Anders Linde

Nye strukturer og foranstaltninger

De nye versioner af ISO/IEC 27001 og ISO/IEC 27002

CISO27
Undervisning & rådgivning i standarder for cybersikkerhed

To standarder er i spil

ISO/IEC 27001

ANNEKS A

ISO/IEC 27002

ISO/IEC 27002: en ny temastruktur

Undervisning & rådgivning i standarder for cybersikkerhed

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!

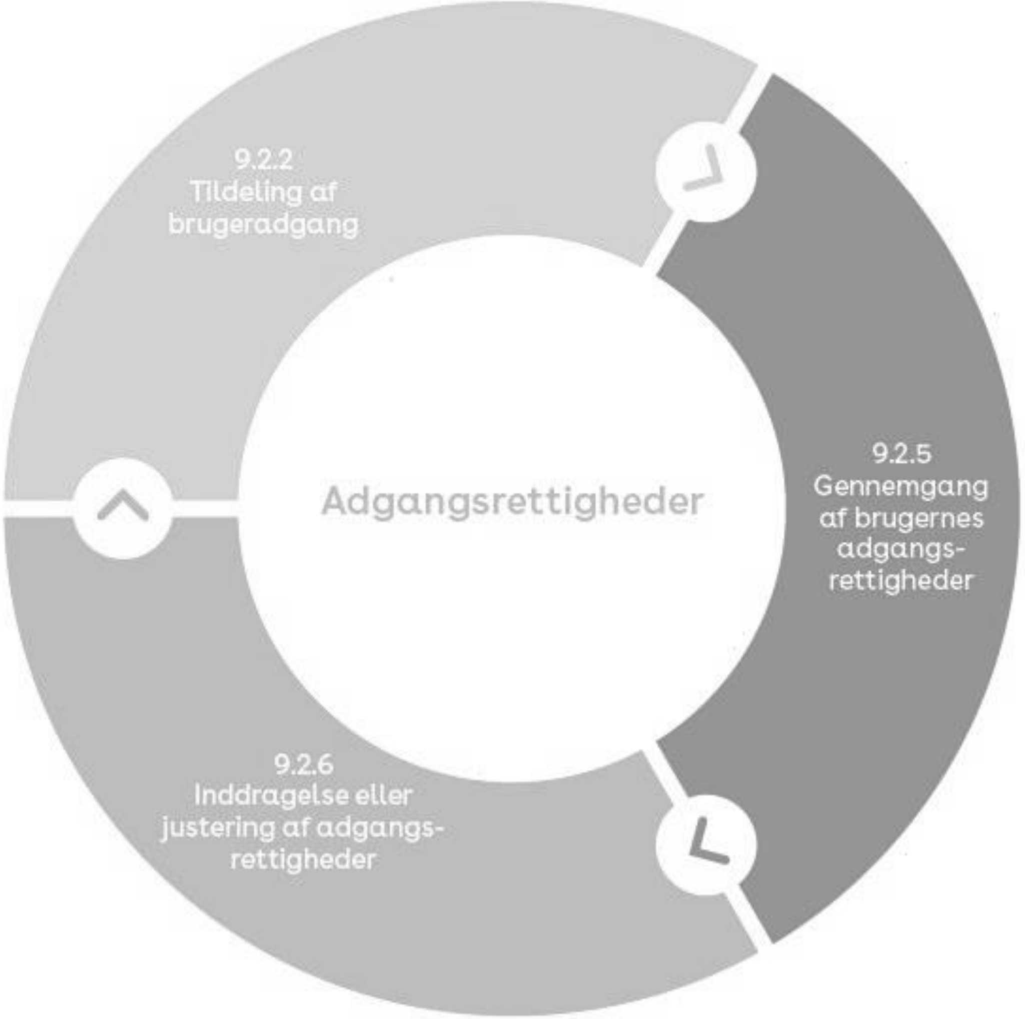
93

○ Livscyklus ○○ Emne ○○○ Omfang

Færre foranstaltninger – eksempel

2013

114

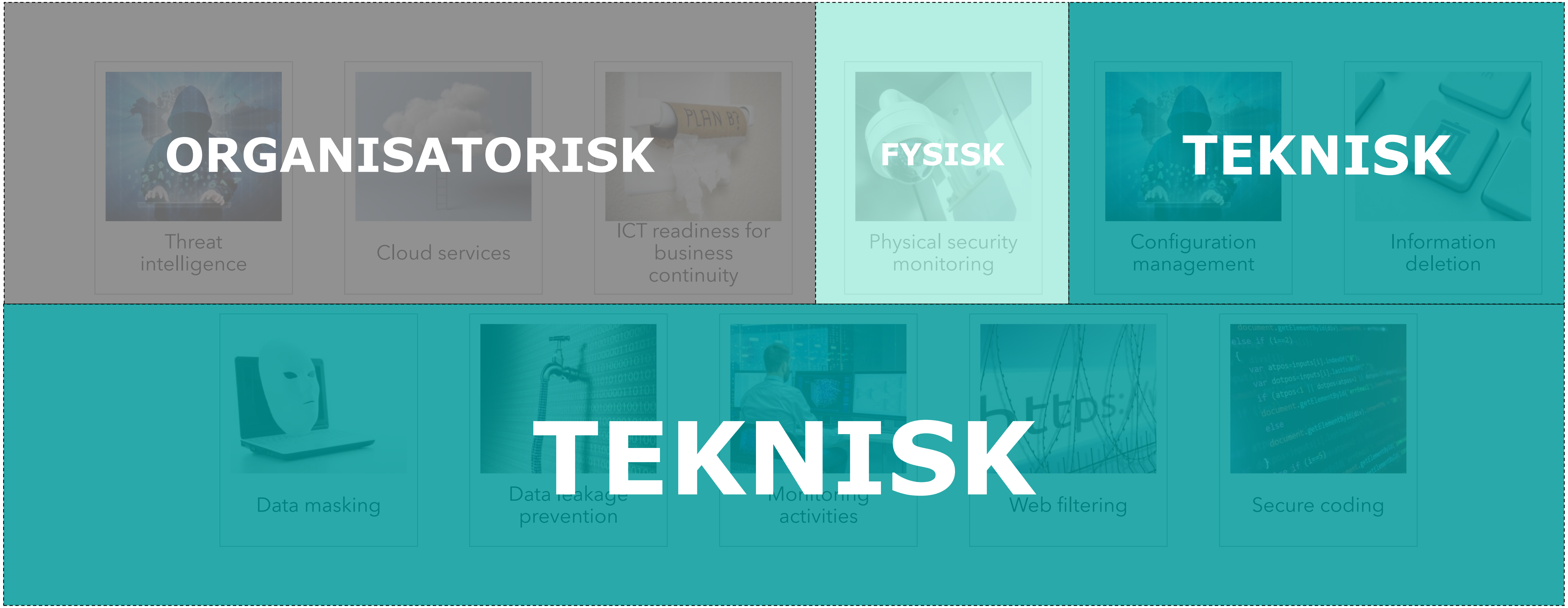

9.2.2
Tildeling af brugeradgang
Adgangsrettigheder
9.2.5
Gennemgang af brugernes adgangs-rettigheder
9.2.6
Inddragelse eller justering af adgangs-rettigheder

2022

93

CISO27
Undervisning & rådgivning i standarder for cybersikkerhed

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)

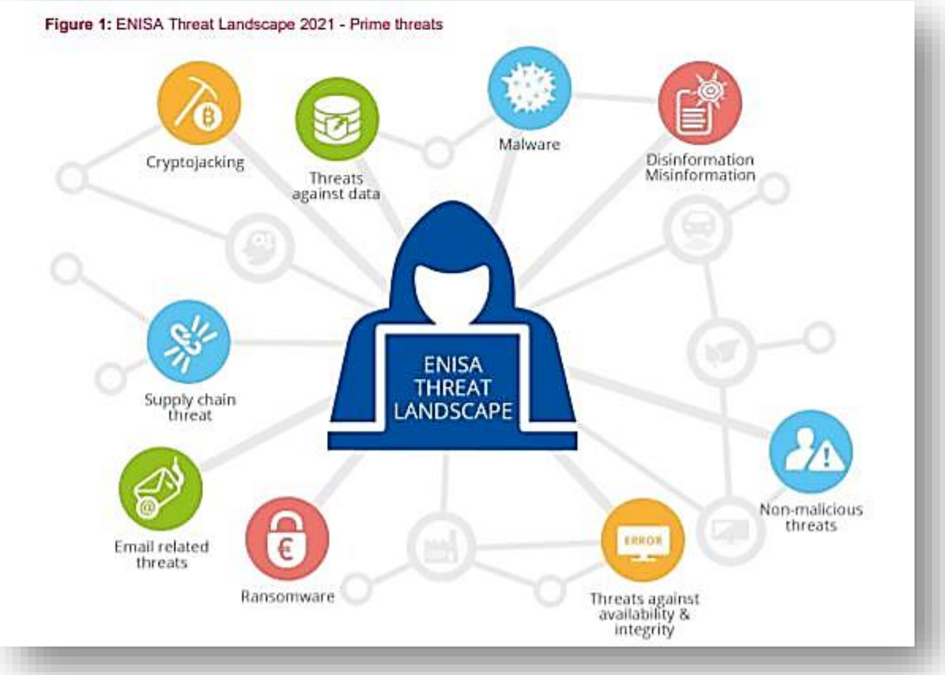


Figure 1: ENISA Threat Landscape 2021 - Prime threats

FE CENTER FOR CYBERSIKKERHED

Trusselsvurdering:

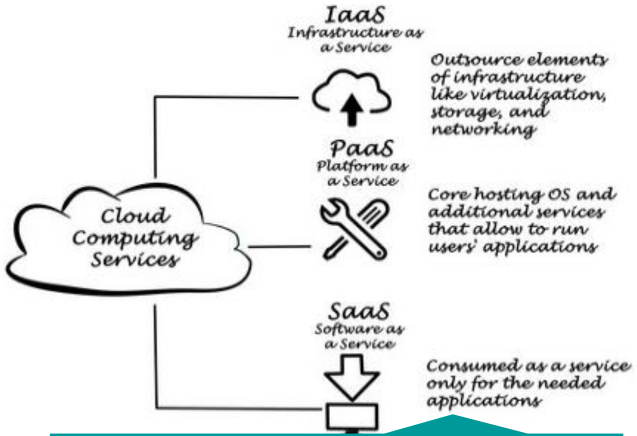
Cybertruslen mod Danmark 2022

1. udgave juni 2022.

Indsamling og analyse af viden om trusler

Kilde: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2022.pdf
Kilde: https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2021.pdf

5.23 Information security for use of cloud services (NY)


IaaS
Infrastructure as a Service
Outsource elements of infrastructure like virtualization, storage, and networking
PaaS
Platform as a Service
Core hosting OS and additional services that allow to run users' applications
Cloud Computing Services
SaaS
Software as a Service
Consumed as a service only for the needed applications

Service

- SAAS, PAAS, IAAS

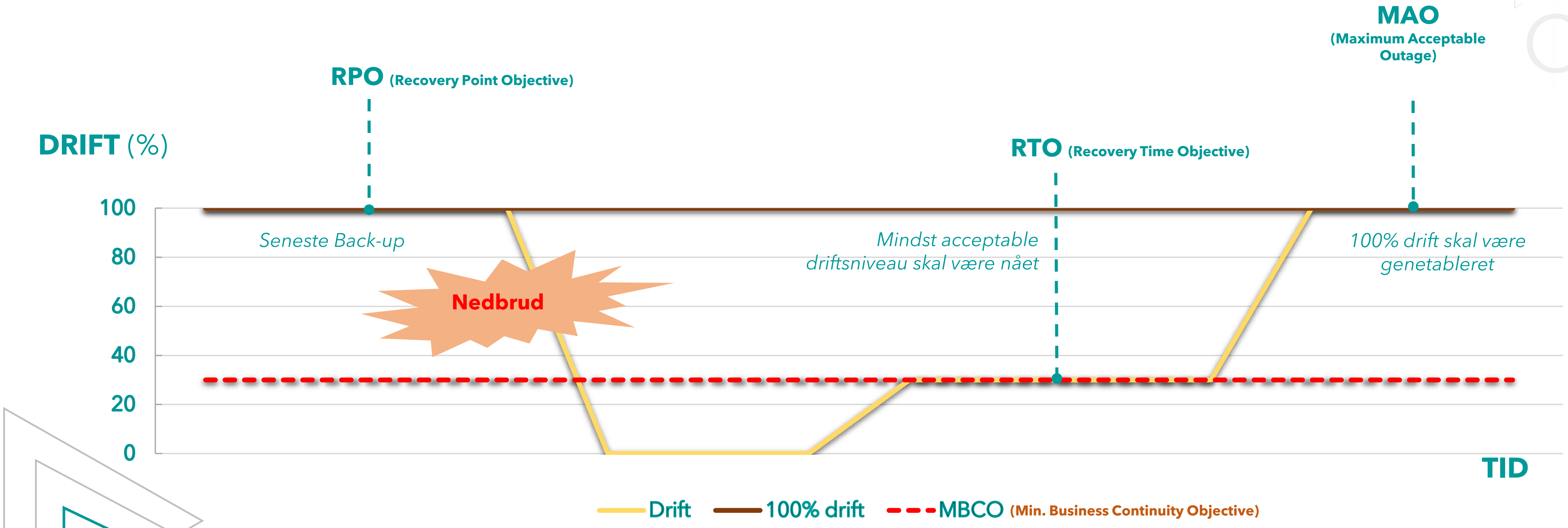
Arkitektur

- 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.

8.23 Web filtering (NY)

Undervisning & rådgivning i standarder for cybersikkerhed

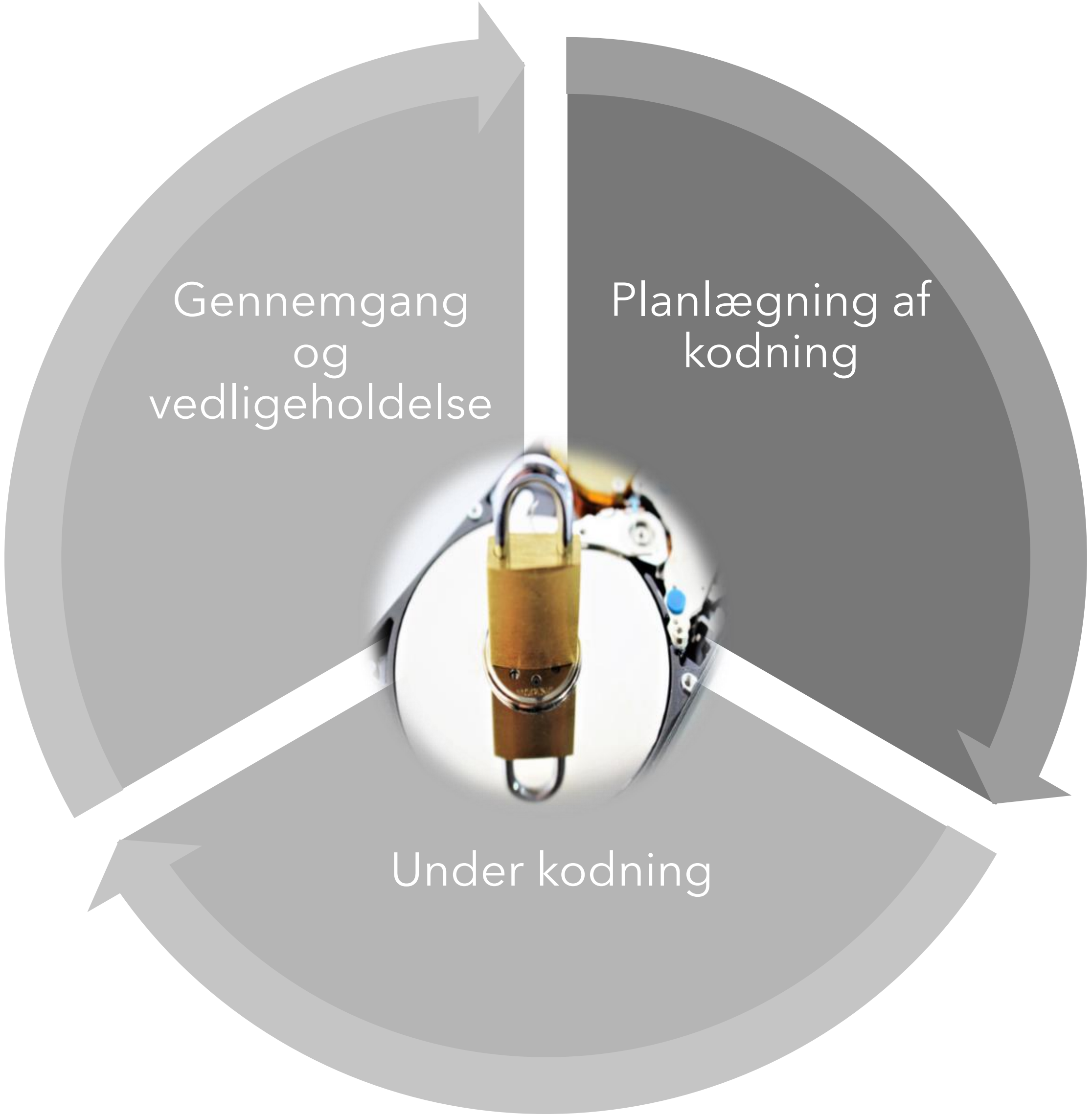
Følgende elementer skal overvejes ved blokering af hjemmesider:

- □ Websteder, der har upload-funktioner af information og som er ikke tilladt i henhold til politik
- □ Kendte eller formodede ondsindede websteder
- □ Kommando- og kontrolserver
- □ Ondsindet websted erhvervet fra trusselsinformation

Inden installation af webfiltre og adresseblokeringer:

- □ Definer politikker og regler for web-filtrering
- □ Kommuniker til de ansatte
- □ Uddan ansatte for at undgå ignorering af browser-advarsler og lignende

8.28 Secure coding (NY)



Nye perspektiver

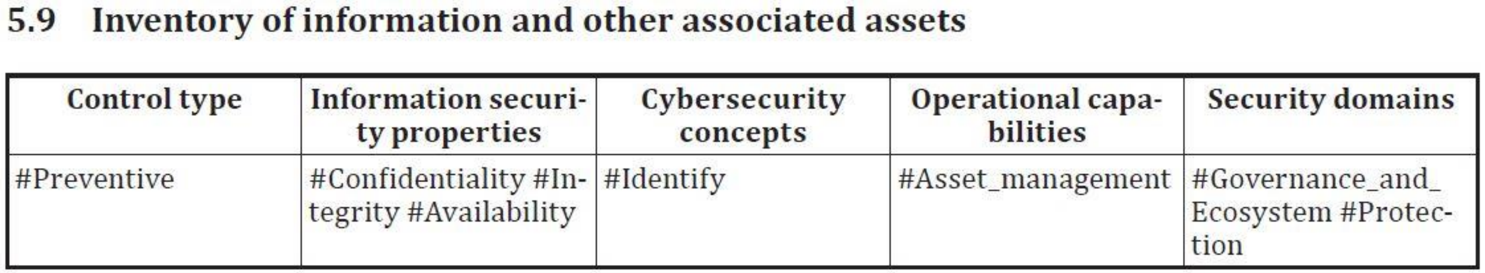
Type af foranstaltning: forebyggende, opdagende og korrigerende

Informationssikkerhed: Fortrolighed, integritet og tilgængelighed

Cybersikkerhedskoncept: Identify, Protect, Detect, Respond, Recover

Operationelle kapabiliteter: fx leverandørstyring og asset management

Sikkerhedsdomæner: EU-sikkerhedskrav til kritiske informationssystemer og netværk.

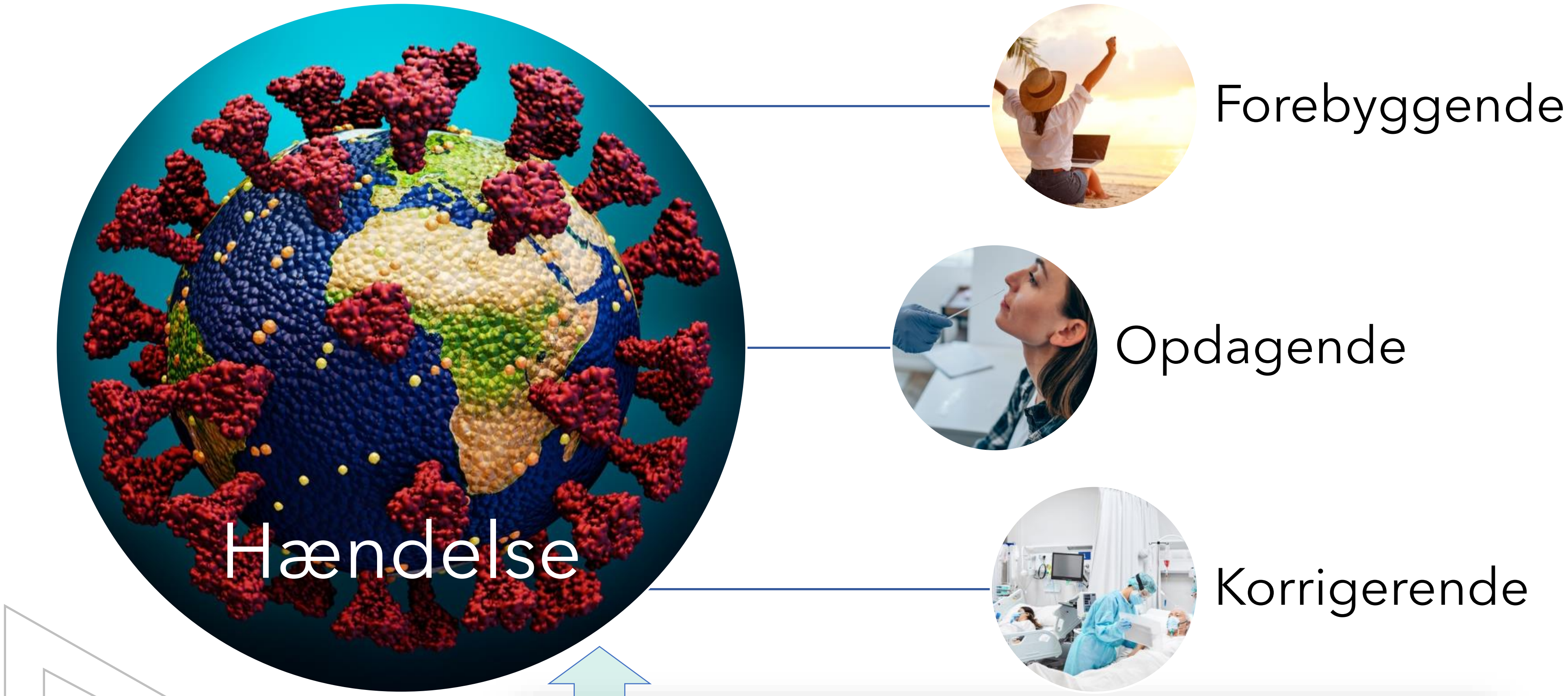


5.9 Inventory of information and other associated assets

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

Undervisning & rådgivning i standarder for cybersikkerhed

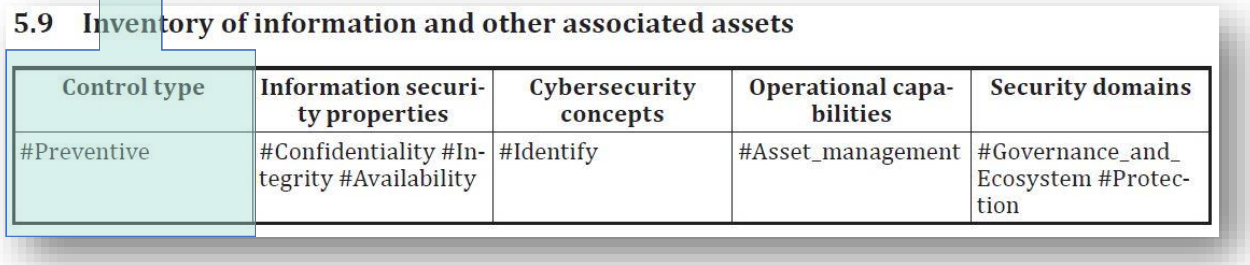


Hændelse

Forebyggende

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

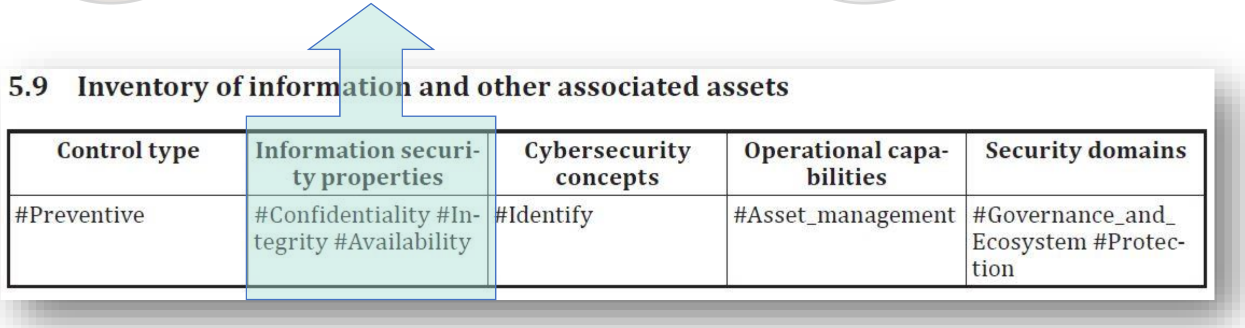
Tab af fortrolighed

- 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

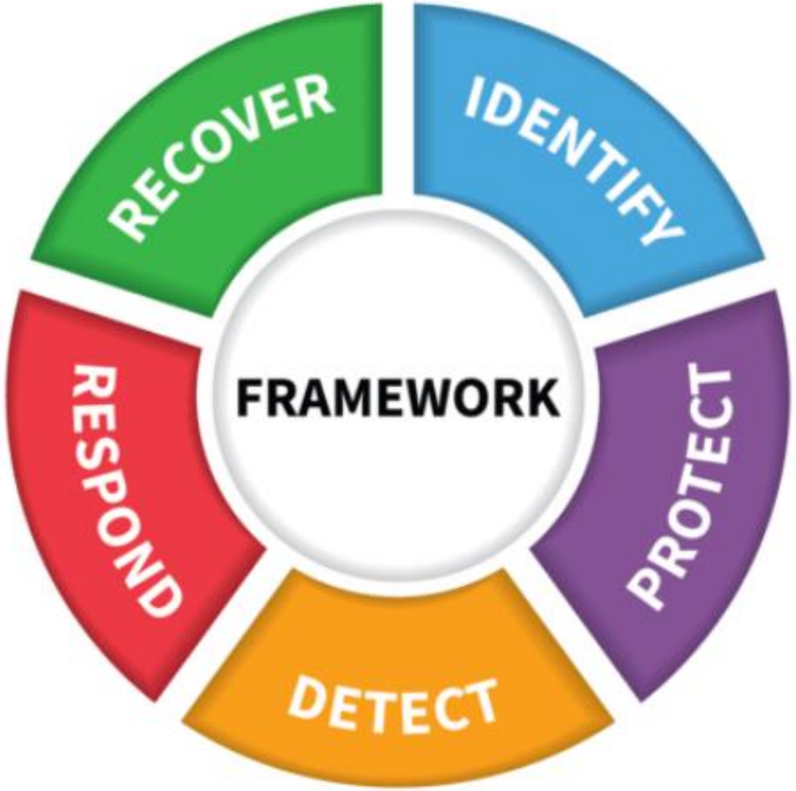
Tab af tilgængelighed



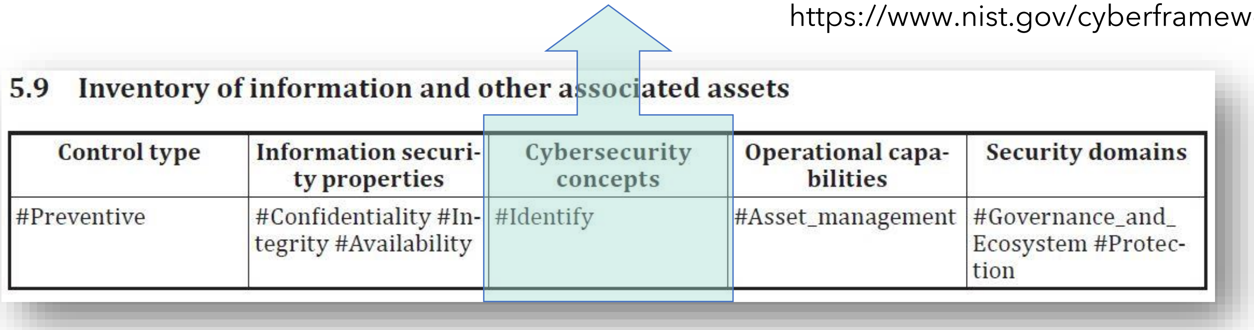
5.9 Inventory of information and other associated assets

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

CISO27
Undervisning & rådgivning i
standarder for cybersikkerhed

Asset management

HR

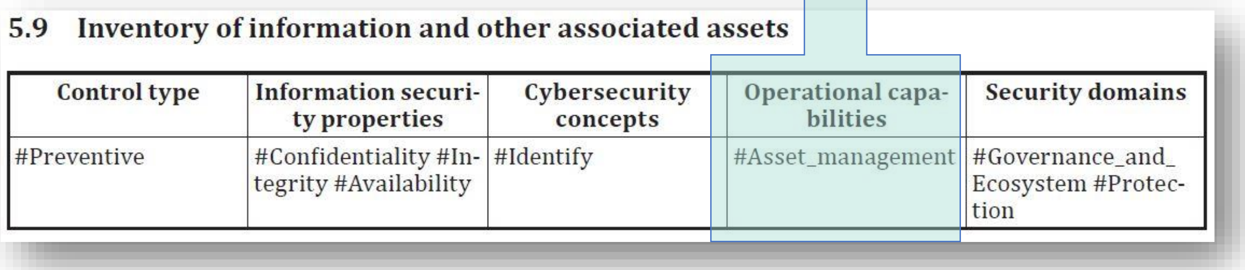
Continuity

Legal

Governance

Facility

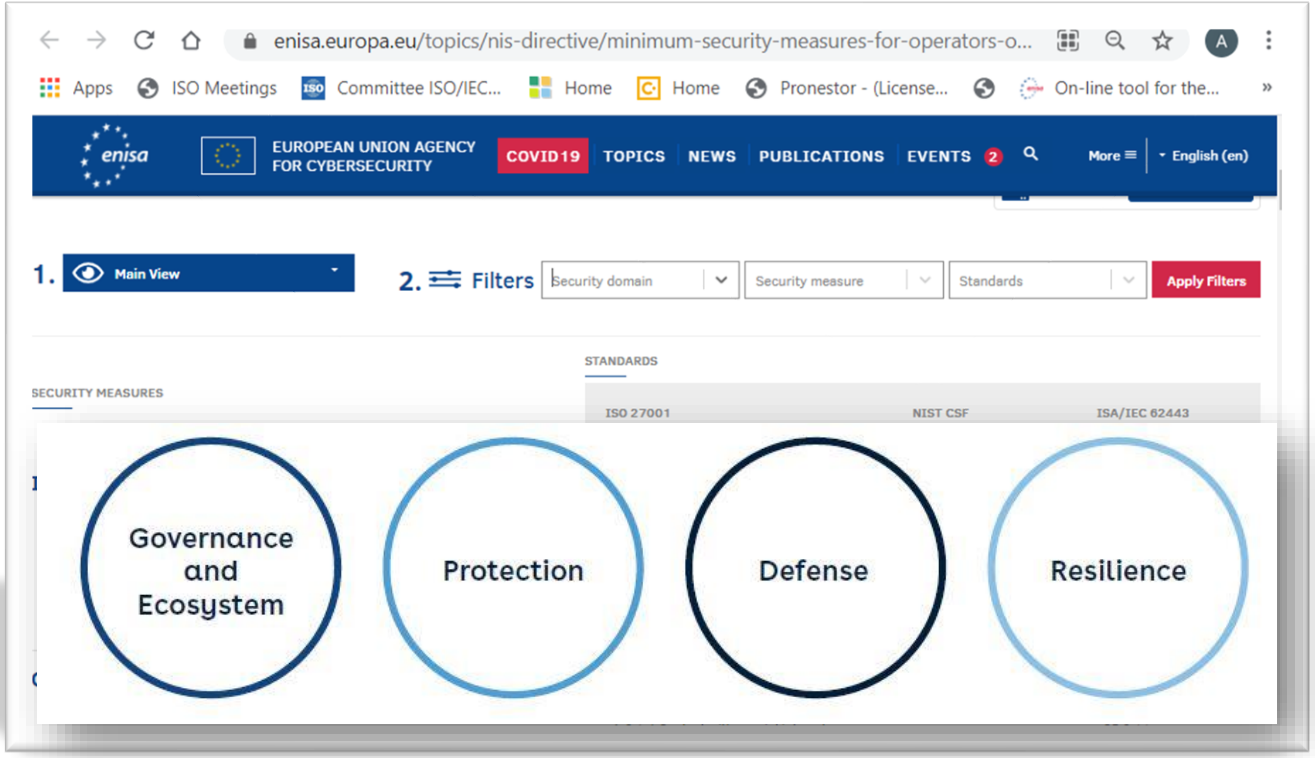
Application security



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

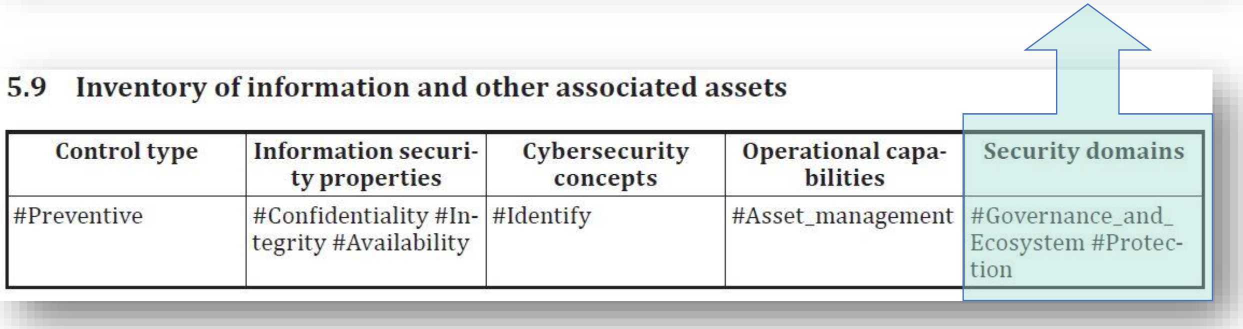


Governance and Ecosystem

Protection

Defense

Resilience

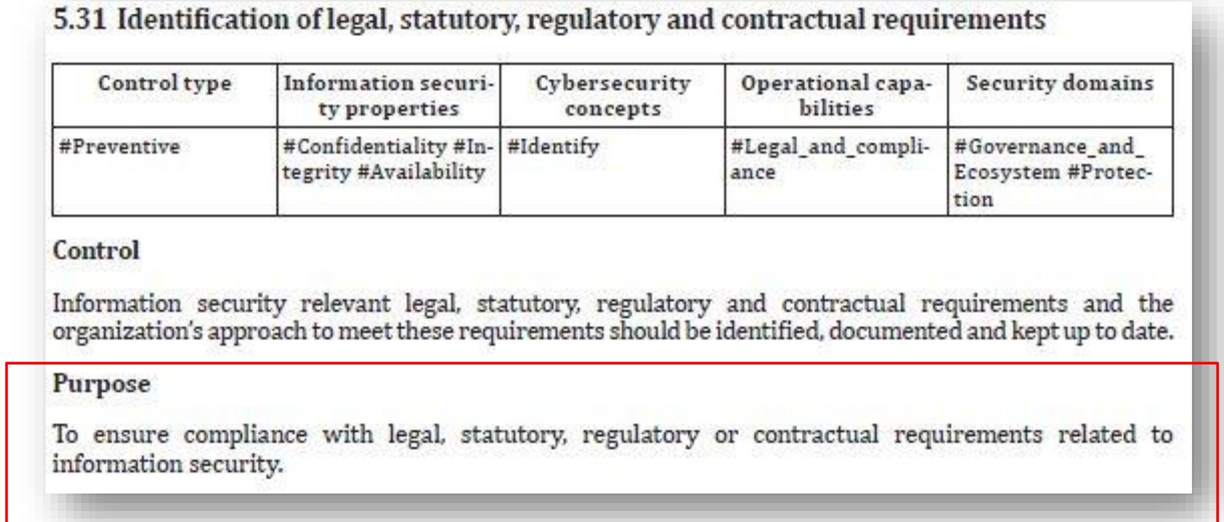


5.9 Inventory of information and other associated assets

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

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

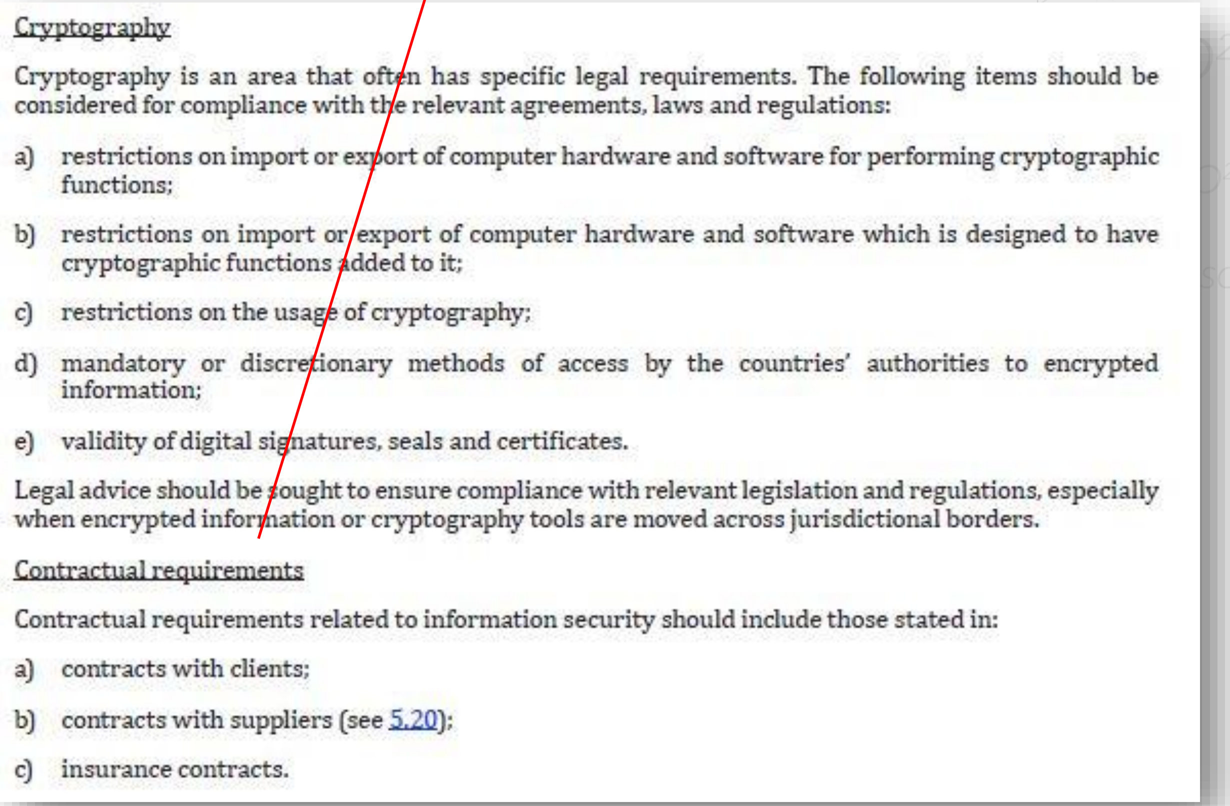
Control

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



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:

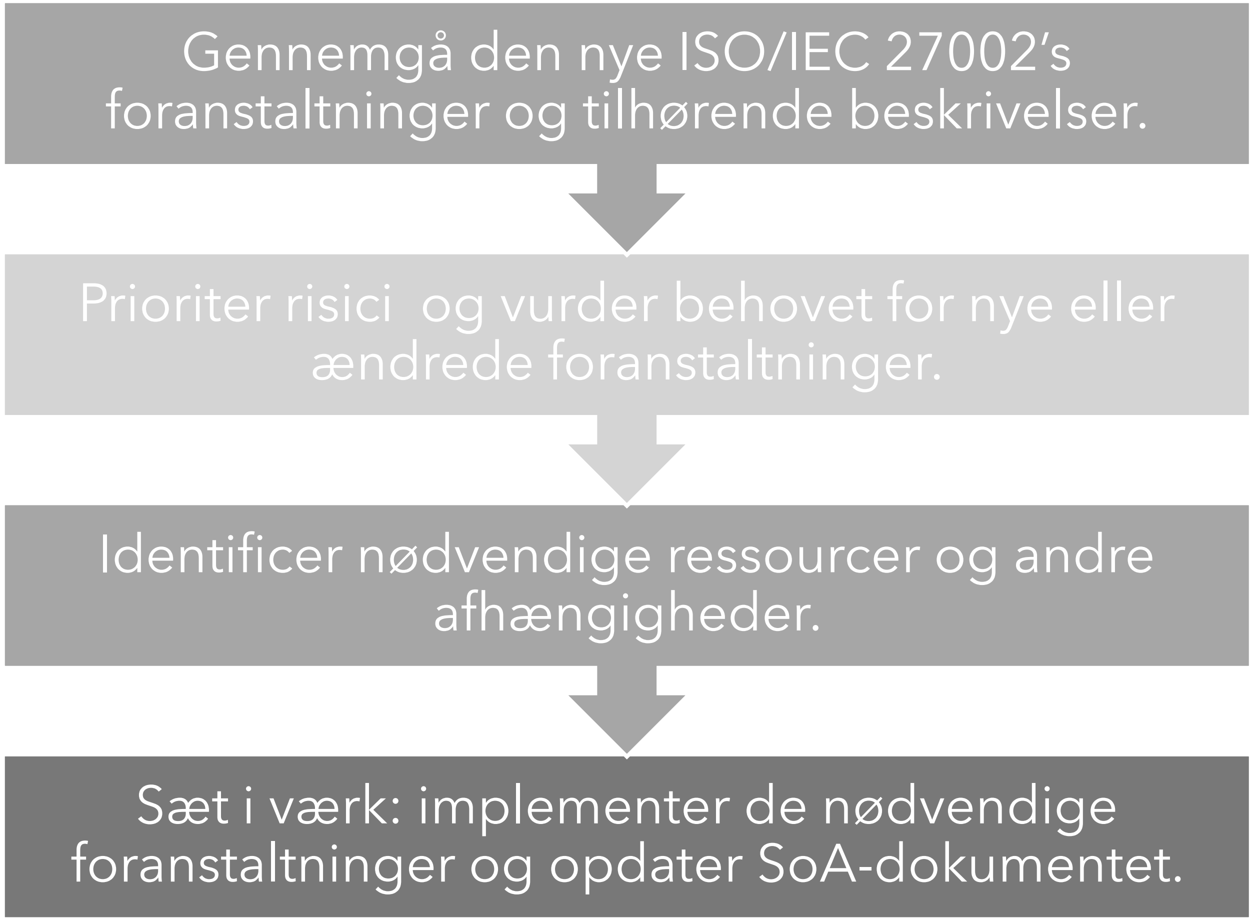
a) contracts with clients;

b) contracts with suppliers (see 5.20);

c) insurance contracts.

Implikationer for ISO/IEC 27001… og for jer

CISO27
Undervisning & rådgivning i
standarder for cybersikkerhed



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.

Tidshorisont

2022, februar

- ISO/IEC 27002

2022, oktober

- **ISO/IEC 27001**

2023 - 2024

- ISO/IEC 27701 m.fl.

Sektorspecifikke standarder

Tak!

anders@ciso27.dk
Tlf. 6162 1500