Ledelsens ansvar i forhold til cyber- og informationssikkerhed

Nov 2021/Michael Ørnø

STATENS IT

CV - Michael Ørnø

2012-	Direktør, Statens It, Finansministeriet
2009-2012	Vice President, Service and Infrastructure Management, PostNord
2004-2009	IT-driftschef, Post Danmark
2000-2004	Manager, Mainframe operations, Scandinavian Airlines System
1996-2000	Systemchef, MultiData/PBS
1985-1996	Programmør/Systemprogrammør, forskellige firmaer
2015-	Næstformand for bestyrelsen Dansk IT
2012-	Formand fagrådet for IT-drift og Servicemanagement, Dansk IT
2021-	Formand for Dansk Datahistorisk Forening (DDHF.DK)

Taler stadig C og elsker Unix ☺

STATENS IT

Statens interne it-driftsafdeling

Statens It er

En styrelse under Finansministeriet, der leverer it-services til 19 ministerområder

Etableret 1. januar 2010

Resultatet af en fusion af seks ministerielle it-fællesskaber med 8 ministerområder

100% kundefinansieret

Nøgletal

Cirka 500 ansatte

Over 35.000 brugere

Cirka 6.000 serverinstanser

Netværk til ca. 700 lokaliteter

STATENS IT

Ministerområder og kunder

Fun facts

- Den første danske computer - DASK fra 1957 - kørte hemmelige opgaver for Forsvaret
- Første gang passwords bruges på en computer er i 1961 og hacket i 1964
- Første virus på PC var ”Brain” fra 1986 og første antivirus program kom i 1987
- Første virus, der spredte sig via netværk, var i de tidlige 70’ere – ”creeper”
- I de første 20 år af Internettets historie var det ikke velset at bruge nettet til kommercielle aktiviteter
- Elektroniske betalinger udbredes i 90’erne med Dankortet
- 9. april 1999 købte PBS direktør Peter Max blomster til Erhvervsminister Pia Gjellerup hos Interflora på nettet med et Dankort.

Hvad er problemet?

- Viden - Hvis det nu var økonomistyring?
- Sølvpapirshatte?, imperiebygning? & salgs FUD? (Fear Uncertainty & Doubt)
- Pinligt for organisationen -> Hemmeligt!!!
- Udviklingshastighed
- ”Cyber” sikkerhed er ved at være et misvisende ord – det er sikkerhed
- Teknisk gæld

- Er der noget vi overser, eller burde havde gjort?

Hvad er så løsningen på at løfte sit ledelsesansvar?

- Man er nød til at erhverve sig et vist niveau af viden
- Arbejdet skal systematiseres
- Vigtigst er, at arbejde systematisk med risikostyring på forretningsniveau
- Et integreret ledelsessystem

- Løsningen er IKKE at købe et eller andet fantastisk
- Løsninger er IKKE at pumpe penge bevidstløst i en eller anden retning

Systematik i ledelse = ISO 27.001

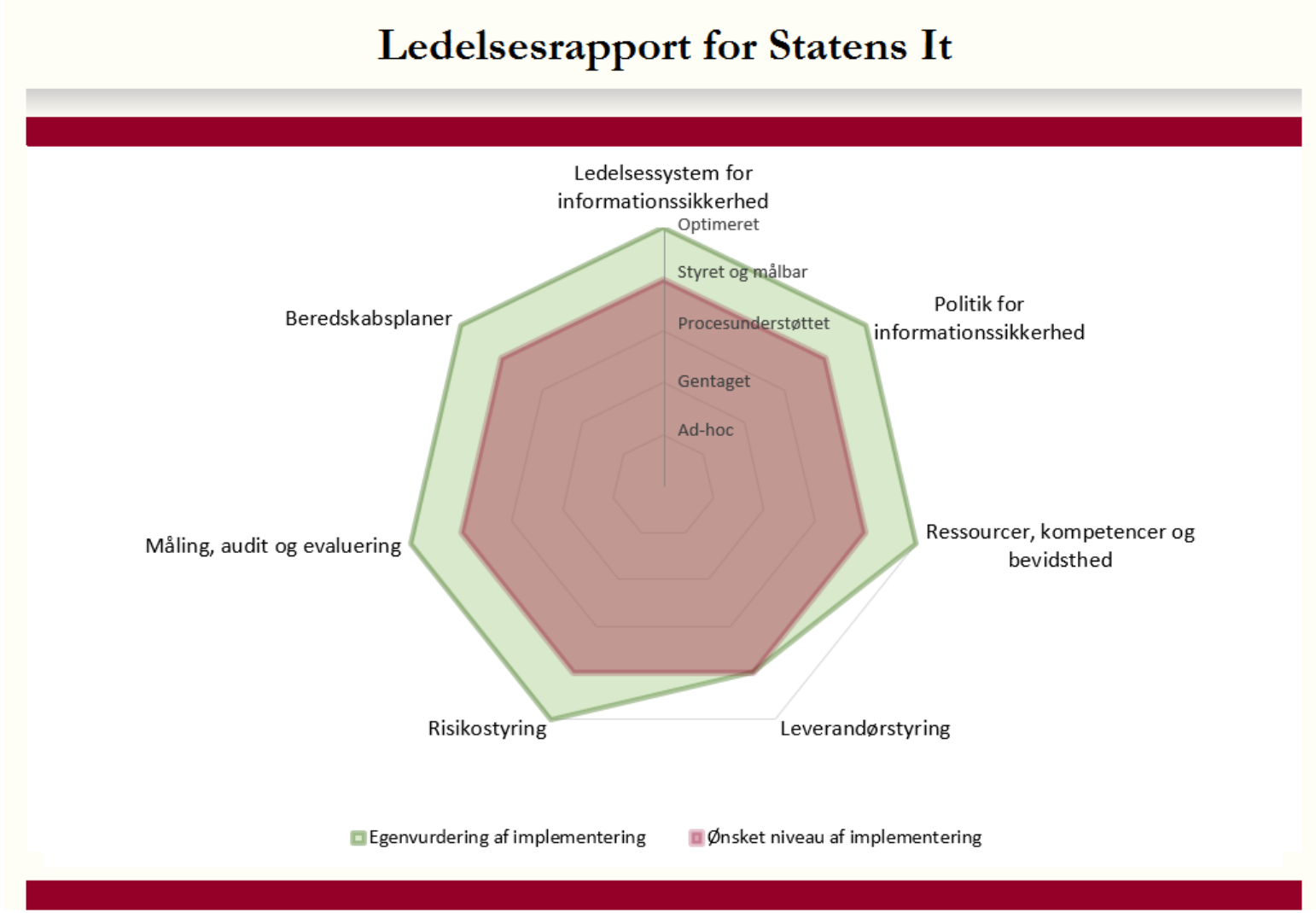
International Standards Organization [edit]

ISO/IEC 27001 specifies 114 controls in 14 groups:

- A.5: Information security policies
- A.6: How information security is organised
- A.7: Human resources security - controls that are applied before, during, or after employment.
- A.8: Asset management
- A.9: Access controls and managing user access
- A.10: Cryptographic technology
- A.11: Physical security of the organisation's sites and equipment
- A.12: Operational security
- A.13: Secure communications and data transfer
- A.14: Secure acquisition, development, and support of information systems
- A.15: Security for suppliers and third parties
- A.16: Incident management
- A.17: Business continuity/disaster recovery (to the extent that it affects information security)
- A.18: Compliance - with internal requirements, such as policies, and with external requirements, such as laws.

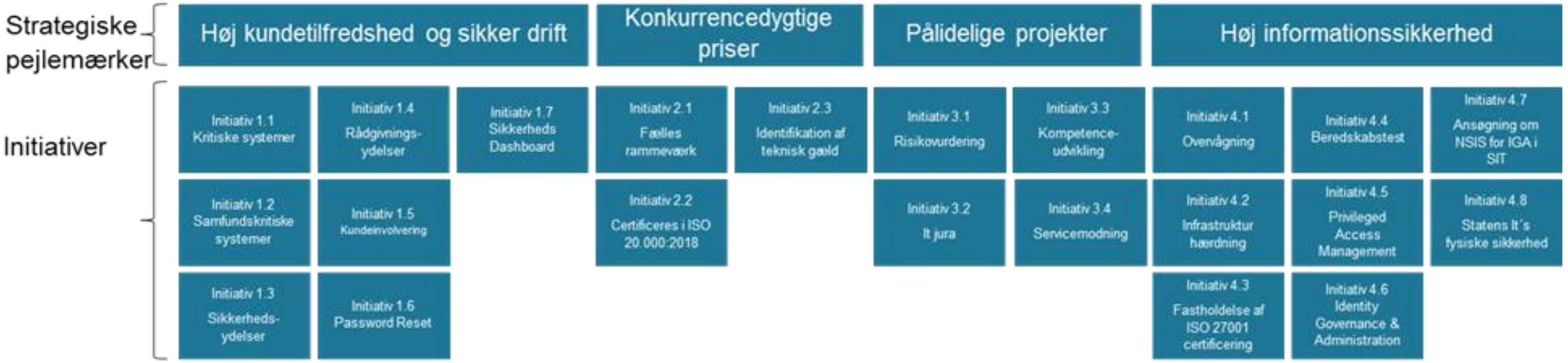
STATENS IT

Evaluering af systematikken



STATENS IT

Eksempel: IT-Sikkerhedsstrategi koblet med forretningsstrategien



STATENS IT

Eksempel: Integreret ledelsessystem

Ugenr.	Dato	Tidspunkt	Procesområde	Ansvarlig
37	**17. september**	Kl. 10.05	Capacity management	Peder
		Kl. 10.15	Proces for dokumenthåndtering	Anders
		Kl. 10.25	RV af Citrix/VIA (herunder ""Sikkerhedshændelse - adgang til [redacted] Confluence")	Ditte
		Kl. 10.35	Brandøvelse - drejebog	Christian H.
		Kl. 10.45	Pause	
		Kl. 10.50	Status på GDPR	Helle
		Kl. 11.00	**Informationssikkerhed & Service Management:** * Nye risici og sikkerhedshændelser * Evt. drøftelse af skriftlige orienteringspunkter - Status på revisioner og tilsyn - Intern audit af leverandørstyring	Vibeke, Anders
		Kl. 11.10	Efterfølgerplaner, nøglemedarbejdere	Pia A.

STATENS IT

Dygtige medarbejdere

- Lettere sagt end gjort
- Råd: Uddan dine egne
  - Proces & styring: Ikke super svært
  - Teknik: Muligt, men en del mere tidskrævende
- Brug markedet klogt
  - Find nogle venner og tag referencer

STATENS IT

Tryghed gennem et integreret ledelsessystem

ISO27001: Informationssikkerhed – Fokus på aktiver

- Statens It certificeret i februar 2014
- Risikobaserede krav til topledelsen, bl.a. evaluering af 'systemet'
- Fortrolighed – Integritet – Tilgængelighed

ISO27701: Privacy Information Management (GDPR)

- Integreret i det eksisterende ISO27001-certifikat i april 2021

ISO20000: IT Service Management – Fokus på services

- Statens It certificeret i februar 2019
- Procesbaserede krav til topledelsen, bl.a. evaluering af 'systemet'
- Kunden i centrum

STATENS IT


Spørgsmål?
STATENS IT