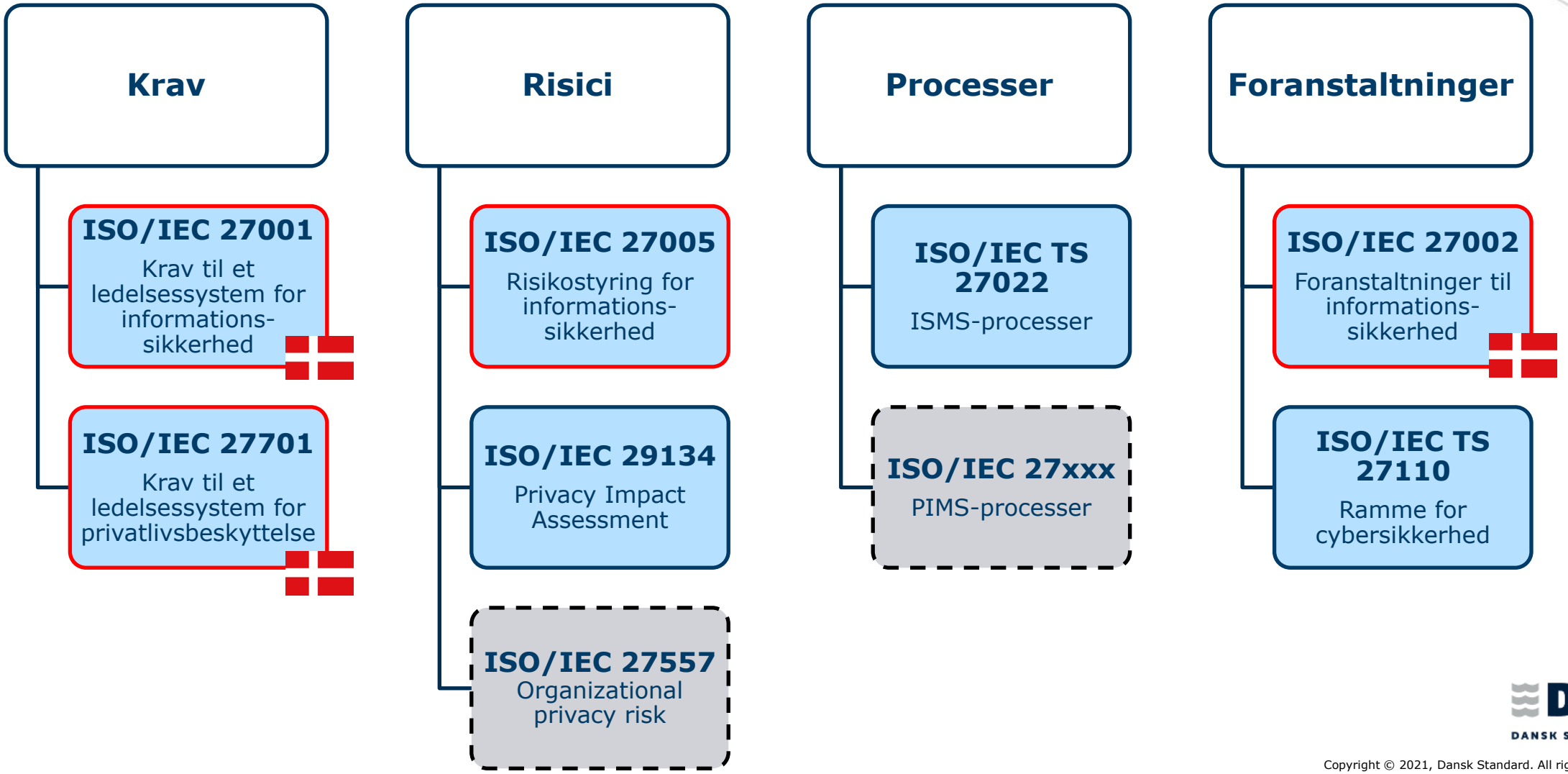
Cybersikkerhed set fra et IT-perspektiv

Lasse Kaltoft, lak@ds.dk

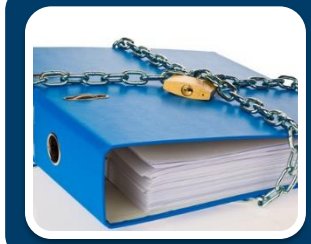
DS
DANSK STANDARD

Standarder for informationssikkerhed og privacy



DS DANSK STANDARD

Informationssikkerhed efter ISO/IEC 27001



Tab af fortrolighed

- Læk af interne strategier
- Ledere deler oplysninger om ansattes sygdomsforløb
- Ansatte taler åbent om sagsbehandling

Tab af integritet

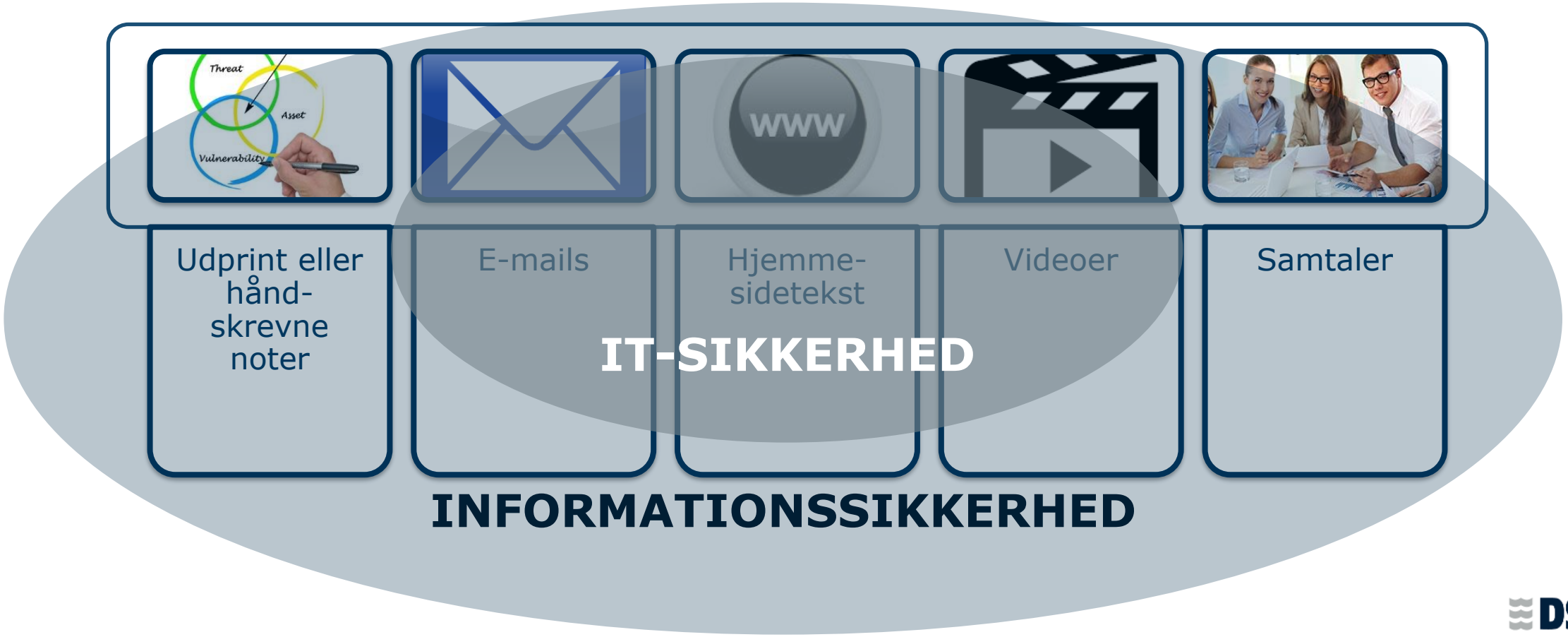
- Fejlbehæftet opdatering af systemer
- Fejl i udprint af filer
- Hackers ændring af kundedata

Tab af tilgængelighed

- Oversvømmelse af arkiver i kælderen
- Overbelastningsangreb
- Ransomware rammer sagsbehandlingssystem

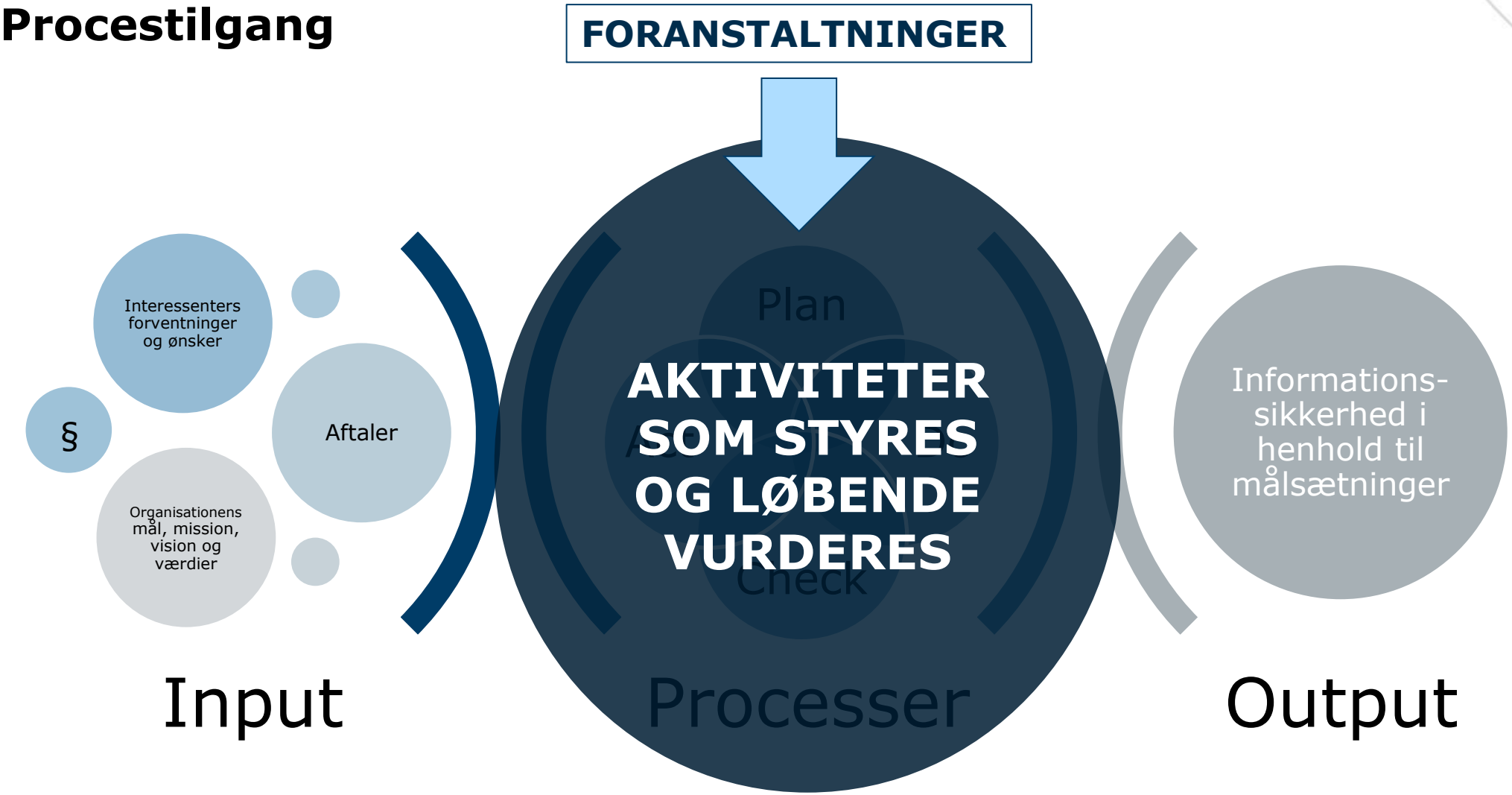
DS DANSK STANDARD

Informationer som skal beskyttes

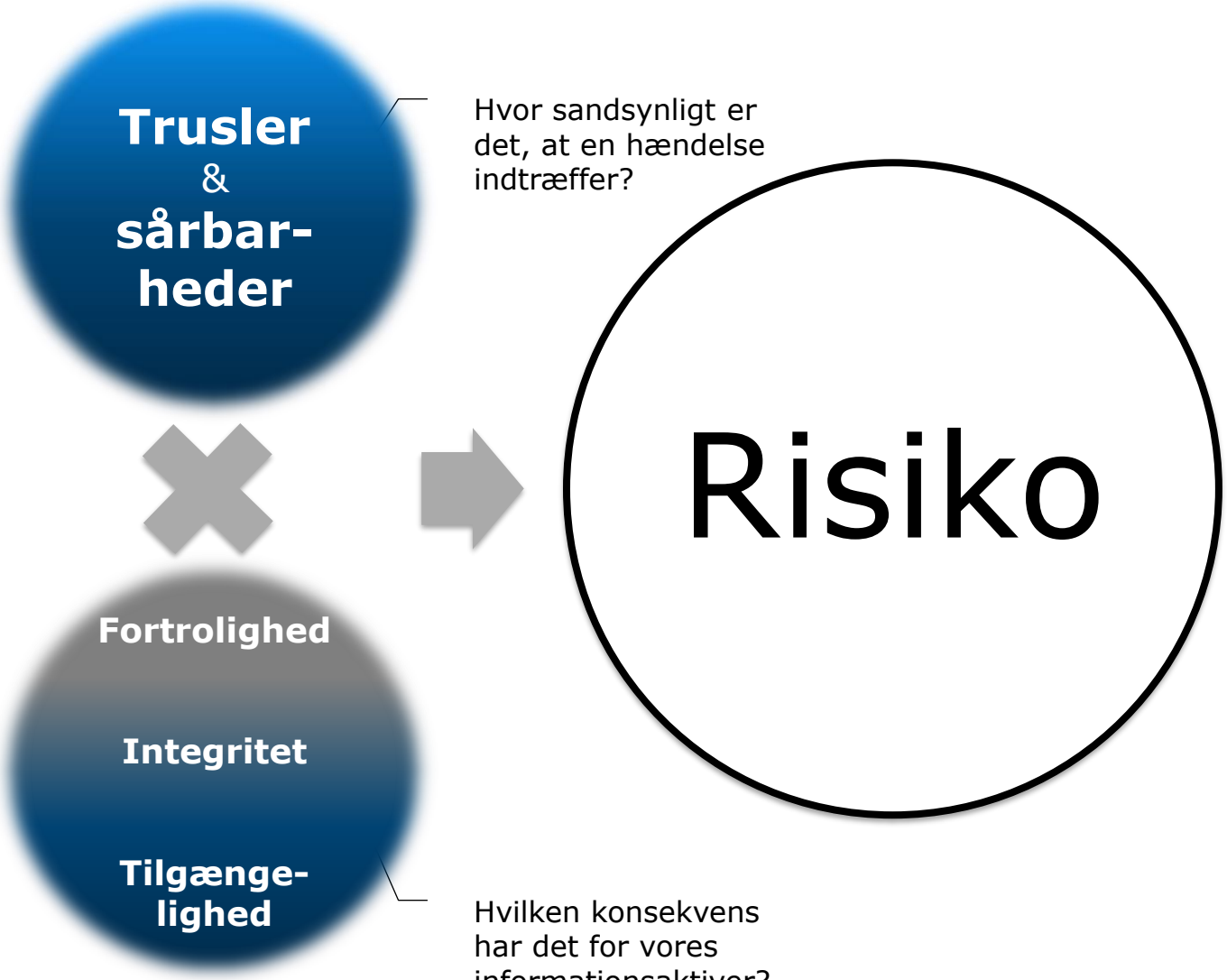


DS
DANSK STANDARD

Procestilgang



Risikometode



Risikovurderingsprocessen

Identifikation

Find aktiver, trusler, sårbarheder og foranstaltninger

Strømafbrud

↓

ingen diesel til generator

Analyse

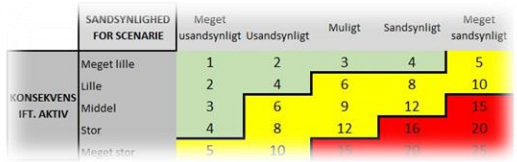
Beregn sandsynlighed og konsekvens

4. Meget sandsynligt
3. Sandsynligt
2. Ret usandsynligt
1. Meget usandsynligt

4. Meget stor konsekvens
3. Stor konsekvens
2. Lille konsekvens
1. Meget lille konsekvens

Evaluering

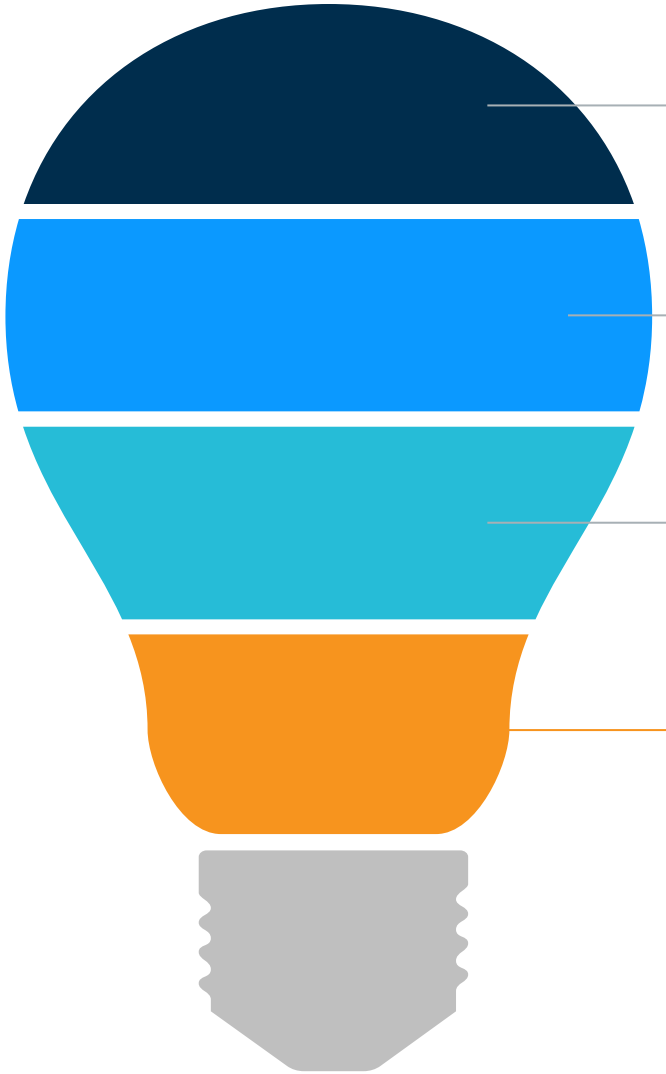
Sammenhold risici med acceptkriterier



KONSEKVENS IFT. AKTIV	SANDSYNLIGHED FOR SCENARIE	Meget usandsynligt	Usandsynligt	Muligt	Sandsynligt	Meget sandsynligt
	Meget lille	1	2	3	4	5
	Lille	2	4	6	8	10
	Middel	3	6	9	12	15
	Stor	4	8	12	16	20
	Meget stor	5	10	15	20	25

DS DANSK STANDARD

Risikohåndtering



D Forøg/mindsk
At håndtere risikoen

C Undgå
At undgå eksponering for risikoen

B Accepter
At vælge at leve med risikoen

A Flyt
At lade 3. part overtage håndtering af risikoen

Anneks A

A.5 Informationssikkerhedspolitikker

A.6 Organisering af informationssikkerhed

A.7 Personalesikkerhed

A.8 Styring af aktiver

A.9 Adgangsstyring

A.10 Kryptografi

A.11 Fysisk sikring og miljøsikring

A.12 Driftssikkerhed

A.13 Kommunikationssikkerhed

A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

A.15 Leverandørforhold

A.16 Styring af informationssikkerhedsbrud

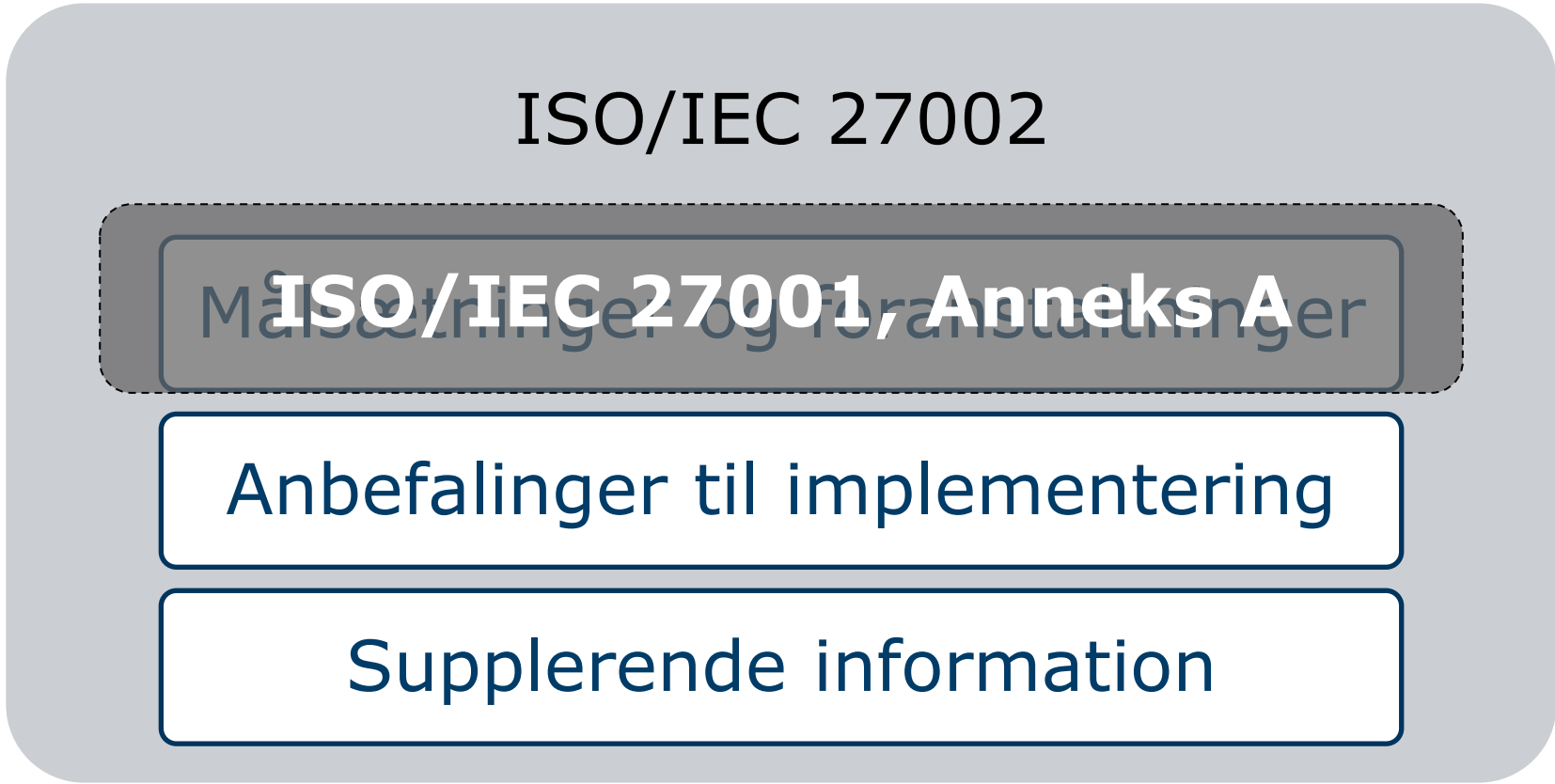
A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

A.18 Overensstemmelse

114 mulige handlinger som velbegrundet skal til- og fravælges – og suppleres med yderligere for organisationen relevante handlinger

DS DANSK STANDARD

Forholdet mellem ISO/IEC 27001 og ISO/IEC 27002



ISO/IEC 27002: informationssikkerhedsforanstaltninger

Informations-sikkerheds-politikker

Organisering af informations-sikkerhed

Personalesikkerhed

Styring af aktiver

Adgangsstyring

Kryptografi

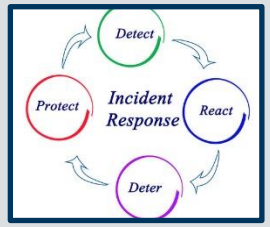
Fysisk sikring og miljøsikring

Driftssikkerhed

Kommunikations-sikkerhed

Anskaffelse, udvikling og vedligeholdelse

Leverandørforhold



Styring af informations-sikkerhedsbrud

Nød-, beredskabs- og reetablering

Overensstemmelse

DS
DANSK STANDARD

Oversigt over ændringer i den nye ISO/IEC 27002

Ny vejledning i foranstaltninger for informationssikkerhed

Download whitepaper om ISO/IEC 27002 her

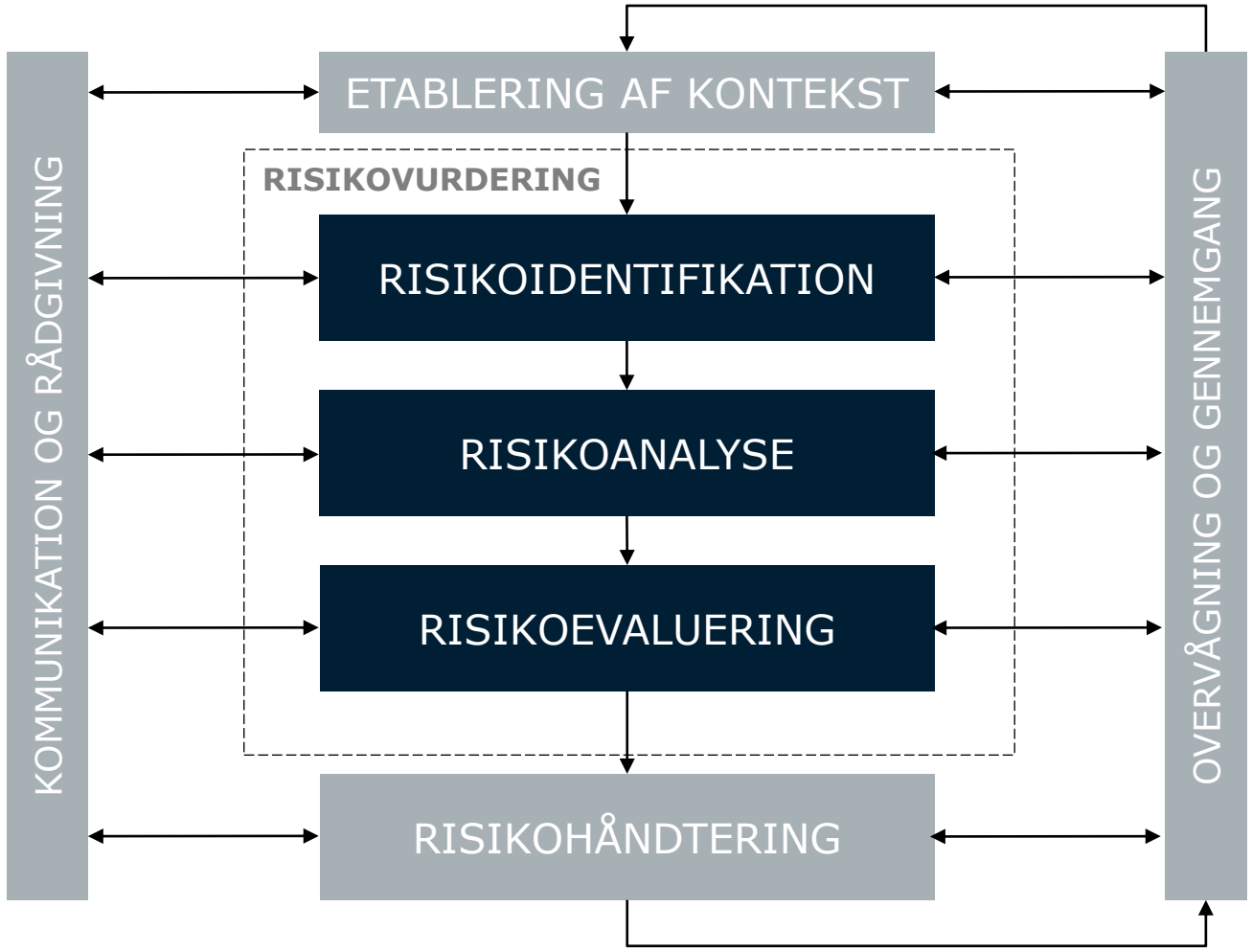
https://www.ds.dk/27002

DANSK STANDARD

ISO/IEC 27005: risikostyring for informationssikkerhed

"Risk: An effect is a deviation from the expected — positive or negative"

"Control: measure that maintains and/or modifies risk."



"Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization."

DANSK STANDARD

Fra informationssikkerhed (ISMS) til privatlivsbeskyttelse (PIMS)

ISO/IEC 27701

Kravene i ISO/IEC 27001, som nævner "informationssikkerhed", skal udvides til at omfatte beskyttelse af privatlivet, der potentielt kunne være påvirket af behandlingen af personoplysninger.

ISO/IEC 27701, 5.1

”Nye” krav til persondatabeskyttelse

Højere bødestraffe

Dokumentation af compliance

Samtykke

DPO: databeskyttelsesrådgiver

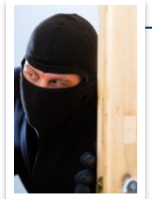
Konsekvensanalyser

Privacy by Design/ by Default

Oplysningspligt

Dataportabilitet

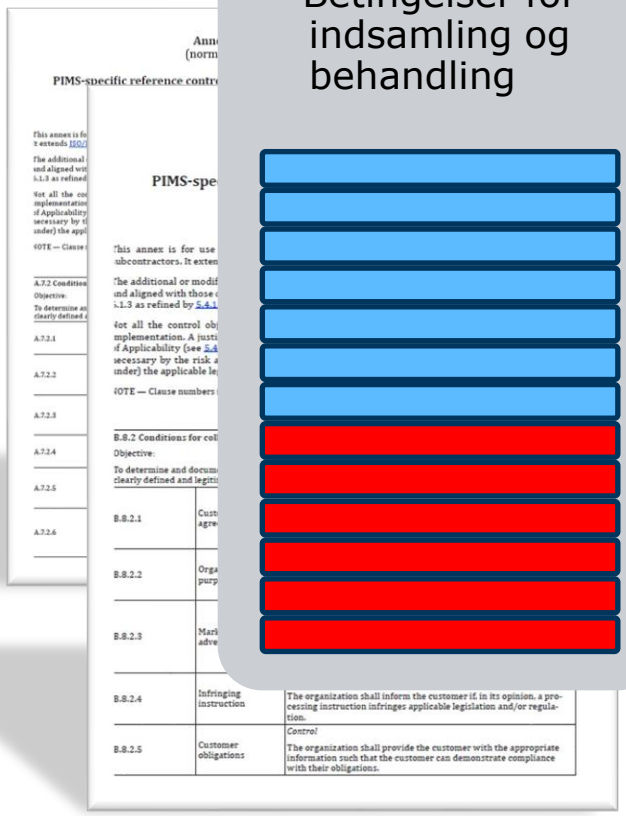
Databehandlere



Anmeldelse

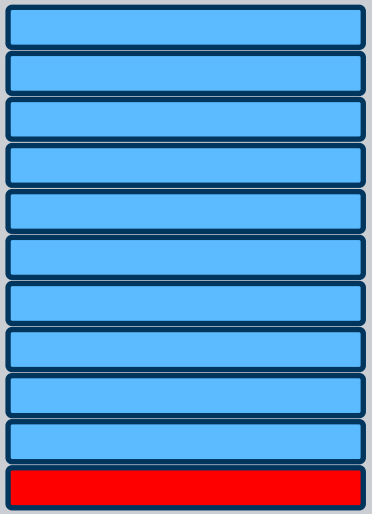
DANSK STANDARD

Foranstaltninger: dataansvarlig (Anneks A) og databehandler (Anneks B)

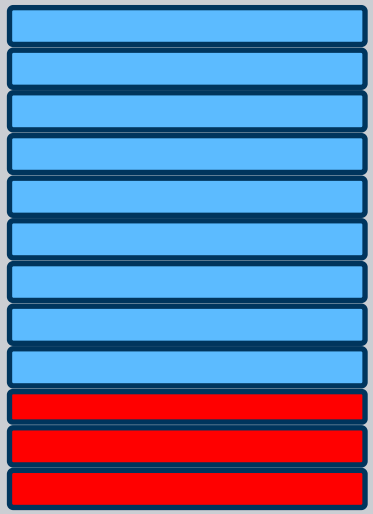


Betingelser for indsamling og behandling

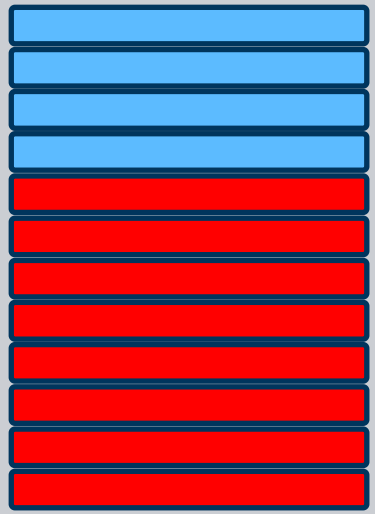
Forpligtelser over for de registrerede



Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

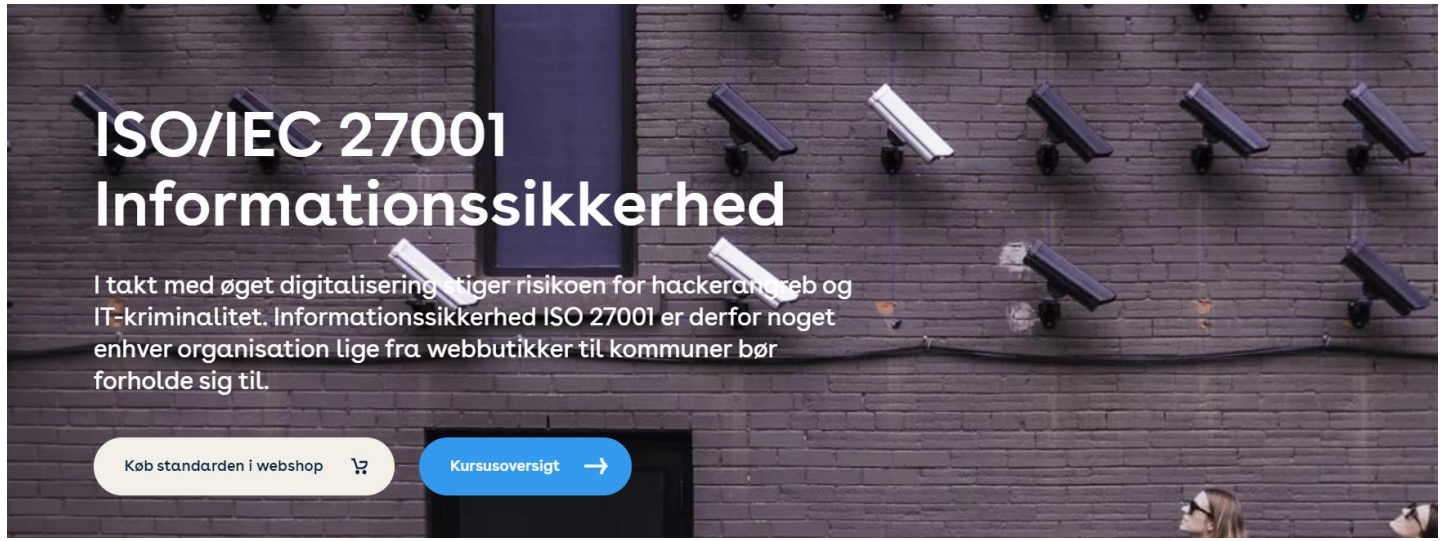


Deling, overførsel og videregivelse af personoplysninger



Mere information

- Hvad er informationssikkerhed?
- Vigtigheden af ISO 27001
- Henvisning til webshop
- Henvisninger til kurser
- Supplerende information



https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed

DANSK STANDARD