10. juni 2022

Nye strukturer og foranstaltninger

ISO/IEC 27001 og 27002

Dagens program

9.00	**Velkommen**
9.05	**Introduktion til ISO/IEC 27001 og ISO/IEC 27002 samt gennemgang af de væsentligste ændringer i de reviderede versioner** v/ Anders Linde, chefkonsulent, Dansk Standard
9.40	**Brødrene A&O Johansens arbejde med informationssikkerhedsstandarder og værdien af at anvende ISO/IEC 27001 og ISO/IEC 27002** v/ Henning Mortensen, CISO, Brødrene A&O Johansen
10.10	**Spørgsmål**
10.30	**Tak for i dag.**

- **Der er mulighed for at stille spørgsmål undervejs gennem chatten.**
- **Præsentationerne sendes ud efterfølgende**
- **Vi optager webinaret.**

DANSK STANDARD

ISO/IEC 27001 & 27002

Få overblik over ændringerne
i de nye standarder

Samspillet mellem de to standarder

ISO/IEC 27001

ANNEKS A

ISO/IEC 27002

ISO/IEC 27002: en ny temastruktur

ISO/IEC 27002: 2022

5. Organisatorisk

Alt det andet

6. Adfærdsmæssig

Personer: ansatte og eksterne

7. Fysisk

De fysiske rammer og enheder

8. Teknisk

Tekniske tiltag

ISO/IEC 27002: 2013

”Measure that modifies or maintains risk”

Risikovurdering, muligheder for risikohåndtering og kriterier for risikoaccept.

Overholdelse af lovgivning, aftaler eller brancherelaterede krav.

Effekten af samspillet mellem forskellige foranstaltninger.

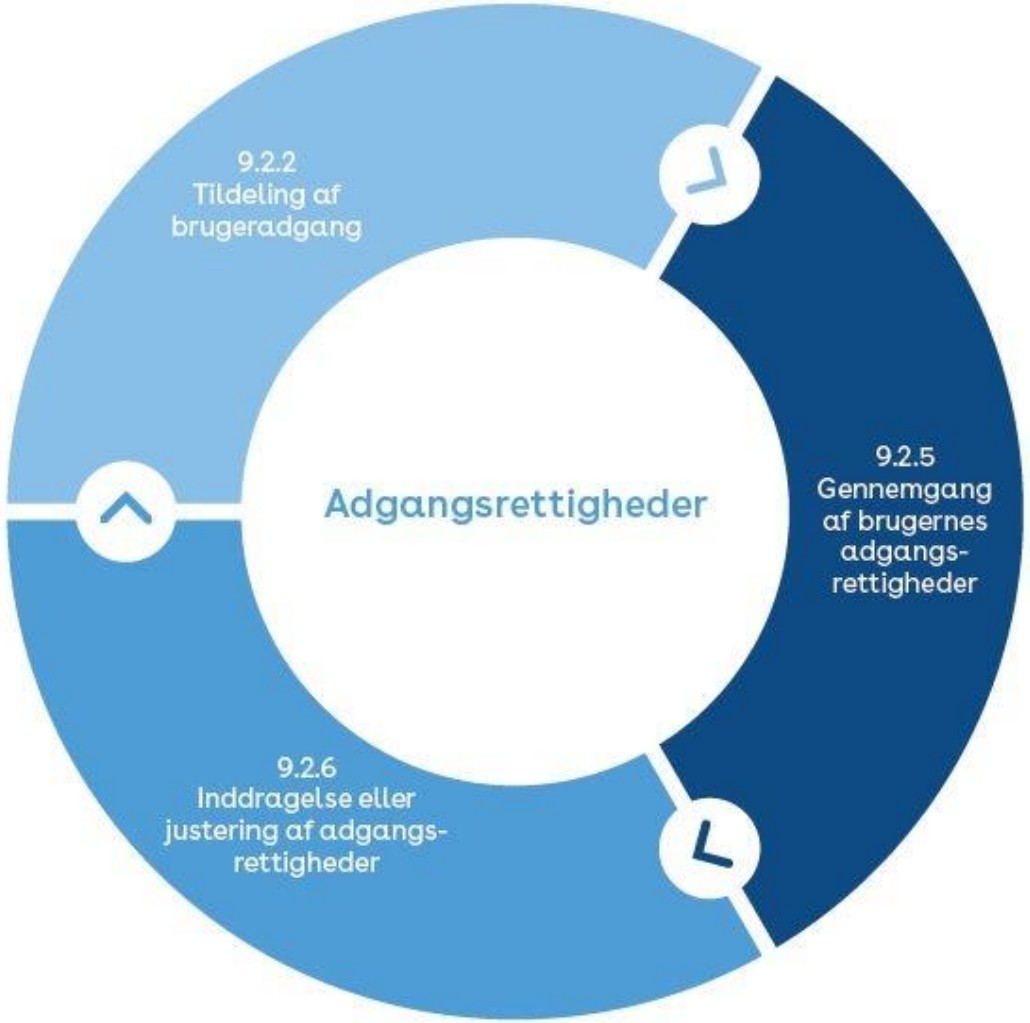
ISO/IEC 27002: less is more!

93

Færre foranstaltninger – eksempel

2013

114



2022

93

ISO/IEC 27002: What's new?

ORGANISATORISK

Threat intelligence

Cloud services

ICT readiness for business continuity

FYSISK

Physical security monitoring

TEKNISK

Configuration management

Information deletion

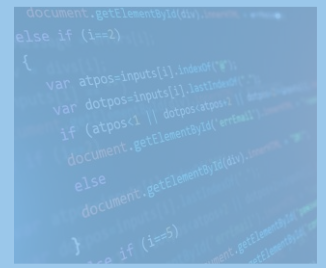
TEKNISK

Data masking

Data leakage prevention

Monitoring activities

Web filtering



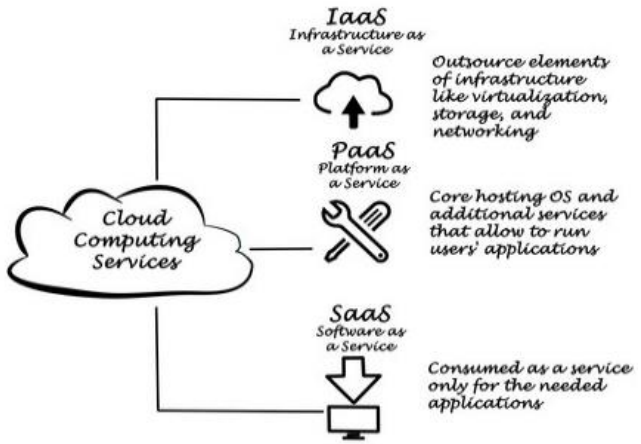
Secure coding

5.7
Threat intelligence (NY)

Indsamling og analyse af viden om trusler

Kilde: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
Kilde: https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2021.pdf

5.23
Information security for use of cloud services (NY)

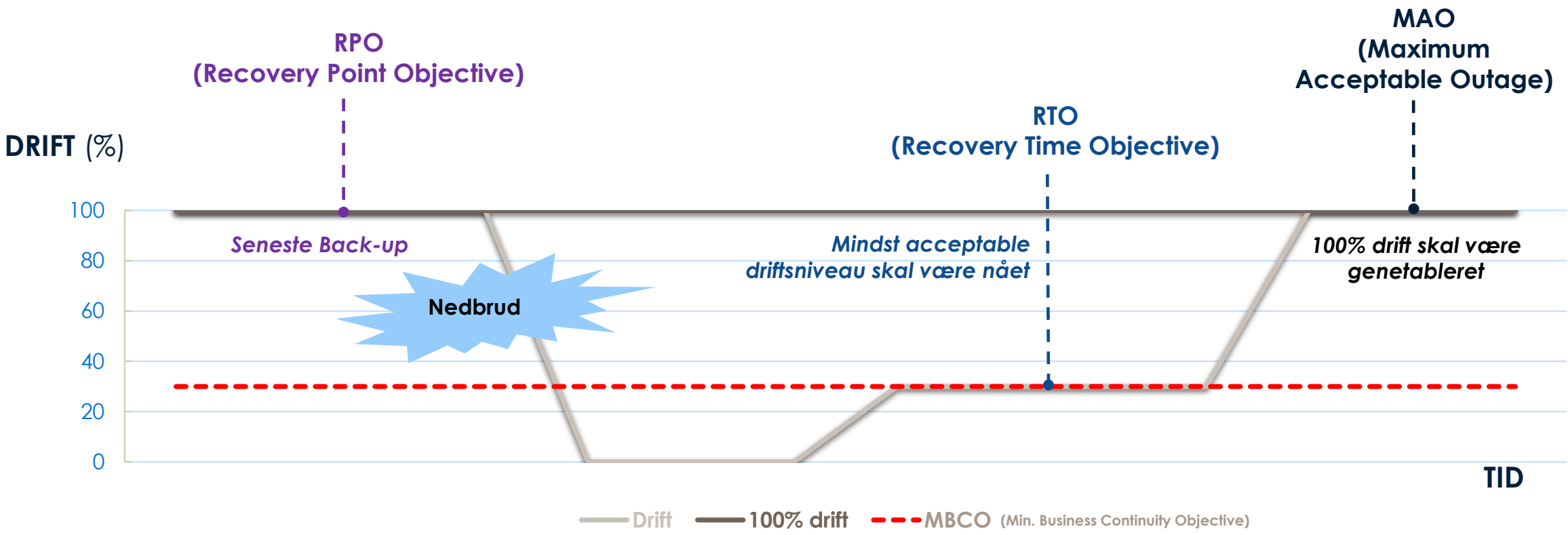


Service
SAAS, PAAS, IAAS

Arkitektur
Privat, offentlig, hybrid

Roller og ansvar
Cloud Service Agreement (CSA)

5.30
ICT readiness for business continuity (NY)



7.4
Physical security monitoring (NY)

Alarmer

Videoovervågning

Bevægelsessensorer

Information deletion, data masking og leakage prevention (NYE)

8.10 Information deletion

Oplysninger i informationssystemer og -enheder bør slettes, når de ikke længere er nødvendige.

8.11 Data masking

Følsomme data, herunder personoplysninger, bør delvist vises eller gemmes eller erstattes af ikke-følsomme data.

8.12 Data leakage prevention

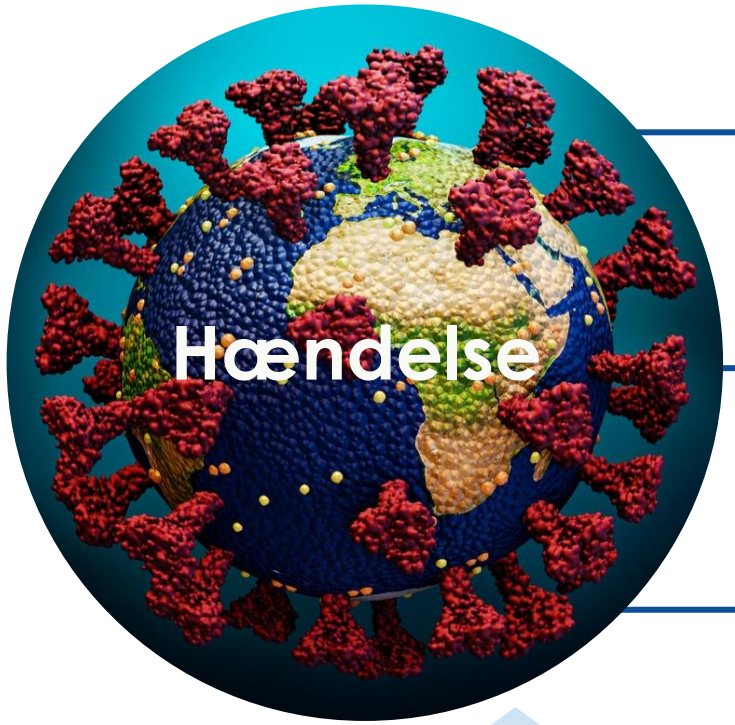
Der bør anvendes foranstaltninger til forebyggelse af datalækage på systemer og netværk, der behandler, lagrer eller overfører følsomme oplysninger.

ISO/IEC 27002: nye perspektiver

5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Attribut 1: typer



Forbyggende

Opdagende

Korrigerende

5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Attribut 2: egenskaber

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

Tab af fortrolighed

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

Tab af integritet

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

Tab af tilgængelighed

5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Attribut 3: cybersikkerhedskoncept

https://www.nist.gov/cyberframework/online-learning/five-functions

5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Attribut 4: driftsressourcer

Asset management

HR

Continuity

Legal

Governance

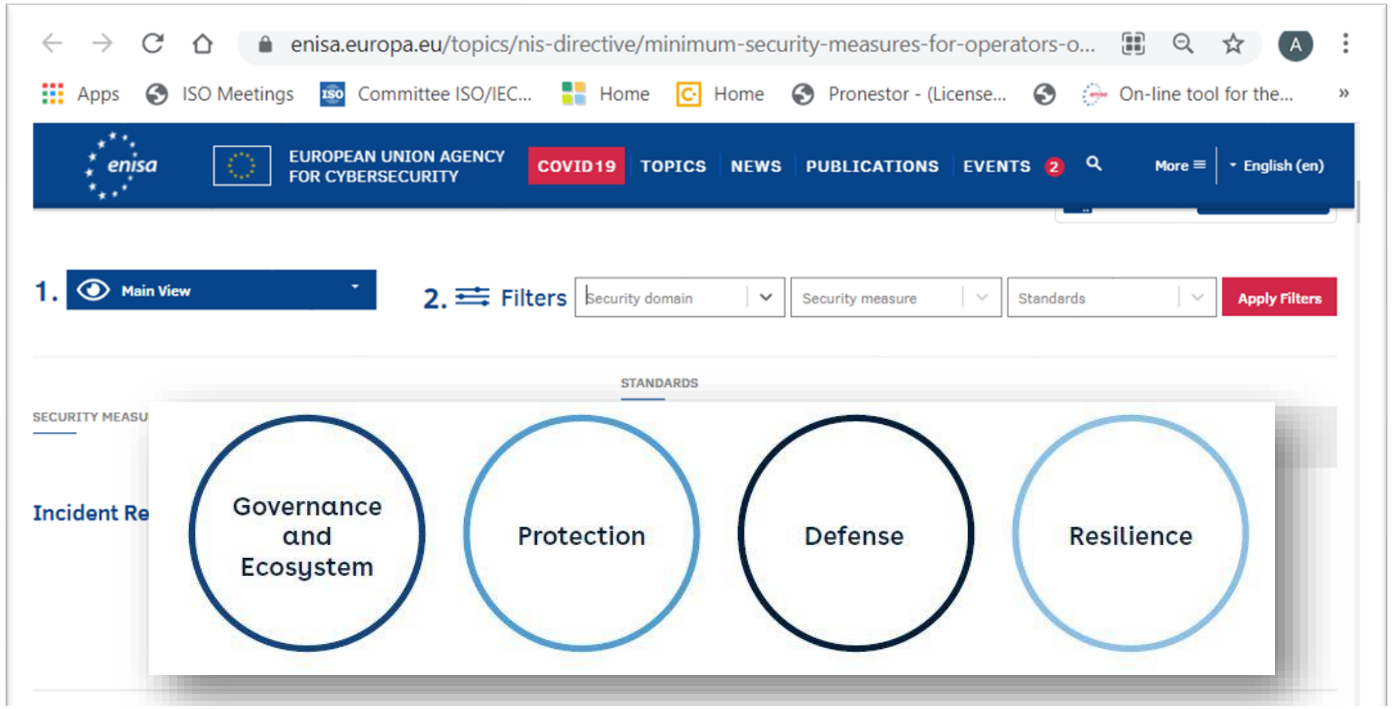
Facility

Application security

5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Attribut 5: sikkerhedsdomæner



5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Formål og underoverskrifter

5.31 Identification of legal, statutory, regulatory and contractual requirements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem #Protection

Control

Information security relevant legal, statutory, regulatory and contractual requirements and the organization's approach to meet these requirements should be identified, documented and kept up to date.

Purpose

To ensure compliance with legal, statutory, regulatory or contractual requirements related to information security.

Et formål per foranstaltning

Underoverskrifter

Cryptography

Cryptography is an area that often has specific legal requirements. The following items should be considered for compliance with the relevant agreements, laws and regulations:

a) restrictions on import or export of computer hardware and software for performing cryptographic functions;

b) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;

c) restrictions on the usage of cryptography;

d) mandatory or discretionary methods of access by the countries' authorities to encrypted information;

e) validity of digital signatures, seals and certificates.

Legal advice should be sought to ensure compliance with relevant legislation and regulations, especially when encrypted information or cryptography tools are moved across jurisdictional borders.

Contractual requirements

Contractual requirements related to information security should include those stated in:

a) contracts with clients;

b) contracts with suppliers (see 5.20);

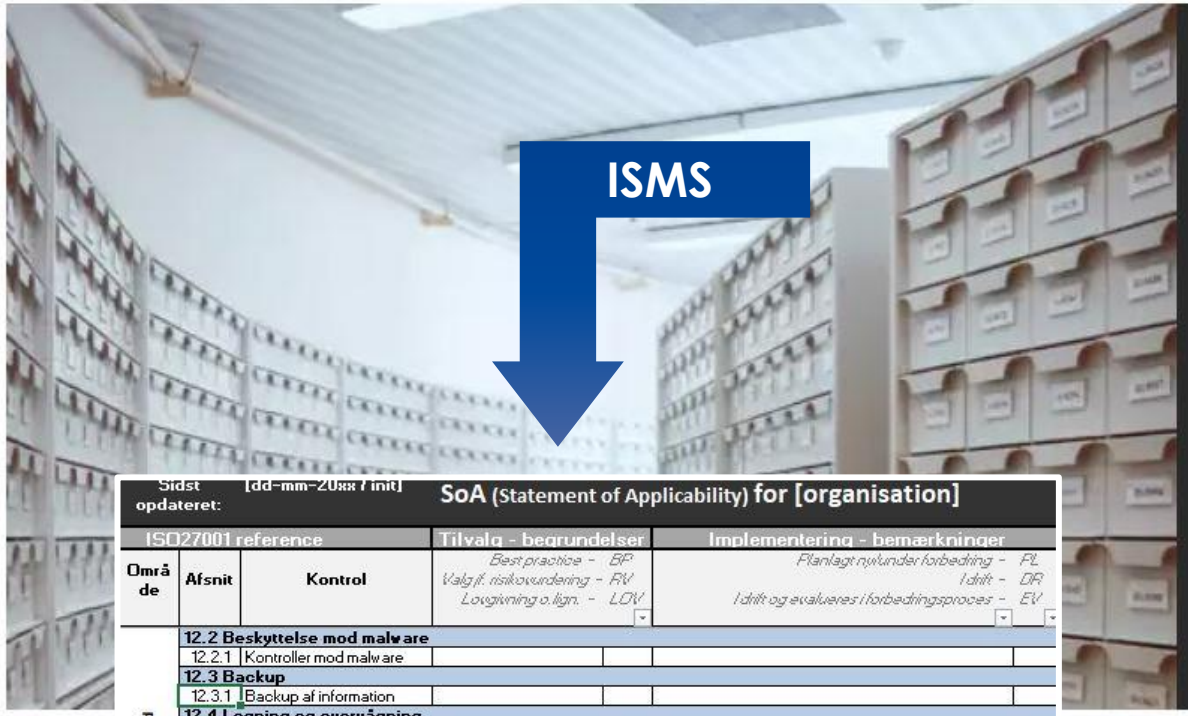
c) insurance contracts.

Implikationer for ISO/IEC 27001… og måske jer

ISO/IEC 27001: 2022

- Gennemgå den nye ISO/IEC 27002's foranstaltninger og tilhørende beskrivelser.
- Prioriter risici og vurder behovet for nye eller ændrede foranstaltninger.
- Identificer nødvendige ressourcer og andre afhængigheder.
- Sæt i værk: implementer de nødvendige foranstaltninger og opdater SoA-dokumentet.

Ind på sikkerdigital.dk



Sidst opdateret: [dd-mm-20xx / init]

SoA (Statement of Applicability) for [organisation]

	ISO27001 reference			Tilvalg - begrundelser		Implementering - bemærkninger	
	Område	Afsnit	Kontrol	*Best practice - BP* *Valg jf. risikovurdering - RV* *Lovgivning o.lign. - LOV*		*Planlagt nylunder forbedring - PL* *I drift - DR* *I drift og evalueres i forbedringsproces - EV*	
		12.2 Beskyttelse mod malware					
		12.2.1	Kontroller mod malware				
		12.3 Backup					
		12.3.1	Backup af information				
		12.4 Logning og overvågning					
		12.4.1	Hændelseslogning				
		12.4.2	Beskyttelse af log-oplysninger				
		12.4.3	Administrator- og operatørlog				
		12.4.4	Tidssynkronisering				
		12.5 Styring af driftssoftware					
		12.6 Sårbarhedsstyring					
		12.6.1	Styring af tekniske sårbarheder				
		12.6.2	Begrænsninger på softwareinstallation				
		12.7 Overvejelser i forbindelse med audit af informationssystemer					
		12.7.1	Kontroller i forbindelse med audit af informationssystemer				
	A.13 Kommunikationssikkerhed						
	A.14 Anskaffelse, udvikling og vedligeholdelse af systemer						
		14.1 Sikkerhedskrav til informationssystemer					
		A.14.2 Sikkerhed i udviklings- og hjælpeprocesser					
		14.2.1	Sikker udviklingspolitik				

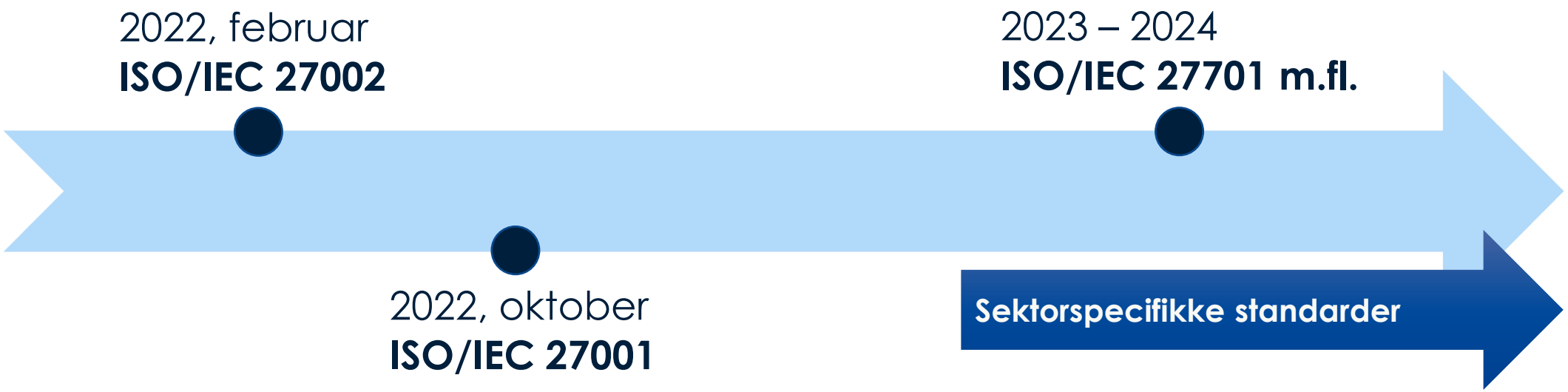
Driftssikkerhed

MYNDIGHED

› Oversigt over vejledninger og skabeloner

Få overblik over samtlige vejledninger og skabeloner til arbejdet med informationssikkerhed.

Tidshorisont



Hvorfor bruge standarder?

Henning Mortensen
CISO / CPO

Målsætning

Vision for IT-sikkerhedsafdelingen

- Beskytte forretningen og samarbejdspartnerne og sikre tillid til forretningen fra alle samarbejdspartnere til enhver tid.

Mission

- Tilvejebringe og understøtte de **tekniske og organisatoriske foranstaltninger** med tilhørende **kontroller** til **informationssikkerhed, databeskyttelse og dataetik** i overensstemmelse med **standarder, best practises og lovgivning**, så forretningens **værdier** bevares og udbygges, og så kunder, medarbejdere, aktionærer og andre samarbejdspartnere kan være **trygge** ved at interagere med forretningen.

Hvorfor bruge standarder?

- Basere sig på den **erfaring**, som standardernes forfattere har: Den **bedste måde** at gøre et eller andet på (man tager ikke den forkerte (om)vej eller **tænker forkert**)
- Sikre sig at man kommer hele vejen rundt om emneområdet (**holisme**) og ikke overser noget (**kvalitet**)
- Signaler til omverdenen for at skabe **tillid**
- Lettere at **finde og auditere leverandører**, hvis man har indrettet sig på samme måde
- Sikre sig at der er en ensartet/**ensrette**t tilgang
- Sikre sig at der er **sammenhæng**, hvis man vælger **flere standarder indenfor samme serie**
- Kan bruge **tools på markedet** til understøttelse, som er designet efter standarderne
- Sikre et ensartet **sprog** på tværs af teknik, jura og forretning.

Hvorfor bruge standarder?

- Kan bruges som **logos-argumentation** ved konflikter (**standarden siger at…**)
- **Understøtte regulatoriske krav**, så vi minimerer “overraskelser” (forudsat at lovgivning lægger sig op af standarderne)
- Det er **formodentlig billigere i længden** at have lagt sig op af standarder, fordi det er en mere effektiv tilgang (struktureret), kan eliminere overlap og styre risici
- Kan bruges til **markedsføring** og gøre due-diligence lettere og kompatibilitet ved fusioner
- Standarder bidrager til bedre faglig dygtighed (**uddannende**)
- Understøtte modenhed i organisationen (**repeterbarhed**)
- **Ledelse** kan godt lidt struktur.

Hvorfor bruge standarder?

Off-topic årsager

- Sikre samspil mellem teknologier (interoperabilitet)
- Sikre innovation
- Sikre miljø
- Produktudvikling
- Produktsammenligning
- Understøtter international handel
- ...

Certificering

- Ikke alle har et mål om certificering
- Uanset, kan man blive rigtig meget klogere og sikrere ved at lade sig inspirere af standarderne.

Et hav af…

… Standarder
… Standardiseringsorganisationer
… Mærkningsordninger, best practices, … og tilgange der ikke er standarder

- ISO27001/2
- (ISO27005)
- ISO27701
- IEC62443 – security levels
- PCI DSS
- (D-mærket)
- (20 tekniske minimumskrav)
- Vi burde nok bruge flere…
- Vi burde nok lave en analyse af, hvilke ekstra standarder vi kunne bruge…

- PS et fromt ønske til DS: Det ville være nyttigt, dersom man kunne bladre gennem en standard og se, om den er relevant for ens arbejdsområde, inden man køber den…

Hvad er output?

- IT-sikkerhedspolitik
- ISMS/PIMS: Organisering af sikkerhedsarbejdet
- Risikovurdering
- Organisatoriske foranstaltninger: Regelsæt + procedurer: “Du skal…!”
- Tekniske foranstaltninger
- Kontroller/Audit: “Kan du dokumentere, at du har gjort…?”
- Årshjul, styringsværktøj, ledelsesrapportering
- Awareness, e-læring

Case: Cloud og tredjelandsoverførsler

ISO 27002 i GDPR-cloudperspektiv

- Informationssikkerhedspolitikker og retningslinjer
  - Medarbejdere og afdelinger bruger cloud uden central godkendelse
  - Uklarhed for medarbejderne om hvad der må deles hvor
- Organisering (rolle, funktionsadskillelse, mobilt udstyr, fjernarbejdspladser)
  - Har vi stadig de nødvendige kompetencer inhouse?
- HR-sikkerhed (før, under og efter ansættelsen)
- Styring af aktiver (ansvar, klassifikation, mediehåndtering)
- Adgangsstyring (politik, brugeradgang, brugeransvar, system og app-adgang)
- Kryptering
  - Vi kan ikke altid selv styre krypteringen
- Fysisk sikring (områder, udstyr)

ISO 27002 i GDPR-cloudperspektiv

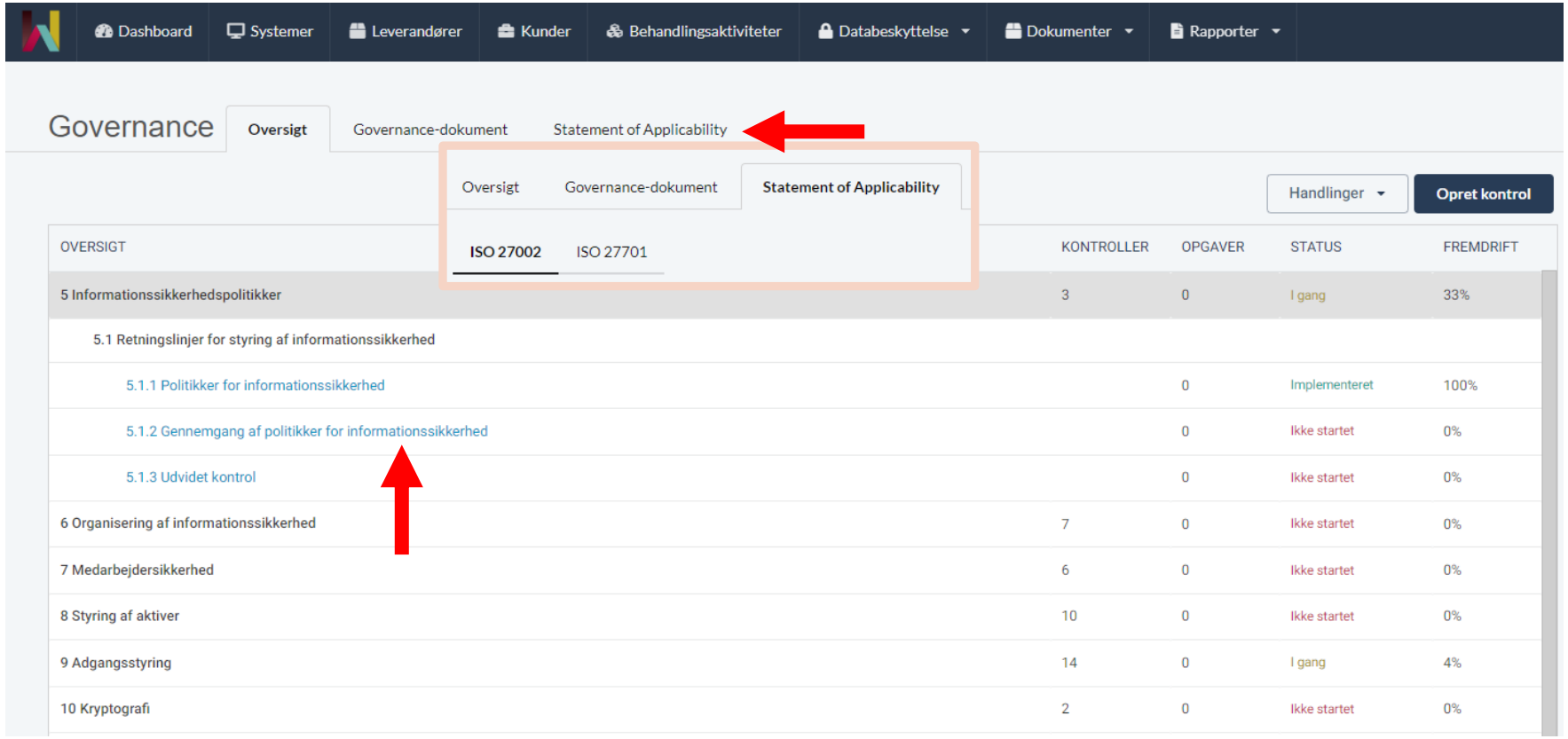
- Driftssikkerhed (procedurer og ansvar, skadelig kode, backup, logning, installation, sårbarheder, audit)
  - Kan vi med tekniske foranstaltninger styre leverandøren?
  - Udnytter vi de tekniske foranstaltninger leverandøren stiller til rådighed – der er masser af knapper at trykke på
- Kommunikationssikkerhed (netværk og segmentering, overførsel af information)
  - Hvor er data – Tredjelandsoverførsler?
  - Brugen af underdatabehandlere og audit heraf
- Anskaffelse, udvikling og vedligehold
- Leverandørforhold (krav til og styring af)
  - Cloudprovideres adgang til data jf. support
  - Cloudprovideres brug af telemetridata til egne formål (forbedring af servicen og intern svindel)
  - Ændringer i service- eller aftalevilkår
  - Stort auditarbejde og hvad gør man med problematiske audit-resultater

ISO 27002 i GDPR-cloudperspektiv

- Styring af brud
  - Vurderinger af hvilke hændelser, der er anmeldelsespligtige
- Beredskab (kontinuitet og retablering)
- Compliance (love, standarder, best practises og kontrakter)
  - Oplysning af de registrerede
  - Retshåndhævende myndigheders krav på data
  - Anden lovgivning cloudprovideren er underlagt
  - Styring af omkostninger / ukontrolleret vækst i brugen

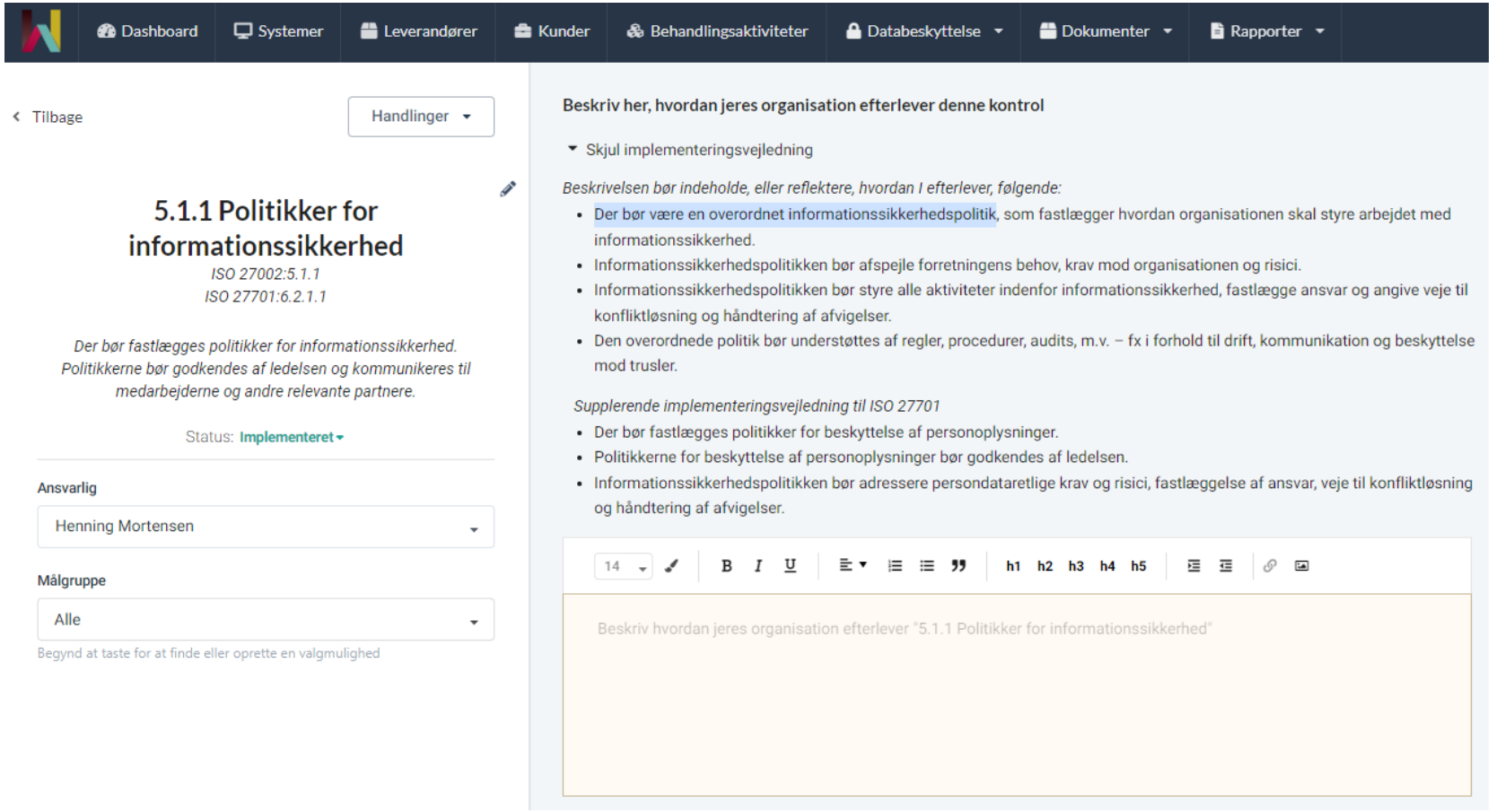
Sådan ser det ud i praksis

Governance

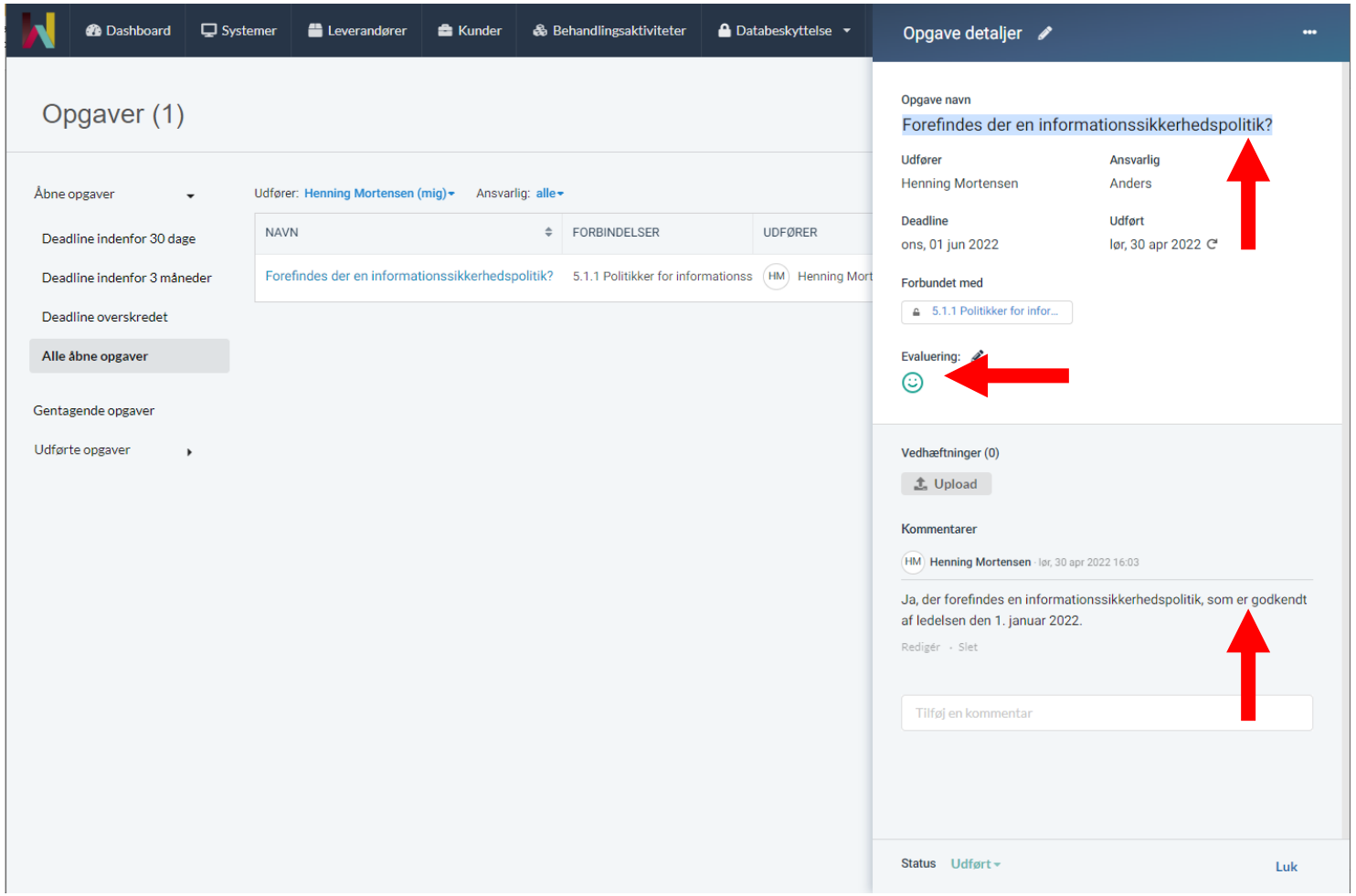


Kilde: https://wiredrelations.com

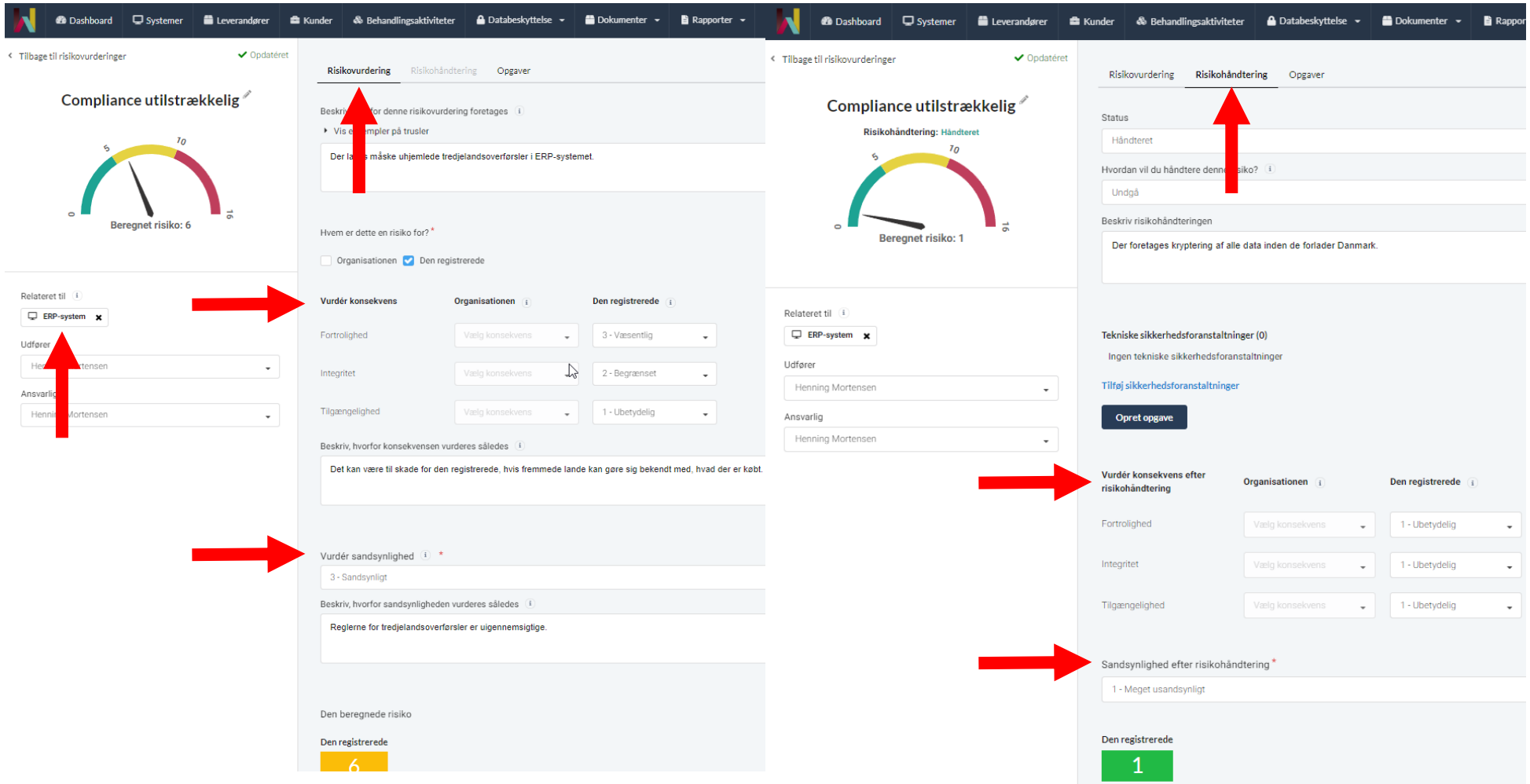
Governance


Dashboard
Systemer
Leverandører
Kunder
Behandlingsaktiviteter
Databeskyttelse
Dokumenter
Rapporter
Tilbage
Handlinger
5.1.1 Politikker for informationssikkerhed
ISO 27002:5.1.1
ISO 27701:6.2.1.1
Der bør fastlægges politikker for informationssikkerhed. Politikkerne bør godkendes af ledelsen og kommunikeres til medarbejderne og andre relevante partnere.
Status: Implementeret
Ansvarlig
Henning Mortensen
Målgruppe
Alle
Begynd at taste for at finde eller oprette en valgmulighed
Beskriv her, hvordan jeres organisation efterlever denne kontrol
Skjul implementeringsvejledning
Beskrivelsen bør indeholde, eller reflektere, hvordan I efterlever, følgende:
Der bør være en overordnet informationssikkerhedspolitik, som fastlægger hvordan organisationen skal styre arbejdet med informationssikkerhed.
Informationssikkerhedspolitikken bør afspejle forretningens behov, krav mod organisationen og risici.
Informationssikkerhedspolitikken bør styre alle aktiviteter indenfor informationssikkerhed, fastlægge ansvar og angive veje til konfliktløsning og håndtering af afvigelser.
Den overordnede politik bør understøttes af regler, procedurer, audits, m.v. – fx i forhold til drift, kommunikation og beskyttelse mod trusler.
Supplerende implementeringsvejledning til ISO 27701
Der bør fastlægges politikker for beskyttelse af personoplysninger.
Politikkerne for beskyttelse af personoplysninger bør godkendes af ledelsen.
Informationssikkerhedspolitikken bør adressere persondataretlige krav og risici, fastlæggelse af ansvar, veje til konfliktløsning og håndtering af afvigelser.
14
h1 h2 h3 h4 h5
Beskriv hvordan jeres organisation efterlever "5.1.1 Politikker for informationssikkerhed"

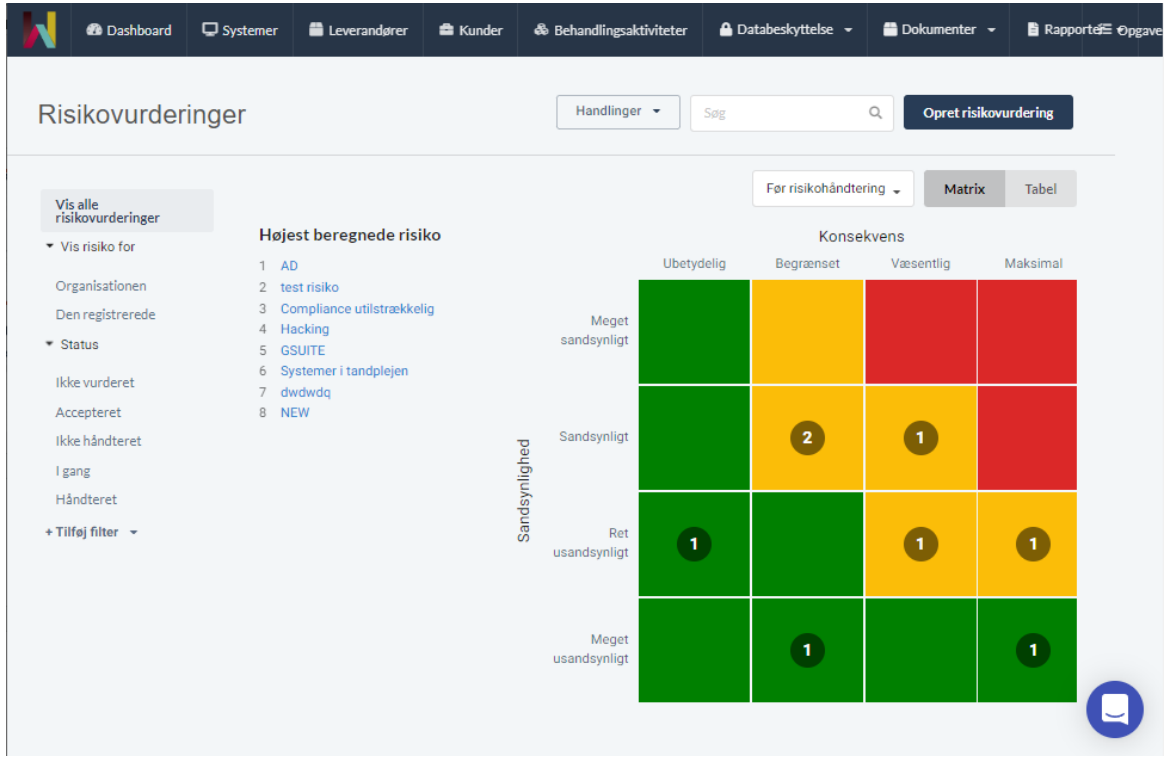
Governance


Dashboard
Systemer
Leverandører
Kunder
Behandlingsaktiviteter
Databeskyttelse
Opgaver (1)
Åbne opgaver
Deadline indenfor 30 dage
Deadline indenfor 3 måneder
Deadline overskredet
Alle åbne opgaver
Gentagende opgaver
Udførte opgaver
Udfører: Henning Mortensen (mig)
Ansvarlig: alle
NAVN
FORBINDELSER
UDFØRER
Forefindes der en informationssikkerhedspolitik?
5.1.1 Politikker for informationss
HM
Henning Mort
Opgave detaljer
Opgave navn
Forefindes der en informationssikkerhedspolitik?
Udfører
Henning Mortensen
Ansvarlig
Anders
Deadline
ons, 01 jun 2022
Udført
lør, 30 apr 2022
Forbundet med
5.1.1 Politikker for infor...
Evaluering:
Vedhæftninger (0)
Upload
Kommentarer
HM
Henning Mortensen · lør, 30 apr 2022 16:03
Ja, der forefindes en informationssikkerhedspolitik, som er godkendt af ledelsen den 1. januar 2022.
Redigér · Slet
Tilføj en kommentar
Status
Udført
Luk

Risikovurdering



Risikovurdering



Konklusion

- Vi kan effektivt lave regler, som følger standarden, til konkrete målgrupper
- Vi har ejere for regler, risici, leverandører, systemer og behandlingsaktiviteter m.v.
- Vi kan kontrollere, at vi efterlever reglerne
- Vi ved hvor vi ikke efterlever reglerne og dermed har vi også tydeliggjort, hvor der skal sættes mere ind (ønskeseddel)
- Vi kan kommunikere reglerne let
- Vi sørger for, at det hele er funderet i risikovurderinger

hmo@ao.dk

https://www.linkedin.com/in/henning-mortensen-343b0/

Spørgsmål

Husk at sætte X i kalenderen den 29. september,
hvor Dansk Standard inviterer til