Webinar: ISO/IEC 27002 – kom på forkant med de nye sikkerhedsforanstaltninger

4. juni 10. 00 – 11.15

Praktisk information

- Sessionen optages
- Stil gerne spørgsmål undervejs via chatten
- Præsentationer sendes ud efterfølgende

Dagens program

10:05 Introduktion til ISO/IEC 27002 samt gennemgang af de væsentligste ændringer i den reviderede version

Lasse Kaltoft, Dansk Standard

10:40 FOSS' arbejde med informationssikkerhedsstandarder og værdien af at anvende ISO/IEC 27002

Kristian Kreiner, FOSS

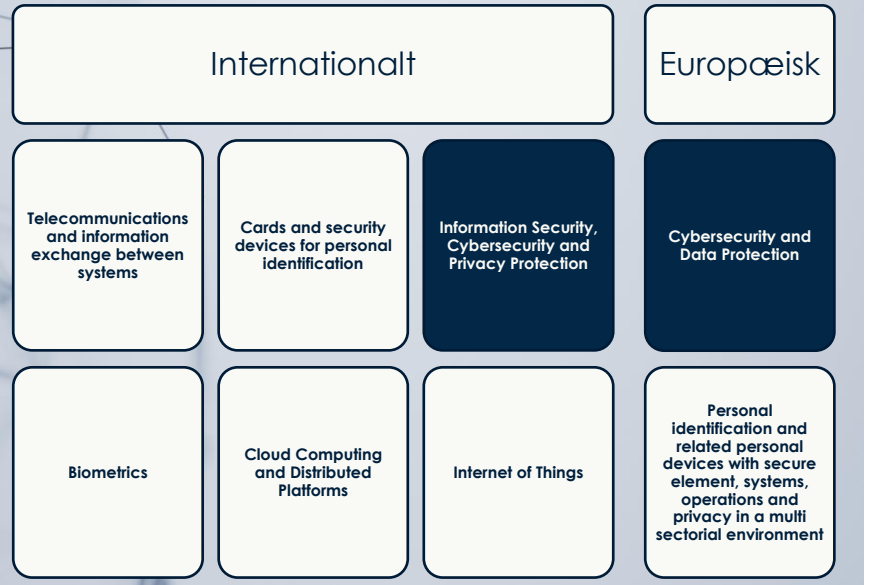
11:00 Spørgsmål

11:15 Tak for i dag

Dansk Standard

- Vi er en erhvervsdrivende fond
- Vi er selvejende – ingen ejere/aktionærer
- Vision: at være drivkraften for en bæredygtig udvikling
- Erhvervspolitisk partnerskab med Erhvervsministeriet
- Grundlagt i 1926
- 150 medarbejdere
- 245 forskellige standardiseringsudvalg
- Over 2100 eksperter

Dansk Standards udvalg for cyber- og informationssikkerhed



Fokusområde

- Ledelsesstandarder – ISO/IEC 27000-serien
- Cybersikkerhed i produkter
- Persondatabeskyttelse/privacy
- Internet of Things (IoT)
- Identifikationskort
- Biometri
- Cloud computing

Aktuelle temaer

- Følge med i og spille ind til Cybersecurity Act og den europæiske cybersikkerheds-certificering
- Revision af ISO/IEC 27002
- Revision af ISO/IEC 27005
- Kommende revision af ISO/IEC 27001
- Persondatabeskyttelse/privacy
- Følge og bidrage til udviklingen af standarder for cybersikkerhed i produkter
- Bæredygtighed og FN's verdensmål

Den nye ISO/IEC 27002

4. juni 2021

Webinar

DANSK STANDARD

Forholdet mellem ISO/IEC 27001 og ISO/IEC 27002

Den nye ISO/IEC 27002

Overblik over ISO/IEC 27002-standardens nye struktur og anvendelse af attributter

DANSK STANDARD

Den nye udformning af ISO/IEC 27002-standarden

TEMAER

FORANSTALTNINGER

- Type af foranstaltning
- Egenskaber for informationssikkerhed
- Cybersikkerhedskoncept
- Operationelle ressourcer
- Sikkerhedsdomæner

ATTRIBUTTER

DANSK STANDARD

Inddeling efter temaer

- A.5 Informationssikkerhedspolitikker
- A.6 Organisering af informationssikkerhed
- A.7 Personalesikkerhed
- A.8 Styring af aktiver
- A.9 Adgangsstyring
- A.10 Kryptografi
- A.11 Fysisk sikring og miljøsikring
- A.12 Driftssikkerhed
- A.13 Kommunikationssikkerhed
- A.14 Anskaffelse, udvikling og vedligeholdelse af systemer
- A.15 Leverandørforhold
- A.16 Styring af informationssikkerhedsbrud
- A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- A.18 Overensstemmelse

5. Organisatorisk
- alt det andet

6. Adfærdsmæssig
- personer: ansatte og eksterne

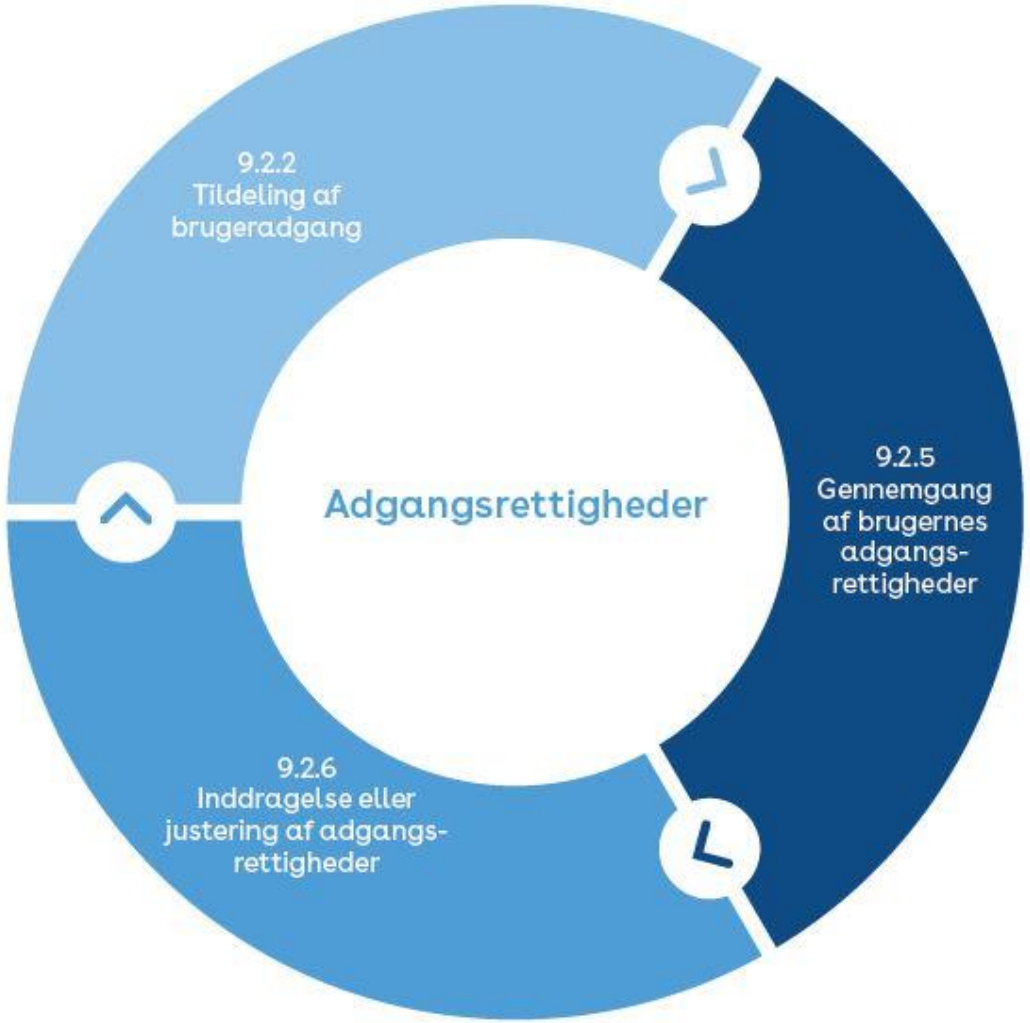
7. Fysisk
- de fysiske rammer og enheder

8. Teknologisk
- tekniske tiltag

DS DANSK STANDARD

Færre foranstaltninger

2013
114



2021
93

DS
DANSK STANDARD

8 Styring af aktiver

8.1 Ansvar for aktiver

- 8.1.1. Fortegnelse over aktiver.
- 8.1.2. Ejerskab af aktiver.
- 8.1.3. Accepteret brug af aktiver.
- 8.1.4. Tilbagelevering af aktiver.

Inventory of information and other associated assets

8.2 Klassifikation af information

- 8.2.1. Klassifikation af information.
- 8.2.2. Mærkning af information.
- 8.2.3. Håndtering af aktiver.

8.3 Mediehåndtering

- 8.3.1. Styring af bærbare medier.
- 8.3.2. Bortskaffelse af medier.
- 8.3.3. Fysiske medier under transport.

Storage Media

DS DANSK STANDARD

12 Driftssikkerhed

12.4 Logning og overvågning

- 12.4.1. Hændelseslogning.
- 12.4.2. Beskyttelse af logoplysninger.
- 12.4.3. Administrator- og operatørlog.
- 12.4.4. Tidssynkronisering.

Logging

12.5 Styring af driftssoftware

- 12.5.1. Softwareinstallation i driftssystemer.

Installation of software on operational systems

12.6 Sårbarhedsstyring

- 12.6.1. Styring af tekniske sårbarheder.
- 12.6.2. Begrænsninger på softwareinstallation.

Installation of software on operational systems

12.7 Overvejelser i forbindelse med audit af informationssystemer

- 12.7.1. Kontroller i forbindelse med audit af informationssystemer.

DANSK STANDARD

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

17.1 Informationssikkerhedskontinuitet

- 17.1.1. Planlægning af informationssikkerhedskontinuitet.
- 17.1.2. Implementering af informationssikkerhedskontinuitet.
- 17.1.3. Verificer, gennemgå og evaluer informationssikkerheds-kontinuiteten.

Information security during disruption

17.2 Redundans

- 17.2.1. Tilgængelighed af informationsbehandlingsfaciliteter.

DANSK STANDARD

Nye foranstaltninger

Adfærdsmæssig	Fysisk Physical security monitoring
Organisatorisk Threat intelligence Information security for use of cloud services ICT readiness for business continuity	Teknologisk Configuration management Information deletion Data masking Data leakage prevention Monitoring activities Web filtering Secure coding

DANSK STANDARD

Attributter

5.9 Inventory of information and other associated assets

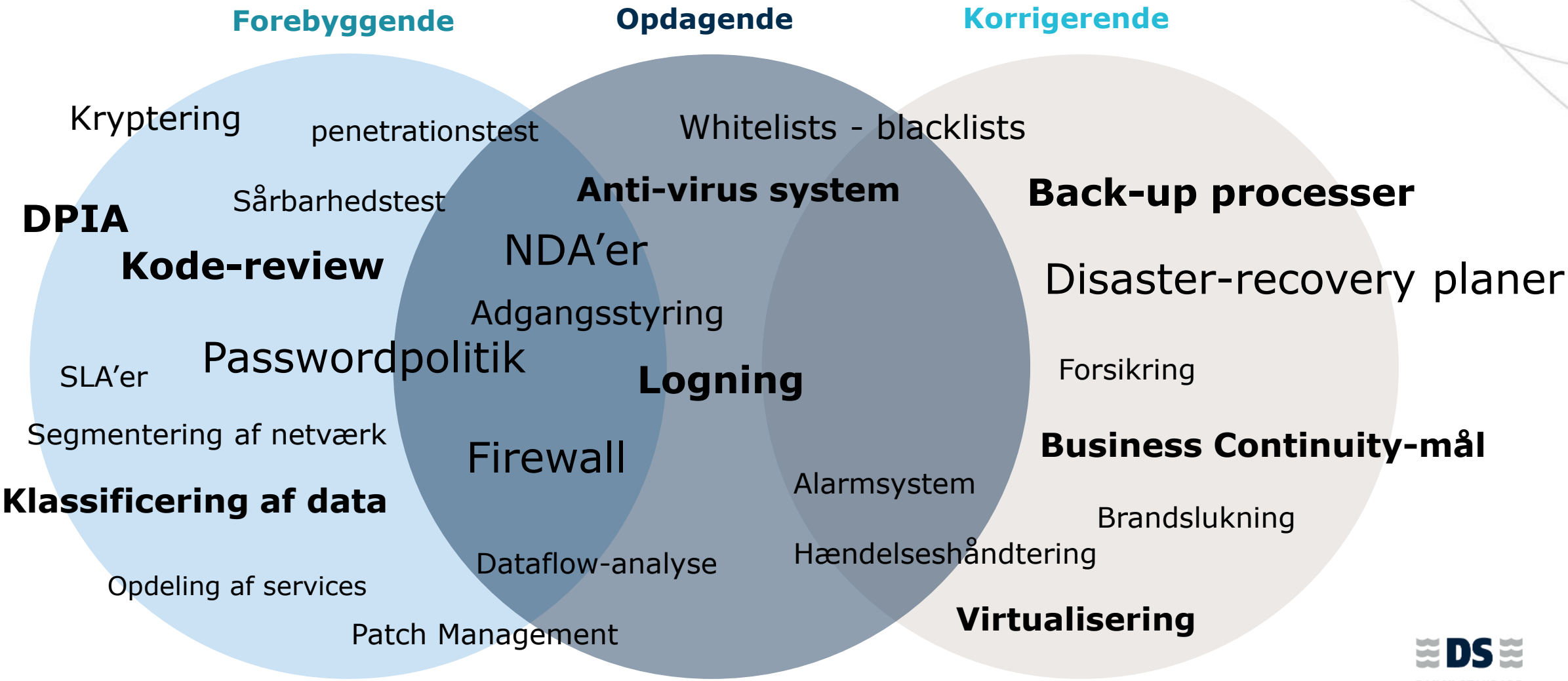
Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

– nye perspektiveringer på foranstaltningerne

Type af foranstaltning

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

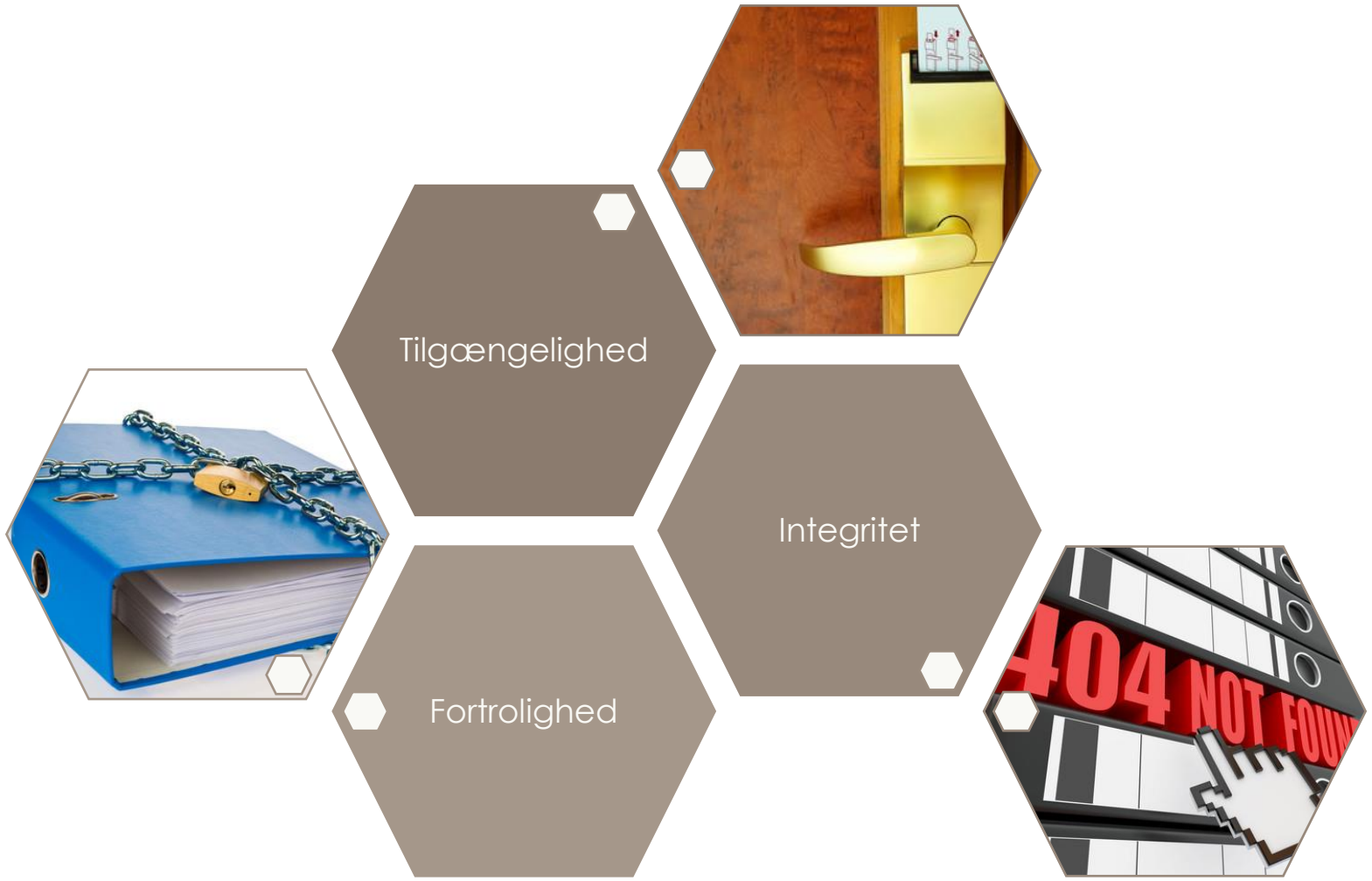


DANSK STANDARD

Egenskaber for informationer

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



Cybersikkerhedskoncept

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

Identify

- hjælper med at udvikle en organisatorisk forståelse af styring af cybersikkerhedsrisiko for systemer, mennesker, aktiver, data og kapaciteter

Protect

- understøtter begrænsning eller inddæmning af potentielle cybersikkerhedshændelser og skitserer sikkerhedsforanstaltninger for kritiske services

Detect

- definerer de relevante aktiviteter til at identificere forekomsten af en cybersikkerhedshændelse

Respond

- inkluderer passende aktiviteter til at gribe ind over for en opdaget cybersikkerhedshændelse og inddæmme konsekvensen heraf

Recover

- identificerer passende aktiviteter til at vedligeholde planer for modstandsdygtighed og genskabe kapaciteter eller services, der blev forringet på grund af en cybersikkerheds-hændelse

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

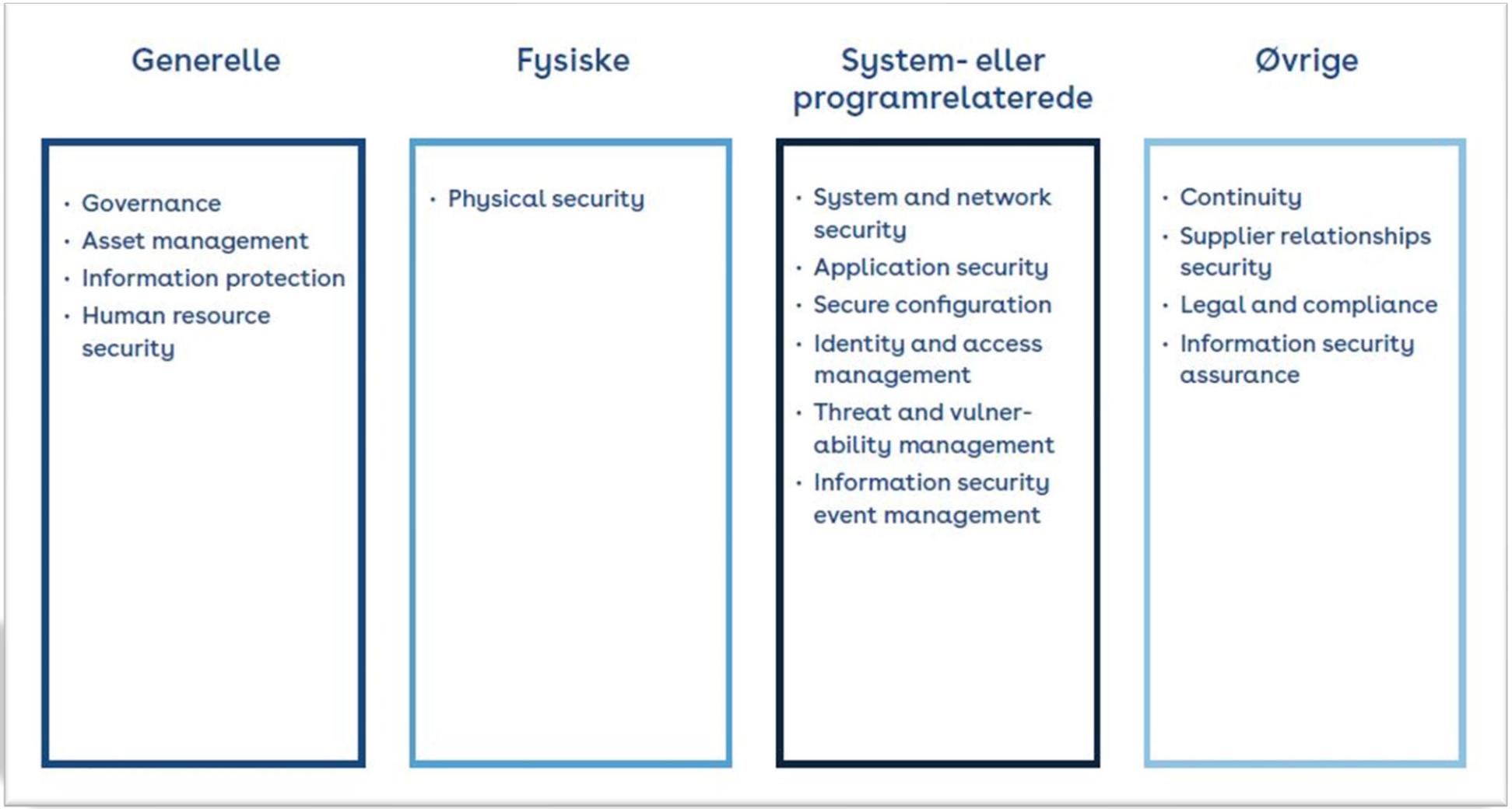
ISO/IEC TR 27110

DS DANSK STANDARD

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

Operationelle ressourcer

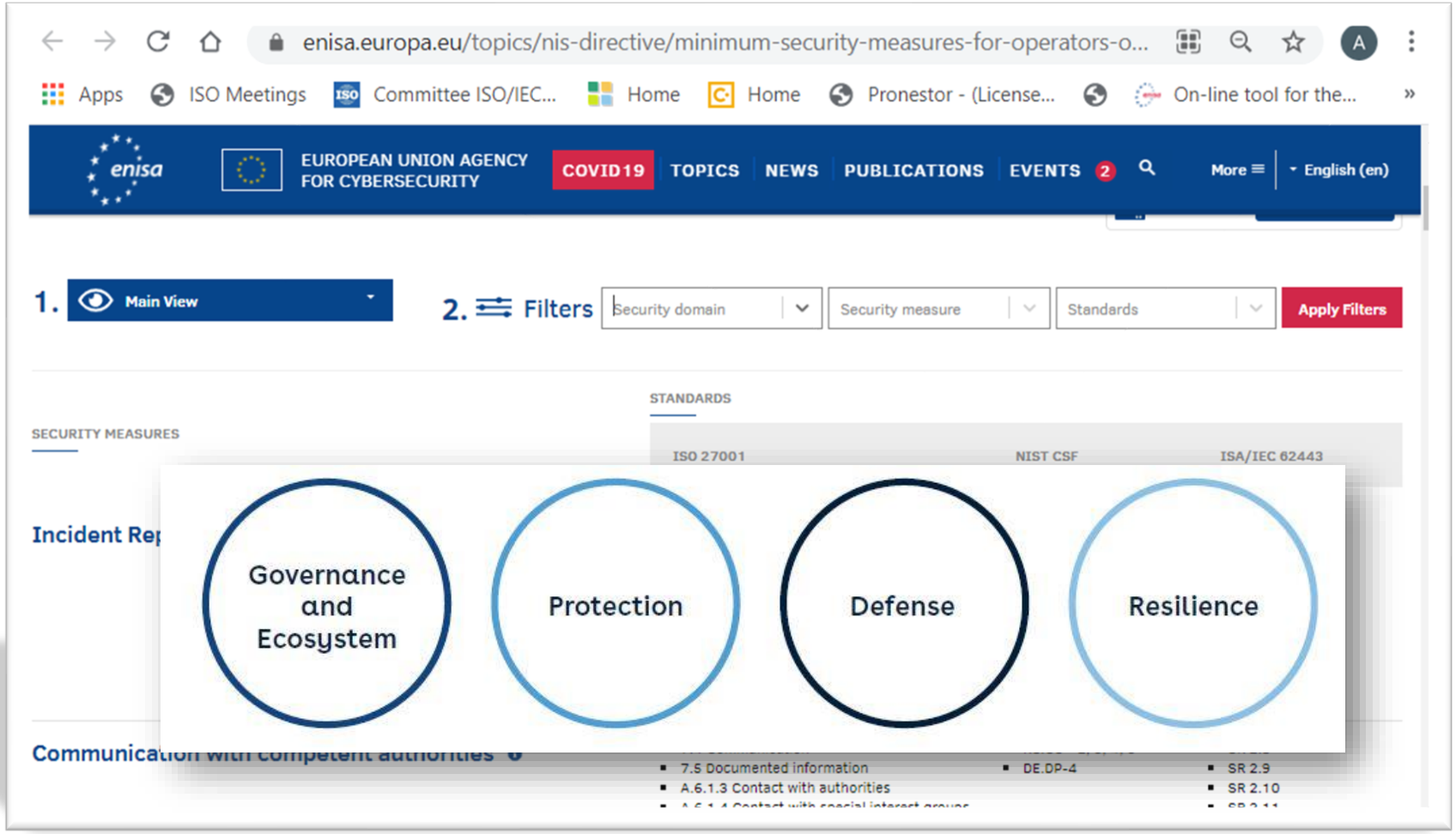


DS DANSK STANDARD

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



https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

DS DANSK STANDARD

Den nye ISO/IEC 27002

Indsigt i ISO/IEC 27002's nye organisatoriske, tekniske, fysiske og adfærdsrelaterede foranstaltninger

DANSK STANDARD

Data masking (NY)

Afidentifikationsteknikker, jf. ISO/IEC 20889

- Fokus: Følsomme data, herunder persondata skal delvist vises eller erstattes af ikke-følsomme data.
- Formål: at begrænse visning af følsomme data, herunder persondata
- Masking ved:
  - Kryptering – kræver nøgle
  - Tegnforvrængning - ændring af sekvenser af tegn
  - Annullering eller sletning af tegn
  - Variation af antal og datoer
  - Erstatning - ændring af en værdi til ngt andet
  - Blanding - hvor stykker følsomme data ændres
  - Delvis visning

DS DANSK STANDARD

Web filtering (NY)

Følgende elementer skal overvejes ved blokering af hjemmesider:

- Hjemmesider, 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 filtering
- Kommuniker til de ansatte
- Uddan ansatte for at undgå ignorering af browser-advarsler og lignende

DS DANSK STANDARD

Threat intelligence (NY)

Oplysninger om informationssikkerheds-trusler bør indsamles og analyseres for at frembringe trusselsefterretninger.

Kilde: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

DS DANSK STANDARD

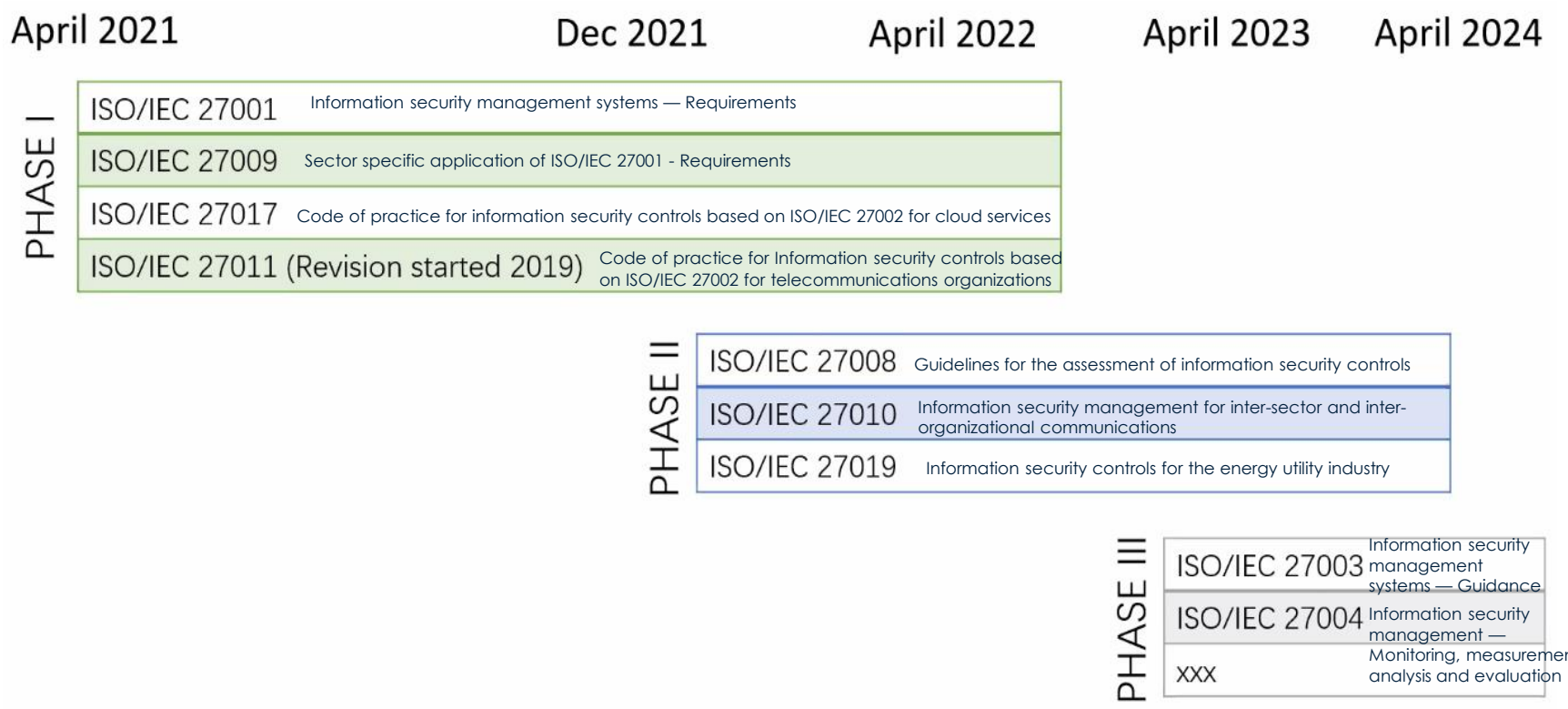
Tidshorisont

DANSK STANDARD

ISO/IEC 27002
Information security controls

Publiceringen af ISO/IEC 27002 har stor indflydelse på en lang række andre standarder (der er referencer til ISO/IEC 27002 i mange standarder).

Der er udarbejdet en business plan ift. ISO/IEC 27002, hvilke standarder den har indflydelse på, og hvilke standarder der derfor bør revideres:



Oversigt over ændringer i den nye ISO/IEC 27002

https://www.ds.dk/27002

DS
DANSK STANDARD

Tak for jeres tid!

Lasse Kaltoft
E-mail: lak@ds.dk

DANSK STANDARD

Cyber- og informationssikkerhed

Vi har samlet et overblik over de mest anvendte standarder inden for privatlivsbeskyttelse og cyber- og informationssikkerhed. Klik på figuren herunder for at læse om de enkelte standarder.

https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder