

DANSK STANDARD | CYBERDAG 2025

ISO 27001 & 27701

**Sådan understøtter internationale
standarder kerneforretningen hos
Falck**



Agenda

1. Introduktion
2. Hvorfor ISO?
3. Implementeringen i Falck DT
4. Fra implementering til drift
5. Q&A





Introduktion



Mudassir Mohammad

Group CISO, Falck

CEH, CCSP

- IT-sikkerhedskonsulent, Københavns Kommune
- IT-consultant across multiple organisations, supporting critical infrastructure and digital transformation
- BSc, DTU



Peter Kaas

- Head Digital Legal & Compliance, Falck
- Advokat
- FIP, CIPP/E, CIPM, CISM
- Ekstern lektor i Teknologiret, IT-kontraktret og European Data Protection Law, Københavns Universitet
- Group DPO og Senior Legal Counsel, NNIT
- Legal Counsel, Atea
- Advokat i førende danske advokatkontorer
- Cand.jur., Københavns Universitet
- LLM, University of Virginia



Our purpose

**Advance
sustainable
healthcare
to meet people's
changing needs**



Falck at a glance



Falck delivers key healthcare services across preventive, acute and rehabilitative care

	Preventive	Acute	Rehabilitative	Type of care
Ambulance		•		Societal
Fire services and prevention	•	•		Societal / Individual
Healthcare at home	•	•	•	Societal / Individual
Healthcare treatment and guidance	•	•	•	Individual
Patient transportation	•		•	Societal / Individual
Roadside and civil assistance		•		Individual
Safety equipment and guidance	•			Individual
Travel and security assistance	•	•		Individual

Founded

1906

Services in 2024

9.5 million

Revenue DKKm 2024

12,134

Highly skilled professionals

+25,000

Countries

25

Our geographical strongholds



US / California

Market attractions

- California is a "G7-sized economy" with the biggest global per capita spend on healthcare
- Big opportunity to bring down spending and strains on healthcare systems with a high willingness to pay and openness to innovation

Falck's position

- A leading Californian 911 position
- Emerging position within Mobile Health market and similar adjacent services



LATAM / Colombia

Market attractions

- Developing economies with ~ 650m population.
- Growing middle classes seeking better healthcare services in a market with scarce healthcare resources
- Colombia is the third largest economy in South America, and a lack of a publicly funded healthcare system facilitates innovation

Falck's position

- A leading provider with strongholds in Colombia, offering subscription-based pre- and post-hospital services
- Globally leading digital healthcare services



Europe / Scandinavia

Market attractions

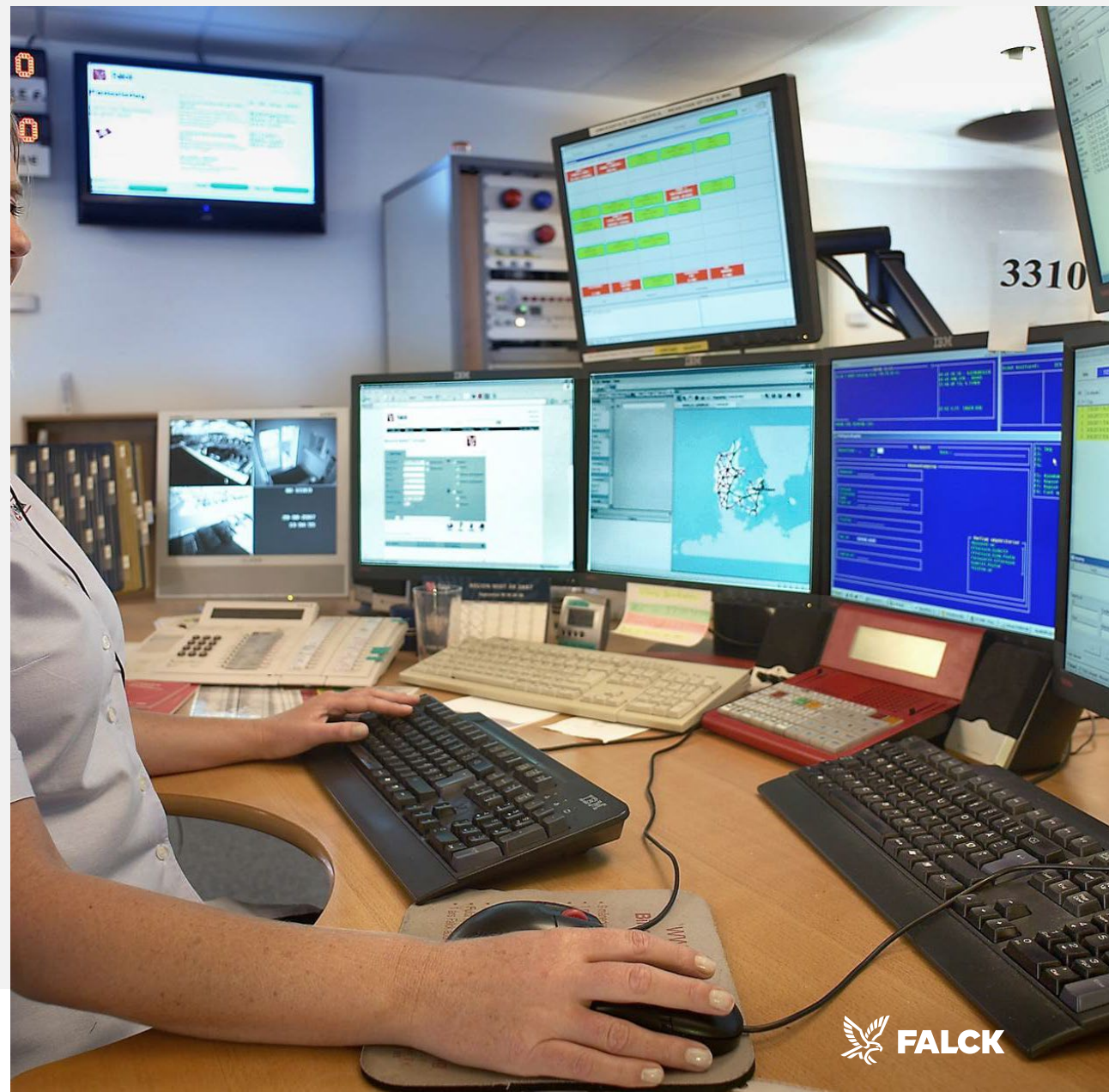
- Mature market with generally publicly funded healthcare systems – challenged financially and capacity wise with high demand for new solutions
- Large, growing and affluent B2B/B2C markets
- European stronghold countries include Denmark, Norway, Sweden, Poland, Germany and Spain

Falck's position

- Falck's original home market
- A fully integrated pan-Scandinavian healthcare provider
- A partner and a supplement to public healthcare systems
- Expanding EMS positions into the emerging market for mobile healthcare services



Hvorfor ISO?



Lidt om standarderne

- ISO 27001 – **ISMS** (Information Security Management System)
 - 2005 (baseret på tidligere standarder fra 1990'erne. Løbende opdateringer (2013, 2017 og seneste version fra 2021)
 - I Danmark erstattede den DS 484. Siden 2016 har det været et krav for offentlige myndigheder.
- ISO 27701 – **PIMS** (Privacy Information Management System)
 - En nyere standard (fra 2019).
 - En certificerbar udvidelse til ISO 27001.
 - For at blive certificeret under 27701 skal man være 27001-certificeret
- Integreret ledelsessystem
 - Andre typer, f.eks. ISO 9000 (kvalitet) og 14001 (miljø).
- Risikobaserede standarder
- Overordnede krav til ledelsessystemet
- Bilag med specifikke krav (kontroller/foranstaltninger)



Dansk standard

DS/EN ISO/IEC 27001:2017

4. udgave
2017-02-28



Dansk standard

DS/EN ISO/IEC 27701:2021

2021-04-28

**Sikkerhedsteknikker – ISO/IEC 27001
og ISO/IEC 27002 udvidet til at omfatte
privatlivsbeskyttelse – Krav og vejledning**

Security techniques – Extension to ISO/IEC 27001 and
ISO/IEC 27002 for privacy information management –
Requirements and guidelines (ISO/IEC 27701:2019)

Business Case



Stærk governance

Én global certificering sikrer ensartet struktur for informationssikkerhed og databeskyttelse på tværs af hele Falck – i stedet for individuelle løsninger.



Effektivitet & besparelser

ISO-certificering reducerer omkostninger og ressourceforbrug markant sammenlignet med ISAE 3000/3402.



Compliance

Opfylder internationale standarder og kundekrav – gør det lettere at vinde udbud og sikre GDPR-overholdelse.



Inspektionsparathed

Certificeringen forbereder Falck på fremtidige audits og sikrer løbende kontrol og transparens.



Implementeringen i Falck Digital Technology



The certification project

Internal "sales pitch"

Purpose



- To obtain **cost effective** security
- To obtain **evidence** for Compliance
- To obtain a **systematic approach** to risks
- To gain a **competitive advantage**

Scope



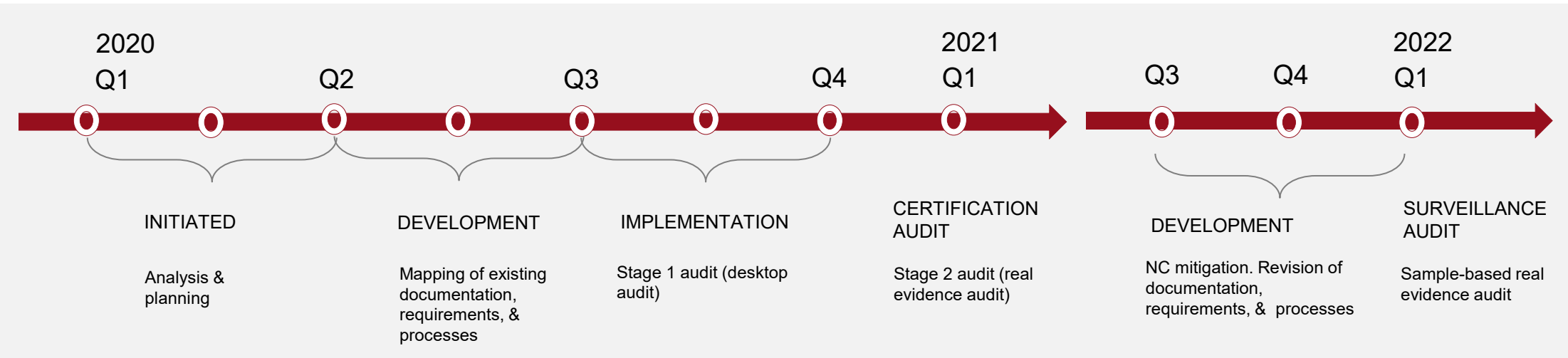
Information Security and PII applicable to management of platform and infrastructure, administration and operation of core IT business systems.

Goal

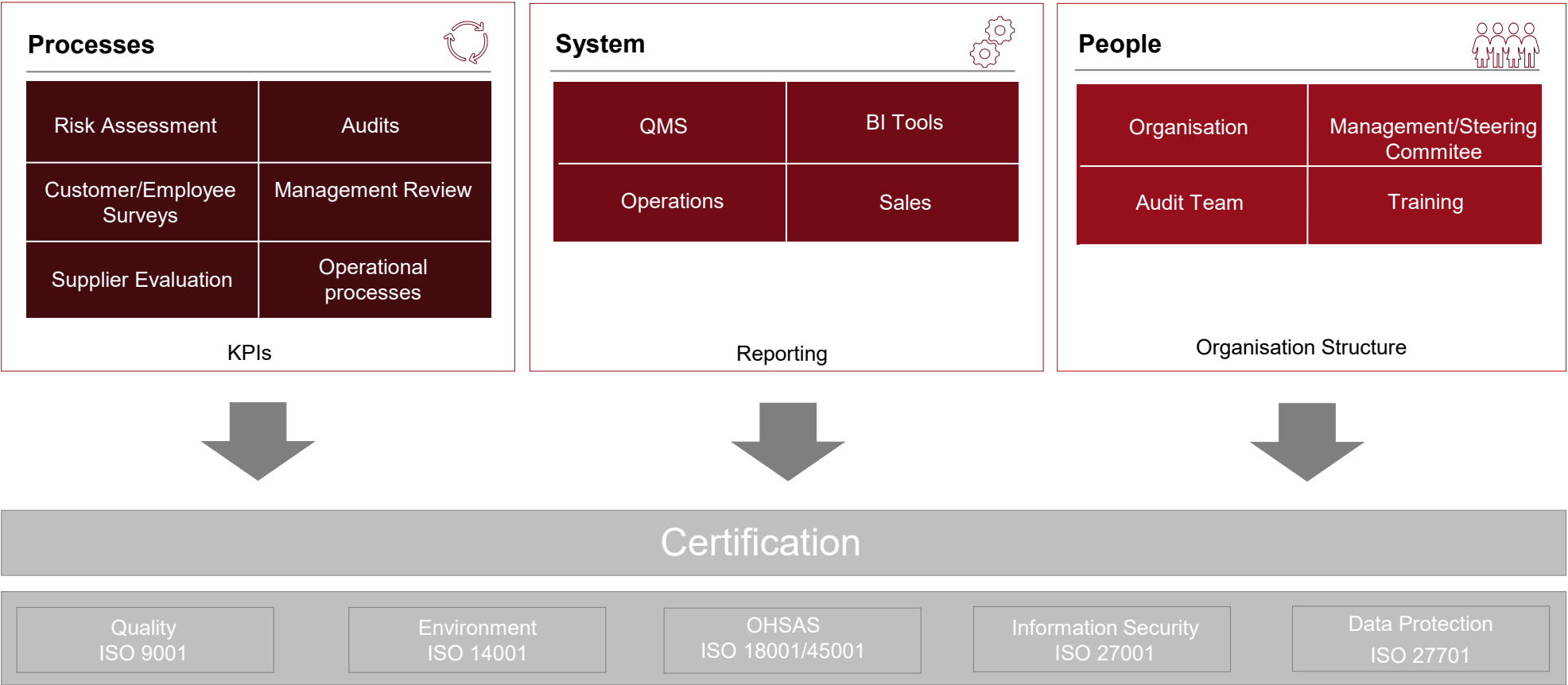


Better work practices within IT security/ GDPR that support business goals

Timeline



Integration with existing management systems

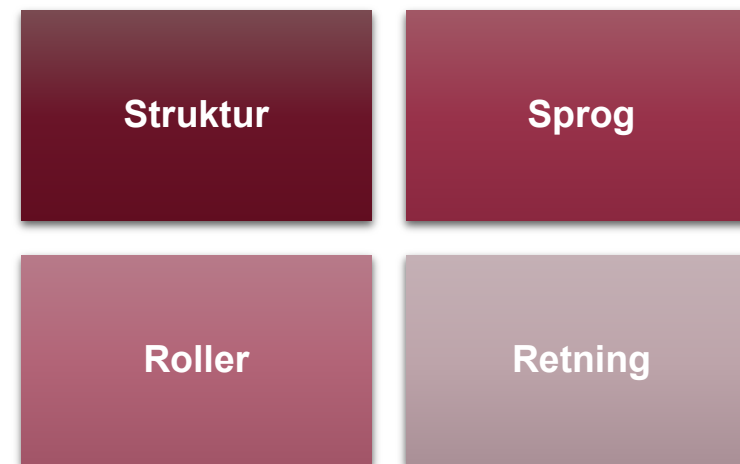




Fra implementering til drift



Fra lokale forskelle til fælles retning

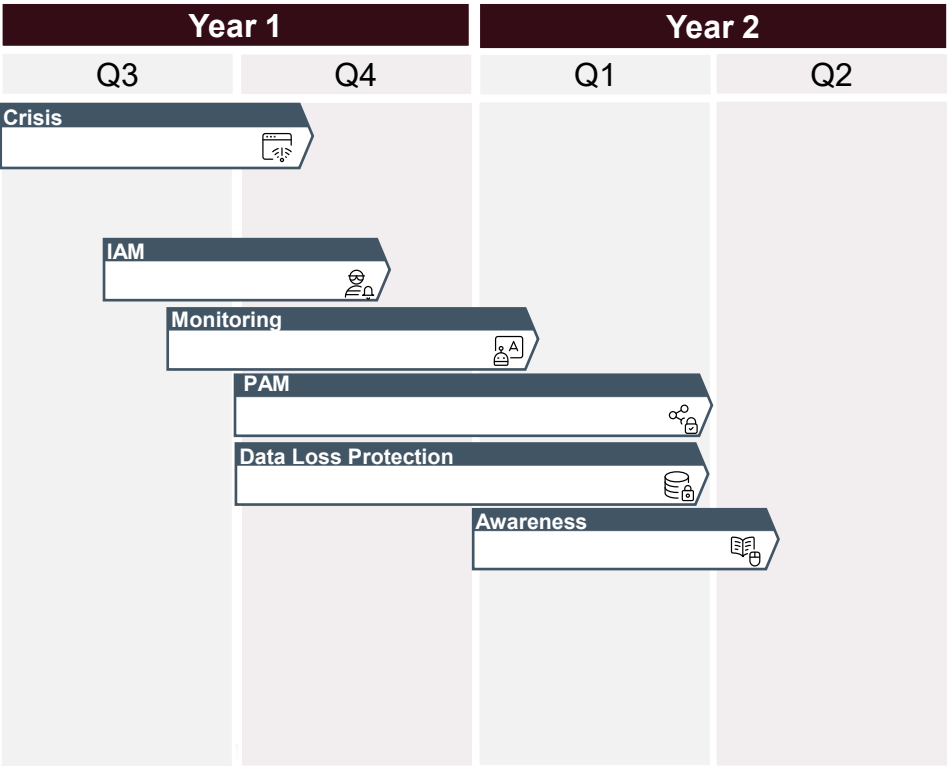


Prioritering og Roadmap

- ISO hjalp os med at identificere gaps
- Tydeliggjorde områder hvor vi manglede modenhed



- Risikovurderinger, NIST CSF og CIS
- → Resultatet blev en fokuseret tilgang til Cyber security roadmap



Risikotilgang og ejerskab



ISMS

ISMS blev vores strukturelle fundament for governance.

Det fungerer som en faciliterende ramme, ikke for at eje risikoen, men for at sikre, at styring og ansvar placeres korrekt i organisationen.



Risikostyring

Risici identificeres og håndteres løbende med fokus på forretningskritikalitet.

ISMS understøtter, at risikovurderinger bliver et aktivt styringsværktøj og skaber overblik til prioritering i vores roadmap.

Summary



Ikke "kun" compliance

ISO gav os mere end bare et stempel.

Det blev en løftestang for at modne sikkerhedsarbejdet og skabe synlig værdi for både IT og forretningen.



Fælles sprog

Fælles udgangspunkt – men vi er ikke i mål.
Dialogen og træning fortsætter.



Vi bygger videre

ISO gav os fundamentet.
NIST CSF og CIS hjælper os nu med at operationalisere, prioritere og måle modenhed, og sikre løbende fremdrift.

Organisatoriske **roller** og artefakter



Governance & Executives

Board of Directors
Audit Committee
Executive Management
Investment Committee



Management

Digital Potential Board
CIO
Business Units
CISO
DPO



Operation

Portfolio Boards
Product Owners
Process & Service Owners
Security Officers
Data Privacy Operations

Code of Conduct, Authorisation Rules & Powers of Attorney, Policies & Standards

Care for More '27, Digital Potential & Data Strategy

ISO 9001, 27001 & 27701

Enterprise Risk Management, Quality Management System, Information & Privacy Management System, ITIL

Certificering – et stop på rejsen...

Projektet

- Ressourcetungt
- Organisatorisk forankring er afgørende (topledelsen og projektledelsen)
- Integration med eksisterende management-systemer (politikker, processer, osv.)

Certificering

- Stage 2 kræver tid og ressourcer
- Dokumentation!
- Audit interviews i alle lag i organisationen
- Klar til audit?

Terminologi

- ISMS og PIMS er teknologineutrale og ikke IT-specifikke som sådan, men kræver i praksis forankring i IT.
- Uoverensstemmelser med GDPR's begrebsverden

NC'ere

- Forvent afvigelser/Non-Conformities (NC'ere)!
- Korte deadlines til udbedring
- Major (3 måneder)
- Minor (plan indenfor 3 måneder)

Scope

- Hele organisationen?
- Central og lokal forankring
- Modenhed
- Begrænset scope (funktionel eller geografisk afgrænsning)

Drift

- Løbende vedligehold (Continuous Improvement)
- Stigende krav fra stakeholders (certificeringsorgan, kunder og tilsynsmyndigheder)
- Teknologi (tekniske foranstaltninger/controller)



Q&A

