Standarder for cyber- og informationssikkerhed

- som et strategisk redskab til at opnå modstands- og konkurrencedygtighed

Anders Linde, Dansk Standard

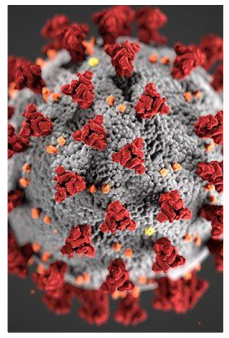
DANSK STANDARD

Den nationale agenda

Regeringsstrategier: Informationssikkerhed efter ISO/IEC 27001

§

Privacy: Beskyttelse af personoplysninger efter ISO/IEC 27701



Pandemi/cyberangreb: Robusthed efter ISO 22301

DANSK STANDARD

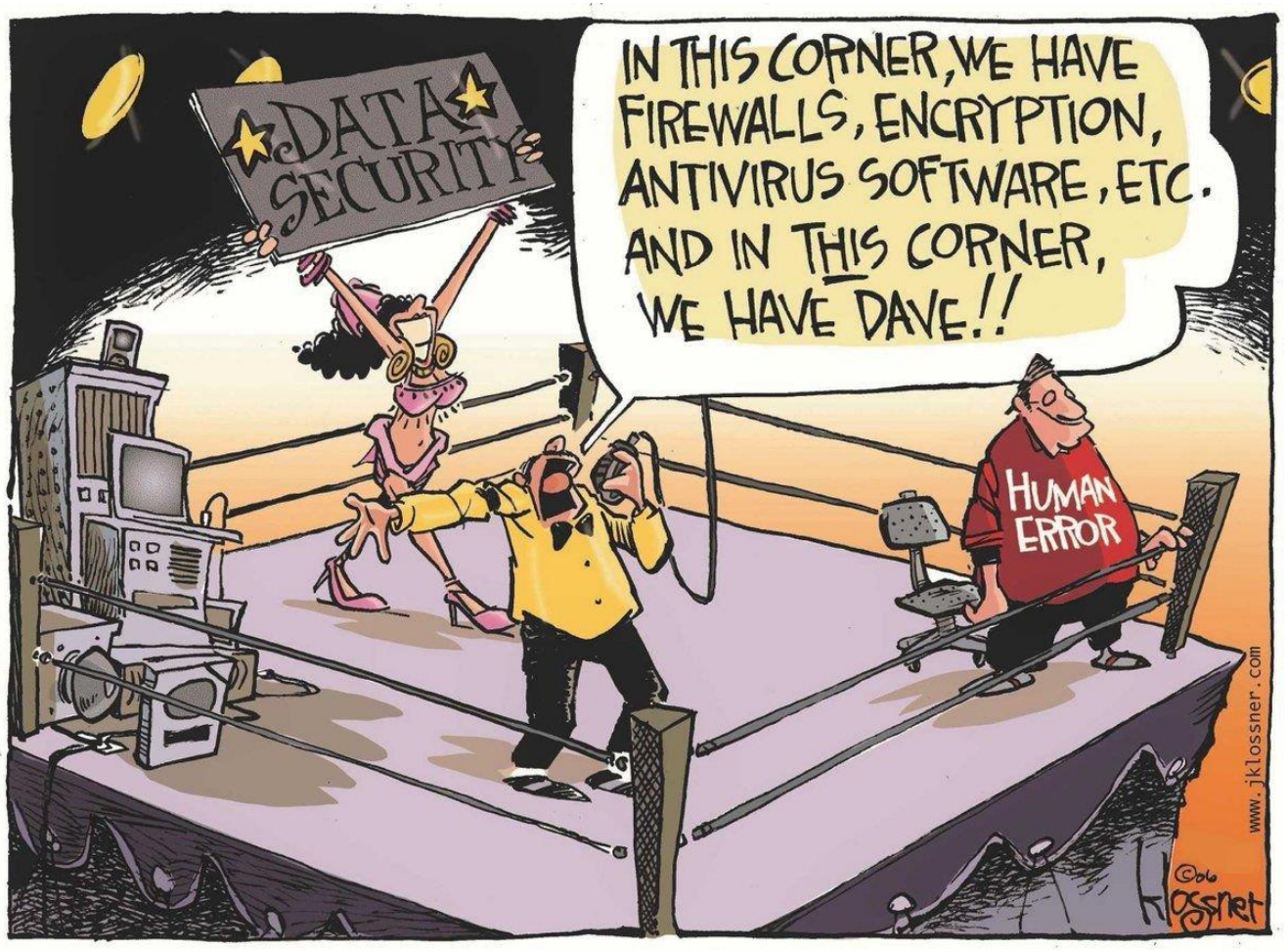
Globale best practices

1. ISO/IEC JTC 1/SC 27:
- IT Security techniques

2. CEN-CENELEC JTC 13:
- Cyber Security and Data Protection

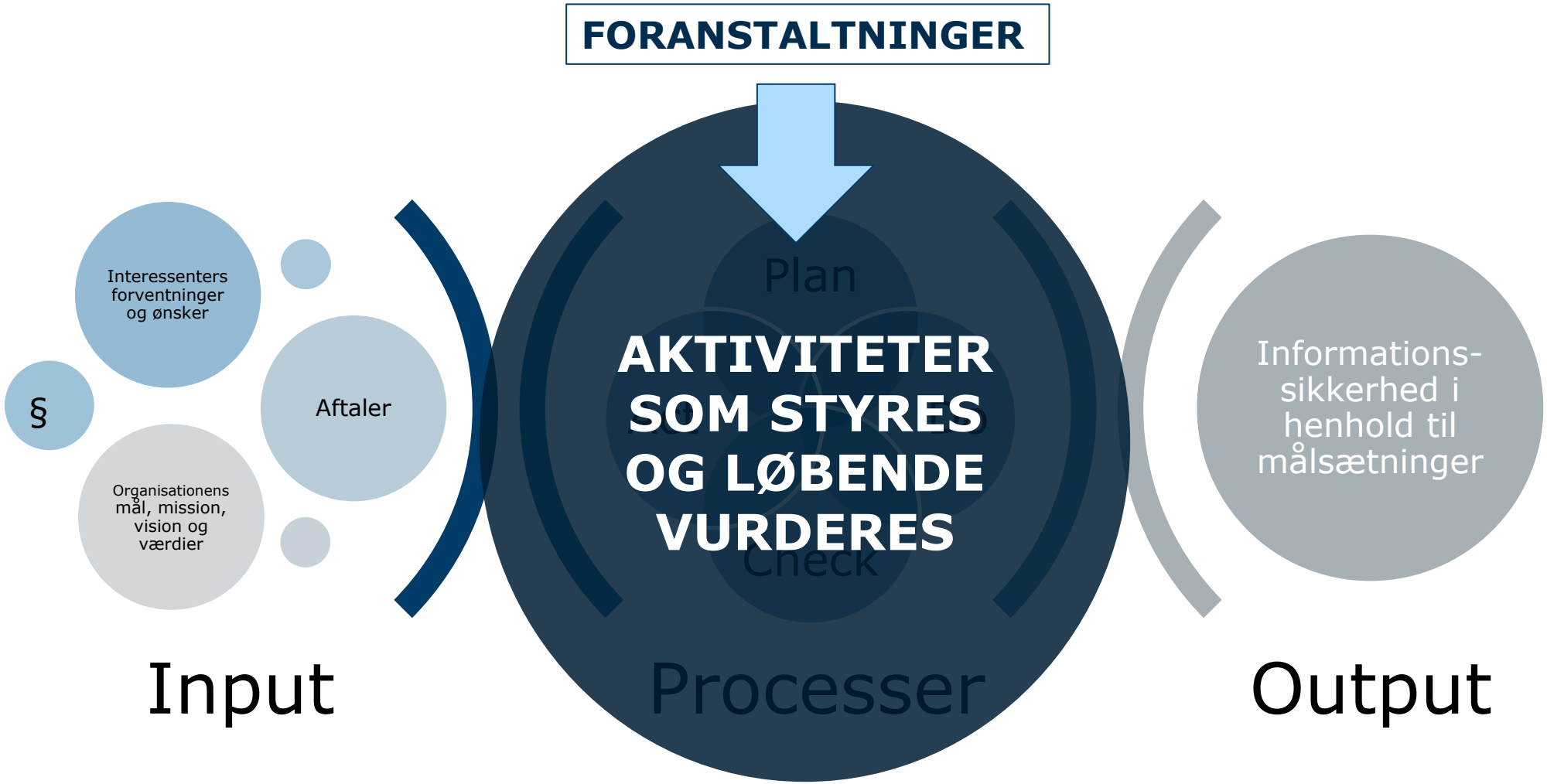
DS
DANSK STANDARD

Standarder til beskyttelse af informationer og forretningen



DANSK STANDARD

Etablering af et ledelsessystem



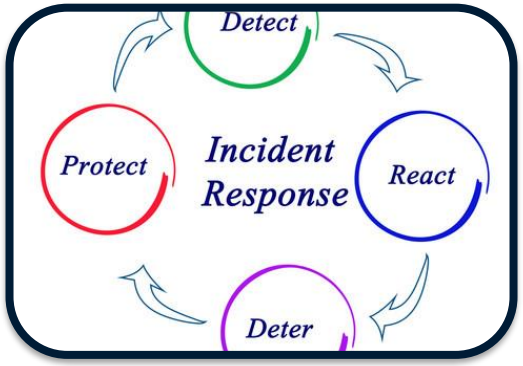
ISO/IEC 27001: grundprincipper for informationssikkerhed

Beskytte informationer

- Vi beskytter imod tab af fortrolighed, integritet og tilgængelighed

Gennemføre risikovurderinger

- Vi vurderer organisationens risikobillede og træffer passende foranstaltninger



Foretage løbende forbedringer

- Vi følger op på vores investering i informationssikkerhed

Dokumentere vores indsats

- Vi forklarer, hvad vi gør og dokumenterer, at det bliver gjort

DANSK STANDARD

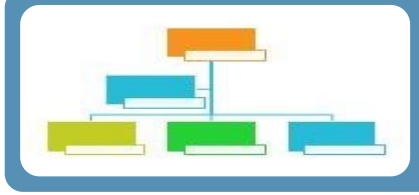
Beskyttelse af informationer forankret i topledelsen

Lederskab og engagement

- Kommunikation, ressourcetildeling og strategisk forankring

Formulering af politikker

- Fastlæggelse af politikken for informationssikkerhed



Roller, ansvar og beføjelser

- Delegering og kommunikation

Evaluering af informationssikkerheden

- Egnethed, tilstrækkelighed og effektivitet

DANSK STANDARD

Ledelsens opfølgning – eksempel fra certificeret kunde

Status fra ledelsens foregående evaluering

- Revision af forretningsgange
- Interessentanalyse opdateret

Ændringer til ledelsessystemet

- Ændringer i interne og eksterne forhold, der er relevante for ISO/IEC 27001
- Ændringer i bindende forpligtelser: lovgivning og kontrakter
- Ændringer af risici og muligheder

Informationssikkerhedspolitik

- Opdatering af politik(ker)

Afvigelser og korrigerende handlinger

- Oversigt over afvigelser og korrigerende handlinger
- Løbende forbedringer – oversigt/status
- Resultater og status på intern og ekstern audits
- Resultat af årshjulsmålinger
- Opfyldelse af mål for informationssikkerhed

Ressourcer i relation til ISO/IEC 27001

- Er der tilstrækkelige ressourcer?

Kommunikation

- Intern kommunikation i relation til informationssikkerhed, fx awareness
- Ekstern kommunikation, herunder evt. klager

Effektivitet af iværksatte handlinger – og mulighed for forbedringer

- Output fra ledelsens evaluering, herunder beslutninger om mulige forbedringer/ændringer
- Resultat af mål og handlingsplaner

Beredskab

- Revision af beredskabsplaner
- Uddannelse og afholdte beredskabsøvelser

DS DANSK STANDARD

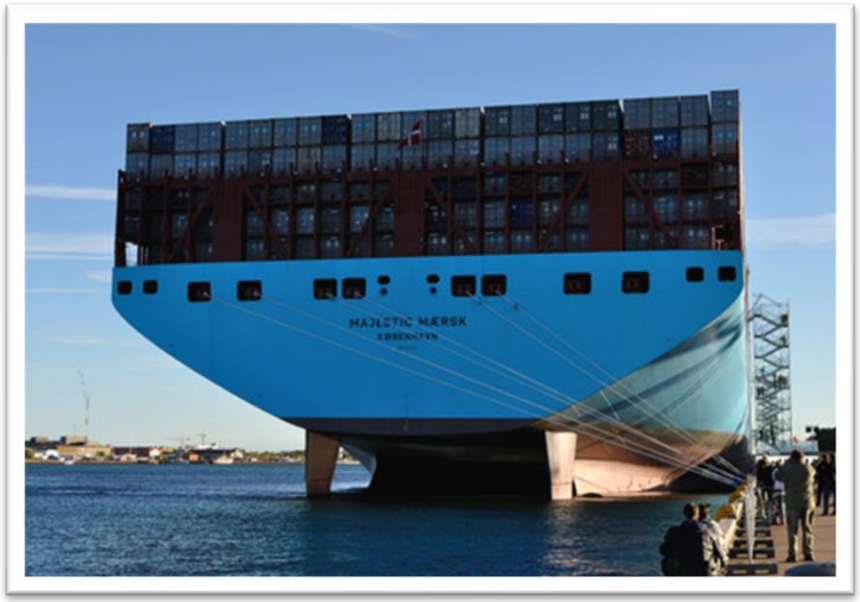
RACI-model til varetagelse af informationssikkerhed

		Styring af informations-sikkerhed	Udvikling af politik for informations-sikkerhed	Risiko-vurdering og håndtering	Leverandør-styring	Hændelses-håndtering	Beredskabs-planlægning	Uddannelse og oplysning	Planer for sikkerheds-aktiviteter	SOA-dokumentet
ROLLER	Topledelsen	A	A	A	A	A	A	A	A	A
	Mellemledere	A	A	A	A	A	A	A	A	A
	Medarbejdere					I	I	I	I	
FUNKTIONER	Informationssikker-hedsudvalget	R	R	R	I					
	Informationssikker-hedskoordinatoren	S	S	S	S					
	Systemejere			C	C					
	Dataejere			C	I					
	DPO		C	C	C					
	Jura/Kontrakt		C	C	C					
	HR		C	C						
	It-ansvarlige, It-arkitekter		C	C	R					
	Økonomi		C	C	I	C	I	I	I	I

https://sikkerdigital.dk/myndighed/iso-27001-implementering/forstaa-arbejdet-med-informationssikkerhed/rejsefortaellingen/

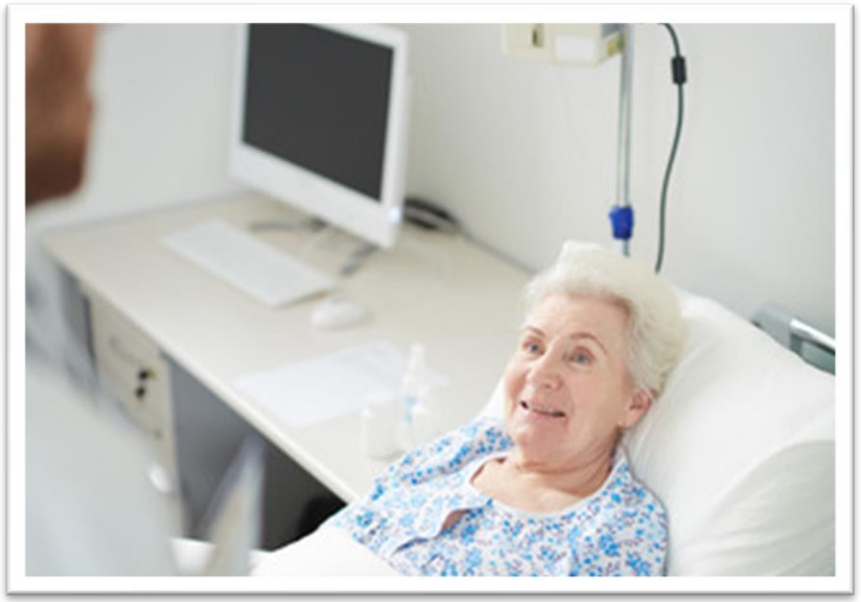
DANSK STANDARD

Forretningen… og privatlivshensyn efter ISO/IEC 27701



”…bevare fortrolighed, integritet og tilgængelighed af information ved hjælp af en risikostyringsproces…”

ISO/IEC 27001



”… beskytte privatlivet, der potentielt kunne være påvirket af behandlingen af personoplysninger”

ISO/IEC 27701

DANSK STANDARD

Supplerende databeskyttelsesprincipper

- Tab af fortrolighed: Uautoriseret adgang til informationer
- Tab af integritet: Uautoriseret ændring af informationer
- Tab af tilgængelighed: Tab, tyveri eller uautoriseret fjernelse af informationer
- Tab af driftskontrol: Overdreven indsamling af persondata
- Uautoriseret eller uhensigtsmæssig sammenkobling af persondata
- Manglende gennemsigtighed: Utilstrækkelig information om formålet med behandlingen af persondata
- Behandling uden orientering af eller samtykke fra den registrerede

DS
DANSK STANDARD

Nøgleprocesser i ISO/IEC 27701 til GDPR-håndtering

DANSK STANDARD

Business Continuity efter ISO 22301

1. Beskytte prioriterede aktiviteter
2. Stabilisere, fortsætte og genetablere prioriterede aktiviteter
3. Mindske, besvare og styre konsekvenser

DANSK STANDARD

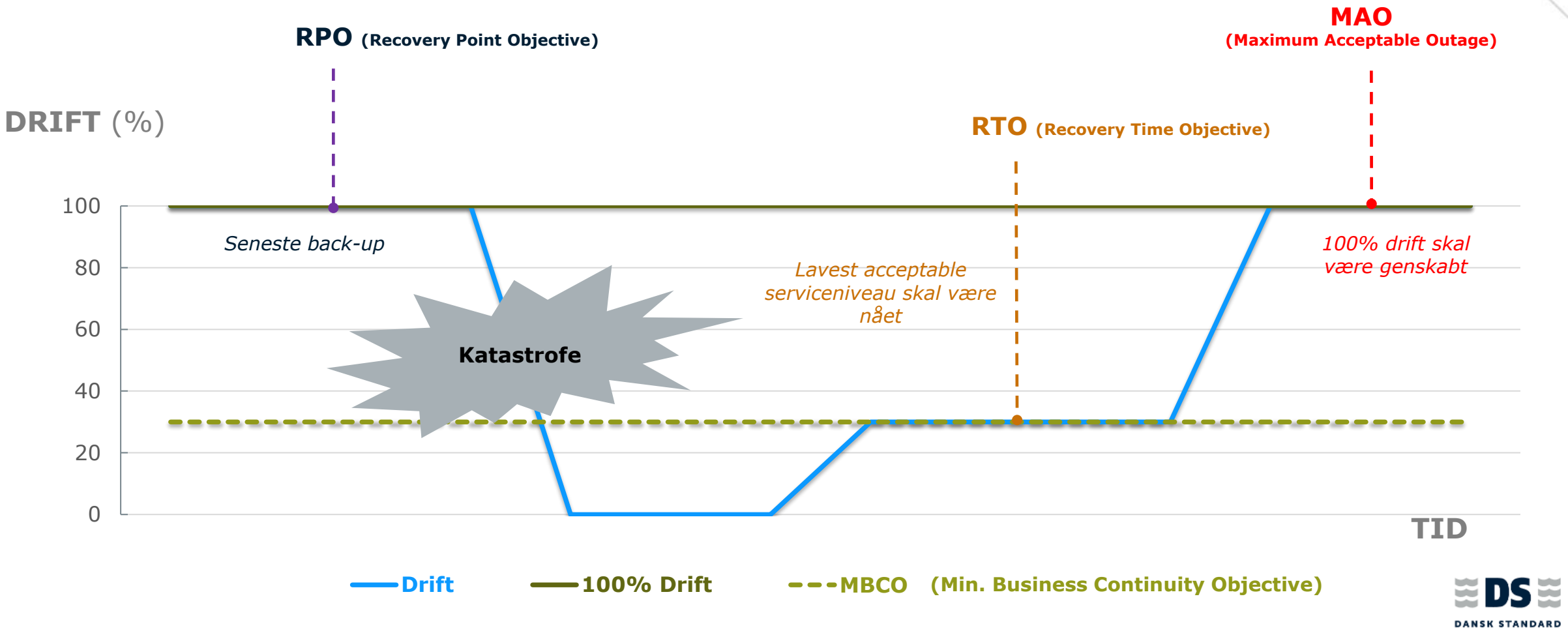
Benhård prioritering via Business Impact-analyse

Formulering af Business Continuity-krav – eksempel

Forretningsproces	Konsekvensniveau	RTO	MAO
Løn	Begrænset	1 uge	2 måneder
Affald	Vigtigt	3 dage	1 uge
Mad	Kritisk	5 timer	1 dag
Rengøring	Alvorligt	2 dage	1 uge
Medicin	Kritisk	1 time	1 time

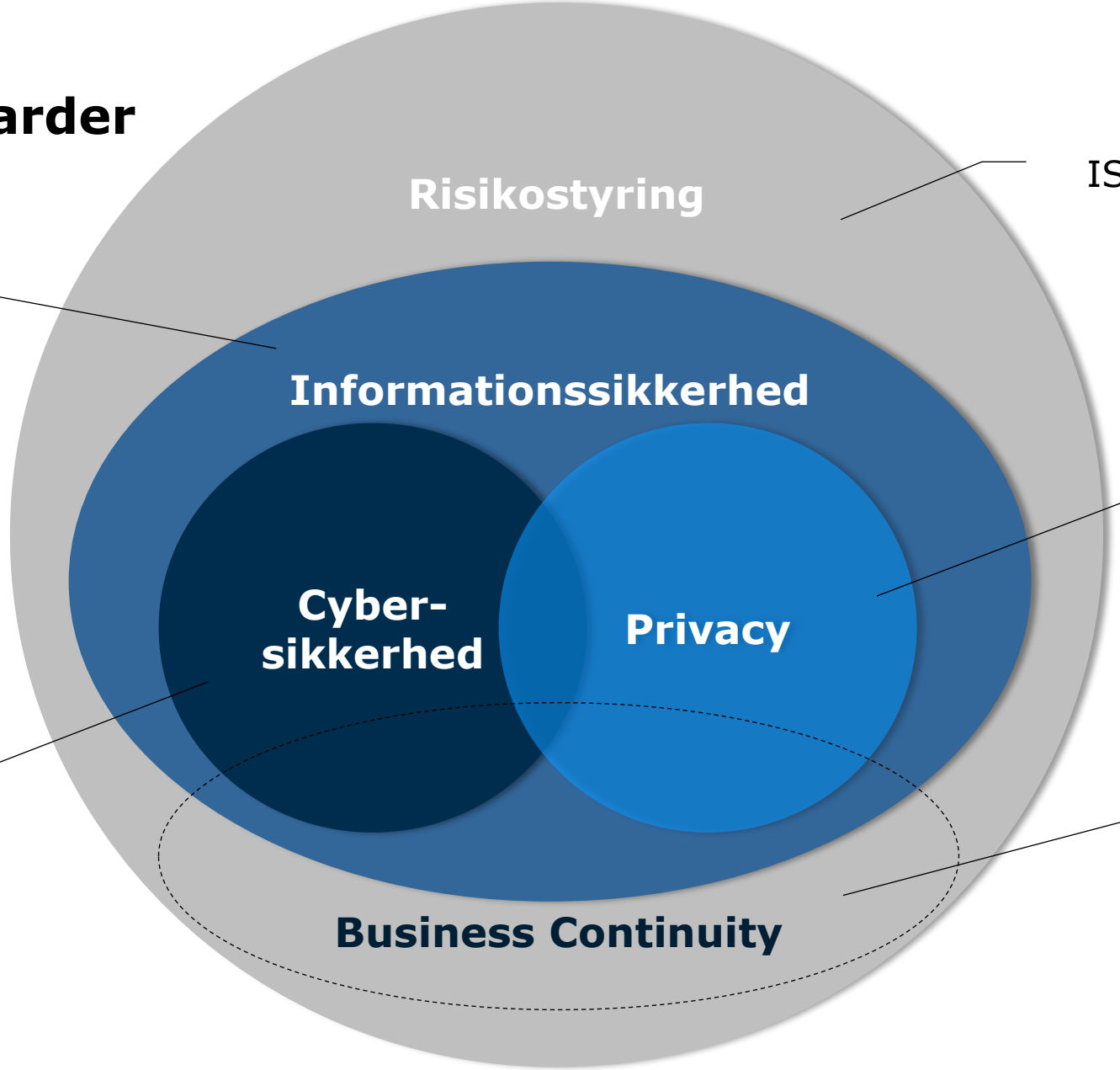
DS DANSK STANDARD

Implementering af målsætninger for Business Continuity



DANSK STANDARD

Vigtigste standarder



ISO/IEC 31000

ISO/IEC 27001

ISO/IEC 27701

ISO/IEC TS
27110

ISO 22301

DANSK STANDARD

Tak for jeres tid!

DANSK STANDARD

Anders Linde
Tlf.: 6162 1500
E-mail: ali@ds.dk