Kom på forkant med kravene i NIS2 med standarder

2. juni 2023
Dansk Standard

Dagens program

13:00 **Velkommen**

13:05 **Baggrund for NIS2 samt status på den danske implementering**

Rasmus Eriksen, Center for Cybersikkerhed

13:25 **Hvordan kan standarder understøtte jeres arbejde med NIS2?**

Majken Prip, Dansk Standard

13:40 **Kom godt i gang med NIS2 – en praktisk vinkel**

Karsten Vandrup, Stealth Computing

13:55 **Spørgsmål og afrunding**

14:00 **Tak for i dag**

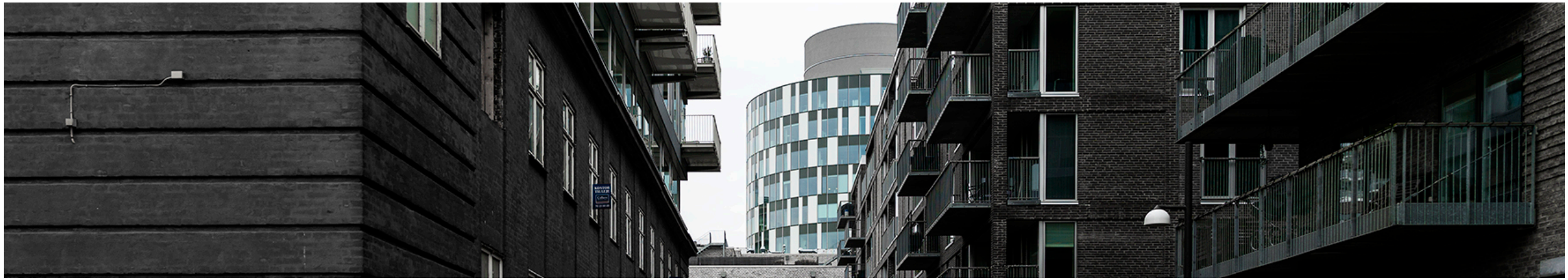
Om Dansk Standard

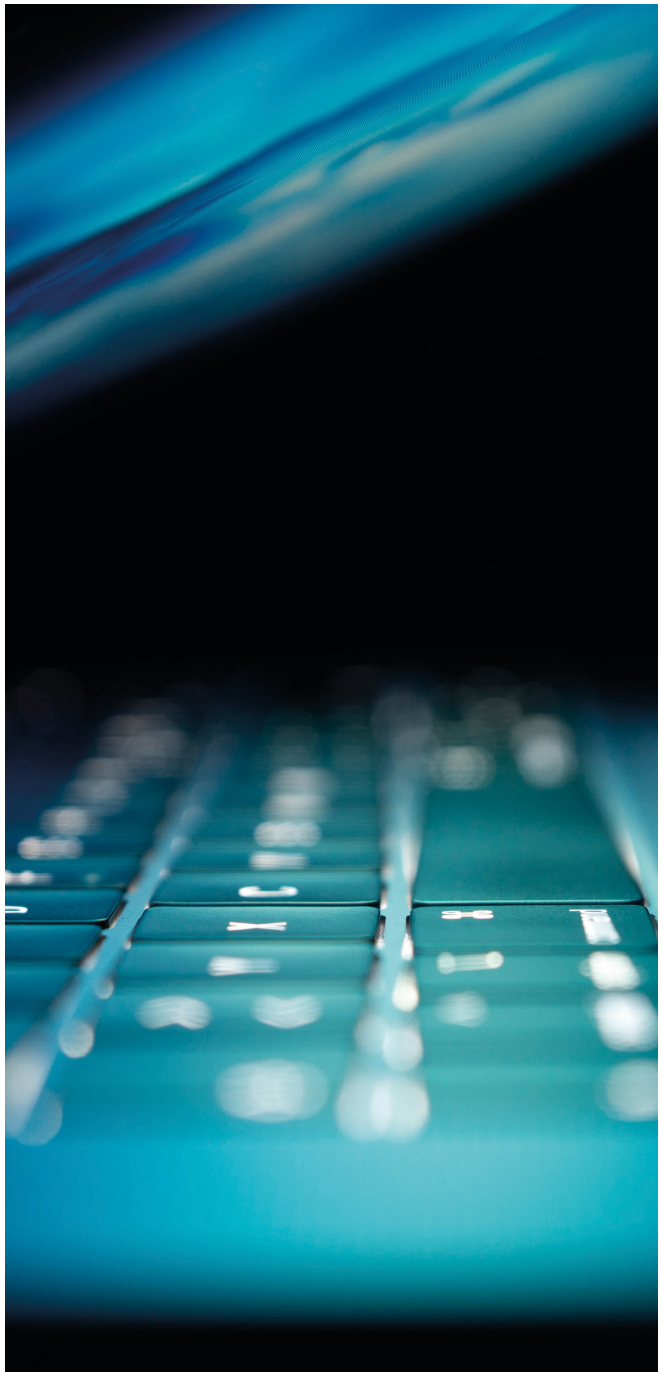
Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- Ca. 170 medarbejdere
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

En stærk platform af solide brands:





Hvorfor sætter vi fokus på NIS2?

Med NIS2 fastsættes der en række minimumskrav til foranstaltninger, der bl.a. indebærer at udarbejde politikker for risikoanalyse og informationssikkerhed, håndtere hændelser og sikre driftskontinuitet.

Artikel 25

Standardisering

1. For at sikre en samordnet gennemførelse af artikel 21, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske og internationale standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi.

CENTER FOR CYBERSIKKERHED

NIS2-direktivet
Baggrund og implementering

CENTER FOR CYBERSIKKERHED

Baggrund

Baggrund: NIS1

- EU vedtog i 2016 et direktiv om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer (EU direktiv 2016/1148 af 6. juli 2016)
- Direktivet er i Danmark implementeret ved en række love og bekendtgørelser
- Implementeringen er sket efter sektoransvarsprincippet, hvor myndighedsopgaverne er fordelt ift. ressortområder

Evaluering af NIS1

Kommissionens evaluering af NIS1 har konstaterede følgende:

- Lav cyber-modstandsdygtighed blandt virksomheder i EU
- Inkonsistent cyber-modstandsdygtighed på tværs af medlemsstater og sektorer
- Lavt niveau af fælles situationsbevidsthed og mangel på fælles kriserespons

NIS2 - overordnet

- Vedtaget med henblik på at udbedre udfordringerne fra NIS1 og øge cybersikkerheden generelt for kritisk infrastruktur på tværs af sektorer i EU.
- Den 16. december 2020 fremsatte Kommissionen et udkast til NIS2, som skulle erstatte NIS1.
- Den 14. december 2022 blev den endelige udgave af NIS2 vedtaget og trådte i kraft den 16. januar 2023.
- NIS2 fastsætter, at direktivet skal implementeres med retskraft i national lovgivning den 18. oktober 2024.
- NIS2 ophæver samtidig NIS1 med virkning fra den 18. oktober 2024.

Overordnet indhold i NIS2

1. Retlig forpligtelse for medlemsstater til at vedtage nationale cybersikkerhedsstrategier

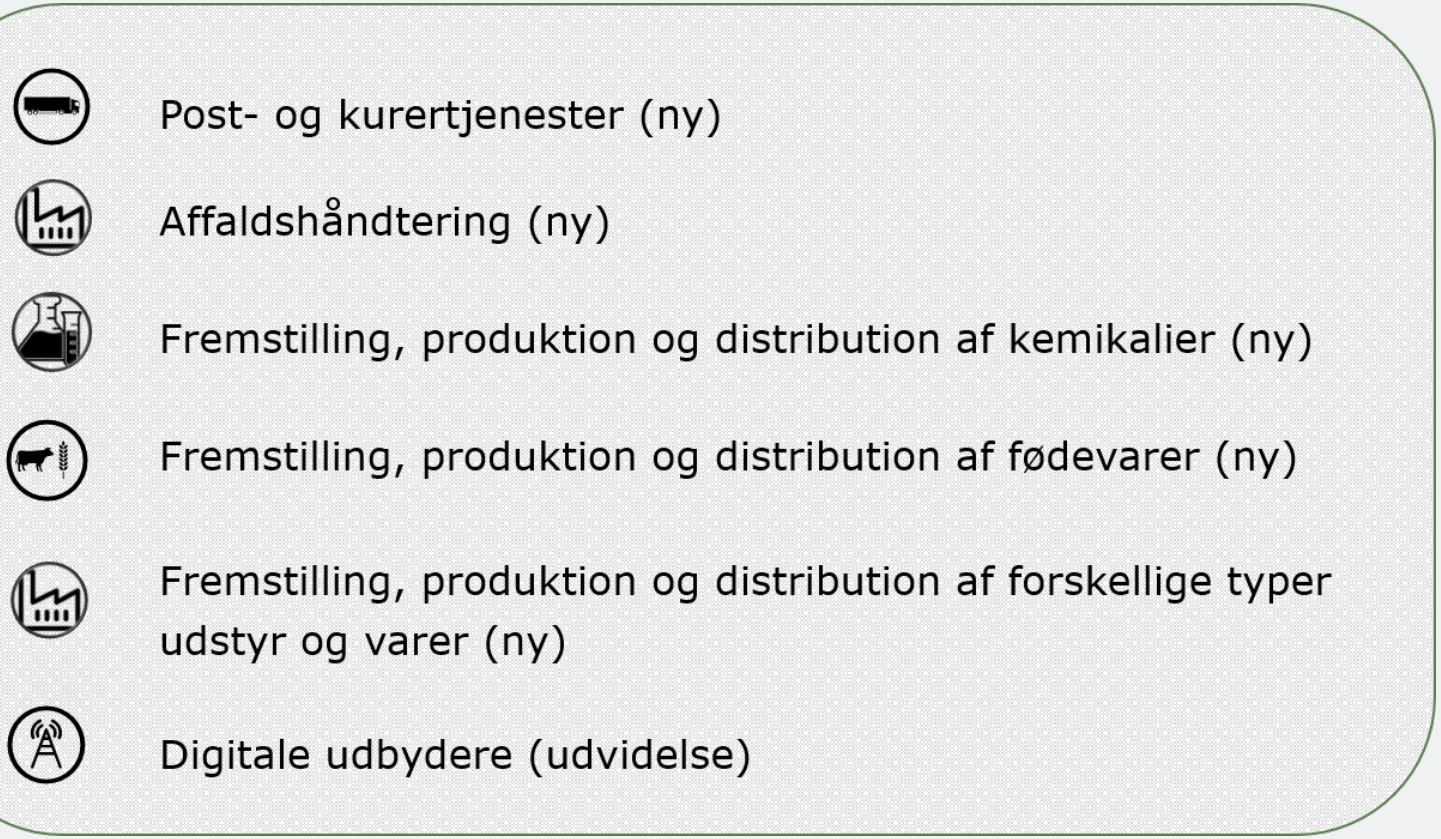
2. Retlig forpligtelse for medlemsstater til at udpege nationale cybersikkerhedsmyndigheder (CSIRT, centralt kontaktpunkt og kompetente myndigheder)

3. Retlig forpligtelse til risikostyring og underretning af cybersikkerhedsrisici for de enheder, der omfattes af direktivet (art. 21 og 23)

Hvem bliver omfattet - væsentlige sektorer i NIS2

- Energi (udvidelse)
- Transport (udvidelse)
- Bank
- Finansielle markedsinfrastrukturer
- Sundhed (udvidelse)
- Drikkevand
- Spildevand (ny)
- Digital infrastruktur (udvidelse)
- Offentlig forvaltning (ny)
- Rummet (ny)

Hvem bliver omfattet - vigtige sektorer i NIS2



Hvad indbefatter risikostyring

Art. 21 (1): […] væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene […]

Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de […] tilvejebringe et sikkerhedsniveau […] der står i forhold til risiciene.

Altså: **Proportionalitet**

Hvad indbefatter risikostyring

Art. 21 (2) – omhandler mindst:

a) politikker for risikoanalyse og informationssystemsikkerhed

b) håndtering af hændelser

c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring

d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere

e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

CENTER FOR CYBERSIKKERHED

NIS2 implementering

Hvor er vi nu ift. implementering i DK?

- Tidligt stadie i forhold til en omfattende lovgivningsprocess. Det er således ikke muligt at komme med sektorspecifikke vejledninger om, hvad de præcise krav bliver, eller udtømmende at svare på hvilke enheder der bliver omfattet.

- Der udestår en tværministeriel proces, der skal adressere spørgsmål om tilsynsmyndigheder, koordination, ressortansvar for de enkelte sektorer mv.

- Det er CFCS's ambition, at implementeringen og håndhævelsen af de nye regler sker på en hensigtsmæssig måde, hvor der tages hensyn til den frist, som de enkelte enheder ender med at have fra lovgivningens endelige vedtagelse.

- Ingen parter er tjent med en forceret implementering i de enkelte sektorer, og der er stor bevidsthed om, at der vil være tale om komplekse regler og krav, som er ressource- og tidskrævende at implementere.

Hvor er vi nu ift. implementering i EU?

- Direktivet har som et kernehensyn at sikre en ensartet tilgang til reglernes fortolkning og anvendelse på tværs af EU-landene. Der er derfor løbende fokus herpå i EU-regi.

- Dette forventes bl.a. at ske gennem såkaldte gennemførelsesretsakter på visse områder, der bliver direkte gældende i medlemsstaterne.

Gennemførelsesretsakter i NIS2

- NIS2 art. 21, (5): EU skal vedtage gennemførelsesretsakter, der fastsætter regler for tekniske og metodologiske krav for risikostyring for visse tjenesteudbydere, blandt andet
  - DNS-tjenester
  - topdomænenavnsadministratorer
  - cloudcomputingtjenester
  - datacentertjenester
  - onlinemarkedspladser
  - onlinesøgemaskiner
  - platforme for sociale netværkstjenester

- Disse gennemførelsesretsakter skal være vedtaget senest den 17. oktober 2024.

- NIS2 art. 21, (5): EU kan derudover vedtage gennemførelsesretsakter for andre væsentlige og vigtige enheder. Ingen frist.

Betydning

- Medlemsstaterne skal vedtage lovgivning, som udmønter bestemmelserne i direktivet.
- For visse særlige tjenester (DNS-tjenester, topdomænenavnsadministratorer, onlinemarkedspladser, onlinesøgemaskiner mv.) skal EU dog fastsætte visse regler.
- For andre væsentlige og vigtige sektorer kan EU fastsætte visse regler.
- Reglerne for de særlige tjenester skal foreligge inden den 17. oktober 2024.
- For andre væsentlige og vigtige sektorer er der ingen frist, og kan derfor blive indført senere.
- EU kan således potentielt få stor betydning for fortolkningen af kravene i NIS2.

Tak for opmærksomheden

CENTER FOR CYBERSIKKERHED
Kastellet 30 / Holsteinsgade 63
2100 København Ø

Telefon: +45 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Hvordan kan standarder understøtte arbejdet med NIS2?

Majken Prip, Dansk Standard

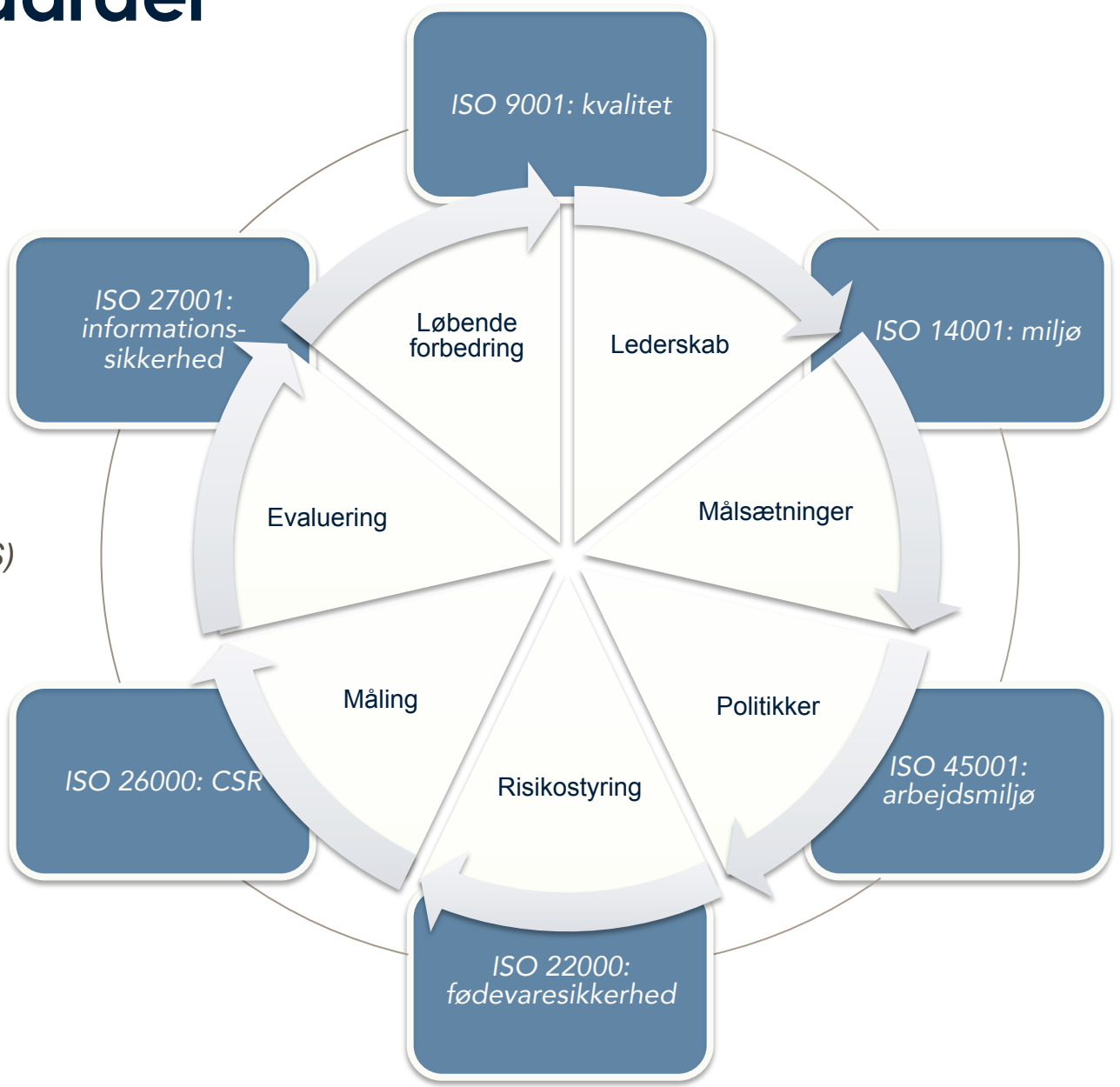
NIS 2 direktiv
Artikel 25

Standardisering

For at sikre en samordnet gennemførelse af artikel 21, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske og internationale standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi

Ledelsesstandarder

Harmonized Structure (HS)



DANSK STANDARD

Definition af ledelsessystem for informationssikkerhed (ISMS)

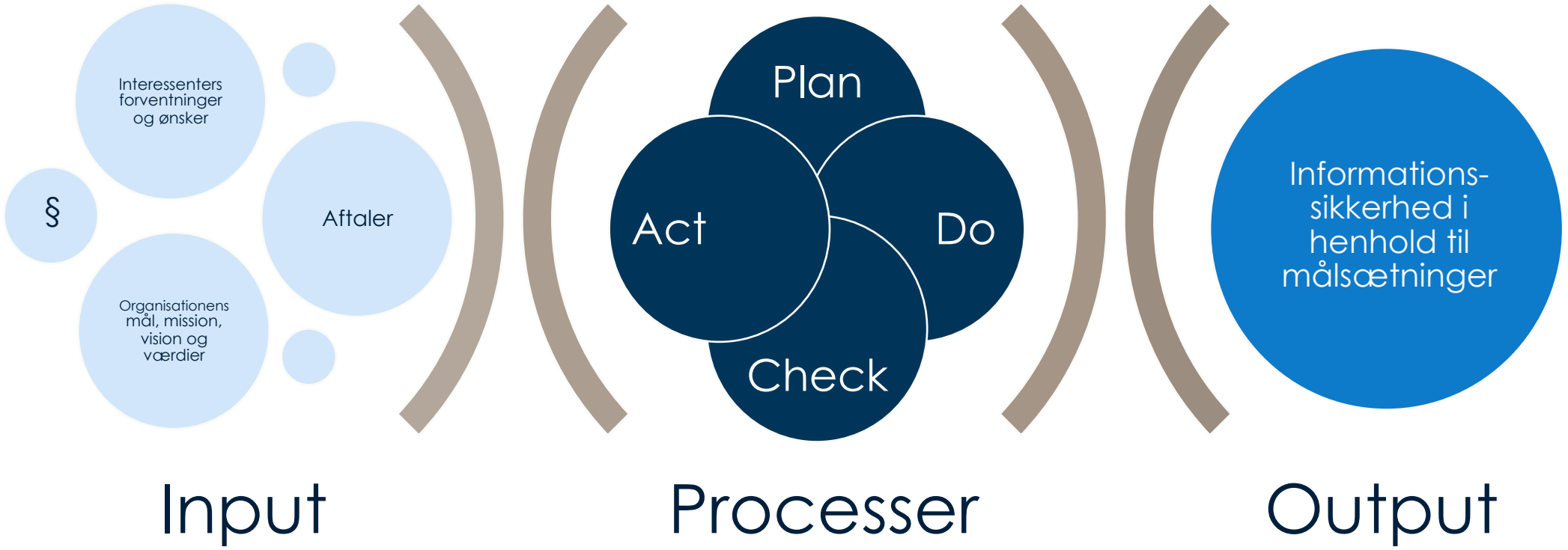
- En struktureret tilgang til organisationens informationssikkerhed for at nå forretningsmålene.
- Baseret på risikovurdering og organisationens risikoaccept til effektiv styring af risici.
- Identifikation af krav til beskyttelse af informationsaktiver.
- Anvendelse af egnede foranstaltninger til sikring af informationsaktiver.

Definition af ledelsessystem for informationssikkerhed (ISMS)

"Ledelsessystemet for informationssikkerhed bevarer fortrolighed, integritet og tilgængelighed af information ved hjælp af en risikostyringsproces og sikrer, at interessenter har tillid til, at risici håndteres på en ordentlig måde."

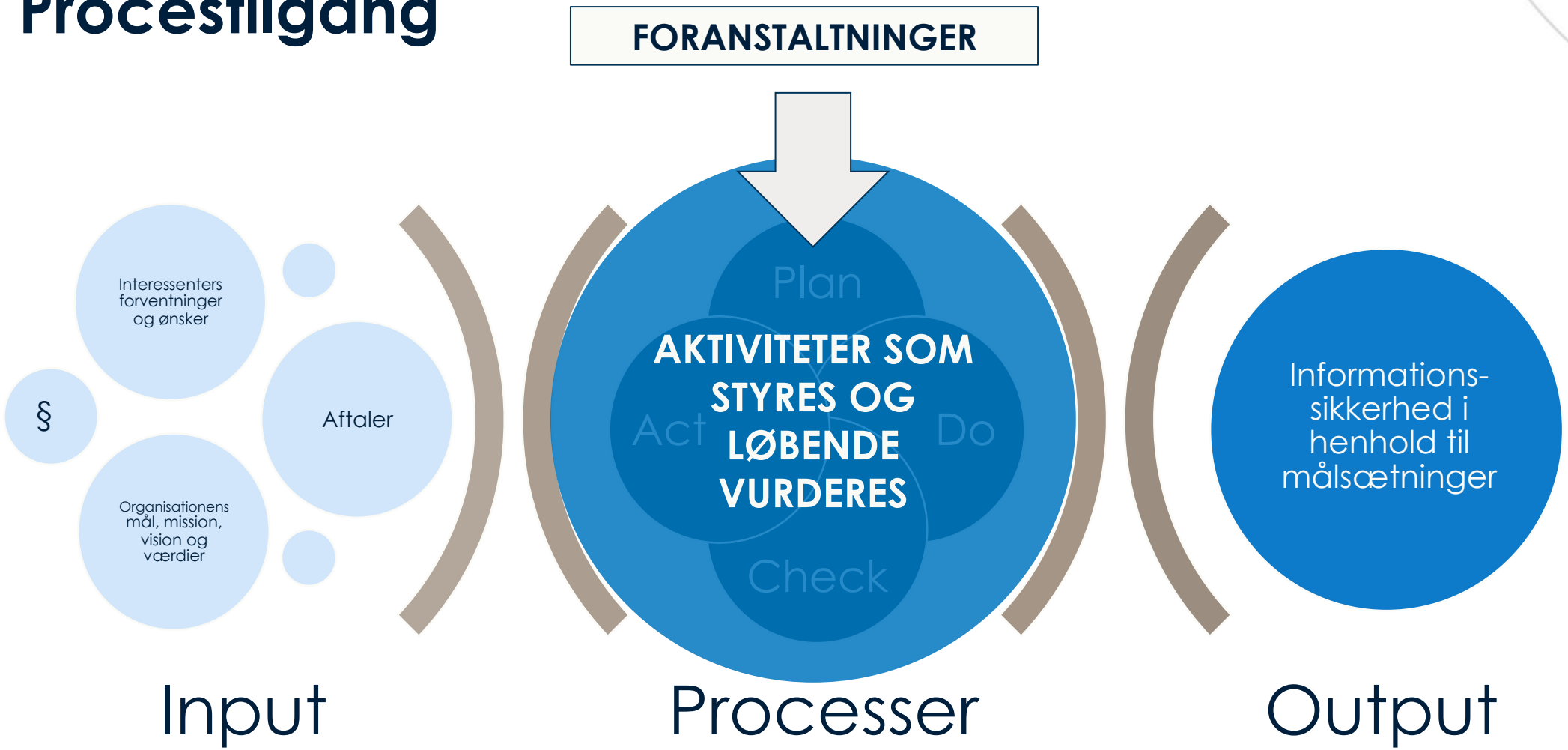
EN ISO/IEC 27001:2017 Indledning, 01

Procestilgang



DANSK STANDARD

Procestilgang



PLAN	DO	CHECK	ACT
Organisationens Målsætninger	Vurdering af risici	Evaluering	Korrigerende handlinger
Interessentkrav og forventninger /	Håndtering af risici	Interne audits	Forbedring
Anvendelsesområde	SoA-dokument	Ledelsens gennemgang	
Politik	Program for implementering		
Tilgang til risikostyring			

DS DANSK STANDARD

De centrale elementer i NIS2 koblet til ISO27001

DANSK STANDARD

ISO27001 Annex A, Foranstaltninger

Organisatorisk
- Alt det andet

Personrelateret
- Personer: ansatte og eksterne

Fysisk
- De fysiske rammer og enheder

Teknologisk
- Tekniske forhold

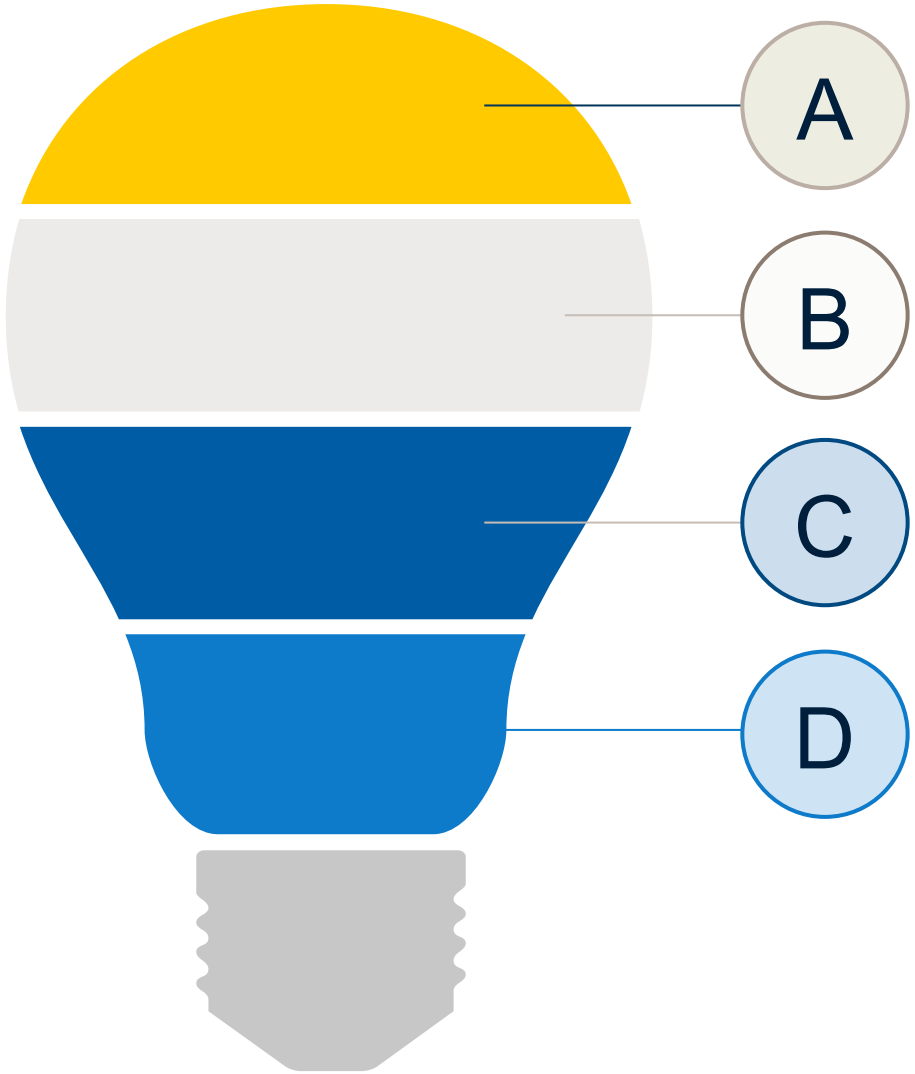
1.Risikovurdering, muligheder for risikohåndtering og kriterier for risikoaccept.

Overholdelse af lovgivning, aftaler eller brancherelaterede krav.

Effekten af samspillet mellem forskellige foranstaltninger.

DS
DANSK STANDARD

Fordele ved anvendelsen af ISO27001



A

Strukturering af det løbende arbejde med informationssikkerhed

B

Fastlæggelse af best practices inden for informationssikkerhed

C

Støtte til en risikobaseret tilgang til styring af informationssikkerhed

D

Simpel tilpasning til fremtidige ændringer i lovgivning, samt lettere integration af lovkrav herunder NIS2 i eksisterende processer og sikkerhedsprogrammer

DS
DANSK STANDARD

Kom godt i gang med NIS2 – en praktisk vinkel

v/ Karsten Vandrup, Stealth Computing

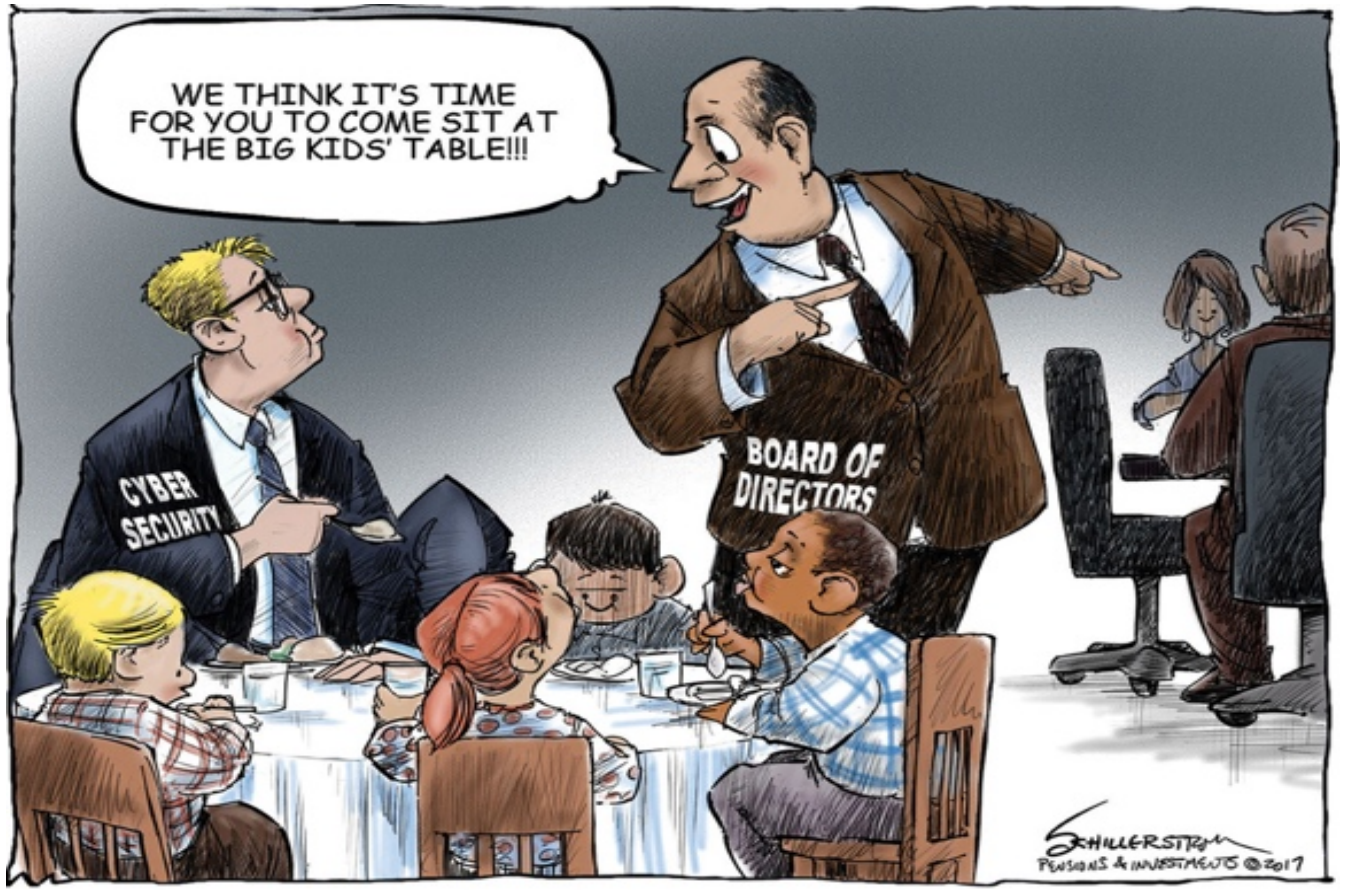
Cybersikkerhed starter og slutter i ledelsen

- ISO/IEC 27001 5.1 Lederskab

  og engagement

- ISO/IEC 27001 9.3 Ledelsens

  gennemgang



NIS2

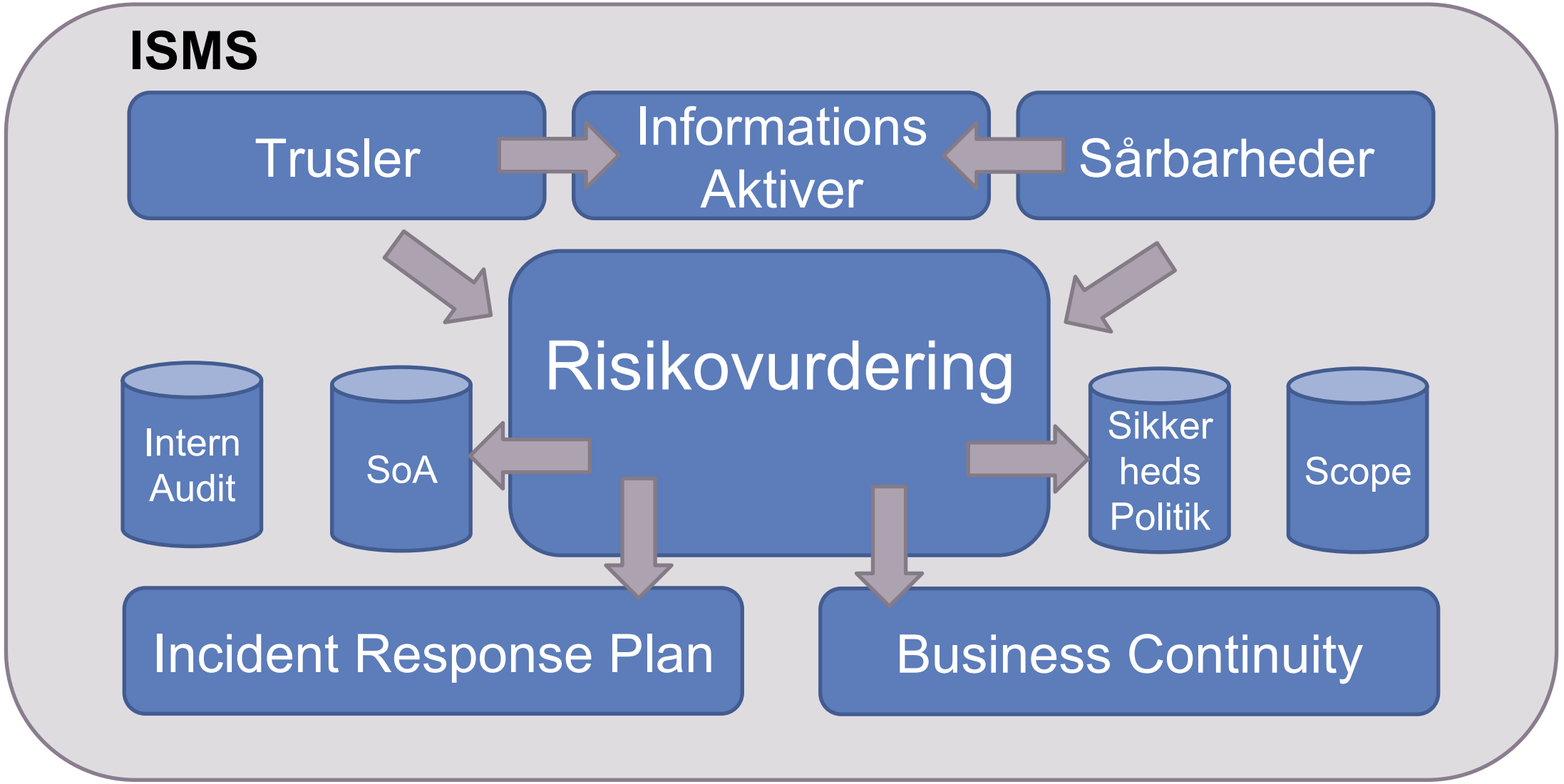
Artikel 20

Styring

1. Medlemsstaterne sikrer, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med dens gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel.
Anvendelsen af dette stykke berører ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

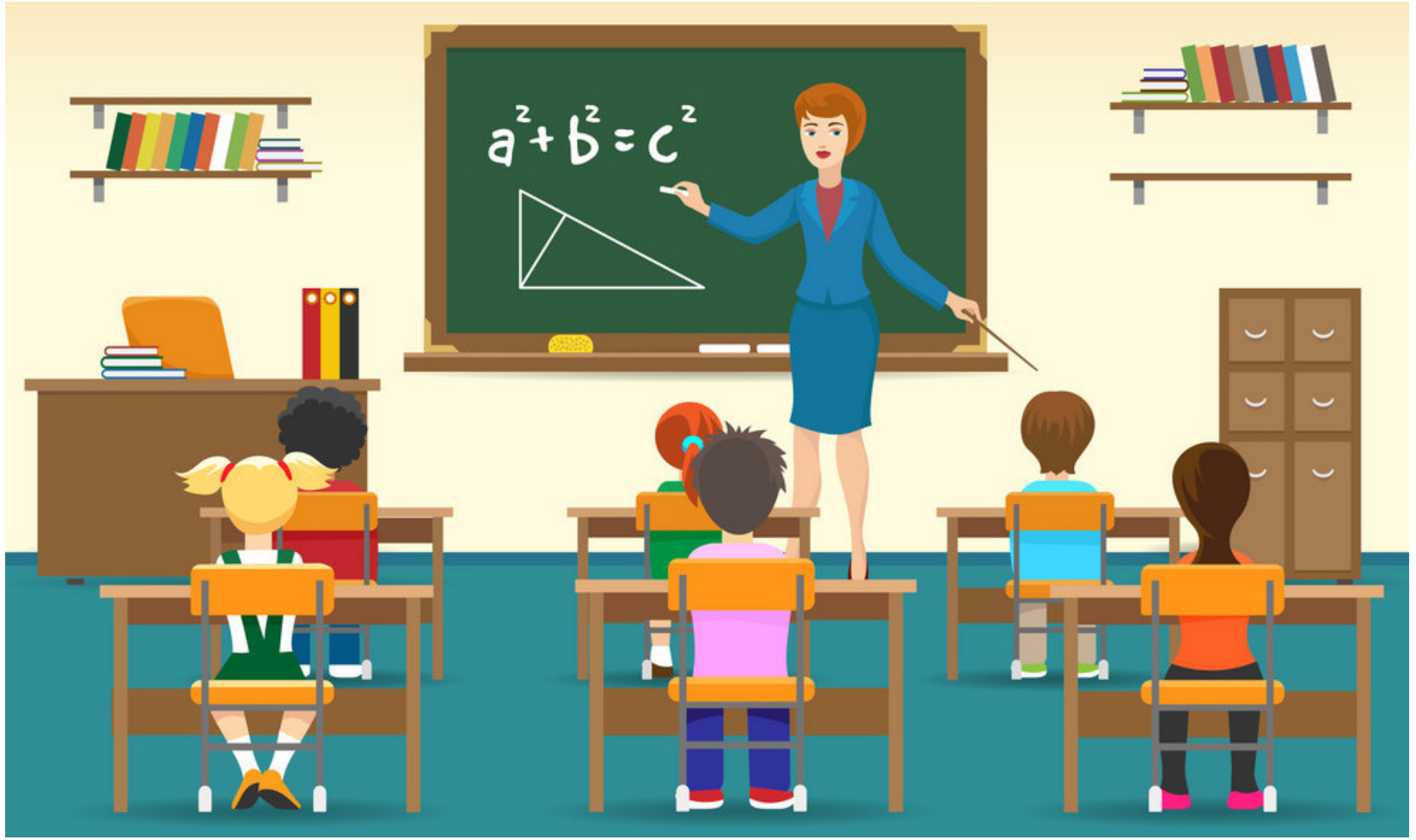
2. Medlemsstaterne sikrer, at medlemmerne af væsentlige og vigtige enheders ledelsesorganer er forpligtet til at følge kurser, og skal tilskynde væsentlige og vigtige enheder til løbende at tilbyde tilsvarende kurser til deres ansatte, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.

Hvordan kommer man i gang?



Træning

Topledelsen
Bestyrelsen
Ansatte



Spørgsmål?

Vil du lære mere om koblingen mellem NIS2 og ISO/IEC 27001?

Tag på kursus hos Dansk Standard:

https://www.ds.dk/da/ydelser/kurser/nis2-med-iso-27001

Et godt sted at starte for smv'er

Guide for risikostyring ift. cyber- og informationssikkerhed.
https://www.ds.dk/risikostyring

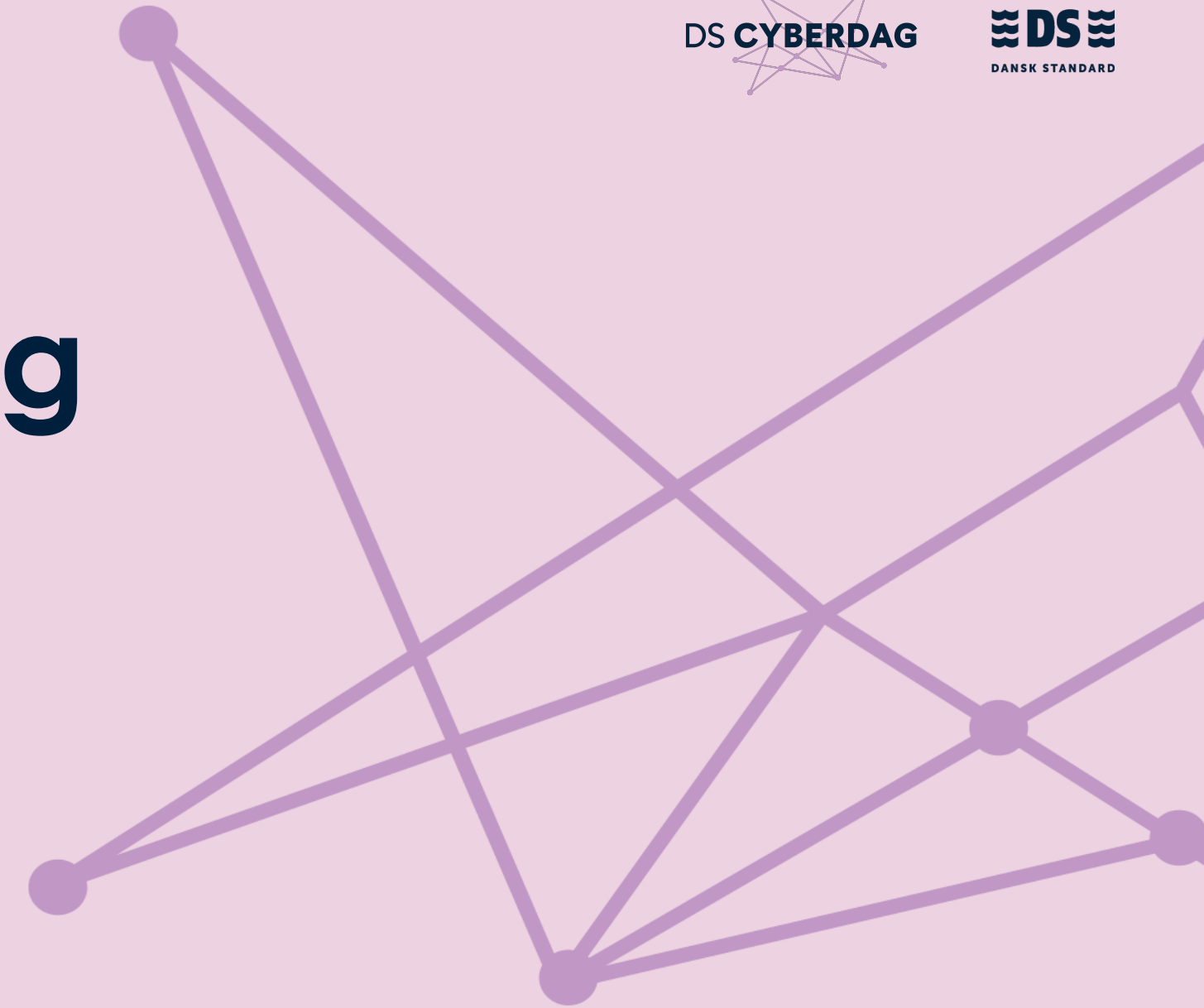
DS CYBERDAG

DS DANSK STANDARD

DS Cyberdag

Sæt x den 5. oktober

Følg med på ds.dk hvor der kommer flere informationer og program




God weekend