# Standarder skaber rammerne for DSB's arbejde med cyber- og informationssikkerhed

3. OKTOBER 2024

# Om DSB

Vi er en selvstændig offentlig virksomhed, der drives kommercielt. Vi har bundet Danmark sammen siden 1885.

Vores omsætning er baseret på salg af vores billetter og trafikkontraktindtægter fra staten. Samt særskilte indtægter fra kiosksalg, ejendomsudlejning og –udvikling.

Danskerne foretager *i runde tal* 160 mio. rejser med vores 400 tog, der samlet kører 50 mio. km årligt fra vores +200 stationer.

Vi har +6.000 kollegaer, der repræsenterer mere end 70 nationaliteter med stor diversitet i køn, alder, uddannelsesbaggrund mm.

Vi har stærke samarbejder med både kommercielle og non-profit organisationer

# Sune Aggergaard Mortensen
CISO

- CISO i DSB siden 2020
- CISO fra 2012 - 2020 i den finansielle sektor
- Tidligere IT-arkitekt, teknisk projektleder, udviklingschef samt rådgiver
- Civilingeniør fra DTU

- Næstformand i IT-Sikkerhedschefkredsen (CISOgroup.dk)
- Årets CISO i 2022
- Bred erfaring inden for Cybersikkerhed, Cloud, Governance, GDPR, NIS/NIS2 og compliance

# Agenda

1. Hvorfor standarder for cyber- og informationssikkerhed
2. DSB’s rejse med ISO 27001
3. Udnyttelse af eksisterende strukturer for at lette implementering
4. De største udfordringer i et ISO 27001 forløb
5. Praktiske råd og anbefalinger
6. Værdi skabelsen for DSB

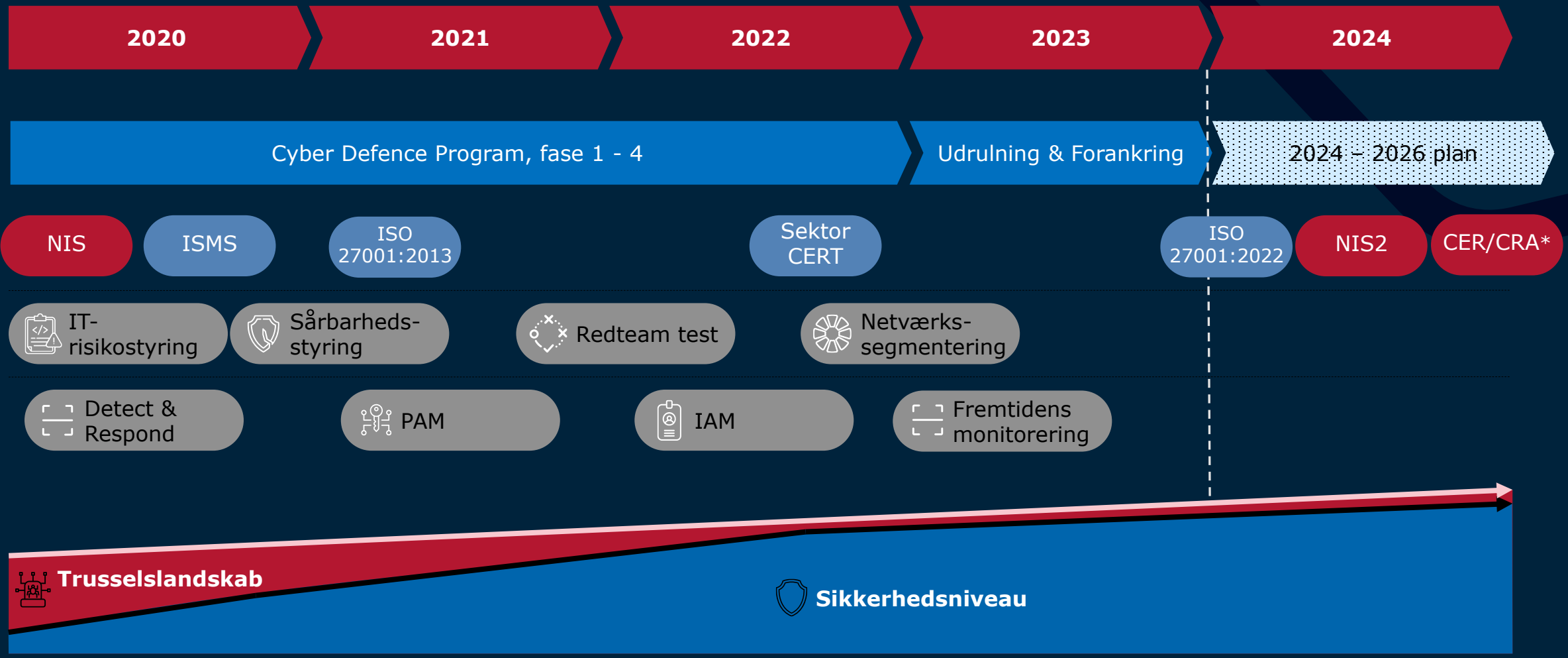
# HVORFOR STANDARDER FOR CYBER- OG INFORMATIONSSIKKERHED?

1. Øget digitalisering og kompleksitet kræver en systematisk tilgang til Cyber- og informationssikkerhed
2. Eksterne forventninger fra myndigheder, samarbejdspartnere og nye kollegaer
3. Angrebsfladen vokser med flere digitale systemer, services, partnere og leverandører
4. Standarder som ISO/IEC 27001 hjælper med at skabe struktur og konsistens i sikkerhedsarbejdet
   - Standarder rammesætter et perspektiv – på godt og ondt
5. ISO-standarder giver en fælles ramme for at måle, styre og forbedre informationssikkerheden over tid

# DSB'S REJSE MED ISO 27001

1. Certificeret efter ISO 27001:2013 første gang i Q1 2021 drevet af krav fra NIS direktivet
2. Beslutning om systemunderstøttelse af risikovurderinger, kontrolopfølgning, afvigelsesstyring mm.
3. Brug af ITIL-rammeværket som grundlag for forankringen i IT operations
4. Opfølgning og krav til leverandør integreret i vores indkøb og udbudsprocesser
5. Seneste fuld certificering i Q1 2024 efter ISO 27001:2022
6. Fokus på løbende forbedring og tilpasning af krav, processer og den tekniske implementering

# DSB har realiseret et løft af cyber-området, hvor vores ISO Certificering var en integreret komponent

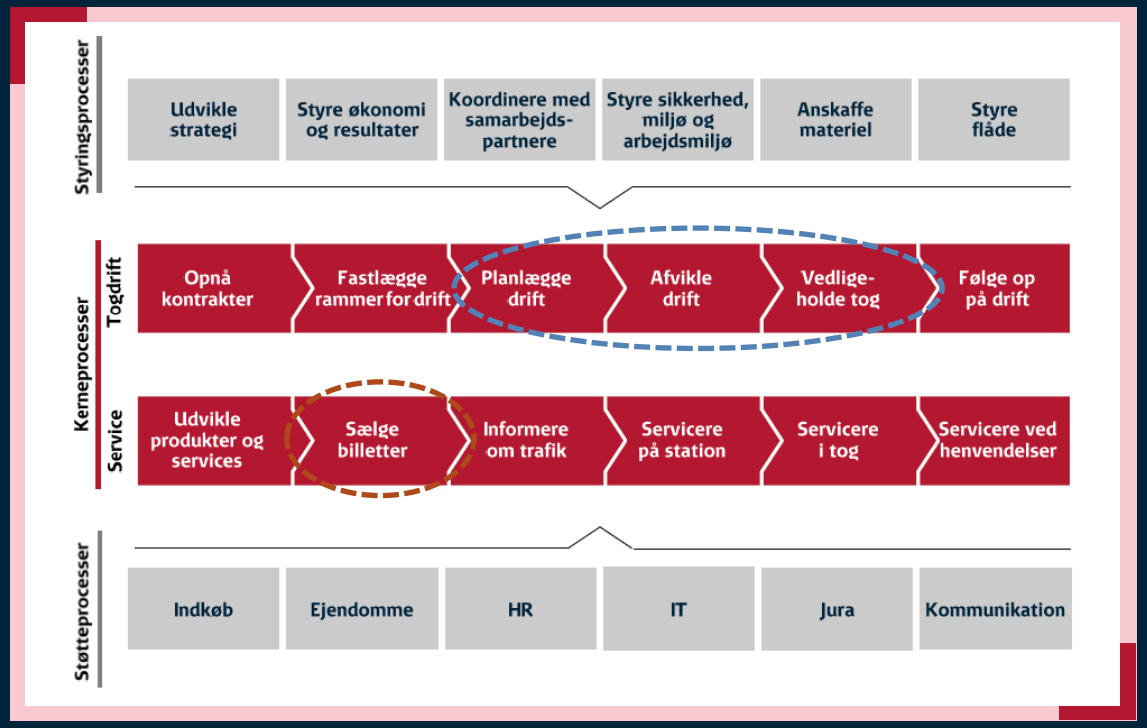



*CER – Critical Entities Resilience Directive & CRA – Cyber Resilience Act

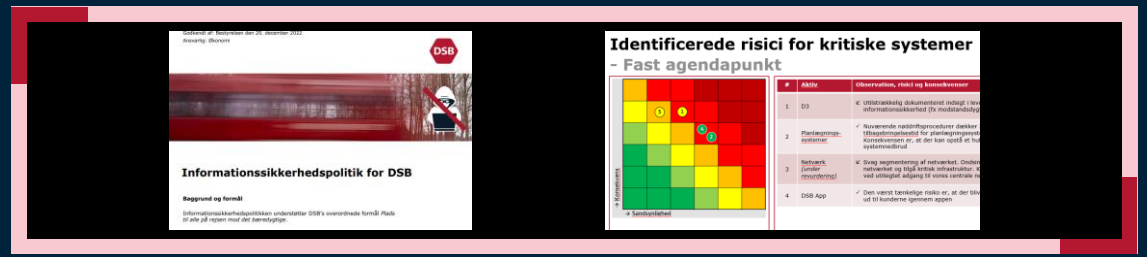
# UDNYTTELSE AF EKSISTERENDE STRUKTURER FOR AT LETTE IMPLEMENTERING

1. Fokus på governance-strukturer, der bygger på eksisterende virksomhedsstyringsdokumenter, strukturer og forretningsprocesser
2. Tager udgangspunkt i virksomhedens eksisterende risikostyring og det etablerede samarbejde i mellem bestyrelse og topledelse samt samarbejde i mellem organisation og topledelse
3. Udnytte eksisterende indkøb- og udbudsprocesser til at sikre krav og opfølgning på leverandører
   - Overvej kompromiser mhp. at sikre stærk forankring
4. Tilpasning af eksempelvis ITIL-proces implementering for at imødekomme relevante it-sikkerhedskrav
5. Anvende og udbygge eksisterende roller
6. Samarbejde mellem sikkerhedsteams og forretningsenheder for at sikre alignment

# Governance og styringsmodel tager udgangspunkt i etableret terminologi







# DE STØRSTE UDFORDRINGER I IMPLEMENTERINGEN AF ISO 27001

1. Mindset som: ”IT-Sikkerhed er det noget foregår i en IT-sikkerhedsafdeling - eller hos CISO”
2. ”Oversættelse” af standard til en DSB kontekst samt afmystificering af kontroller i ISO 27002
3. Organisatorisk modstand/manglende prioritering i forbindelse med tilpasning og forankring af nye krav
4. Gøre risikovurderinger til noget alle relevante parter forstår og kan arbejde med
5. Ressource- og kapacitetsproblemer – at finde balance mellem daglig drift og nye sikkerhedsforanstaltninger og løbende opfølgning på kontroller
6. Sikre ledelsesforankring og forståelse af langsigtede sikkerheds-målsætninger

# Råd og anbefalinger i forbindelse med et ISO 27001 forløb

## FØRSTE CERTIFICERING

- Fokuser på at få etableret og defineret indholdet af de væsentligste ”roller” som systemejer, systemansvarlig, etc. Så der opnås et tydeligt ejerskab af hvem der er ansvarlig for implementering og hvorledes effektivt egentlig måles
- Skarphed på hvor sikkerhedskrav ”blot” følger eksisterende niveau og hvor niveauet hæves
- Inviter din Auditor ind til et forudgående forløb før selve certificeringen – få den gode dialog. Brug rådgivere med omtanke
- ”Dress rehearsal” – gør din organisation bekendt med og tryg på de konkrete audit forløbet
- Fokuser på simplicitet inden for både risikostyring, opfølgning og processer

## LØBENDE VEDLIGEHOLD OG UDVIKLING

- Som udgangspunkt daler modenhed i et ”alt andet lige scenarie”
- Evaluering og opdatering af processer, der blev etableret i forbindelse med 1. certificering (måske det gik lidt stærk ☺)
- Systemunderstøttelse og automatisering skal løbende overvejes
- Proaktivitet i forhold til nye teknologier, partnerskaber og implementeringer
- Få etableret et ”ambassadørnetværk” de væsentligste steder i organisationen
- Få delt budskaber og resultater om audits, beredskabsafprøvninger, Pentest, etc.

# HVILKEN VÆRDI HAR ISO 27001 FORLØBET SKABT FOR DSB?

1. Øget sikkerhedsbevidsthed på alle niveauer af organisationen
2. Bedre samarbejde og et fælles sprog mellem IT, forretning og ledelse om sikkerhedsspørgsmål og it-risiko
3. Større bevidsthed om risikostyring og fokus på hvad der reelt driver risiko
4. Øget compliance i forhold til regulatoriske krav
5. Solidt grundlag for overgang til – og implementering af NIS2
6. Mere ensartet sikkerhedskrav og implementering på tværs af teknologi og processer


DSB