

BESTYRELSENS PRAKTISKE ERFARINGER MED MODSTANDSDYGTIGHED

Kurt Nørrisgaard, bestyrelsesmedlem

BOARD OFFICE – PRAKTISK TILGANG OG ERFARINGER

1. Introduktion til Board Office A/S, kunder og produkter
2. Tilgang til risikostyring
3. Forståelse af outsourcing
4. Bestyrelsens involvering i risikostyring og mitigering
5. Kompetencer i organisation og hos samarbejdspartnere
6. Kontrolregime
7. Bestyrelsens tilbagevendende involvering



BOARD OFFICE

Virksomheden:

- Ansatte < 10
- Det meste it er outsourcet
- Privatejet

Kunder:

- Bestyrelser for danske og skandinaviske virksomheder
- Bestyrelseskandidater

Partnere:

- Nordea, Danske Advokater, Dansk Erhverv, Alm. Brand Group

Produkter:

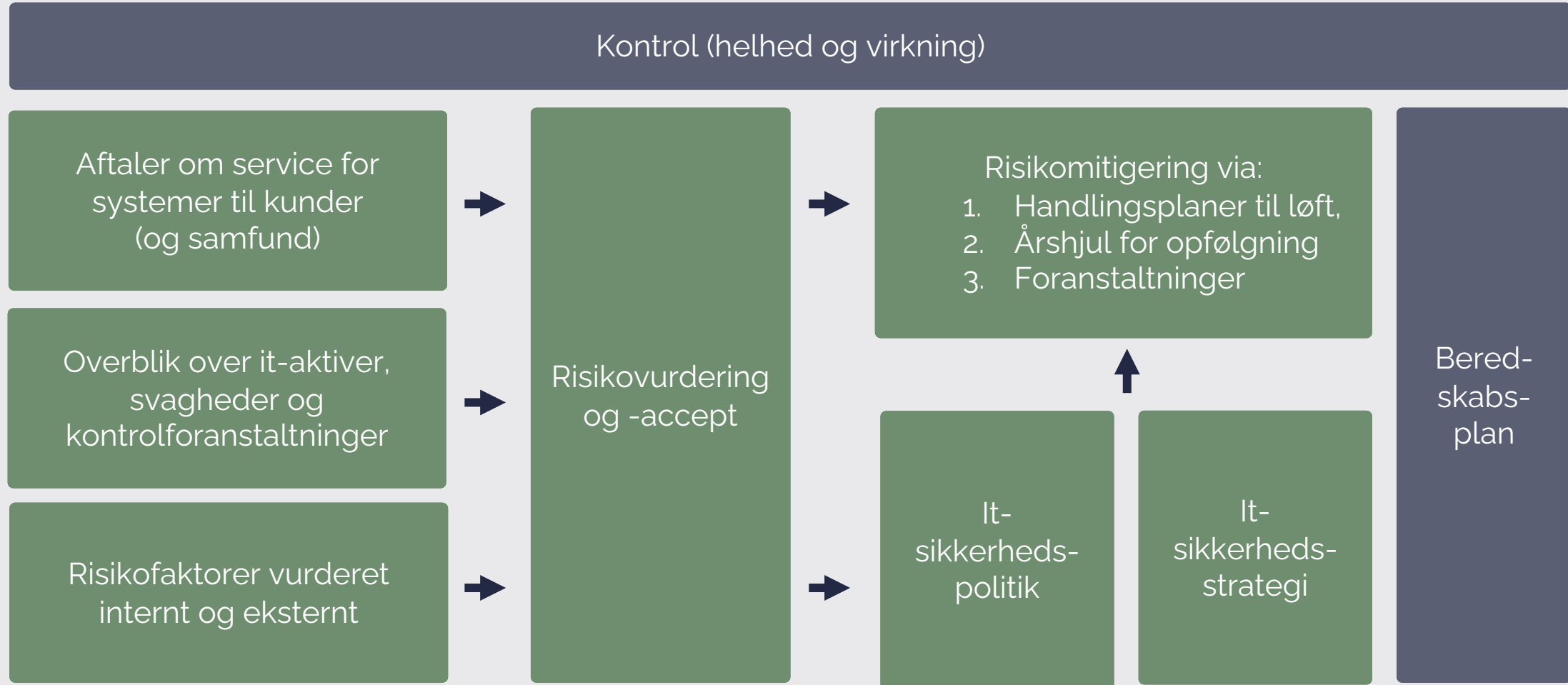
Bestyrelsesportal samt portal med CV'er med

- Effektiv administration rundt om bestyrelsens virke
- Krypteret dokumentopbevaring, mails og beskeder.
- Datarum
- Specifik tildeling af adgangsforhold til bestyrelses- og ledelsesmedlemmer, bank, advokat, revisor etc.
- GDPR-klassificering af informationer
- Underskriftsrum med Nem-ID, Mitid mv.

Data:

- Bestyrelsesmaterialer, referater, strategier, bestyrelsesevalueringer etc.
- Legitimation af bestyrelsesmedlemmer (sundhedskort, pas, kørekort ..)
- Dialoger med bank, revision, advokat
- CV'er

MODSTANDSDYGTIGHED HANDLER OM RISIKOSTYRING OG MITIGERING



Fokus i denne context er it-risikostyring med formål at hindre og reducere manglende systemtilgængelighed og misbrug af systemer (cyber og internt) herunder håndtering af informationssikkerhed.

PRAKTISKE EKSEMPLER PÅ, HVAD VI GØR

Risikoarbejdet:

- Er ikke certificerede, men anvender ISO27001 og ISO27002. Leverandører er certificerede
- Risikovurdering - sikkerdigital.dk – gode værktøjer
- Skeler til NIST-frameworket
- Egenkontrol ift ISAE 3000 (GDPR)

Risikotolerance:

- Sikkerhedspolitik og
- Sikkerhedsstrategi (fx dataopbevaring og teknologiappetit)

Foranstaltninger:

- Databehandleraftaler
- Medarbejderhåndbog og uddannelse
- Procesbeskrivelser og procedurer
- Kryptering
- D-mærket - drøftes

Beredskabsplan:

- Afprøvninger
- Cyberforsikring (tab og prioritet)

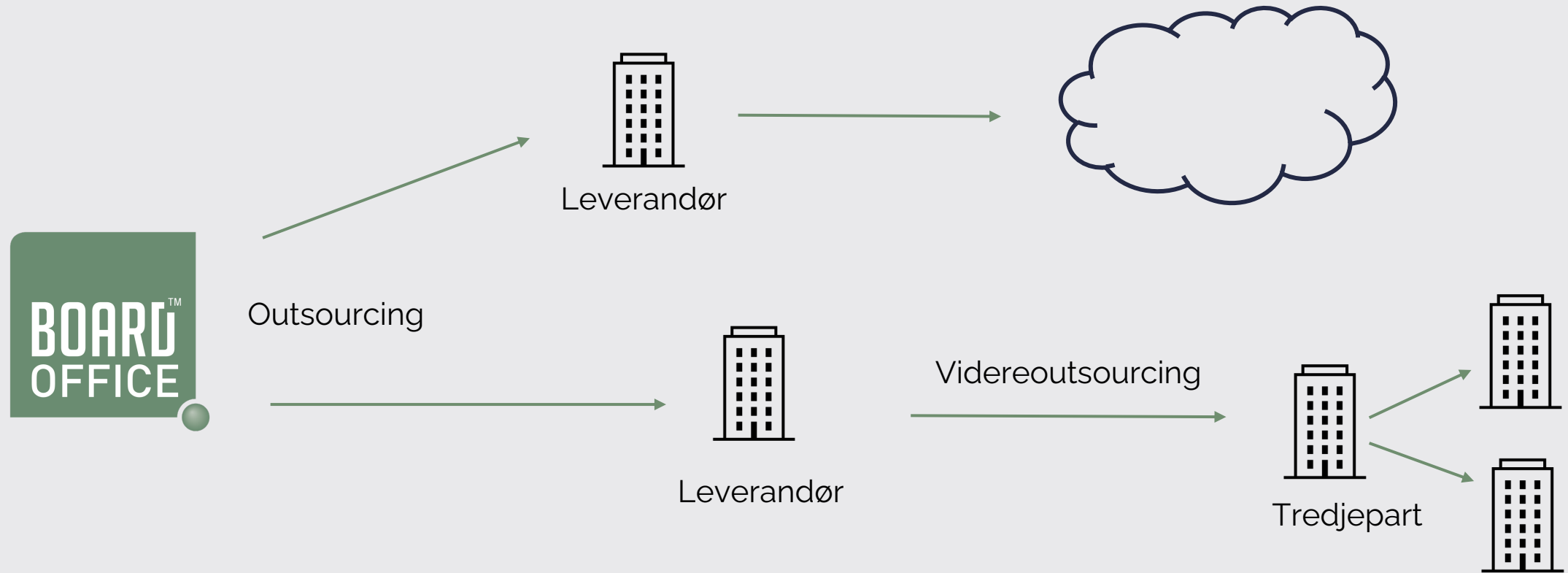
Kontrol:

- ISAE 3000 og ISAE 3402-erklæringer fra centrale leverandører
- Årlig kontrol af leverandører og deres cybertests
- Revision – planlagt

Bestyrelsen:

- Årshjul
- Bestyrelseskompetence
- Inspiration i bestyrelsesforeningens vejledninger

KRITISK/VIGTIG OUTSOURCING SKAL FORSTÅS



- Leverancekædens kvalitet
- Ændringer i leverancekæden – incl. muligheder for exit
- Leverancekædens sammensætning i kritiske situationer fx økonomisk og operationelt

BESTYRELSEN SER OG GODKENDER CENTRALE DOKUMENTER

Kontrol (helhed og virkning)

3000 og 3402-
erklæringer

Aftaler om service for
systemer til kunder
(og samfund)

Overblik over it-aktiver,
svagheder og
kontrolforanstaltninger

Risikofaktorer vurderet
internt og eksternt

Risikovurdering
og -accept

Risikomitigering via:

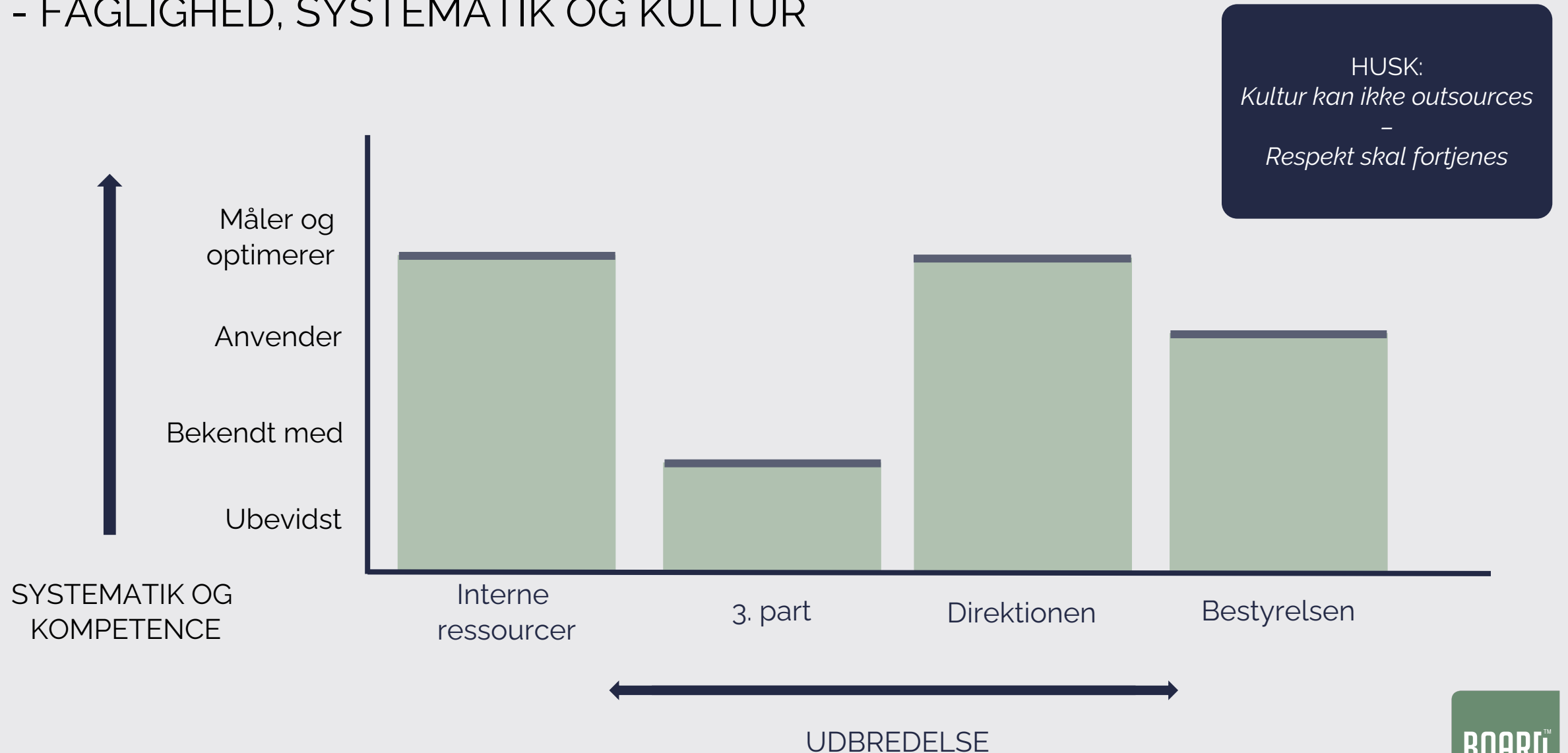
1. Handlingsplaner til løft,
2. Årshjul for opfølgning
3. Foranstaltninger

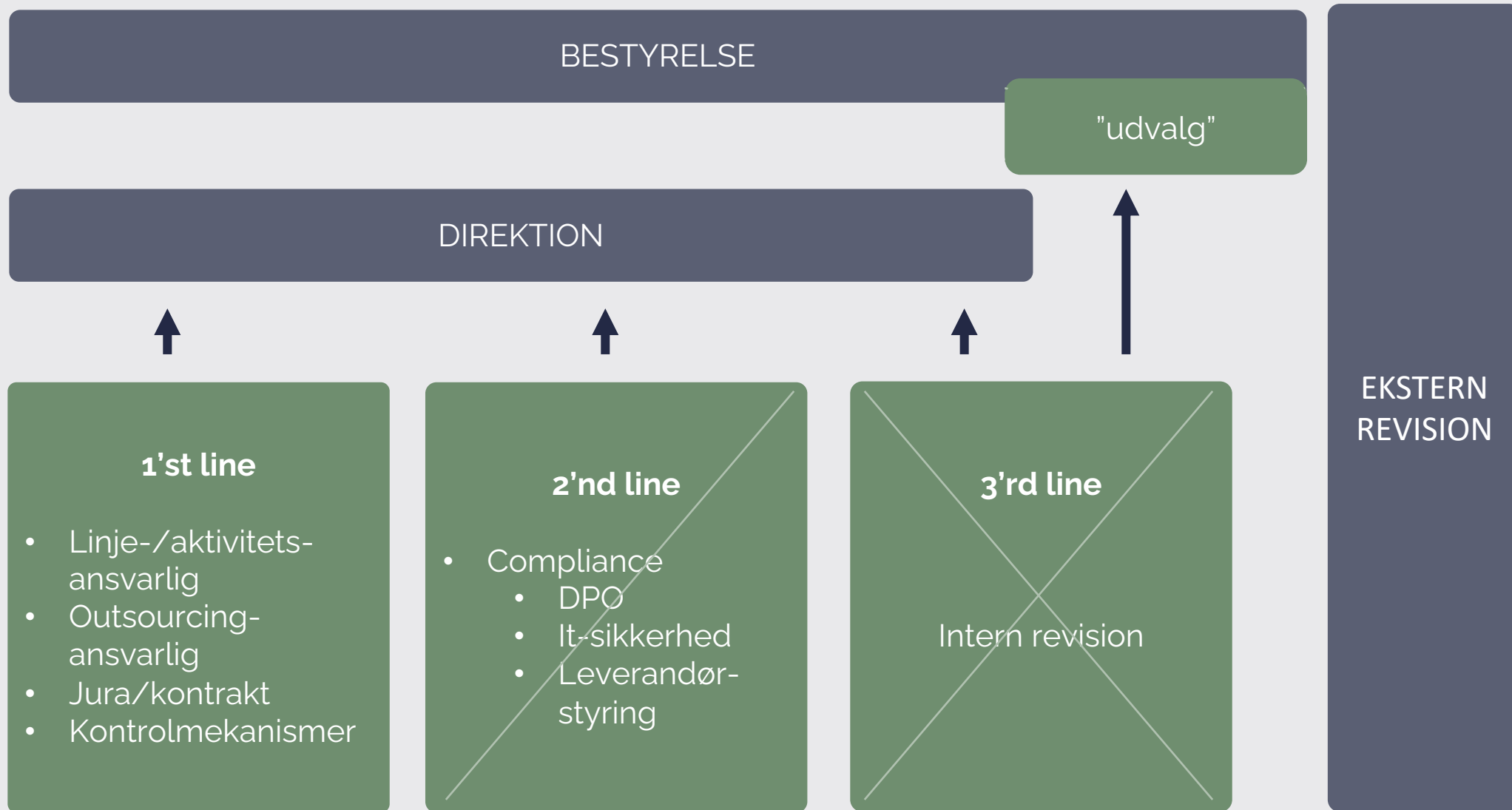
It-
sikkerheds-
politik

It-
sikkerheds-
strategi

Bered-
skabs-
plan

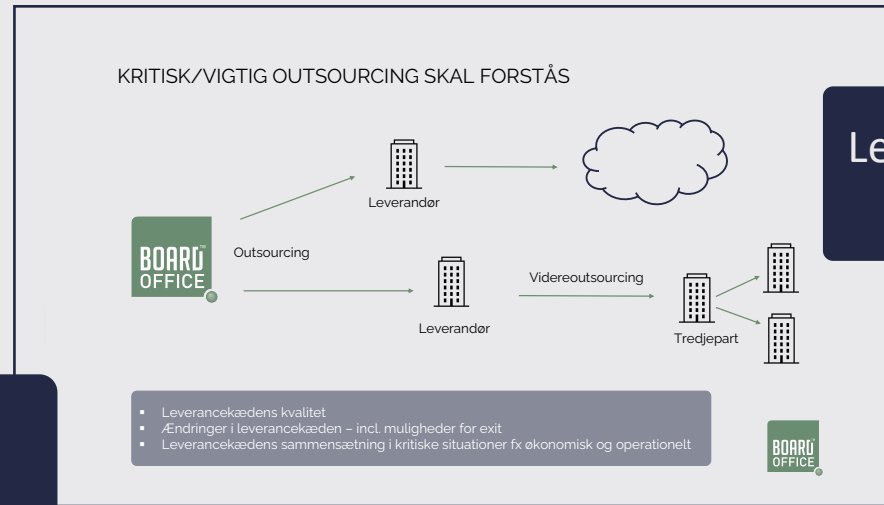
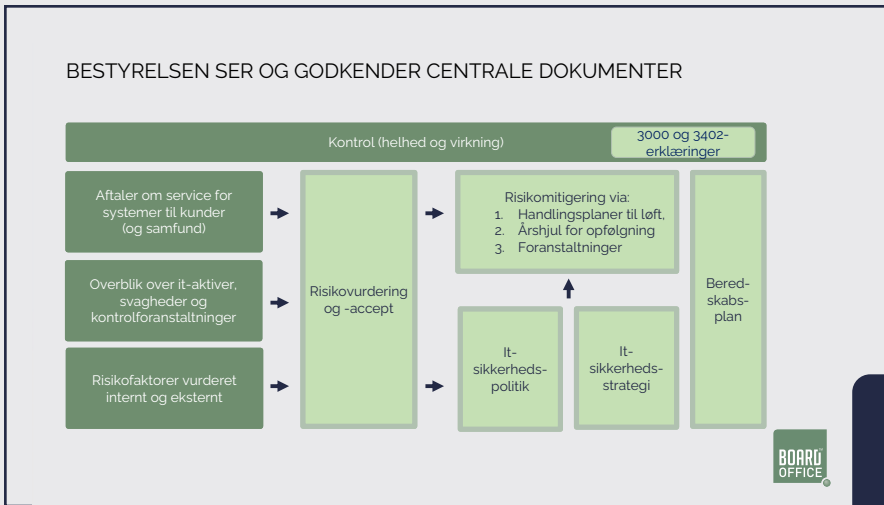
ALIGNMENT AF SPECIALISTER, LEDELSE, DIREKTION OG BESTYRELSE - FAGLIGHED, SYSTEMATIK OG KULTUR



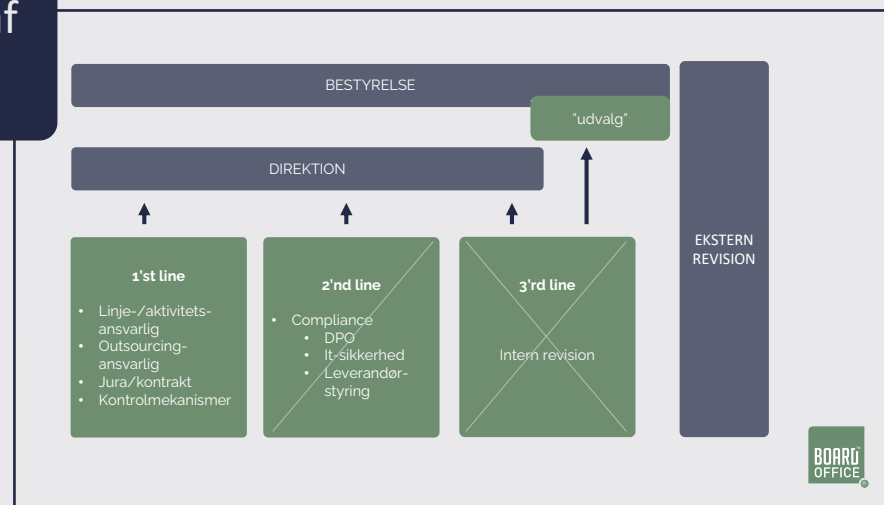
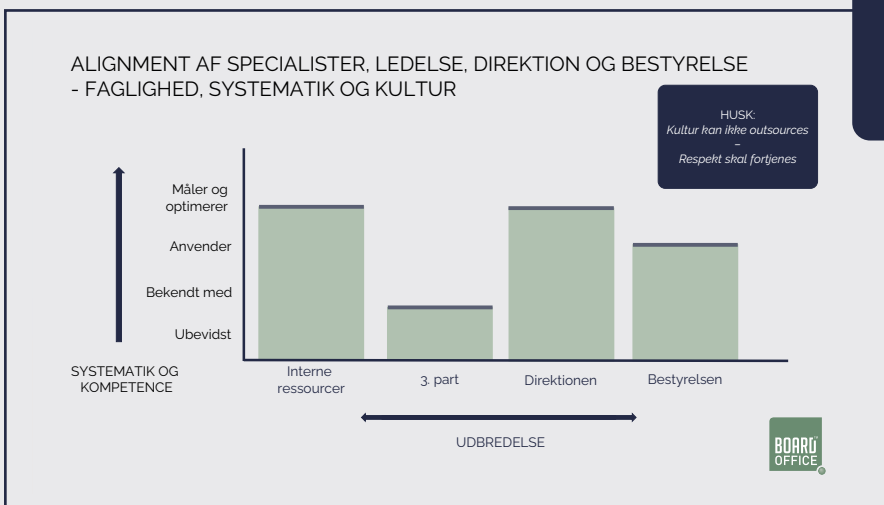


BESTYRELSENS ANSVAR KAN IKKE OUTSOURCES

- Betyggelse sker via indsigt, drøftelser, godkendelser og kontrol



Interesse
-
Vedligeholdelse af viden





SPØRGSMÅL?



kurt"@kn-consiglio.dk



+45 40 14 20 81

