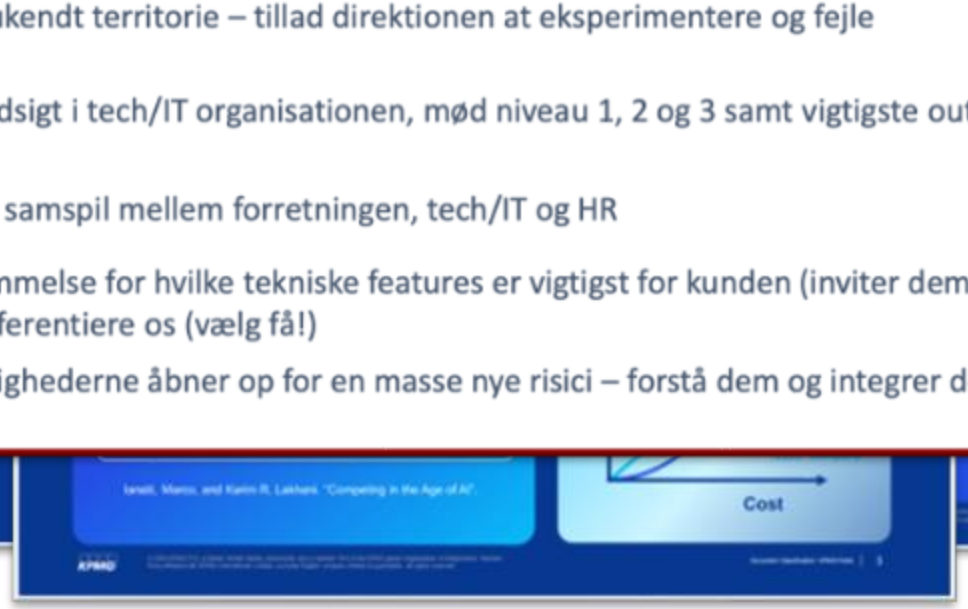
Søren Skibsted / Partner Kromann Reumert

… Så hvad er de bedste råd, jeg kan give til andre bestyrelser

Jacob Dahl / Best.medl. Danske Bank

1. Få nogle gode tech/IT profiler ind i bestyrelsen
2. …Men gør der til bestyrelsens **fælles** ansvar og integreret med overordnet strategi
3. Invester meget i uddannelse/opdatering af bestyrelsen – vær åben for mange eksterne perspektiver
4. Vi er på ukendt territorie – tillad direktionen at eksperimentere og fejle
5. Få dyb indsigt i tech/IT organisationen, mød niveau 1, 2 og 3 samt vigtigste outsourcing partnere
6. Sikre tæt samspil mellem forretningen, tech/IT og HR
7. Få fornemmelse for hvilke tekniske features er vigtigst for kunden (inviter dem ind) – og på hvilke måder vi kan differentiere os (vælg få!)
8. Tech mulighederne åbner op for en masse nye risici – forstå dem og integrer dem i risiko komiteens arbejde





Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

LEDELSENS OPGAVER og ANSVAR … og NY LOVGIVNING (NIS2 og DORA)

Kilde: Kromannreumert.dk

Ledelsens opgaver og ansvar

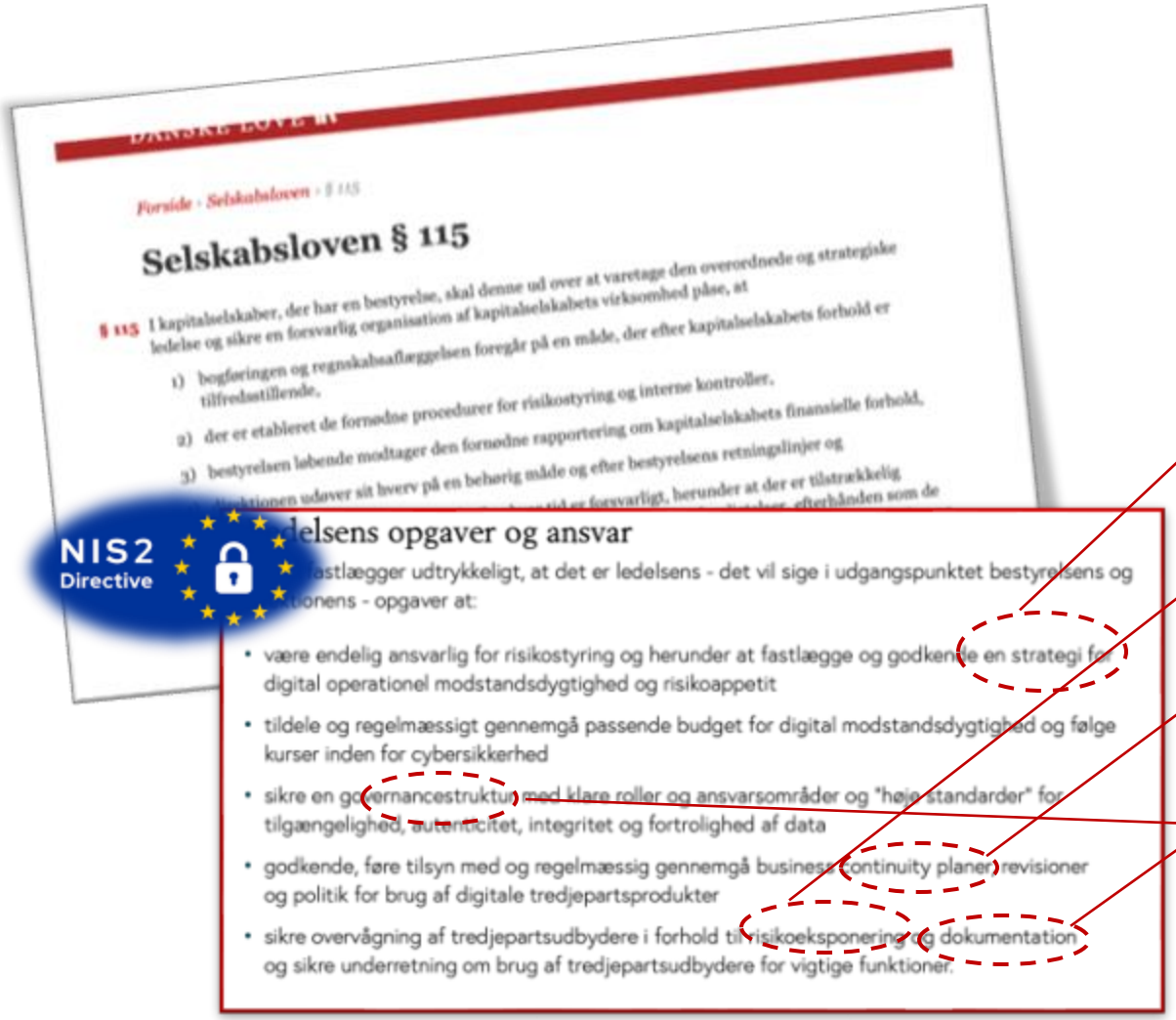
DORA fastlægger udtrykkeligt, at det er ledelsens - det vil sige i udgangspunktet bestyrelsens og direktionens - opgaver at:

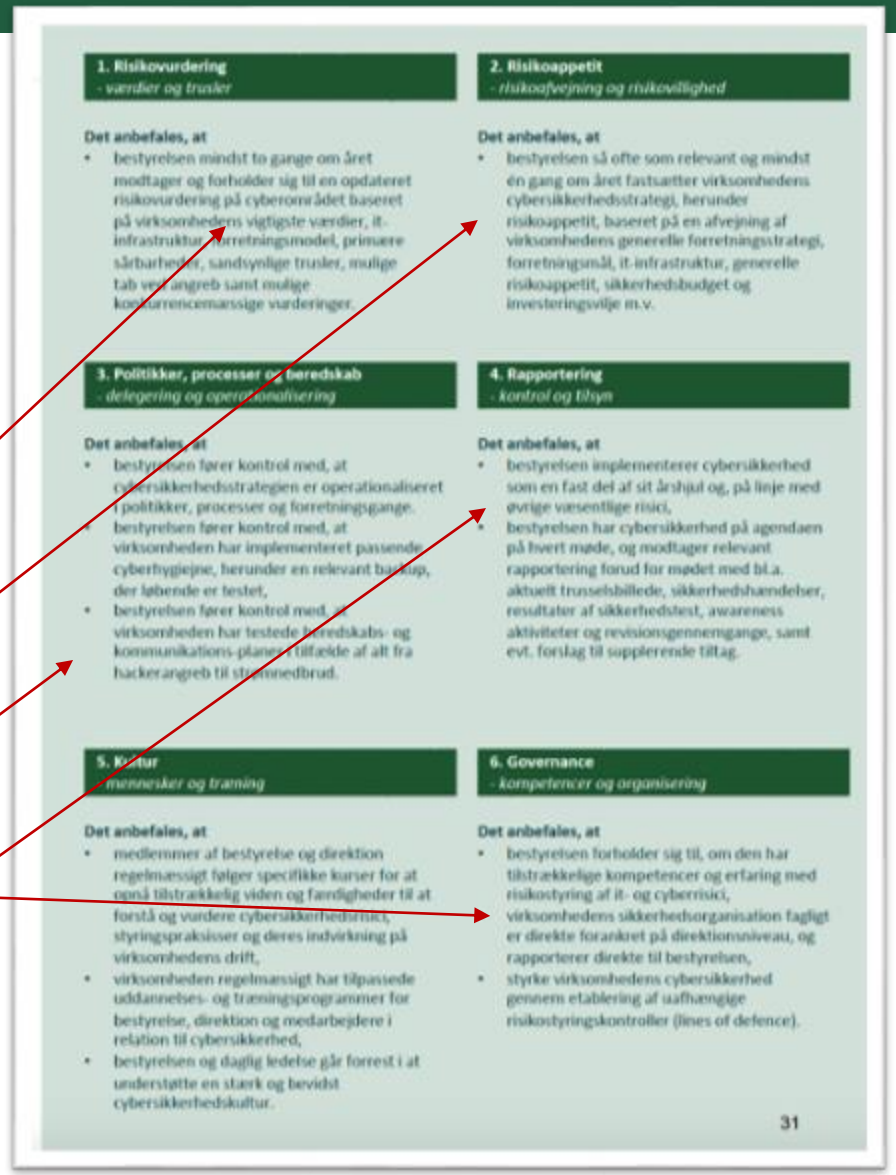
- være endelig ansvarlig for risikostyring og herunder at fastlægge og godkende en strategi for digital operationel modstandsdygtighed og risikoappetit
- tildele og regelmæssigt gennemgå passende budget for digital modstandsdygtighed og følge kurser inden for cybersikkerhed
- sikre en governancestruktur med klare roller og ansvarsområder og "høje standarder" for tilgængelighed, autenticitet, integritet og fortrolighed af data
- godkende, føre tilsyn med og regelmæssig gennemgå business continuity planer, revisioner og politik for brug af digitale tredjepartsprodukter
- sikre overvågning af tredjepartsudbydere i forhold til risikoeksponering og dokumentation og sikre underretning om brug af tredjepartsudbydere for vigtige funktioner.

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

LEDELSENS OPGAVER og ANSVAR … og NY LOVGIVNING (NIS2 og DORA)





Bestyrelsesforeningens Center for Cyberkompetencer

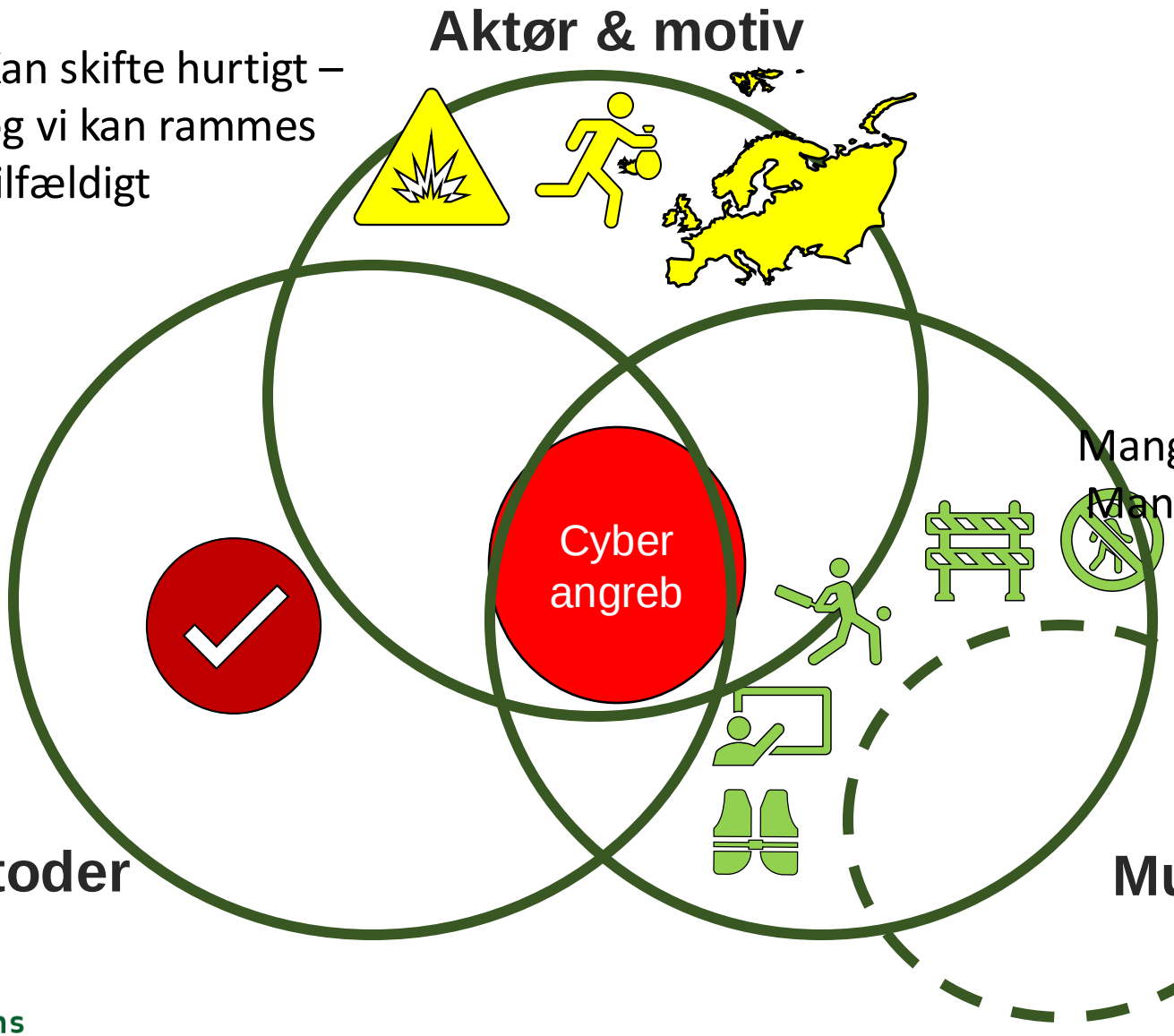
INDUSTRIENS FOND

Why and **how** Board and Management must prioritize Cybersecurity

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

VIRKELIGHEDEN FOR KOMMUNER OG VIRKSOMHEDER



Kan skifte hurtigt – og vi kan rammes tilfældigt

Desværre har de rigtig mange evner og metoder…

Dårlig systemssikkerhed
Manglende system adskillelse
Manglende fokus på adgange
Manglende træning
uopmærksomhed
Leverandører
Insidere
Osv osv …

INDUSTRIENS FOND

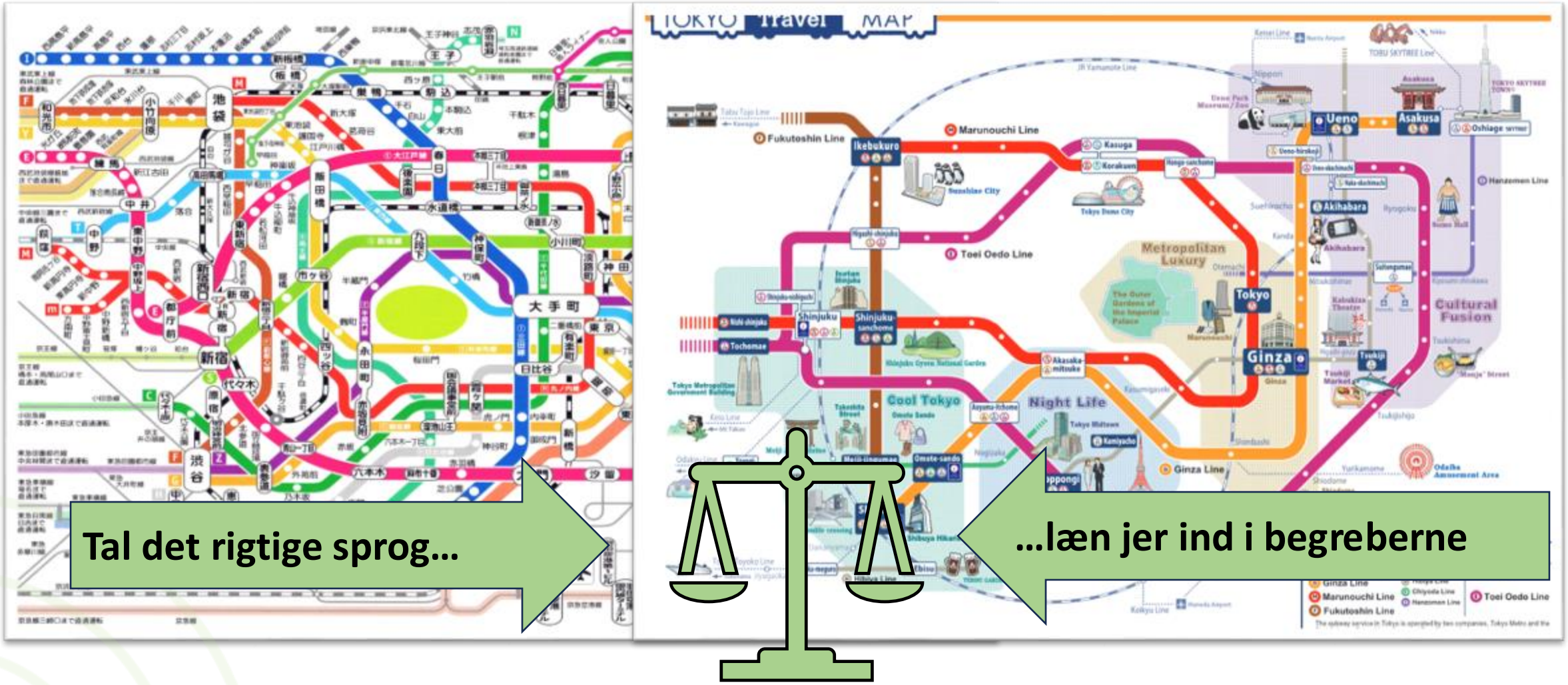
BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

- Det har vi outsourcet…
- Vi er ikke IT-specialister…
- Det har IT-Morten styr på…
- Vi har en forsikring…
- Det har vi i cloudløsninger

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

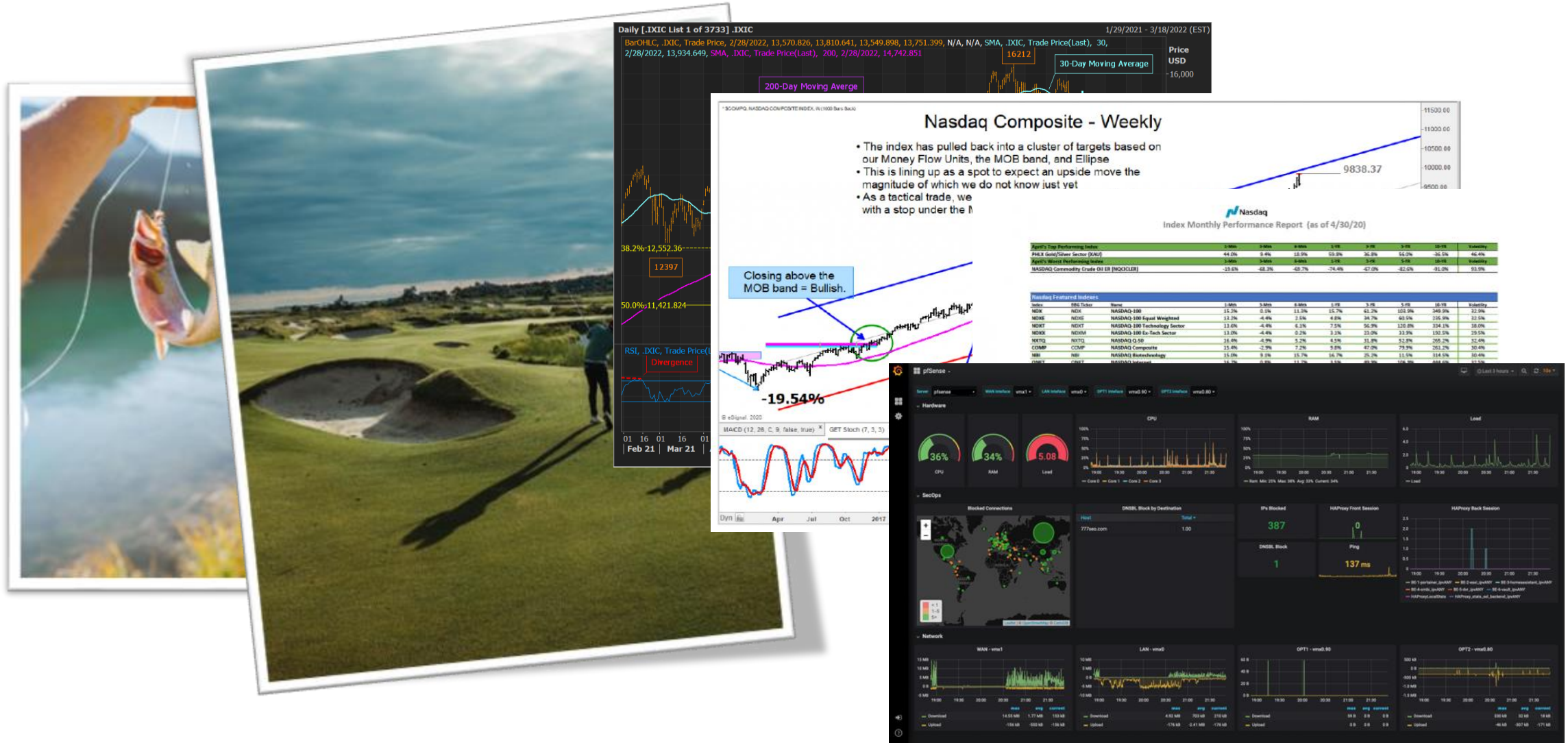
BESTYRELSENS ARBEJDE MED CYBERSIKKERHED



Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED



Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

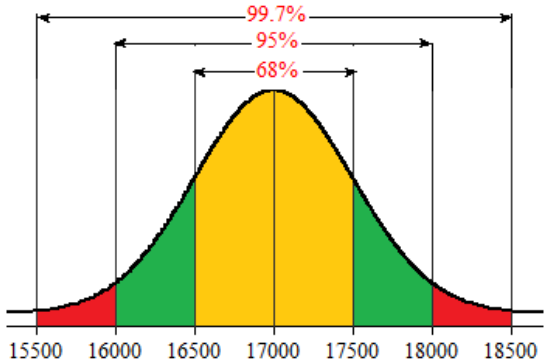
1

➢ Aktuel risikostatus
➢ Myndighedskrav
➢ Interne
➢ Eksterne
➢ Proje
➢ Syste
➢ Træning

2

Skab struktur - og vær konkret!

4



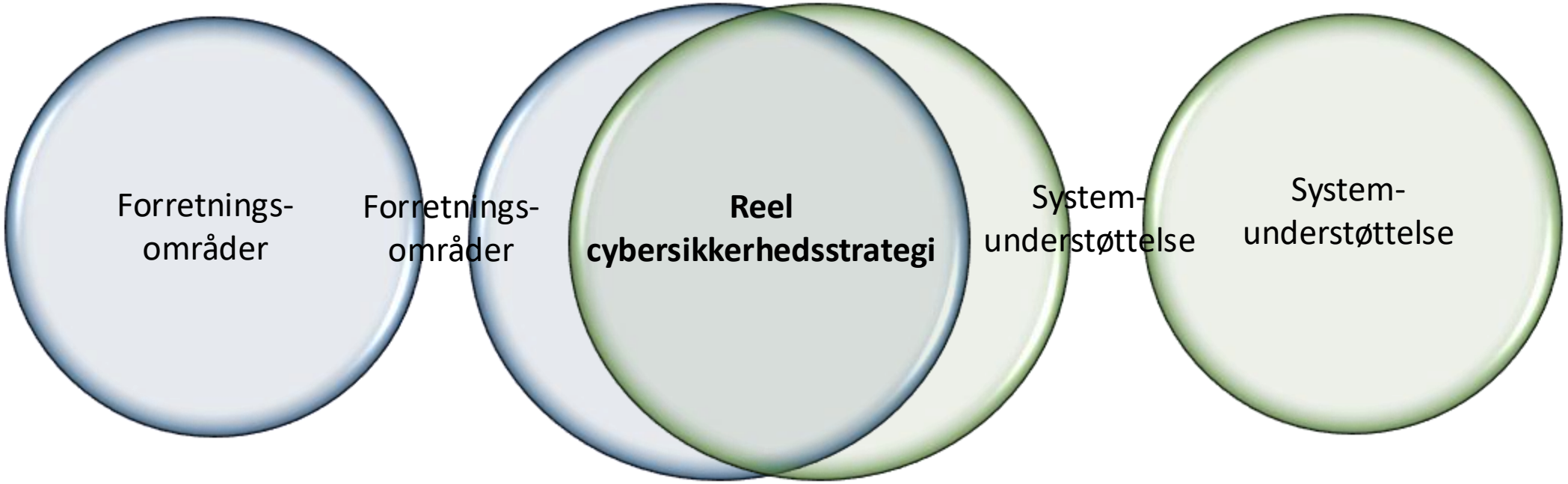
3

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

Skab indgang det rigtige sted
= forretningsområde versus systemfokus…

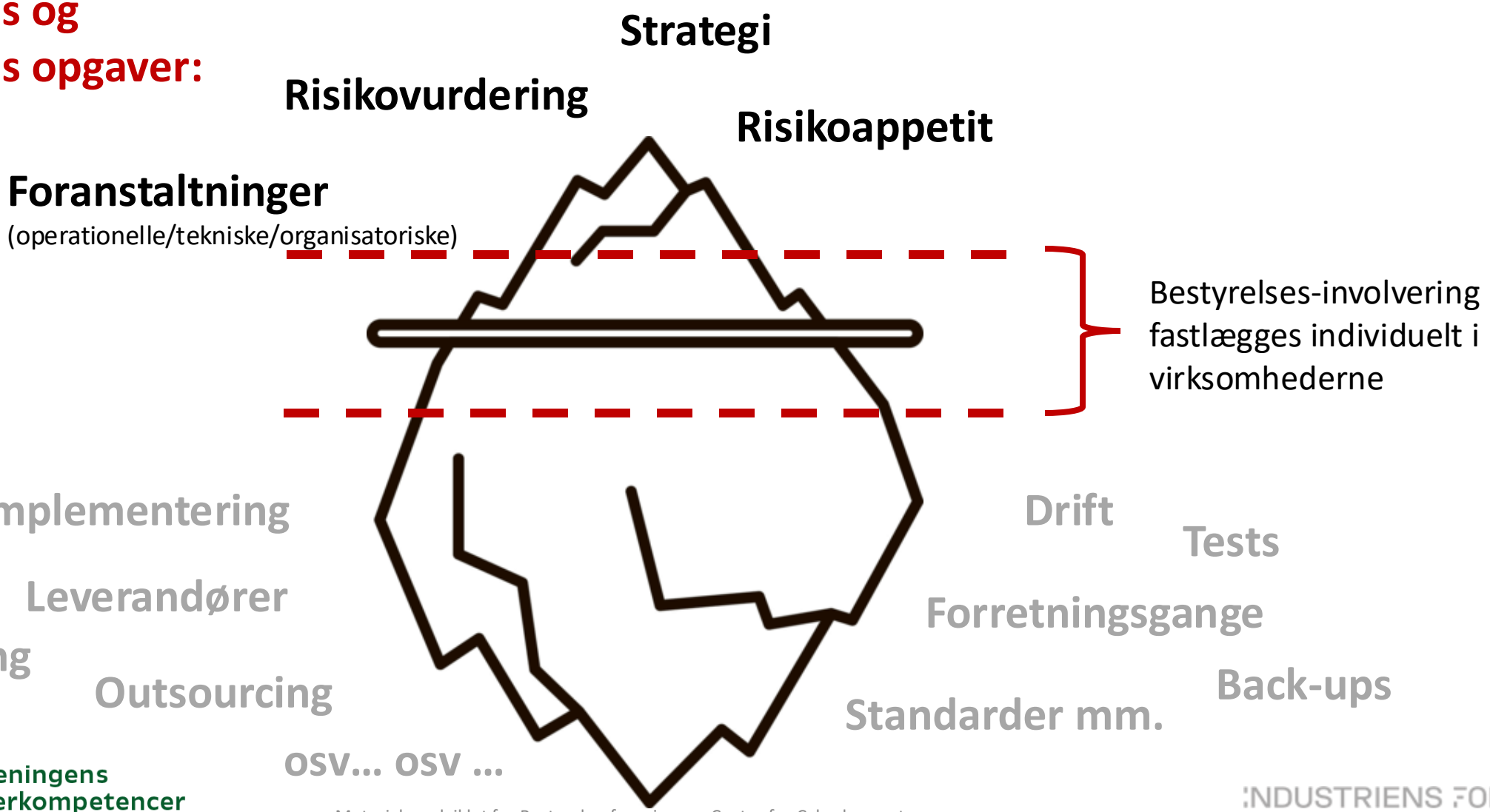


Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

Bestyrelsens og direktionens opgaver:



Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING september 2023

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING sep. 2023

1. Risikovurdering
- værdier og trusler

Det anbefales, at

- bestyrelsen så ofte som relevant og mindst én gang om året modtager og forholder sig til en opdateret **risikovurdering** på cyberområdet baseret på virksomhedens **vigtigste værdier, it-infrastruktur, forretningsmodel, primære sårbarheder, sandsynlige trusler**, mulige tab ved angreb samt mulige konkurrencemæssige vurderinger.

. Risikoappetit
- risikoafvejning og risikovillighed

Det anbefales, at

- bestyrelsen så ofte som relevant og mindst én gang om året fastsætter **virksomhedens cybersikkerhedsstrategi**, herunder **risikoappetit**, baseret på en afvejning af virksomhedens generelle **forretningsstrategi, forretningsmål, it-infrastruktur,** generelle risikoappetit, sikkerhedsbudget og investeringsvilje m.v.

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING sep. 2023 / TJEKLISTE

1. Risikovurdering – værdier og trusler

- Hvad er vores vigtige License to Operate (LtO) aktiver? (dvs. **hvad vil vi gerne beskytte**, hvad er vigtigt for vores forretning, hvad er kronjuvelerne?)
- Hvad truer vores vigtige LtO aktiver (**trusselsvurdering**)?
- Hvorfor skulle dette kunne ske (**sårbarhedsvurdering**)?
- Hvad er sandsynligheden for, at det sker?
- Hvad er konsekvensen af, at det sker (**konsekvensanalyse**)?
- Hvad **har vi gjort for at reducere risikoen** (i form af forebyggelse og beredskab)?

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

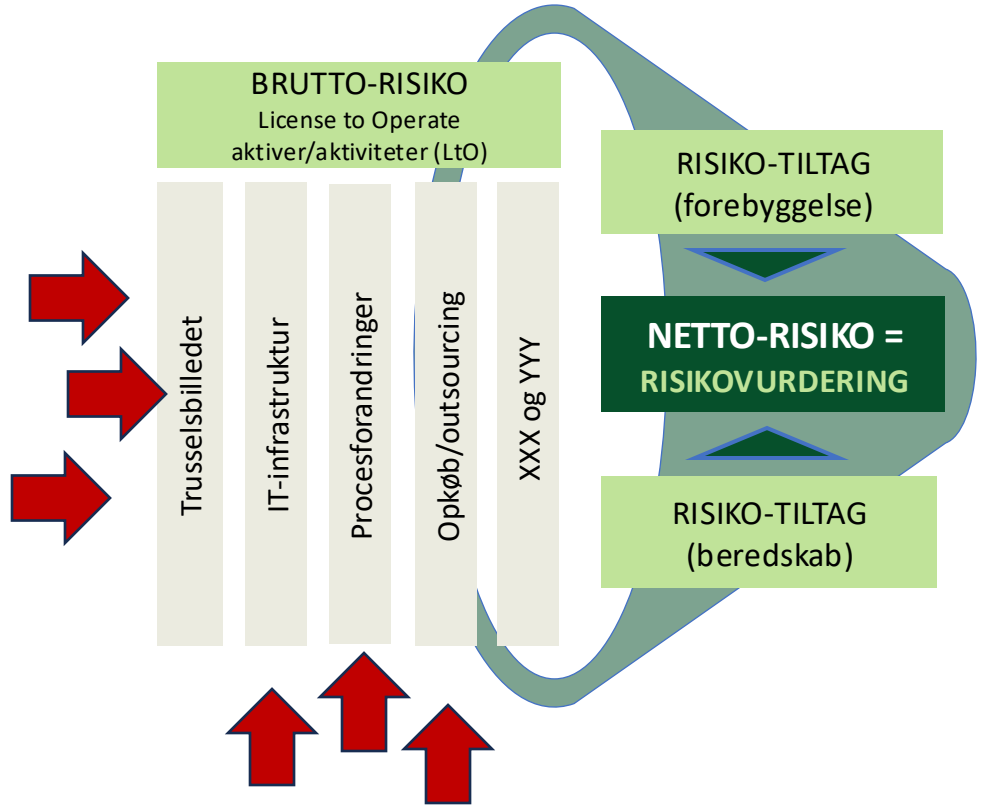
Tema 1 – License to Operate aktiver/aktiviteter LtO

Aktiver og aktiviteter fastsættes ift. strategi/formål/forretningsmodel

- Produktion
- Salg
- Administration
- Udviklingsafdelingen

Tema 1 - Risikovurdering

Udarbejdes af organisationen på baggrund af LtO aktiver og aktiviteter



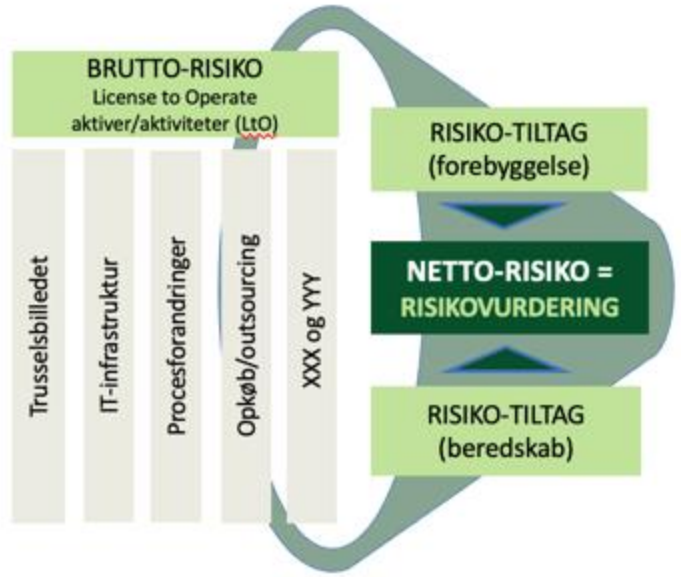
Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

LEDELSENS ARBEJDE MED CYBERSIKKERHED

Tema 1 - Risikovurdering

Tema 2 - Risikoappetit



C = Confidentialitet
(Fortrolighed = er data godt nok beskyttet)

- Medarbejderinformation
- Kundeinformation
- Leverandørinformation
- Patientinformation
- …

I = Integritet
(Pålidelighed = kan vi stole på data)

- Miljøcertificeringer
- Forureningsrapporter
- Farligt affald
- Byggetilladelse
- produktionsinstrukser
- …

A = Availability
(Tilgængelighed = kan vi komme til data)

- Arbejds-/kørelister
- Selvbetjeningsmodeller
- Hjemmeside
- …

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

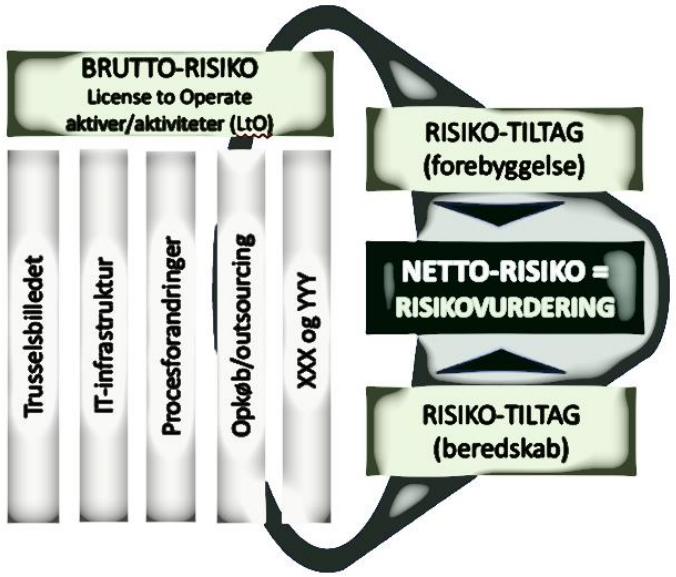
2. Risikoappetit – risikoafvejning og risikovillighed

- 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 kvalitetssikringsprocesser** (udvikling, indkøb, salg, outsourcing mv.)?
- 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.?

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

Tema 1 - Risikovurdering

Tema 2 - Risikoappetit



C = Confidentialitet
(er data godt nok beskyttet)

I = Integritet
(kan vi stole på data)

A = Availability
(kan vi komme til data)

RISIKO GAP =
ANBEFALINGER
inkl.
investeringsbehov

RISIKO
APPETIT/ACCEPT
Udtrykt i kr. / tid /
omdømme /
fortrolighedskrav
/ xxx

Bestyrelsen

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

Tema – 1 og 2
= Risikovurdering og Risikoappetit

Tema 3 og 4 = Daglig drift / operations samt dokumentation og rapportering

Bestyrelsen

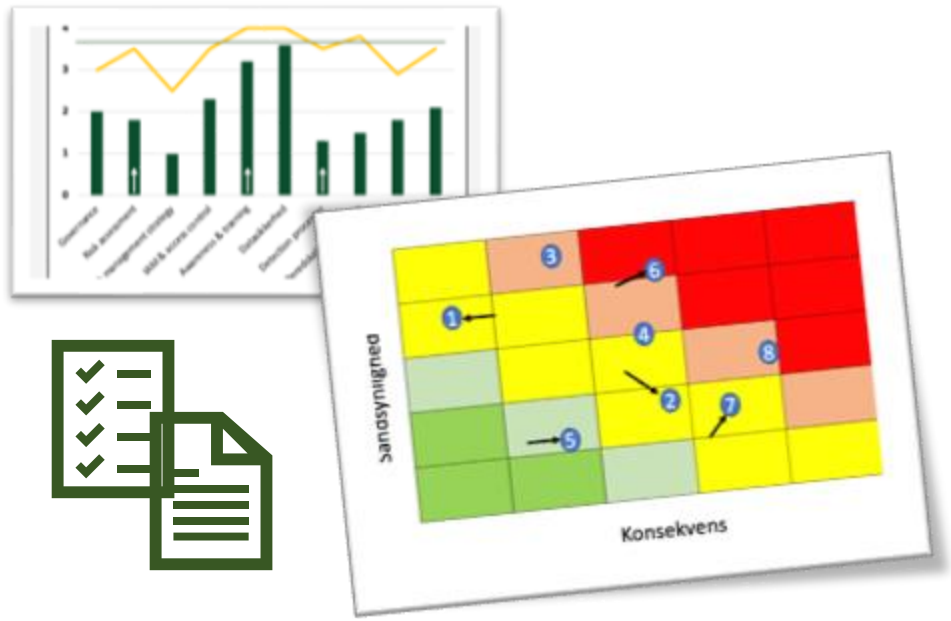
RISIKO GAP = ANBEFALINGER inkl. investeringsbehov

RISIKO APPETIT/ACCEPT Udtrykt i kr. / tid / omdømme / fortrolighedskrav / xxx

Tema 3
Politikker, processer og beredskab

Tema 4
Dokumentation, rapportering og kontrol

Identificer | Beskyt | Opdag | Håndter | Genopret



Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING sep. 2023

3. Politikker, processer og beredskab
- delegering og operationalisering

Det anbefales, at

- bestyrelsen fører **kontrol** med, at cybersikkerhedsstrategien er operationaliseret i **politikker, processer og forretningsgange.**
- bestyrelsen fører kontrol med, at virksomheden har implementeret **passende cyberhygiejne,** herunder en relevant **backup,** der løbende er testet,
- bestyrelsen fører kontrol med, at virksomheden har testede **beredskabs- og kommunikations-planer** i tilfælde af alt fra hackerangreb til strømnedbrud.

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.

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

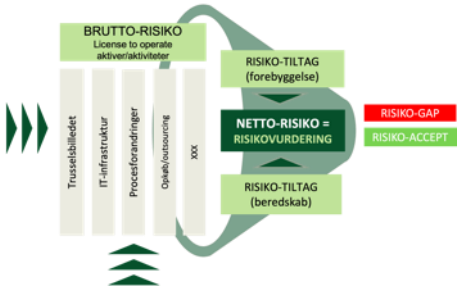
Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

BESTYRELSENS ARBEJDE MED CYBERSIKKERHED

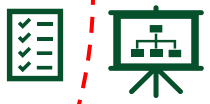
Tema 1
Risikovurdering

Tema 2
Risikoaccept

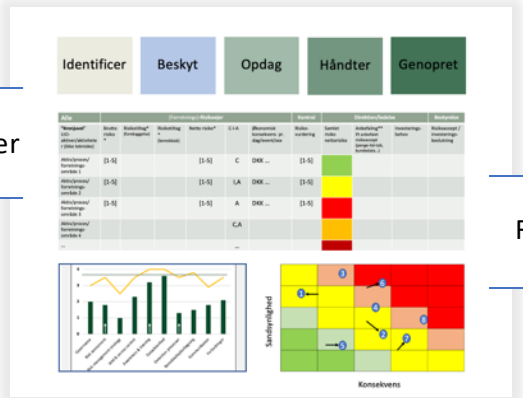


Tema 5
Kultur og mennesker

Tema 6
Organisering og governance



Tema 3
Politikker, processer og beredskab



Tema 4
Rapportering og kontrol

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING sep. 2023

5. Kultur
- mennesker og træning

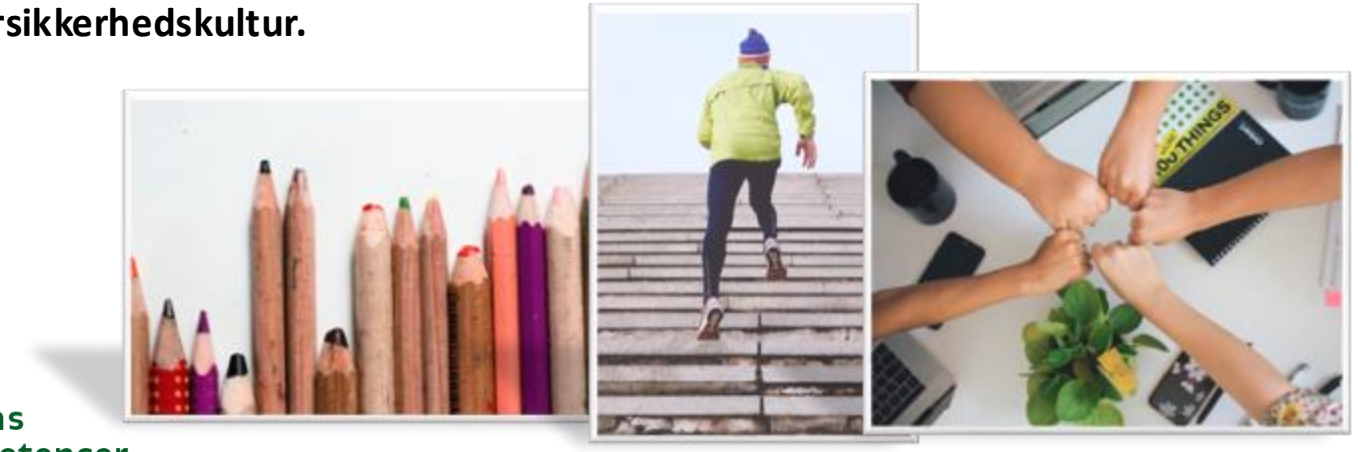
Det anbefales, at

- medlemmer af **bestyrelse og direktion regelmæssigt følger specifikke kurser for at opnå tilstrækkelig viden og færdigheder** til at forstå og vurdere cybersikkerhedsrisici, styringspraksisser og deres indvirkning på virksomhedens drift,
- virksomheden regelmæssigt har **tilpassede uddannelses- og træningsprogrammer for bestyrelse, direktion og medarbejdere** i relation til cybersikkerhed,
- bestyrelsen og daglig ledelse går forrest i at understøtte en stærk og bevidst **cybersikkerhedskultur.**

6. Governance
- kompetencer og organisering

Det anbefales, at

- bestyrelsen forholder sig til, om den har tilstrækkelige **kompetencer og erfaring** med risikostyring af it- og cyberrisici,
- virksomhedens sikkerhedsorganisation fagligt er direkte forankret på direktionsniveau, og rapporterer direkte til bestyrelsen,
- styrke virksomhedens cybersikkerhed gennem etablering af **uafhængige risikostyringskontroller** (lines of defence).



Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

BCFC.DK

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

… og BESTYRELSENS KOMPAS – er som altid :

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

TAK FOR I DAG

…og lad os sammen styrke cybersikkerheden i Danmark

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND