MODSTANDSDYGTIGHED CYBERSIKKERHED

Er der styr på beredskabsplanerne?

GERT LÆSSØE MIKKELSEN, HEAD OF SECURITY LAB

Sammen kommer vi #forandigitalt

ALEXANDRA INSTITUTTET

Forsknings-enhed og konsulent-hus i ét

> Alexandra Instituttet er det tandhjul, som passer ind mellem universiteter og virksomheder.
>
> **Alexander Larsen**
> *Udviklingsdirektør i Grundfos*

DABAI
Manufacturing Academy of Denmark
CYBERSECURE IOT IN DANISH INDUSTRY
infinit
Innovationsnetværk for it
Uddannelses- og Forskningsministeriet
Styrelsen for Forskning og Uddannelse
Innovationsfonden
INDUSTRIENS FOND
FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation
European Commission
KØBENHAVNS UNIVERSITET
AARHUS UNIVERSITET
IT-byen KATRINEBJERG
IT-UNIVERSITETET I KØBENHAVN
LEGO
Vejdirektoratet
DSB
kamstrup
Topdanmark
Forsikring • Pension
ERHVERVSSTYRELSEN
movia
midt regionmidtjylland
SYSTEMATIC
PASCAL
GRUNDFOS
AARHUS KOMMUNE
HOUNÖ
DIGITALISERINGSSTYRELSEN
Miljø- og Fødevareministeriet
Miljøstyrelsen

Konsekven

PENGE

Hackeran
Mærsk m

Mærsk anslår, at hackera
1,3 til 1,9 milliarder kron

Amerikans
ramt af ka
greb: 9.00
rørledning

Et cyberangreb mod Colo
benzinpriser.

VIRKSOMHEDSCASE

› Hackerangreb gjorde DESMI konkurrencedygtig

https://sikkerdigital.dk/virksomhed/den-sikre-investering

- 40 pct. af de danske SMV'er har et *utilstrækkeligt* digitalt sikkerhedsniveau i forhold til deres risikoprofil.

Trusselsniveau:

CENTER FOR CYBERSIKKERHED

- Truslen fra cyberspionage er **MEGET HØJ**
- Truslen fra cyberkriminalitet er **MEGET HØJ**
- Truslen fra cyberaktivisme hæves fra **LAV** til **MIDDEL** (pga. Ruslands angreb på Ukraine)
- Truslen fra destruktive cyberangreb er **LAV**
- Truslen fra cyberterror er **INGEN**

https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

Krav fra kunder

... og fra samfundet

- GDPR
- NIS 2 Direktivet
- Artificial intelligence act
- Radio udstyrs direktivet
- Cyber Security Act

> ICO fines British Airways £20m for data breach affecting more than 400,000 customers
>
> Date **16 October 2020**

- D-Mærket (www.d-maerket.dk)

Hvad gør vi så?

Ledelsesforankring

Risikobaseret tilgang

Udfordringer i hverdagen:

- Manglende fokus fra ledelsen
- Manglende krav fra ledelsen

- “Man får hvad man måler”

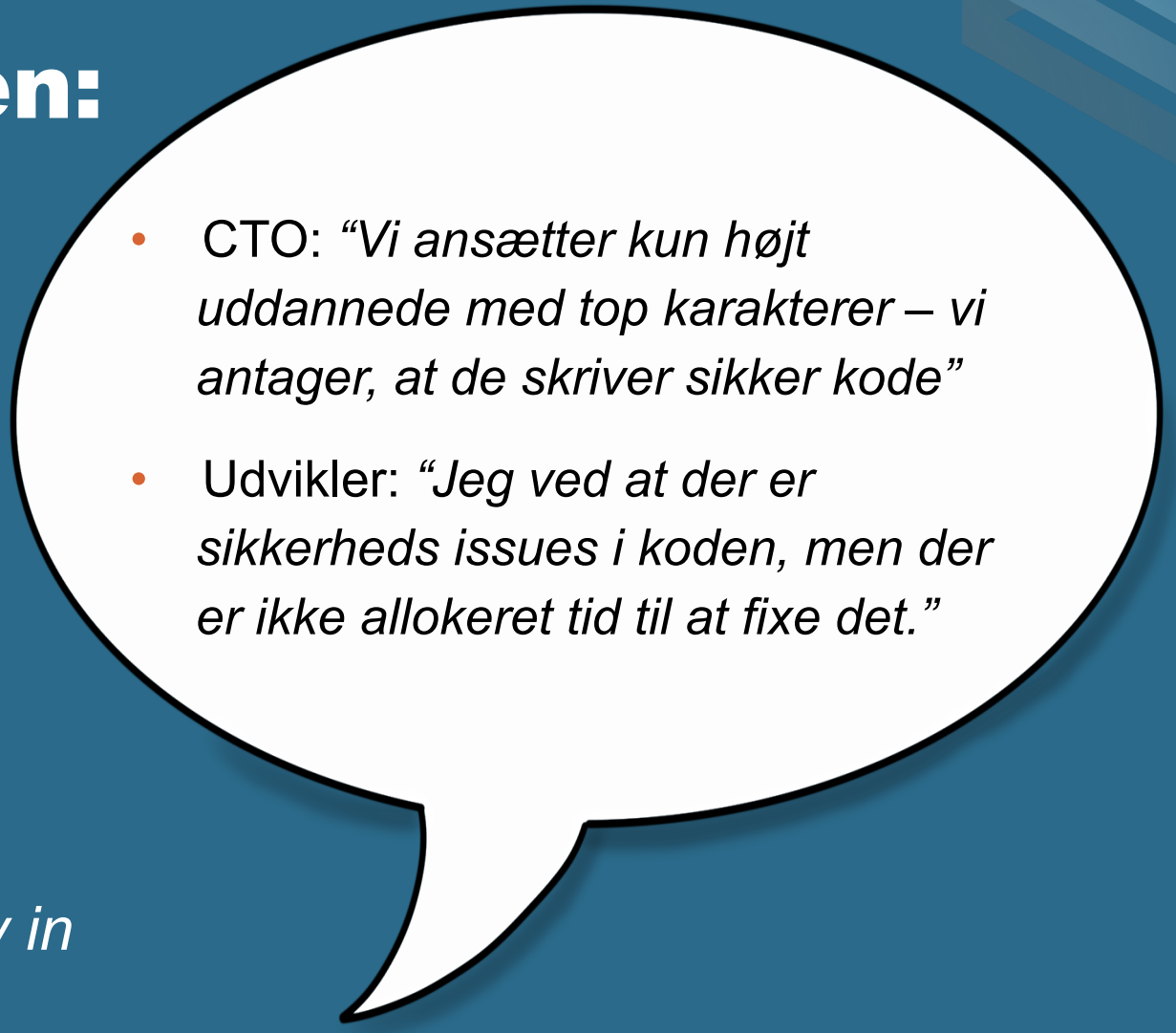
”Manglende tid, gør at sikkerhed sommetider får lavere fokus”

”Test og dokumentation passer ikke med vores agile metoder (ad hoc)”

Udfordringer i hverdagen:

- Manglende forståelse fra ledelsen

[*Assessment on the Status of Cybersecurity in Denmark, ITU, SDU*]



Hvad og hvordan

- Hvad skal gøres?
- Hvor skal vi fokuserer?

- På den største risiko

Risiko = Sandsynlighed x Konsekvens

- Sandsynlighed:
- Motivation +
- Kompetencer +
- Systemets styrke –
- Konsekvens:
- Teknisk
- Forretningen

CIA

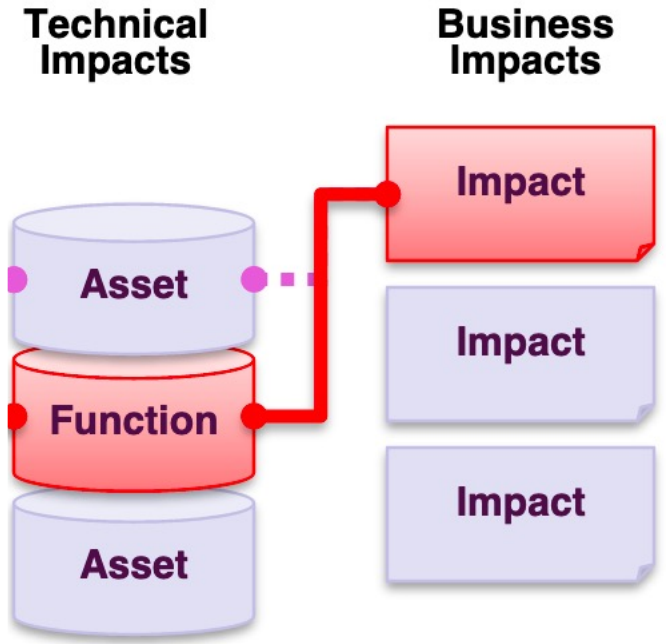
- C: Confidentiality – Fortrolighed
  Data der skulle holdes hemmeligt er blevet lækket

- I: Integrity – Integritet
  Data er blevet ændret

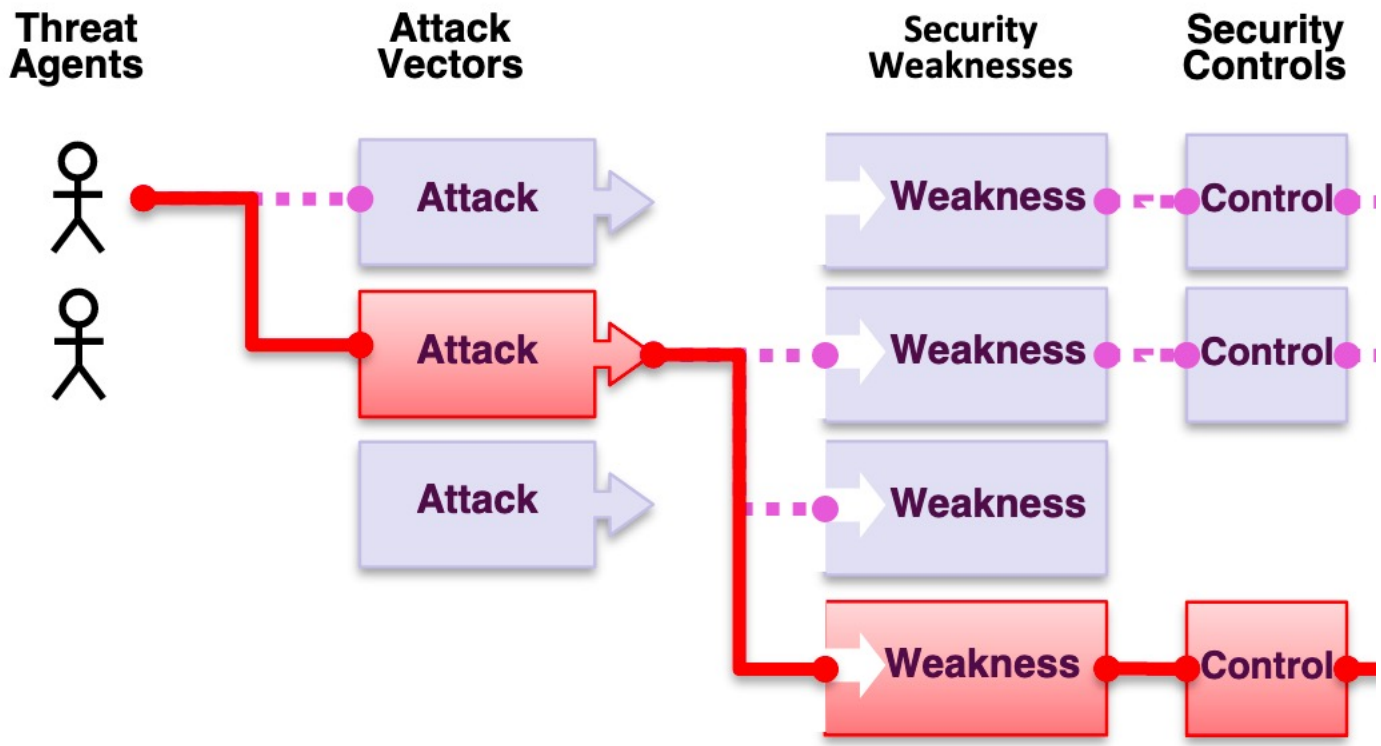
- A: Availability – Tilgængelighed
  Data eller IT-funktioner/-systemer er ikke tilgængelige

Risiko – Konsekvensen

- Teknisk konsekvens
- Uautoriseret adgang til data
- Uautoriseret adgang til funktion
- Ødelægge noget
- …
- Forretning
- Tab af kunder
- Bøder
- Tid og ressourcer for at rydde op
- …

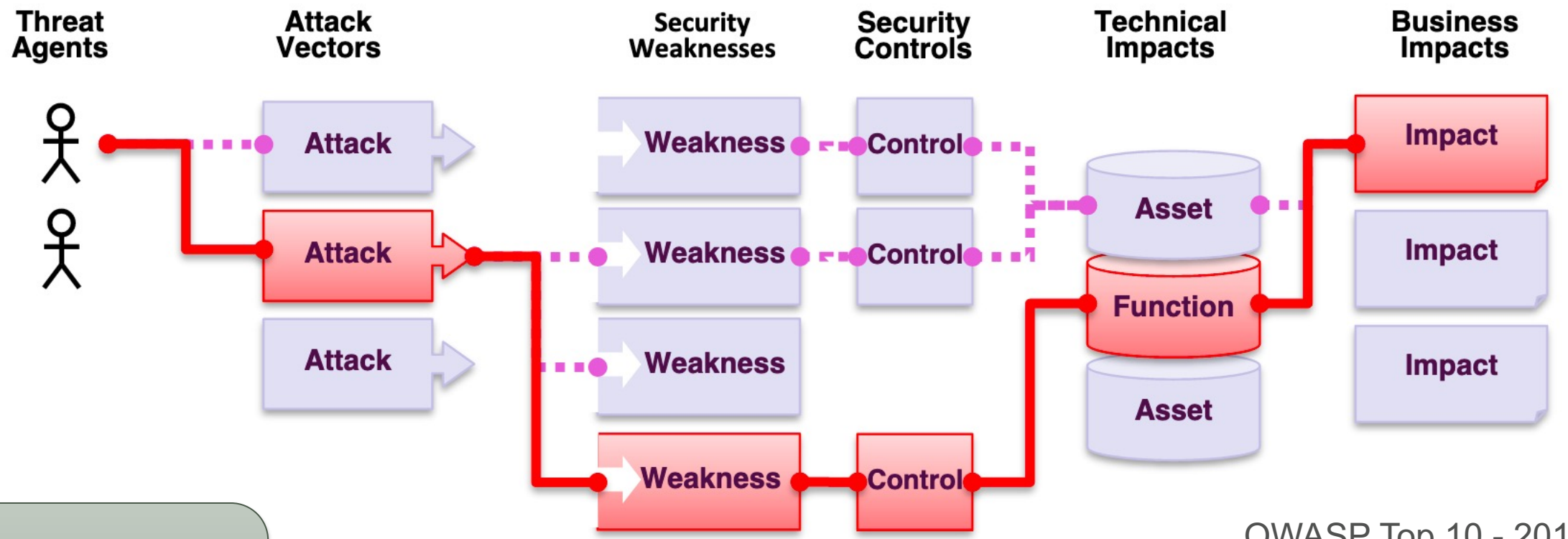


Risiko – sandsynlighed



- Agenten
- Motivation
- Kompetencer
  - Teenager
  - Organisede kriminelle
  - Fjendtlige nationer
  - Konkurrenter
  - Et mix
- Styrke af systemet
- Undgå svagheder
- Sikkerhedskontroller
- Collateral damage
- fx Mærsk

Risiko



OWASP Top 10 - 2017

- C – Confidentiality
- I – Integrity
- A – Availability

Risiko = Sandsynlighed x Konsekvens

Risiko – ledelsen kan forstå

SANDSYNLIGHED	Meget lav	Lav	Medium	Høj	Meget høj
Meget lav	2	3	4	5	6
Lav	3	4	5	6	7
Medium	4	5	6	7	8
Høj	5	6	7	8	9
Meget høj	6	7	8	9	10

KONSEKVENS

Kom godt i gang

1. Kortlæg og vurder virksomhedens væsentligste informationer
2. Skab et overblik over virksomhedens IT-udstyr og software
3. Lav en liste over de mest sandsynlige trusler
   - Ransomware, Phishing inkl. CEO fraud, DDoS, Malware, Interne trusler
4. Implementér de mest basale sikkerheds- tiltag
5. Udpeg en ansvarlig person

Andre guides

https://sikkerdigital.dk/virksomhed

- Sikkerhedschecket
- IT-Risikovurderingsværktøj
- Virksomhedscases
- ”Når skaden er sket”

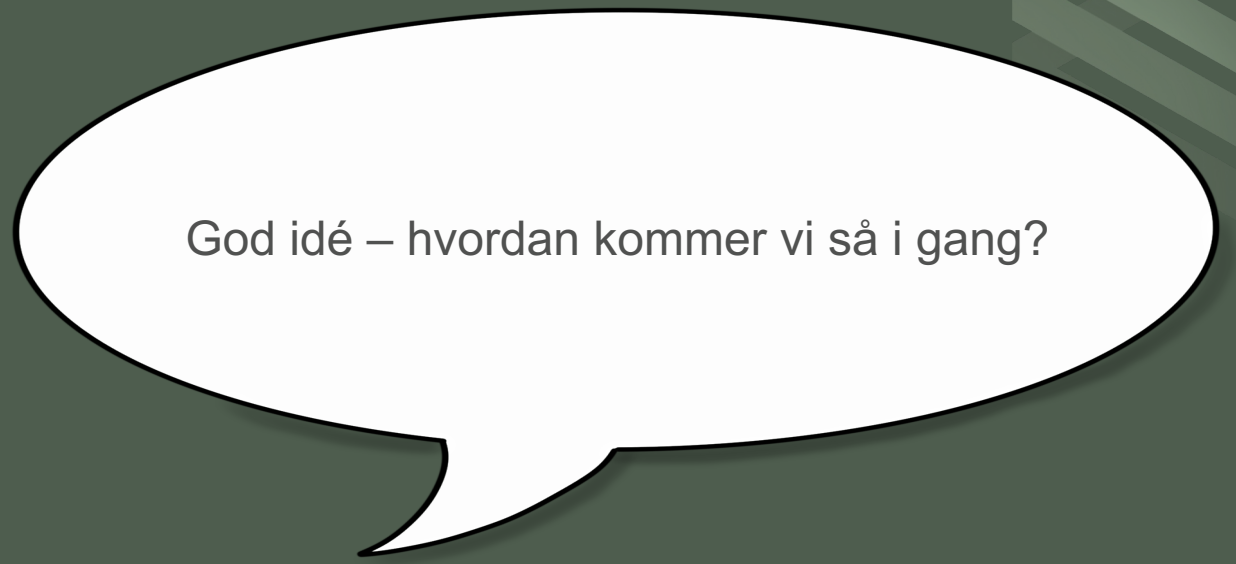
Andre guides

- CIS Controls - Center for Internet Security
  Meget konkrete controller til sikkerhed
- OWASP - Open Web Application Security Project
- IoT Security Foundation
- D-Mærket – Dansk mærkningsordning
- Cybersikkerhed for bestyrelser – Bestyrelsesforeningen

Generelt krav til sikkerhedsniveauet

Virksomheden skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger, der sikrer et sikkerhedsniveau, der passer til risikoen.

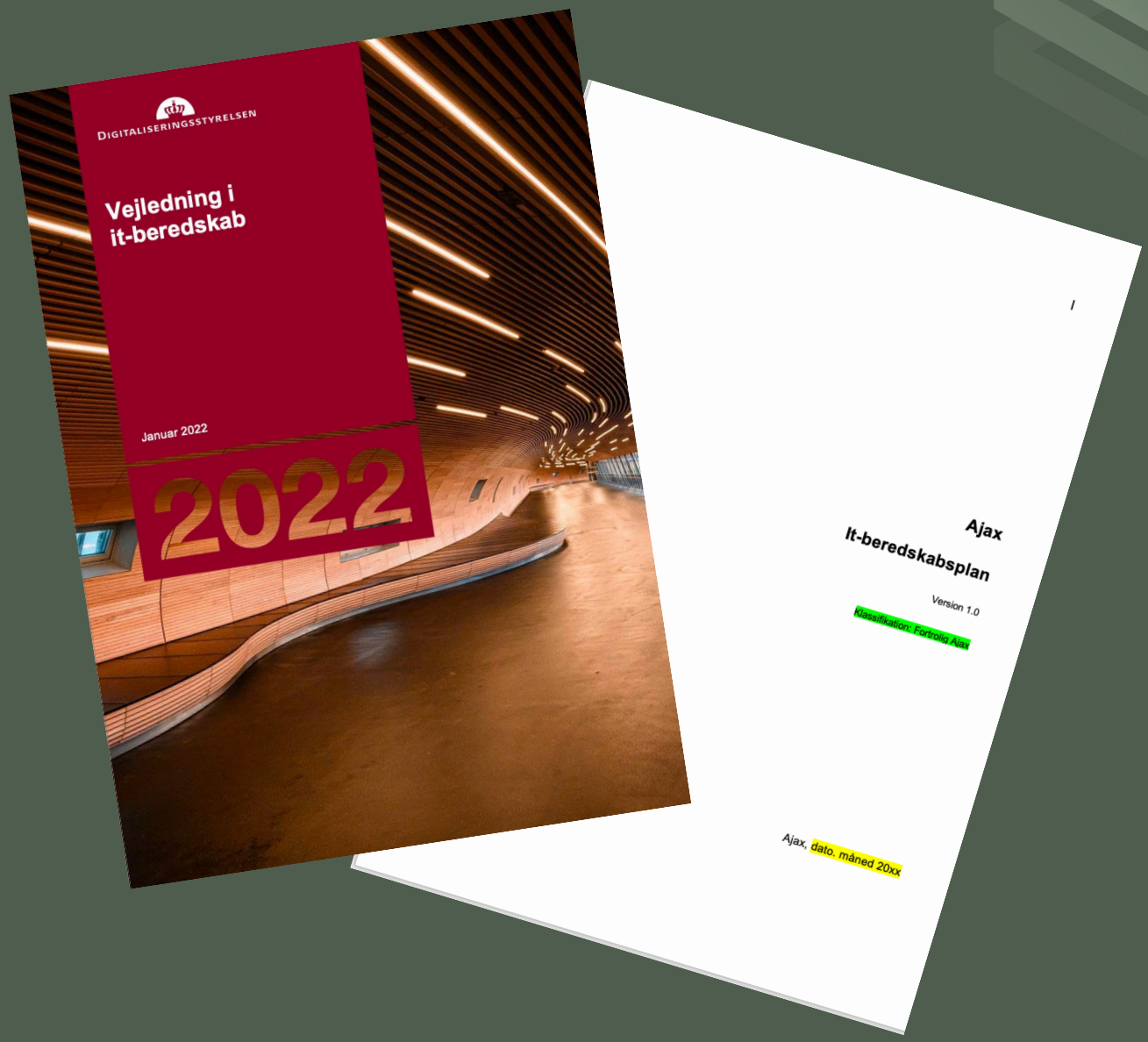
Beredskabsplan



- Plan der bygger på IT-risikovurdering
- Plan der fortæller hvad der skal gøres når/hvis skaden sker
- Vend tilbage til den – den skal følge med tiden

Beredskabsplan

www.sikkerdigital.dk

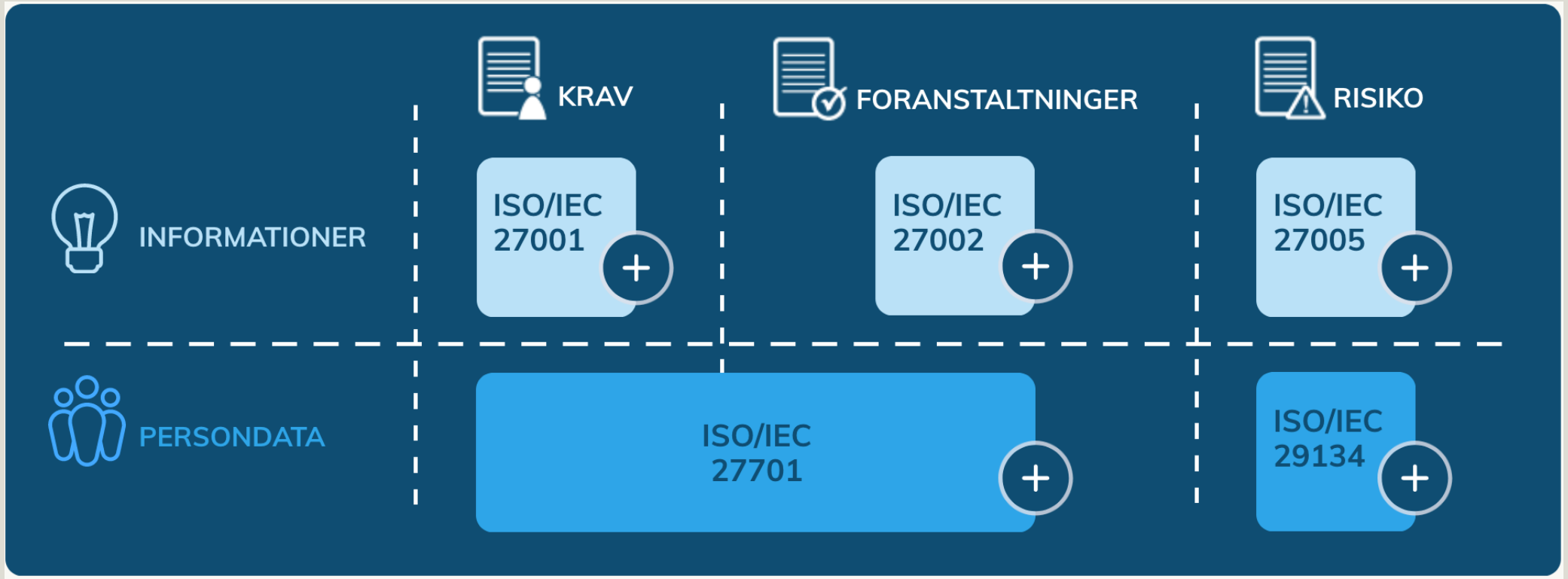


Relevante standarder:

- DS/EN ISO/IEC 27001:2017
  IT-Sikkerhed – Ledelsessystemer for informations-sikkerhed – Krav
- DS/ISO/IEC 27002:2022
  IT-Sikkerhed – Regelsæt for styring af informationssikkerhed
- DS/ISO/IEC 27005:2018
  IT-Sikkerhed – Risikoledelse i tilknytning til informationssikkerhed

- www.ds.dk/cybersikkerhed

www.ds.dk/cybersikkerhed



Tal sammen om cybersikkerhed...

- Vi skal udnytte mulighederne i IT, data og kunstig intelligens
- Cybersikkerhed er fundamentet, hvis det skal lykkedes

- Ledelsesforankring
- Risiko

Alexandra Instituttet giver offentlige og private virksomheder let adgang til den nyeste forskning indenfor digitalisering og IT

gert.l.mikkelsen@alexandra.dk