KROMANN REUMERT

Operational resilience | Cybersecurity | Data economy | Privacy | New technologies

Kommende EU-regulering på cyberområdet i et strategisk perspektiv

Hvordan forbereder man sig bedst på EU-krav på cyberområdet

Dansk Standard og Bestyrelsesforeningen | 18. september 2023

Christel Teglers | Advokat og partner | Kromann Reumert

EU skruer op for beskyttelsen af det digitale

Artificial Intelligence

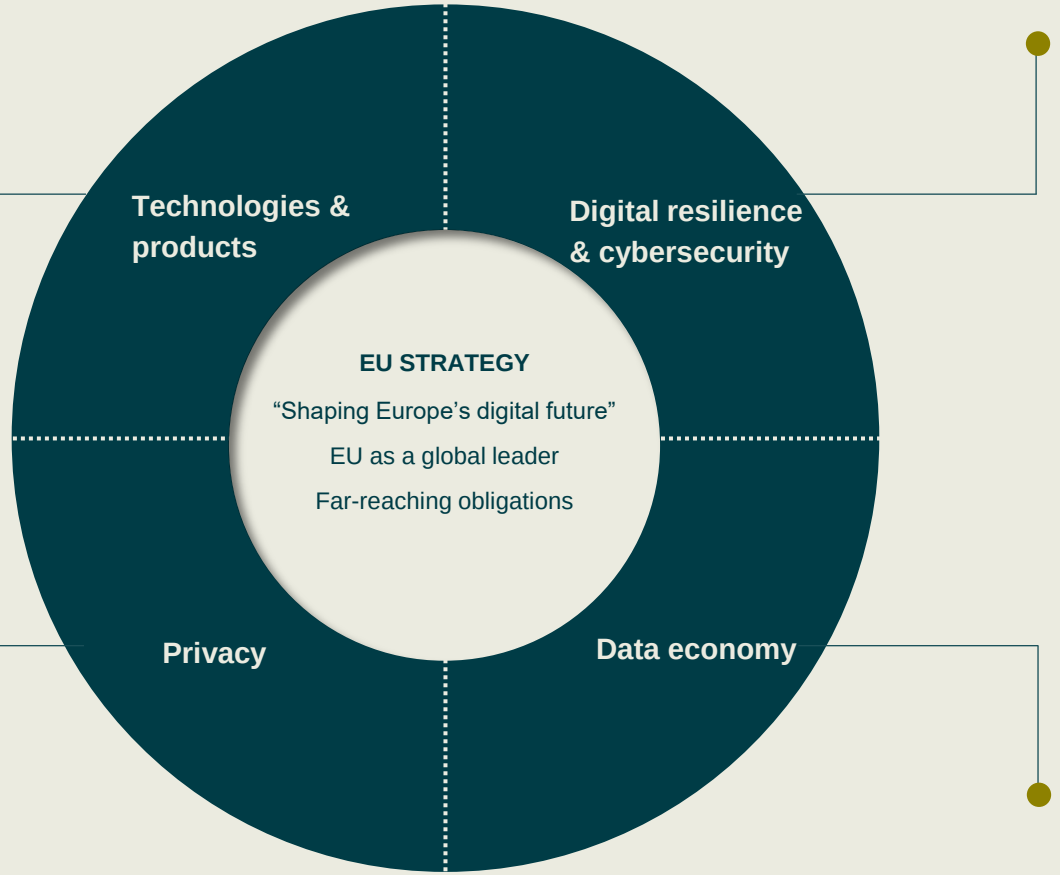
- AI Act
- New Product Liability Directive
- AI Liability Directive

IoT products

- Cyber Resilience Act

Industry specific regulations

- ePrivacy Regulation
- GDPR



Organisational level

- NIS2
- DORA
- Resilience of Critical Entities

Platforms

- Digital Services Act
- Digital Markets Act

Open data

- Data Governance Act
- Sector data spaces
- Data Act

To centrale reguleringer på cyberområdet

NIS2

Nyt horisontalt EU direktiv med mindstekrav til cybersikkerhed. Bøder og ledelsesansvar (direktion og bestyrelse). Gældende i DK fra **18. oktober 2024**.

DORA

Ny forordning med krav til digital og operational resiliens indenfor den finansielle sector. Ledelsesansvar (bestyrelse og direktion). Lex specialis ift. NIS2. Gældende i DK fra **17. januar 2025**.

Bekræfter ledelsens ansvar for styring af (digitale) risici

Artikel 20

Styring

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.

Artikel 5

Forvaltning og organisation

1. Finansielle enheder skal have indført en intern forvaltnings- og kontrolramme, der sikrer en effektiv og forsigtig styring af IKT-risiko, i overensstemmelse med artikel 6, stk. 4, for at opnå et højt niveau af digital operationel modstandsdygtighed.

2. Ledelsesorganet i den finansielle enhed fastlægger, godkender, fører tilsyn med og har ansvar for gennemførelsen af alle ordninger vedrørende de rammer for IKT-risikostyring, der er omhandlet i artikel 6, stk. 1.

Med henblik på første afsnit er det ledelsesorganet, som

a) har det endelige ansvar for styringen af den finansielle enheds IKT-risiko

Selskabsloven

§ 115

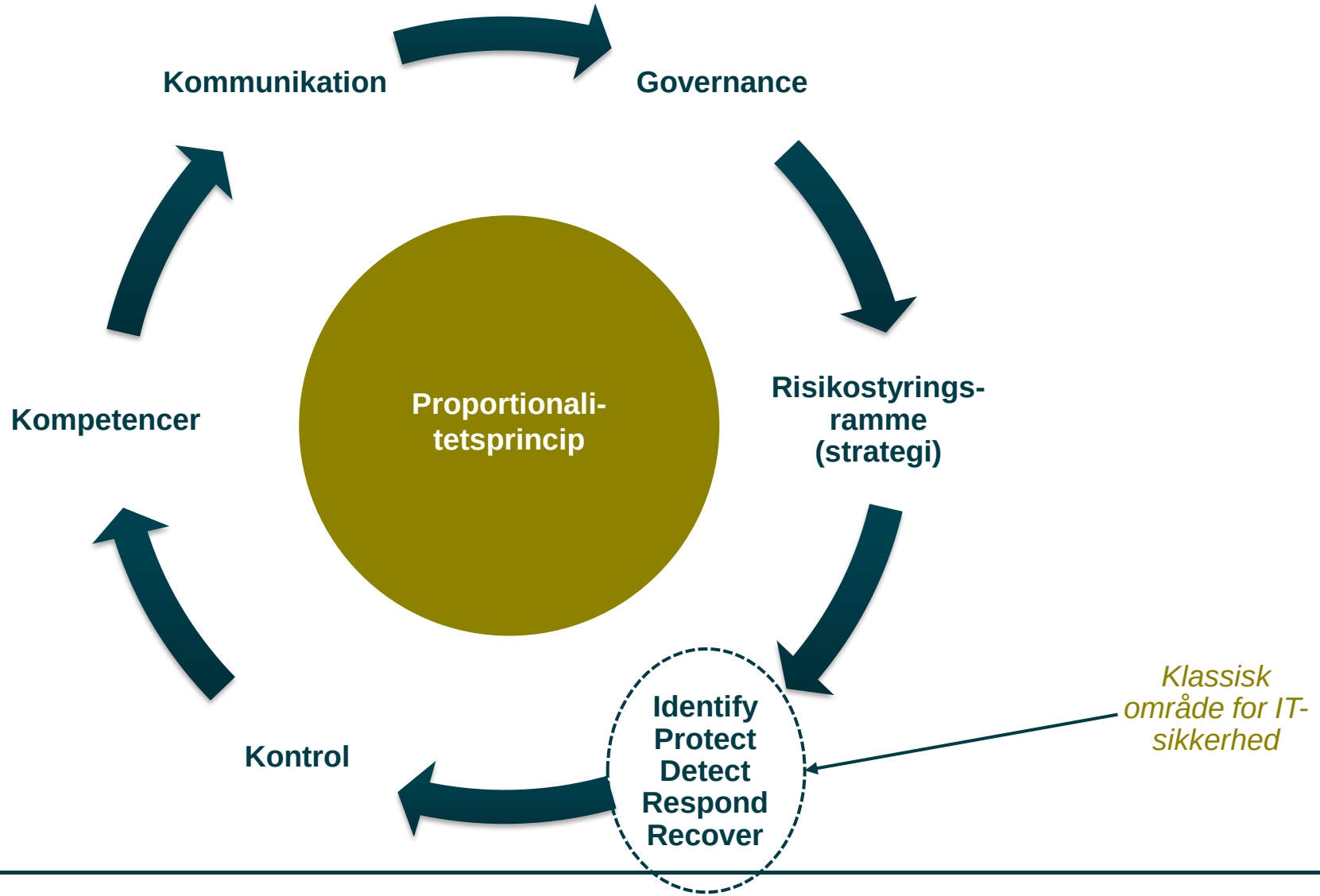
755 I kapitalselskaber, der har en bestyrelse, skal denne ud over at varetage den overordnede og strategiske ledelse og sikre en forsvarlig organisation af kapitalselskabets virksomhed 756 påse, at

1) bogføringen og regnskabsaflæggelsen foregår på en måde, der efter kapitalselskabets forhold er tilfredsstillende, 757

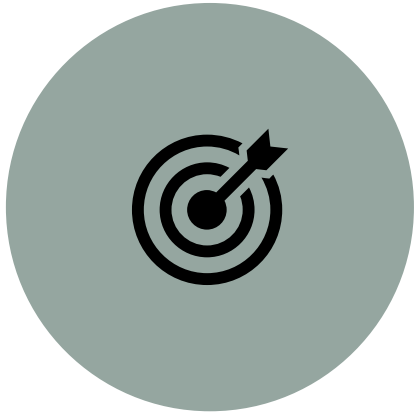
2) der er etableret de fornødne procedurer for risikostyring og interne kontroller, 758

Bestyrelse (og direktion) kan ifalde ansvar for utilstrækkelig risikostyring og sikkerhedsbrud efter almindelige regler (det ændrer NIS2 og DORA ikke på)

NIS2 og DORA (meget!) kort fortalt

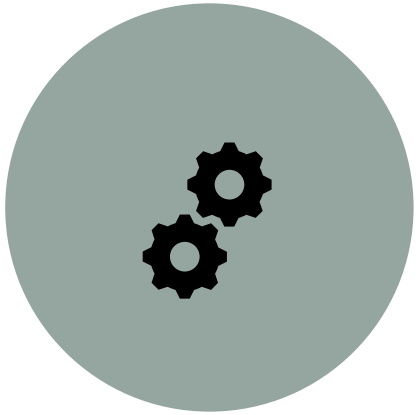


Digital risikostyring er i udgangspunktet operationelt men går på tværs af risikoområder



Strategiske risici

Finansielle risici



Operationelle risici

Juridiske risici

Hvordan ser det ofte ud i organisationerne?

”Cybersikkerhed har høj prioritet. Det har vi også meddelt ledelsen. Så vidt vi er orienteret, har vi et højt sikkerhedsniveau.”

”Den digitale understøttelse er helt afgørende for vores forretning (men ikke vores kerneydelse). Det ligger under CFO. IT og CISO arbejder med mange tiltag, vi løbende får rapporteret.”

Udvikling

”Sikkerhed og compliance skal ikke obstruere vores arbejde – det er os, der skaber værdi”

IT / CISO

”Vi ejer IT og informations-sikkerhed – NIS2/DORA er et projekt under vores ansvar.”

LEGAL

”Det handler vist mest om teknik. Juras rolle ser begrænset ud – bare det ikke bliver et nyt GDPR projekt.”

RISK

”Vi kontrollerer ikke IT/digitale risici – er det ikke CISO’s opgave?”

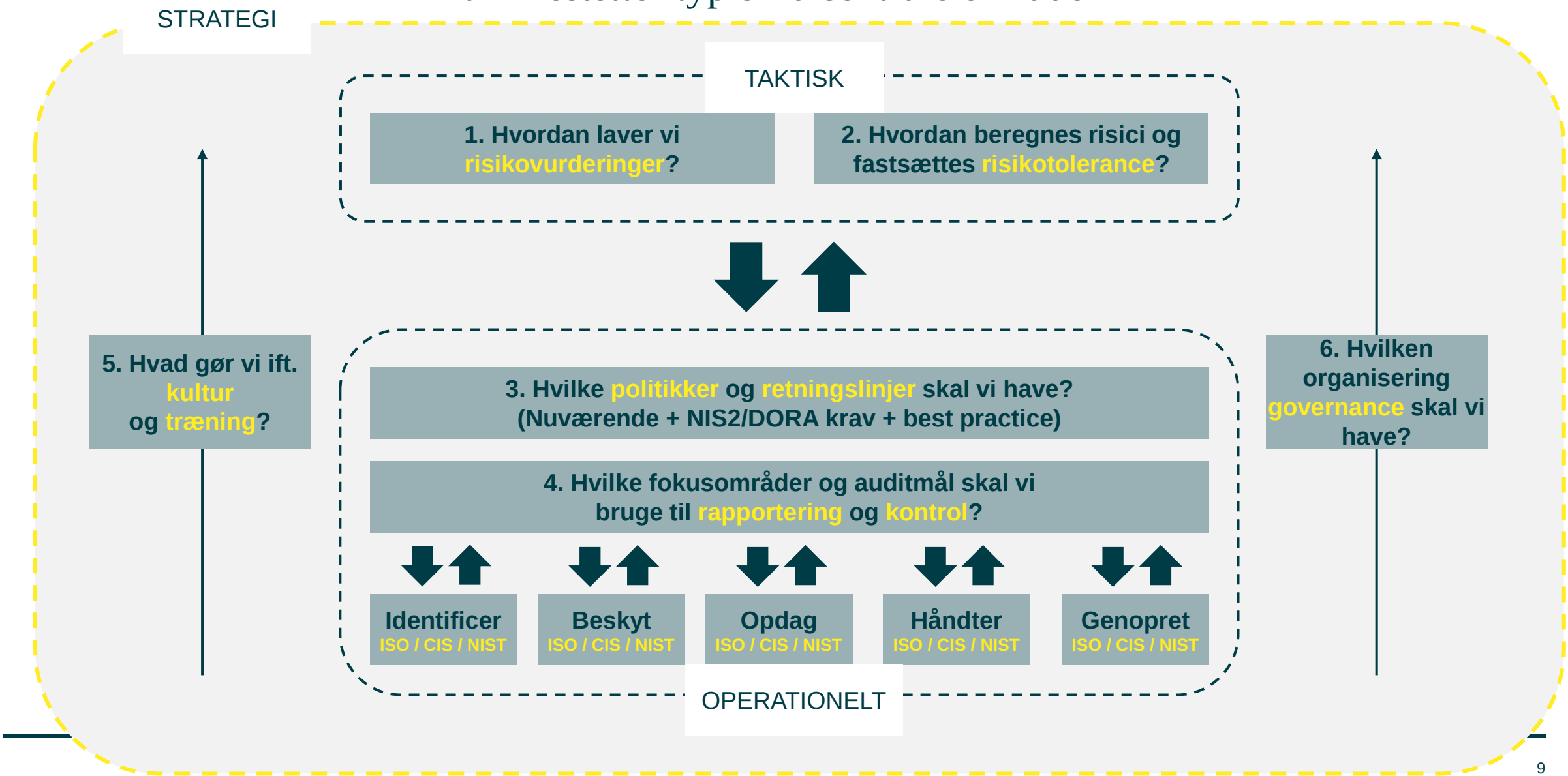
COMPLIANCE / INDKØB

”Det ser omfattende ud – er der et certifikat eller en standardliste vi kan bruge til udbud og compliance?”

DPO

”Gad vide hvordan dette hænger sammen med GDPR?”

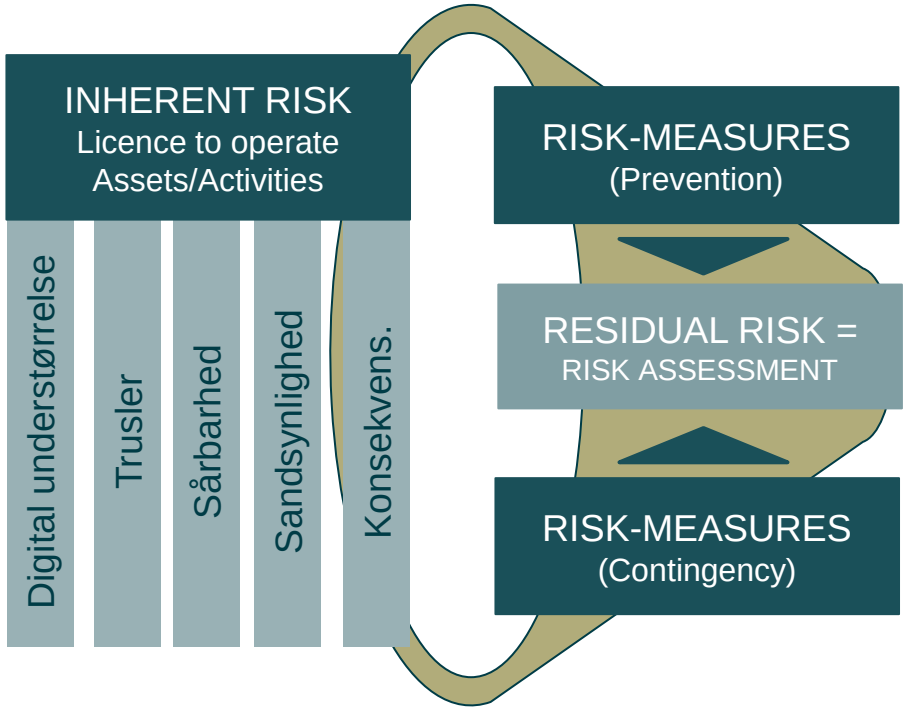
En overordnet ledelsesgodkendt (digital) risikostyringsstrategi rammesætter typisk 6 centrale områder



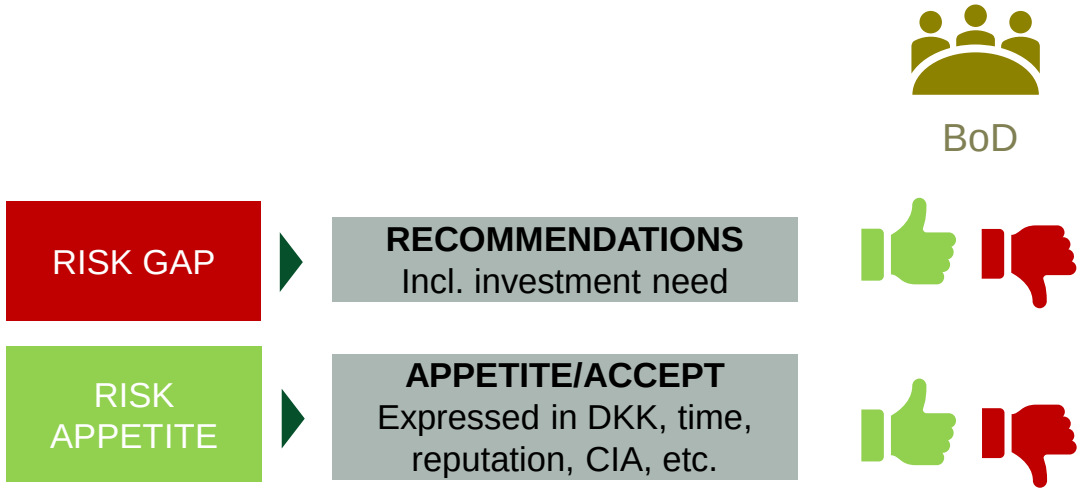
Fælles forståelse af hvad risiko er, hvornår risiko er væsentlig/uvæsentlig, hvordan risici kvantificeres / kvalificeres og hvem-gør-hvad-hvornår-og-hvordan er afgørende

(og dette skal ledelsen rammesætte)

Risikovurdering



Risikotolerance



Tre basale spørgsmål ledelsesrepræsentanter bør stille sig selv

1. Har vi kortlagt organisationens "license to operate" aktiver og hvordan de er digitalt understøttet?

2. Forstår vi hvordan disse aktiver er eksponeret for (digitale) risici?

3. Har vi en ledelsesgodkendt strategi og governance på plads til at beskytte de digitale aktiver og håndtere potentielle angreb, fejl eller nedbrud?

Kontakt

Christel Teglers
Partner, København

Mob. +45 61 61 30 34

cht@kromannreumert.com