DS Cyberdag

Ledelsens ansvar ift. cyber- og informationssikkerhed

3. oktober 2024

v/Henriette Rolskov, CISO Coop Danmark og
Mette Krogh Sørensen, seniorkonsulent Dansk Standard

Henriette Rolskov

Som CISO i Coop Danmark rådgiver jeg om informationssikkerhed.

Jeg har en baggrund som jurist men har igennem de sidste 20 år arbejdet med **it** - risikostyring, -regulering, -kontrakter, -governance… ***men først af alt har jeg arbejdet med mennesker***

Mette Krogh Sørensen

Underviser og rådgiver om cyber- og informationssikkerhed og standarder om det hos Dansk Standard.

Jeg har arbejdet med informationssikkerhed de sidste 9 år i en blanding af private og offentlige organisationer.

ISO/IEC 27001

- En ledelsesstandard
- Baseret på risikotankegang, procesorientering og Plan Do Check Act
- Et rammeværk der tilpasses ens egen organisation
- International standard udarbejdet af internationale og danske eksperter
- Opstiller krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for informationssikkerhed (ISMS)
- Ser på informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse

2024
Crowdstrike

Antivirusprogram havde fejl, der var angiveligt er årsag til it-nedbruddet hos Microsoft., lufthavne, hospitaler.

2024
Ticketmaster

Angreb via cloud-leverandør som adgangsvej.

2024
Microsoft

Angreb ramte flere organisationer, da flere kunder om, at deres e-mails blev kompromitteret i forbindelse med angrebet.

2023
Hjemmesider

DDos angreb på Københavns Lufthavn, syv danske banker , Nationalbanken og
7 kommuner.

2023
DSB

DDoS-angreb, som lagde deres billetsystemer ned i flere timer.

2023
Netcompany

Lækkede store mængder data om blandt andet kildekode, scripts og passwords til udviklingsprogrammer. Aktien faldt i kurs efterfølgende

2023
EDC

Angreb af ransomeware

2017
Mærsk

Ransomware, som også involverede nogle IoT-enheder (Containerhånd-tering og logistik på havne via kameraer, sensorer mm.)

2019
Global Maritime

Angreb via deres IoT-enheder, der var forbundet til skibes navigations-systemer (GPS, AIS, ekkolod, sonar, overvågnings-kameraer)

2020
ISS

Ransomware-angreb, som kostede virksomheden mellem 450 og 800 millioner.

2021
Vestas Wind Systems

Et malware angreb kompromitterede virksomhedens netværk og IoT-enheder

2021
JBS Foods

Fødevareprodu-cent, blev ramt af ransomware, som påvirkede IoT-enheder i deres produktions-faciliteter. (sensorer til temperatur og fugtighed, video)

2022
Fertin Pharma

Udsat for et IoT-baseret angreb, der ramte deres produktions-systemer.

2023
Energisektoren

Angreb ramte 22 virksomheder.

Hvilken virkelighed har I?

Jf. afsnit 4 Organisationens rammer og vilkår i ISO/IEC 27001

Interne forhold
Eksempelvis organisationens kultur, politikker, målsætninger, strategi, roller og ansvarsfordeling, processer, procedurer, fysisk infrastruktur

Interessenter
Hvem er vores relevante interessenter? Og hvilke krav, har de, som vores ISMS skal adressere?

Eksterne forhold
Eksempelvis lovgivning, aftaler, branchekrav, interessenter, konkurrenter, kulturelle, politiske og samfundsmæssige forhold

Topledelsens ansvar jf. ISO/IEC 27001

UDVISE LEDERSKAB

FASTLÆGGE POLITIK OG MÅL

SIKRE INTEGRATION MED FORRETNINGS-PROCESSER

KOMMUNIKERE

SIKRE RESSOURCER

LEDE OG STØTTE MEDARBEJDERE OG LEDERE

SIKRE RESULTATER

FREMME LØBENDE FORBEDRING

SIKRE DELEGERING AF ROLLER, ANSVAR OG BEFØJELSER

Hvordan kan ledelsestilgangen implementeres?

First line: Forretningsledelse

Risikoejer med ansvaret for forretningsområdet.

Her udføres kontroller og sikres *ressourcer* til at drive og vedligeholde de daglige opgaver.

1st line skal fungere uafhængigt af 2nd og 3rd line.

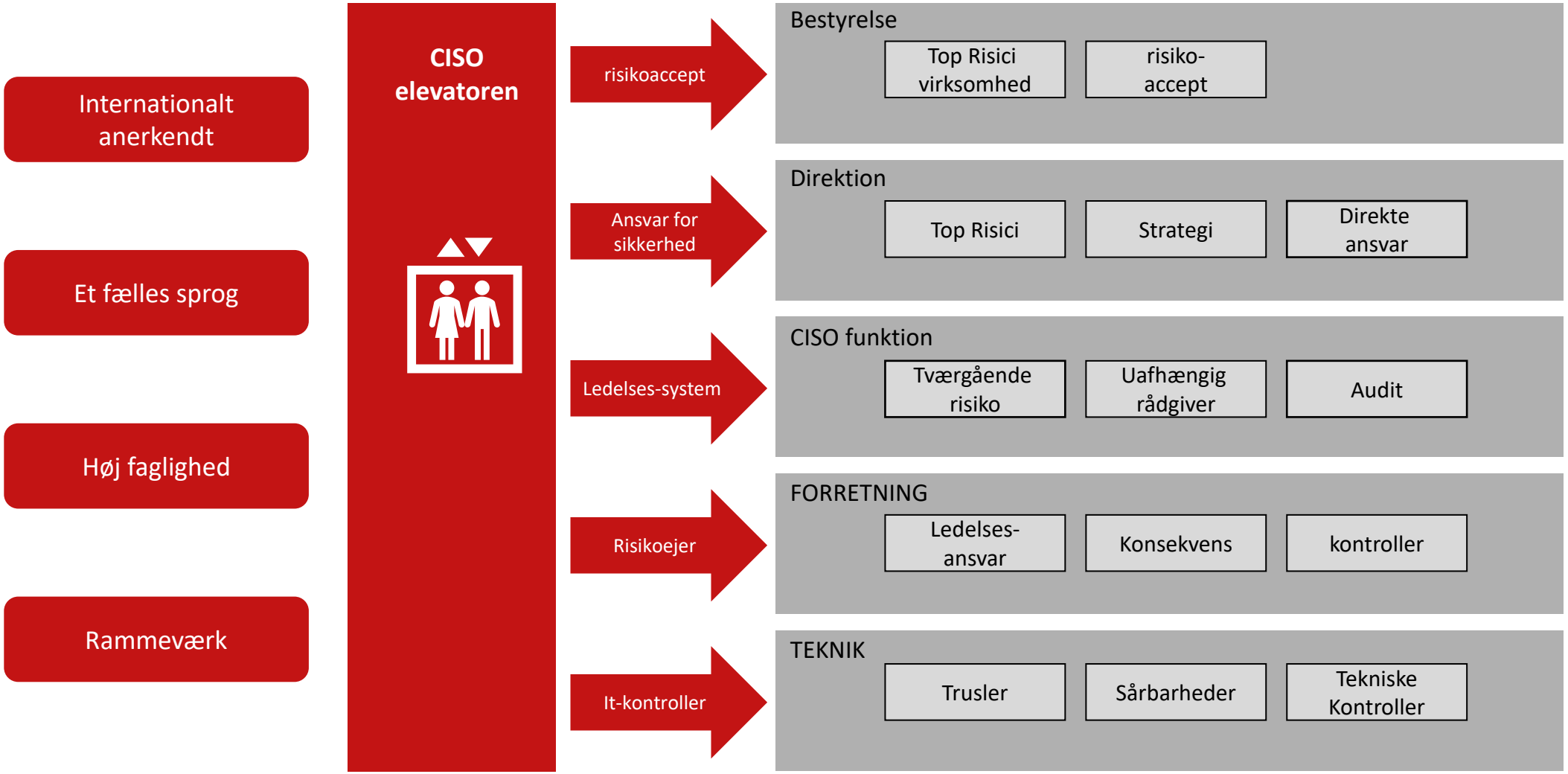
Second line: Uafhængig rådgiver

Vurderer og rapporterer *risici på tværs* af organisationen. Sikrer et *ledelsessystem* og overvåger væsentlige sikkerhedsforanstaltninger. Er øverste ledelses uafhængige *rådgiver.*

Third line: kontrolinstans - Intern revision

Øverste ledelses uafhængige *kontrolinstans*. Reviderer alle forhold, der er relevante for årsregnskabet og god revisionsskik. *Deltager ikke i forretningsledelse.*

Hvorfor bruge standarder?



Ledelsen skal løbende forholde sig til sit ledelsessystem for informationssikkerhed

Jf. ISO/IEC 27001

Hvorfor?

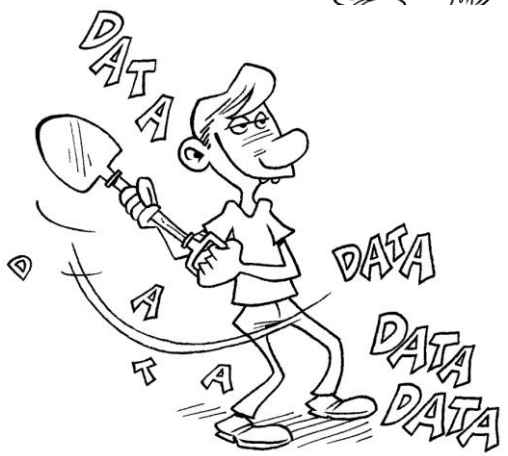
- Risici forandrer sig hele tiden
- Organisationer og deres kontekst forandrer sig også
- Så der er altid mulighed for løbende forbedring og justering

Hvordan?

- Ved at topledelsen med planlagte intervaller evaluerer om ISMSet fortsat er egnet, tilstrækkeligt og effektivt

HACKERE ER LIGEGLADE MED…..

jeres projekt scope
at, det er en tredje parts service
at det er et legacy system
at det er for risikabelt at patche
jeres out of support windows
jeres budget
at I altid har gjort sådan
jeres go-Live dato
at det kun er en pilot
non-disclosure aftaler
at det ikke var et krav i kontrakten
at det er et internt system
at det er svært at rette
at det er i gang med udfasning
at I ikke ved hvordan det skal rettes
at det er håndteret som cloud service
at jeres leverandør ikke supporterer den konfiguration
at det er en midlertidig løsning
at det er [indsæt tilfældig standard] compliant
at det er disk krypteret
at cost benefit ikke balancerer
at ingen andre vil kunne gennemskue det
at I ikke kan forklare risikoen til forretningen
at I har andre prioriteter
at det ikke kan forsvares forretningsmæssigt
at der ikke er return of Investment
at leverandøren har taget risikoen i kontrakten



GOD SIKKERHED BETALER SIG

Gode kilder til viden

- **Sikker Digital**
- **Bestyrelsesforeningen Center for Cyberkompetence**
- **SMV:Digital**
- **Center for Cybersikkerhed**
- **Europol Cybercrime**
- **ENISA**
- **Sikker:Cyber**
- **Industriens Fond**
- **Dansk Standard**

Podcasts

- DRs Prompt
- SANS Daily Stormcase
- Datatilsynets podcast om GDPR
- Heartsbeats True Cybercrime
- Malicious Life
- Cyber Security Headlines