



MODUL 3 AF 6

NIS-2 Standarder D-Mærket

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- Ca. 200 medarbejdere
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:



En stærk platform af solide brands:



Mød jeres underviser

Mette Krogh Sørensen

Seniorkonsulent Dansk Standard

Underviser i standarder der har med cyber- og informationssikkerhed

Har arbejdet med informationssikkerhed de sidste 9 år

Har siddet med risikovurderinger, leverandørvurderinger, awarenessprogrammer og ledelsesrapportering

A vast, undulating landscape of white sand dunes under a clear blue sky. The dunes are smooth and rounded, creating a rhythmic pattern of light and shadow across the horizon. The sky is a uniform, bright blue, suggesting a clear day. The overall scene is serene and minimalist.

Hvad er NIS2?

Baggrunden for NIS2

- Formålet er at øge robustheden i flere organisationer på tværs af sektorer for i sidste ende at øge samfundets robusthed og modstandsdygtighed
- Skærpet fokus på cybersikkerhed i forsyningskæder
- NIS2 opstiller en række minimumskrav for cyber- og informationssikkerhed for virksomheder og organisationer, som varetager kritiske funktioner i samfundet
- Vil afløse det nuværende NIS-direktiv
- Ønskede at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i EU

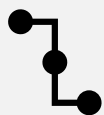
Hvad er nyt?



Flere virksomheder og organisationer er omfattet



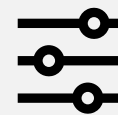
Flere sektorer kategoriseres som kritisk infrastruktur



Øget fokus på sikkerhed i forsyningskæder



Strengere tilsynsforanstaltninger



Flere sanktionsmuligheder












Underretningspligt på 24 timer



Større bøder

Hvem gælder NIS2 for?

Væsentlige enheder

-  Energi
-  Transport
-  Bankvirksomhed og finansielle markedsinfrastrukturer
-  Sundhed
-  Drikke- og spildevand
-  Digital infrastruktur
-  IKT-service management (B2B)
-  Offentlig administration
-  Rummet

Vigtige enheder

-  Post- og kurertjenester
-  Affaldshåndtering
-  Fremstilling, produktion og distribution af kemikalier
-  Produktion, tilvirkning og distribution af fødevarer
-  Fremstilling
-  Digitale udbydere
-  Forskning



Sammenhæng mellem NIS2 og standarder

Hvorfor tale om ISO/IEC 27001 i forbindelse med NIS2?

- NIS2-direktivet opfordrer til at anvende internationale, anerkendte standarder, jf. artikel 25
- ISO/IEC 27001
 - International og europæisk standard inden for cyber- og informationssikkerhed
 - Tilbyder en struktureret tilgang til at arbejde med informationssikkerhed
 - En række af de minimumskrav, der er nævnt i NIS2, bliver konkretiseret i standarden og yderligere uddybet i standarden ISO/IEC 27002 Foranstaltninger til informationssikkerhed
 - Er en ledelsesstandard, der har fokus på ledelsesforankring og strategi
 - Har fokus på ens organisations omverden og interessenter
 - Fokus på reelle forbedringer inden for informationssikkerhed

NIS2, 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.

NIS2 opstiller minimumskrav til

- **Risikostyring:** minimumsforanstaltninger
 - Artikel 20, 21
- **Ledelsen:** herunder krav til ledelsens tilsyn og kontrol med blandt andet risikovurderinger, minimumsforanstaltninger, leverandørstyring, rapporteringsforpligtelser
 - Artikel 20
- **Rapporteringsforpligtelser:** underrette kunder/samarbejdspartnere og tilsyn om væsentlige aktuelle og potentielle sikkerhedshændelser. Der er frist på underretning til tilsyn på 24 timer for tidlig varsling og 72 timer for hændelsesunderretning.
 - Artikel 23
- **Tilsynsbeføjelser og sanktioner:** blandt andet udvidede audit- og kontrolbeføjelser og sanktionsmuligheder. Det er inklusiv suspension af og ansvar for ledelsesmedlemmer, pligt til at offentliggøre manglende overholdelse af forpligtelser samt bøder på op til 75 mio. DKK eller 2 % af virksomhedens omsætning.
 - Tilsyn artikel 31, 32, 33
 - Bøder og sanktioner artikel 26, og 34

NIS2, artikel 21

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder **træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger** for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

Foranstaltninger fortsat

- a) Politikker for risikoanalyse og informationssikkerhed
- b) Håndtering af hændelser
- c) Driftskontinuitet (back-up) og krisestyring
- d) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører og 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 uddannelse i cybersikkerhed
- h) Politikker og procedurer ift. brug af kryptografi og, hvor det er relevant, kryptering
- i) Personalesikkerhed, politikker for adgangskontrol 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.

NIS2, artikel 23

Rapporteringsforpligtelser

1. Hver medlemsstat sikrer, at væsentlige og vigtige enheder **uden unødigt ophold underretter dens CSIRT** eller i givet fald dens kompetente myndighed i overensstemmelse med stk. 4 om **enhver hændelse, der har en væsentlig indvirkning på leveringen af deres tjenester** som omhandlet i stk. 3 (væsentlig hændelse). **Hvor det er relevant, underretter de pågældende enheder uden unødigt ophold modtagerne af deres tjenester om væsentlige hændelser**, der sandsynligvis vil påvirke leveringen af disse tjenester negativt.

[...]

Væsentlig hændelse

Artikel 23, stk. 3: En hændelse anses for at være væsentlig, hvis:

- a) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed
- b) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade

Rapportering

Tidlig varsling

**Hændelses-
underretning**

Endelig rapport

Hændelseshåndtering

Tidlig varslng

Væsentlige og vigtige enheders skal give "tidlig varslng" til CSIRT og den kompetent myndighed om "væsentlige hændelser" inden for 24 timer:

En hændelse anses for at være væsentlig, hvis

- 1) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller
- 2) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.



Hændeshåndtering

Hændelsesunderretning

En hændelsesunderretning, skal give:

- 1) en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger,
- 2) sendes uden unødigt ophold og under alle omstændigheder inden for 72 timer efter, at enheden har fået kendskab til den væsentlige hændelse



Hændeshåndtering

Endelig rapport

En endelig rapport sendes senest en måned efter fremsendelsen af den hændelsesunderretning, der er omhandlet i nr. 2. Rapporten skal indeholde følgende:

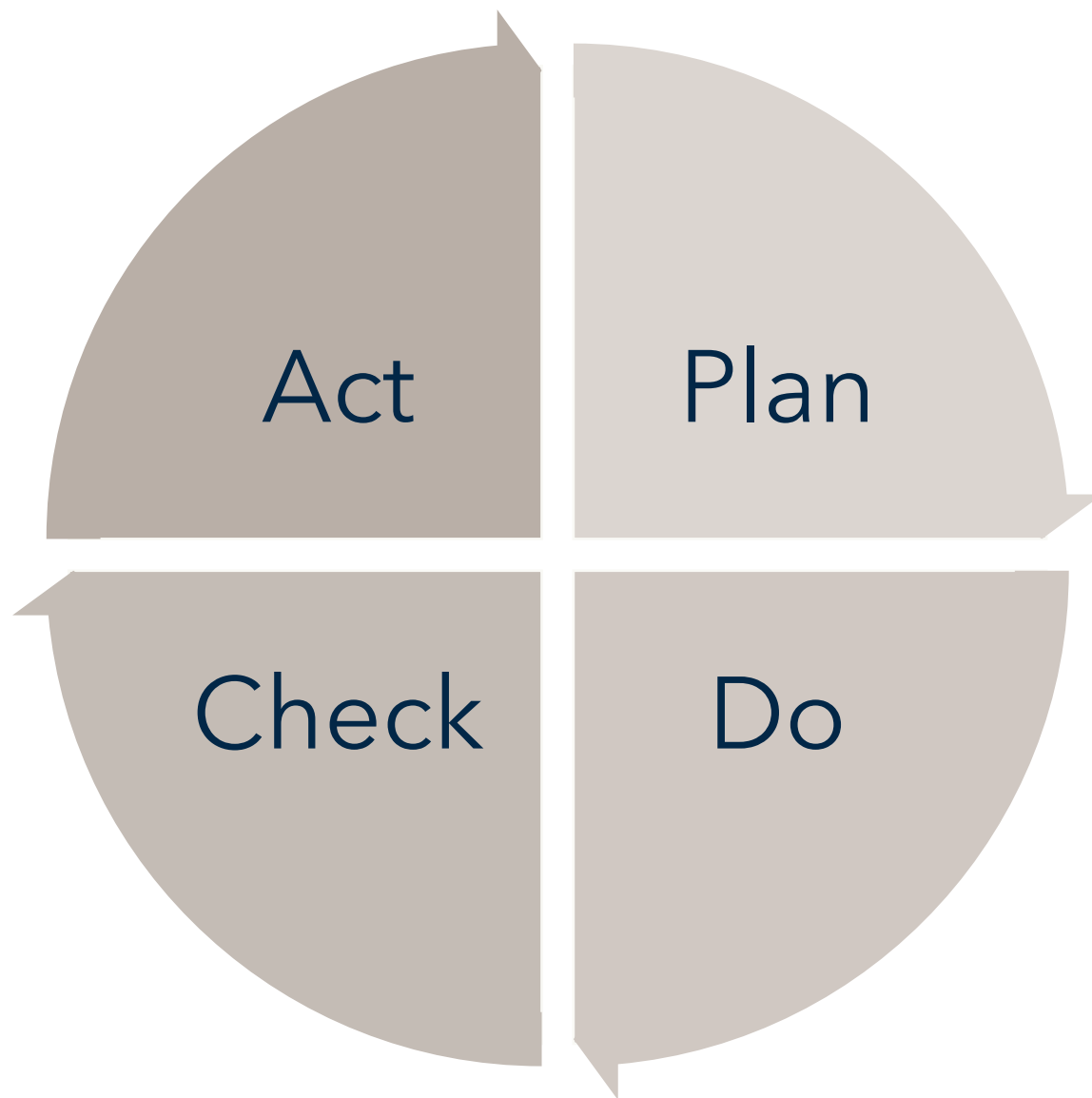
- a) En detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning.
- b) Den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen.
- c) Anvendte og igangværende afbødende foranstaltninger.
- d) De eventuelle grænseoverskridende virkninger af hændelsen.



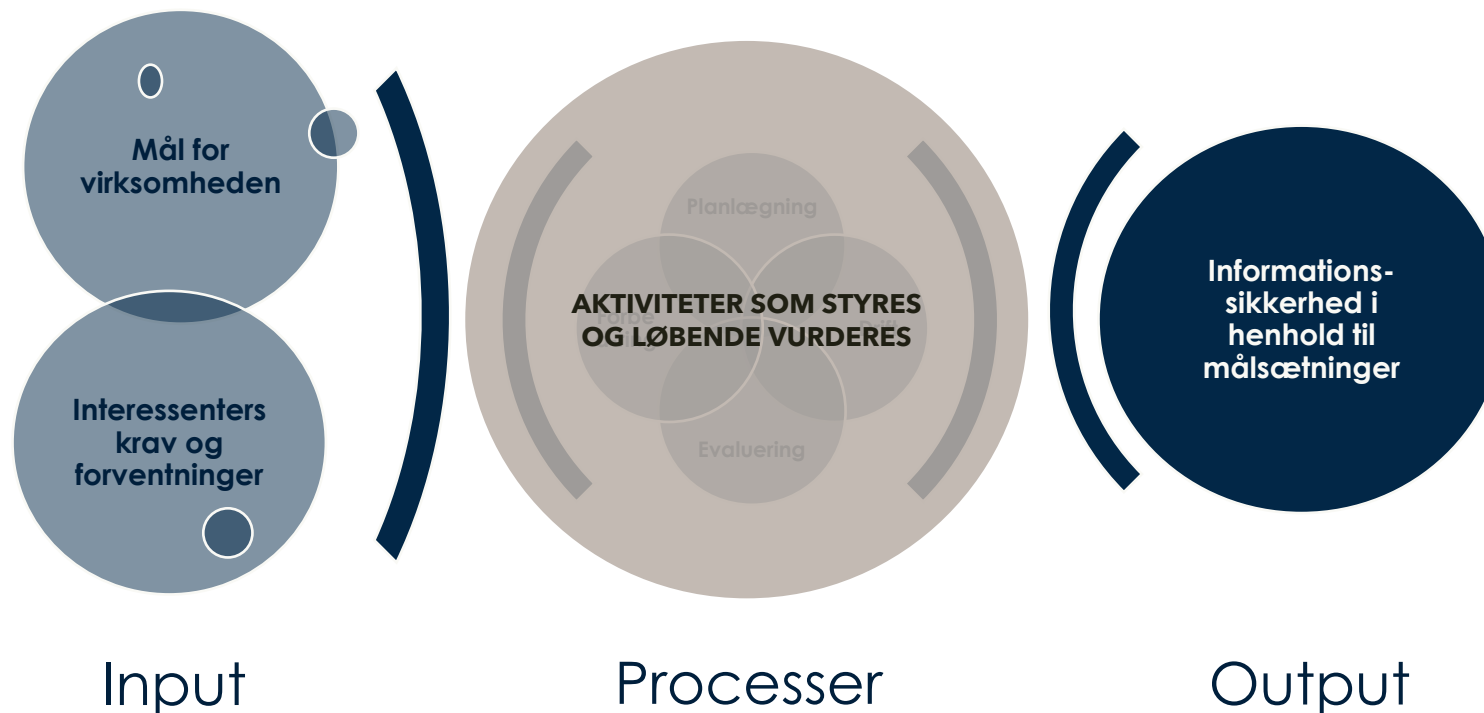
Hvad er standarder?

Hvad er standarder? Og hvad er ISO?

- En standard er et *“Dokument til fælles og gentagen anvendelse der angiver regler, vejledning eller karakteristiske træk ved aktiviteter eller ved resultaterne af disse. Dokumentet er fastlagt ved konsensus og vedtaget af et anerkendt organ. Hensigten er at opnå optimal orden i en given sammenhæng.”*
- Hvad er ISO?
 - Den største internationale standardiseringsorganisation med 164 nationale medlemsorganisationer fra hele verden
 - ISO faciliterer udviklingen af globale standarder, der fremmer international handel med varer og services.
 - ISO varetager alle standardiseringsområder bortset fra telekommunikation og elektroteknik, som varetages af ITU og IEC



Procestilgang



Integreres (hvor muligt) i eksisterende processer

Risikotankegang



ISO/IEC 27001

Hvad er formålet med ISO/IEC 27001?

"[...] at opstille krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for informationssikkerhed (ISMS)."

ISO/IEC 27001:2023, 0.1

Eks

-

-

-

-

-

-

-

-

-

-

-

-

-

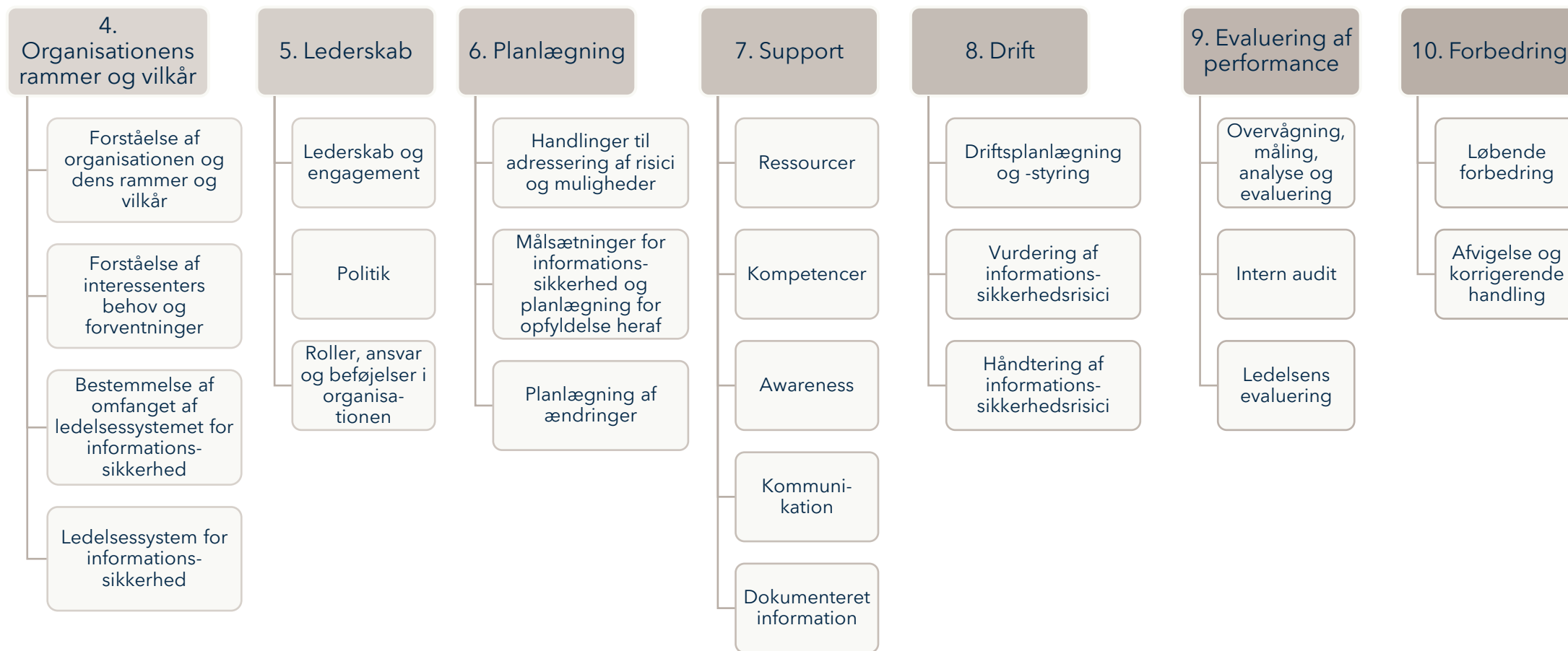




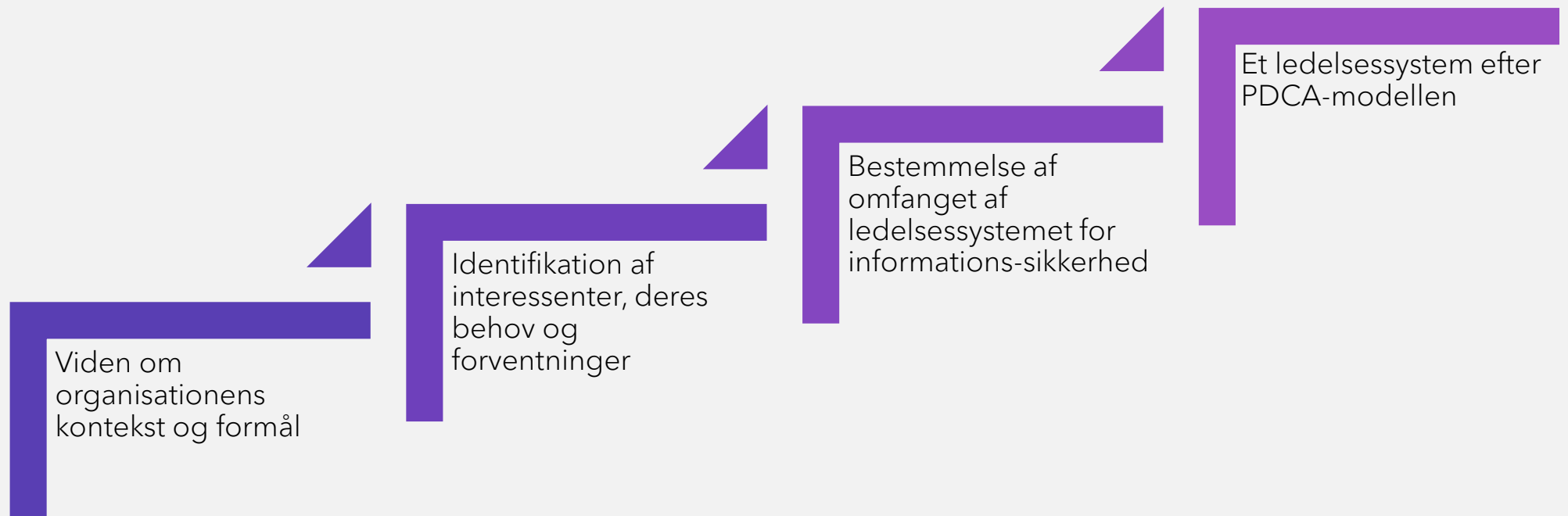
FORTROLIGHED

INTEGRITET

TILGÆNGELIGHED



4. Organisationens rammer og vilkår



5. Lederskab

Lederskab og engagement

- Kommunikation, ressourcefordeling og strategisk forankring

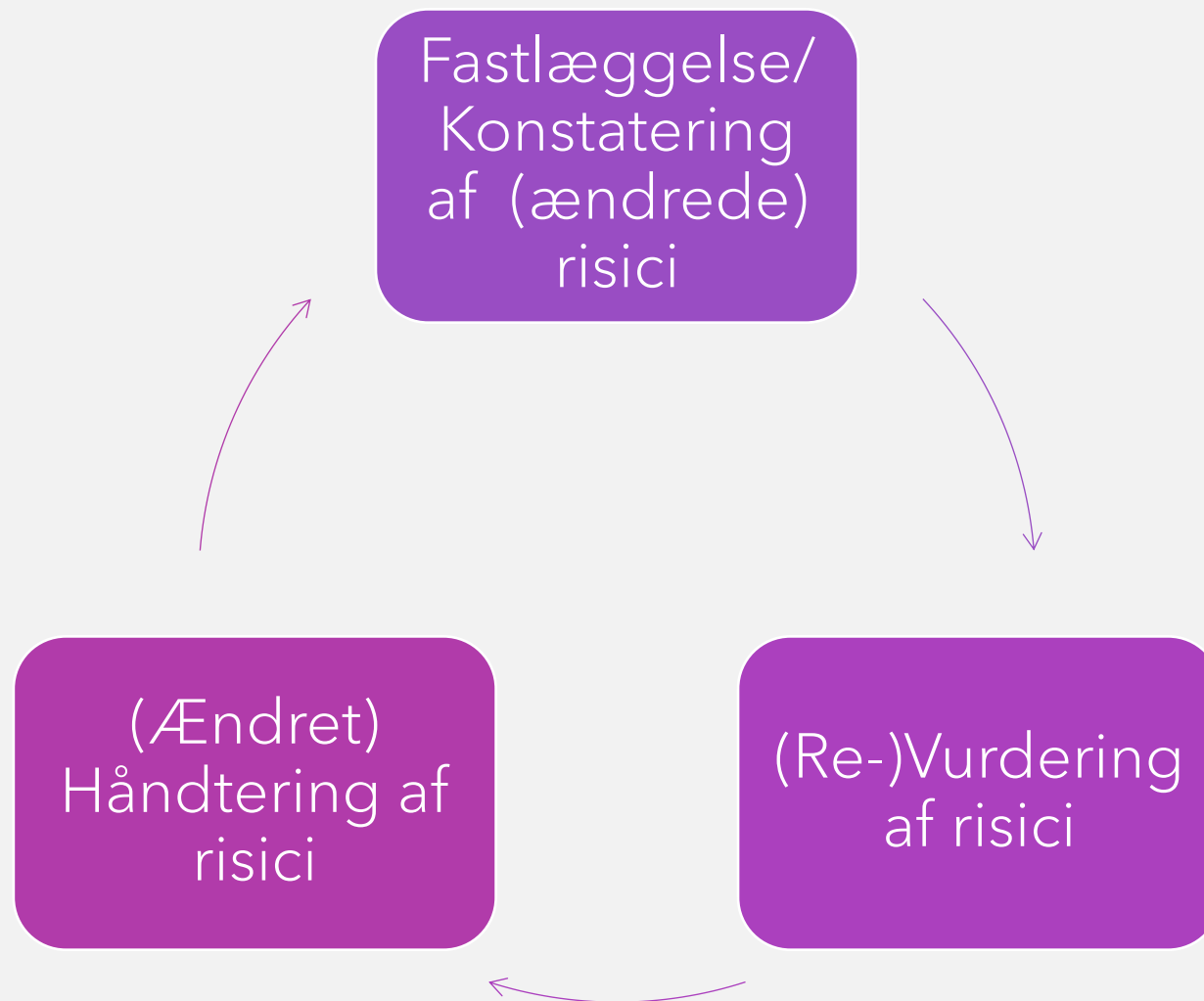
Politik

- Fastlæggelse af målsætninger og politikken for informationssikkerhed

Roller, ansvar og beføjelser i organisationen

- Delegering og kommunikation

6. Planlægning



7. Support



Ressourcer



Kompetencer



Awareness

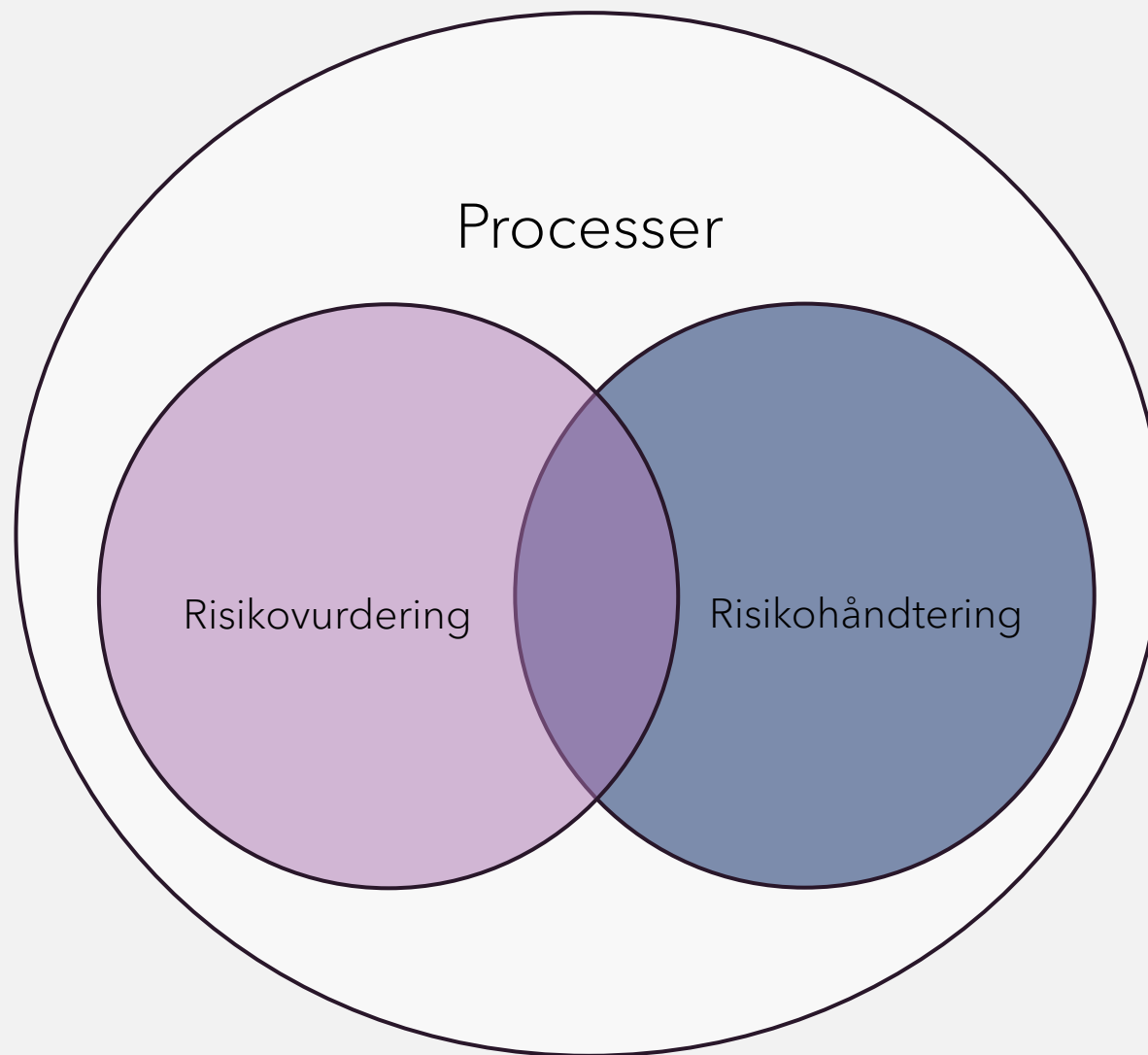


Kommunikation

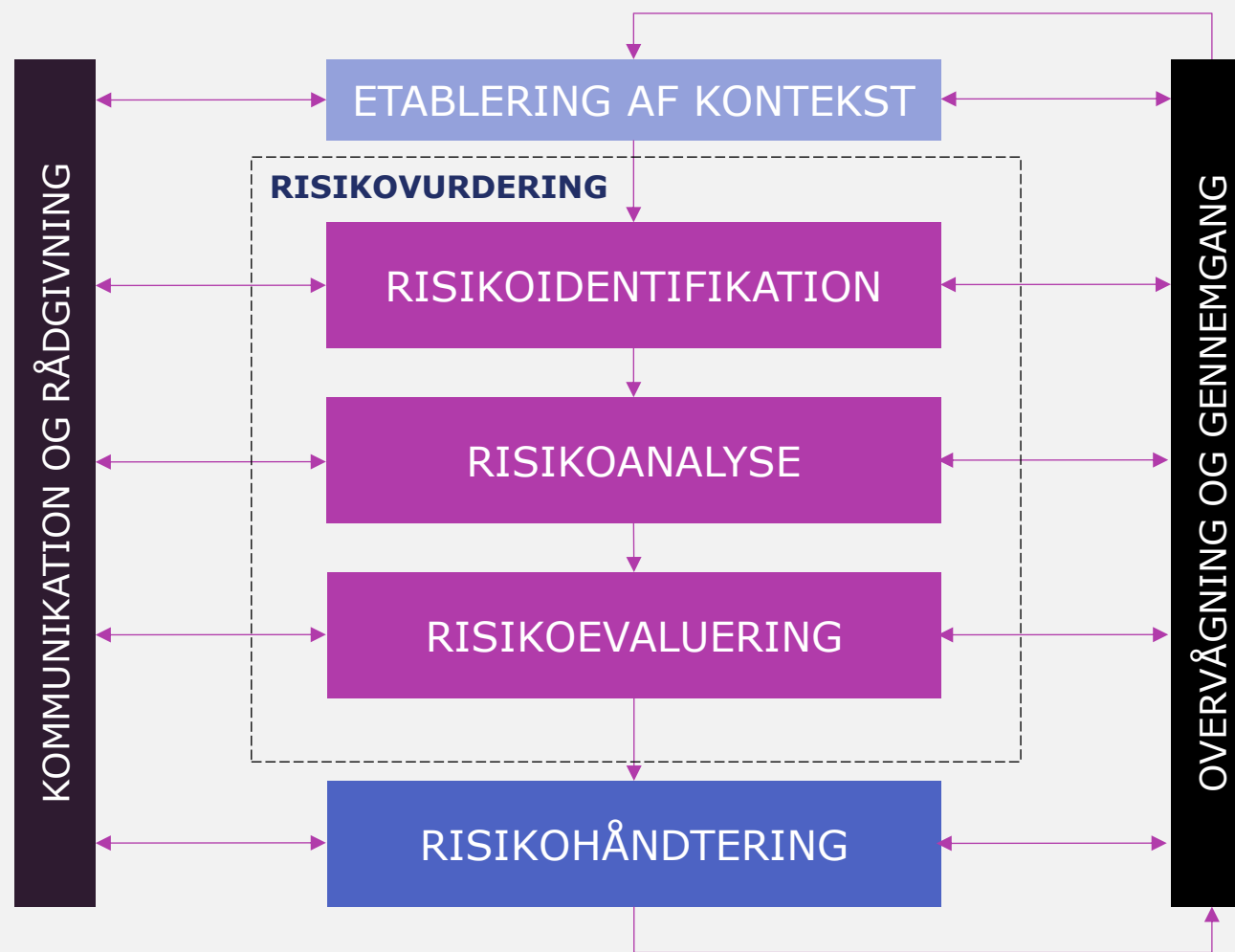


Dokumentation

8. Drift



Risikostyring, jf. ISO/IEC 27005



9. Evaluering

Overvågning, måling, analyse og evaluering

- Hændelser
- Processers effektivitet
- Risikovurderinger

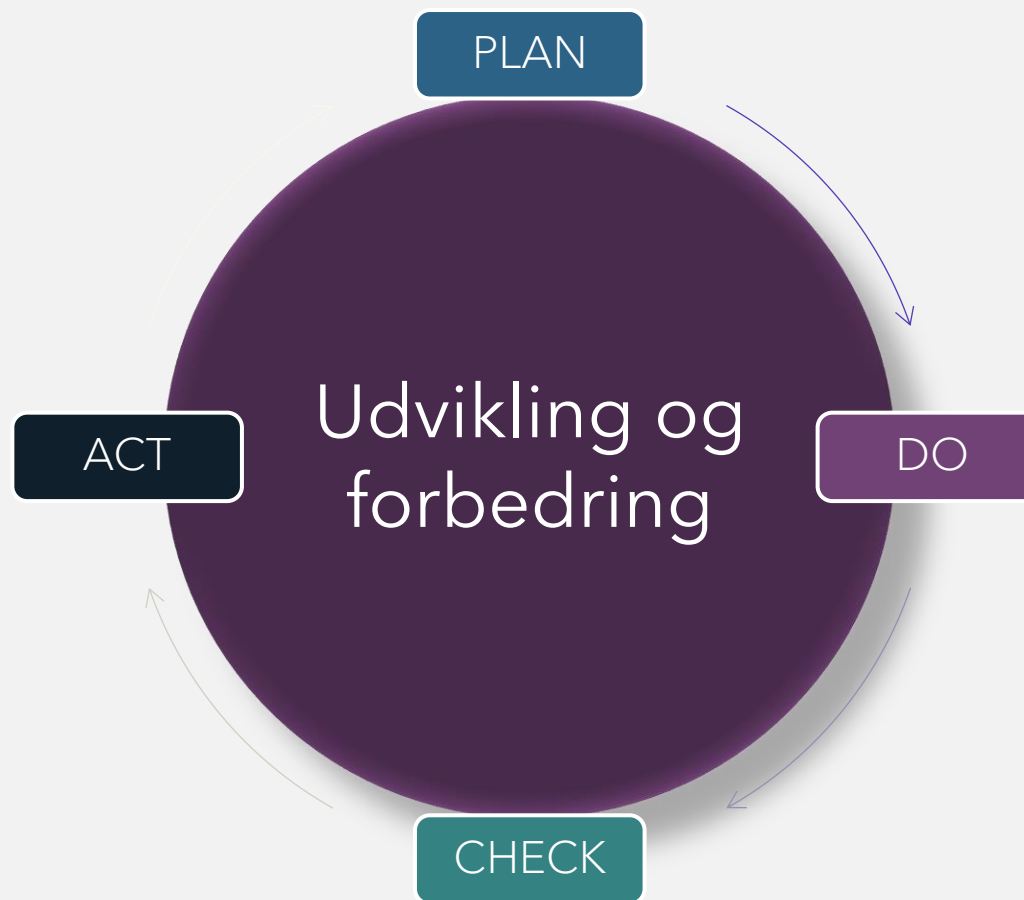
Interne audits

- Efterlevelsgrad og udbytte
- Forbedringspotentialer

Ledelsens evaluering

- Formulering af målsætninger for informationssikkerhed
- Resultater af overvågning og måling, interessent- og audit-input
- Resultater fra risikovurdering og -håndtering
- Muligheder for løbende forbedringer

10. Forbedring



Dokumentationskrav ISO/IEC 27001

Omfanget af ISMS - anvendelsesområde (4.3)

Informationssikkerhedspolitik (5.2)

Metode til vurdering af informationssikkerhedsrisici (6.1.2)

Processen for at håndtere informationssikkerhedsrisici og SOA dokument (6.1.3)

Målsætninger for informationssikkerhed (6.2)

Medarbejderkompetencer (7.2)

Driftsdokumentation for at processer er udført som planlagt (8.1)

Resultaterne af vurderingerne af informationssikkerhedsrisici (8.2)

Resultaterne af håndteringen af informationssikkerhedsrisici (8.3)

Bevis for at man overvåger og måler på sit ISMS (9.1)

Interne audits (9.2.2)

Ledelsens gennemgang/evaluering (9.3.3)

Afvielser og iværksætte handlinger og resultater af eventuelle korrigerende handlinger (10.2)

+ anden dokumentation, som organisationen har bestemt, er nødvendig for et effektivt ISMS

Anneks A

- Indeholder en tabel over foranstaltninger for informationssikkerhed
- Er afstemt med foranstaltningerne i ISO/IEC 27002

Foranstaltninger ISO/IEC 27001 og NIS2

Foranstaltninger fra artikel 21 og ISO 27001

- Foranstaltningerne fra artikel 21 kan genfindes i anneks A eller i kapitlerne i ISO 27001
- Et par eksempler er
 - Politikker for risikoanalyse og informationssikkerhed
 - Artikel 21, stk. 2, a: Politikker for risikoanalyse og informationssystemssikkerhed
 - ISO 27001: 5.2 Politik og 6.1 Handlinger til håndtering af risici og muligheder
 - ISO 27001 anneks A: 5.1 Politikker for informationssikkerhed
 - Cyberhygiejnepraksikker og cybersikkerhedsuddannelse
 - Artikel 21, stk. 2, g: Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse
 - ISO 27001 anneks A : 6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed
 - Kryptografi
 - Artikel 21, stk. 2, h: Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering
 - ISO 27001 anneks A : 8.24 Brug af kryptografi

Andre relevante standarder i NIS2 arbejdet

- ISO/IEC 27001: Krav til ledelsessystemer for informationssikkerhed
- ISO/IEC 27002: Foranstaltninger til informationssikkerhed
- ISO/IEC 27003: Vejledning til implementering af ledelsessystemer for informationssikkerhed
- ISO/IEC 27005: Vejledning i styring af informationssikkerhedsrisici
- ISO/IEC 27035: Styring af informationssikkerhedshændelser
- ISO/IEC 27036 Cybersikkerhed - Leverandørforhold
- ISO/IEC 22301: Business continuity management-systemer
- IEC 62443 serien: Industrial communication networks - Network and system security (OT/SCADA)

Tak for den her gang

Mette Krogh Sørensen

Tlf.: 2285 6224

Email: mks@ds.dk