

MODUL 3 AF 6

# **NIS-2 D-Mærket Standarder**

# Dagens program

- Velkomst og præsentationsrunde
- Hvad er NIS2?
- Sammenhæng mellem NIS2 og standarder
- Hvad er standarder?
- ISO/IEC 27001
- Foranstaltninger fra ISO/IEC 27001 og NIS2
- Opsamling og kilder til inspiration
- Tak for i dag

# 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 erfaring fra både det offentlige og det private

Har siddet med risikovurderinger, leverandørvurderinger, awarenessprogrammer og ledelsesrapportering



A vast desert landscape with rolling sand dunes under a hazy, purple-tinged sky. The dunes are smooth and undulating, creating a sense of depth and movement. The sky is a soft, hazy purple, suggesting a sunset or sunrise. The overall mood is serene and contemplative.

**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 modstandsdugtlighed
- 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

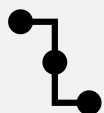
# Hvad er nyt?



Flere virksomheder og organisationer er omfattet



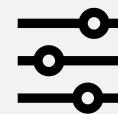
Flere sektorer kategoriseres som kritisk infrastruktur



Øget fokus på sikkerhed i forsyningskæder



Strengere tilsynsforanstaltninger



Flere sanktionsmuligheder



Underretningspligt på 24 timer



Større bøder



# Status på den danske lovgivningsproces

- Høringsfrist på det danske lovforslag den 22. august 2024
- Forventning: lovforslaget forventes at blive fremsat i februar 2025 og træde i kraft 1. juli 2025
- Bekendtgørelser for de enkelte sektorer



# 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

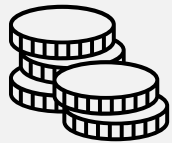


Forskning

NIS 2-loven gælder kun for mellemstore virksomheder, der lever op til en eller flere af følgende krav, og er en væsentlig eller vigtig enhed:



+50 medarbejdere i virksomheden



+75 mio. kr. i omsætning (+10 mio EUR)



+75 mio. kr. i formueopgørelse (+10 mio. EUR)



# **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 sikre 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



# Hændelseshåndtering

## 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.

# NIS2, artikel 34

## Generelle betingelser for pålæggelse af administrative bøder til væsentlige og vigtige enheder

4. Medlemsstaterne sikrer, at hvor væsentlige enheder overtræder artikel 21 eller 23, straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 10 000 000 EUR eller et maksimum på mindst 2 % af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter hvad der er højest.

5. Medlemsstaterne sikrer, at hvor vigtige enheder overtræder artikel 21 eller 23, straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 7 000 000 EUR eller et maksimum på mindst 1,4 % af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter hvad der er højest.



A vast, undulating landscape of white sand dunes under a clear blue sky. The dunes are smooth and flowing, creating a sense of movement and depth. The text "Hvad er standarder?" is overlaid in the center in a bold, black, sans-serif font.

**Hvad er standarder?**

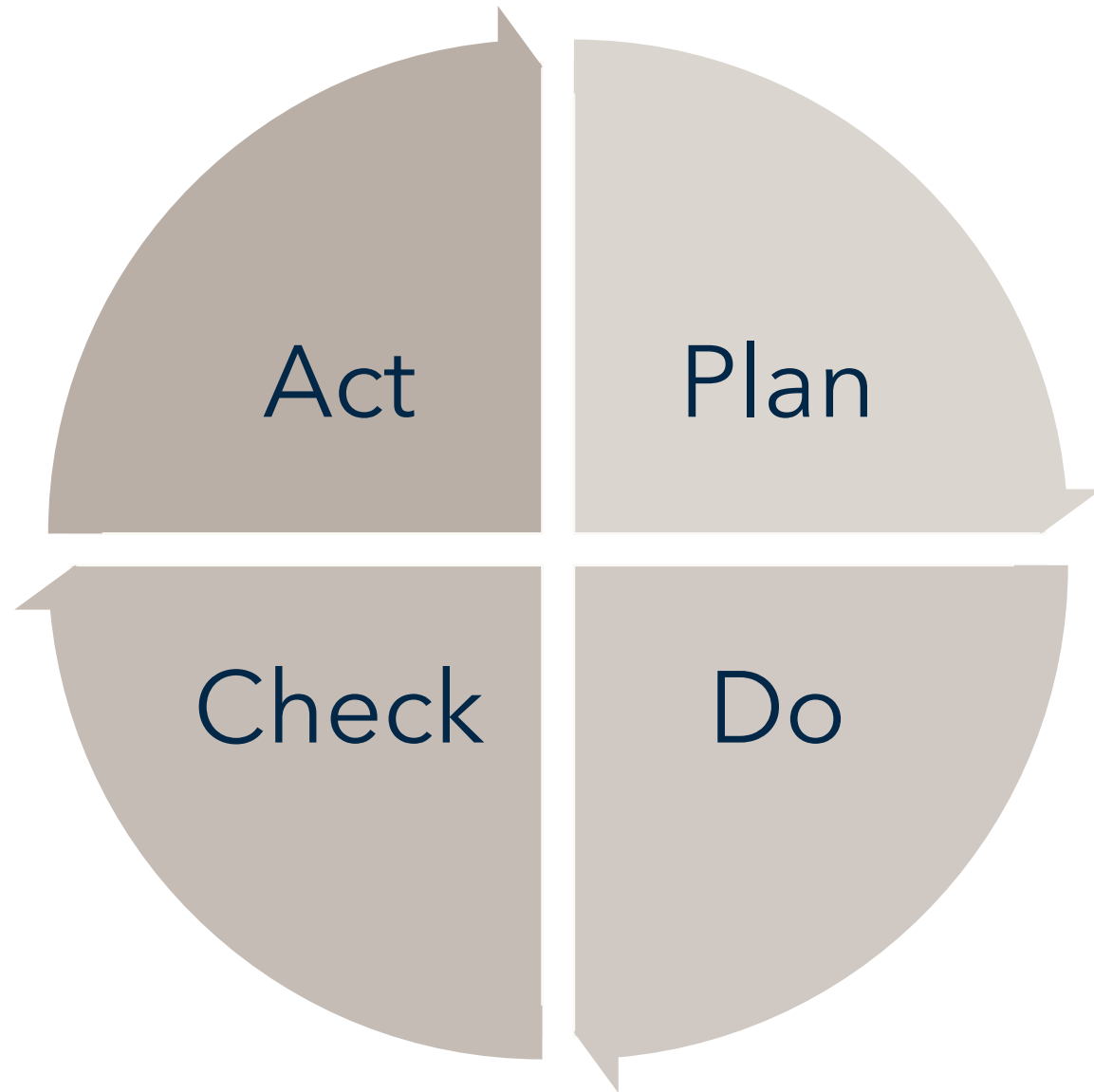


# Hvad er standarder? Og hvad er ISO?

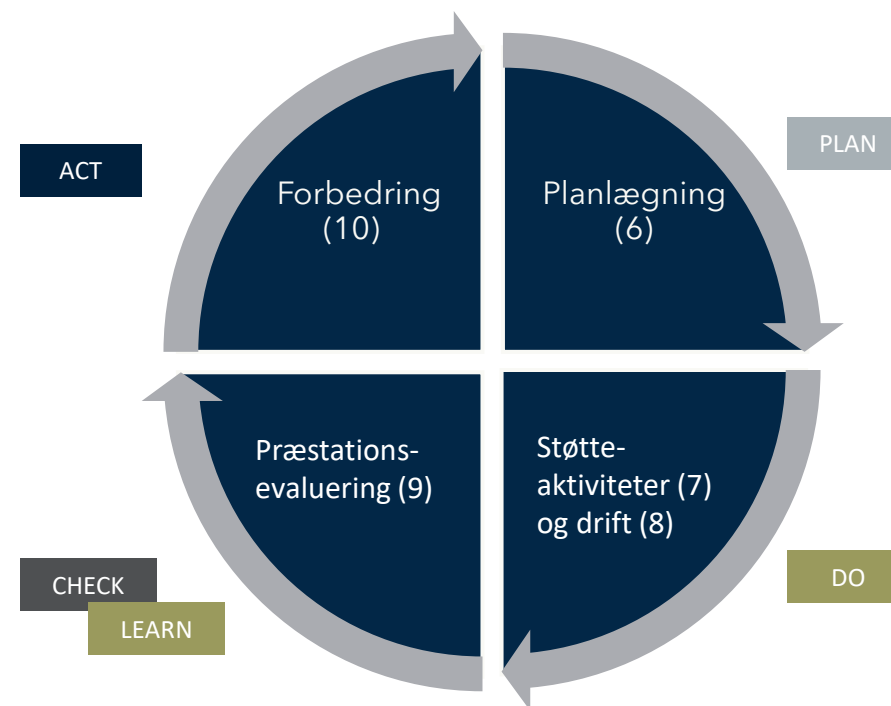
- En standard er et *"Dokument til fælles og gentagen anvendelse der angiver regler, vejledning eller karakteristiske træk ved aktiviteter eller ved resultaterne af disse. Dokumentet er fastlagt ved konsensus og vedtaget af et anerkendt organ. Hensigten er at opnå optimal orden i en given sammenhæng."*
- 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

# Ordvalg og bestemte formuleringer

- "i passende omfang"
  - "fastlægge"
  - "skal vedligeholde dokumenteret"
  - "sikre"
  - "skal overveje"
  - "passende dokumenteret information"
  - "bevare dokumenteret information som det er passende"
  - "dokumenteret information som organisationen finder nødvendigt"
- 
- "skal" = krav
  - "bør" = anbefaling
  - "kan" = tilladelse, mulighed eller evne

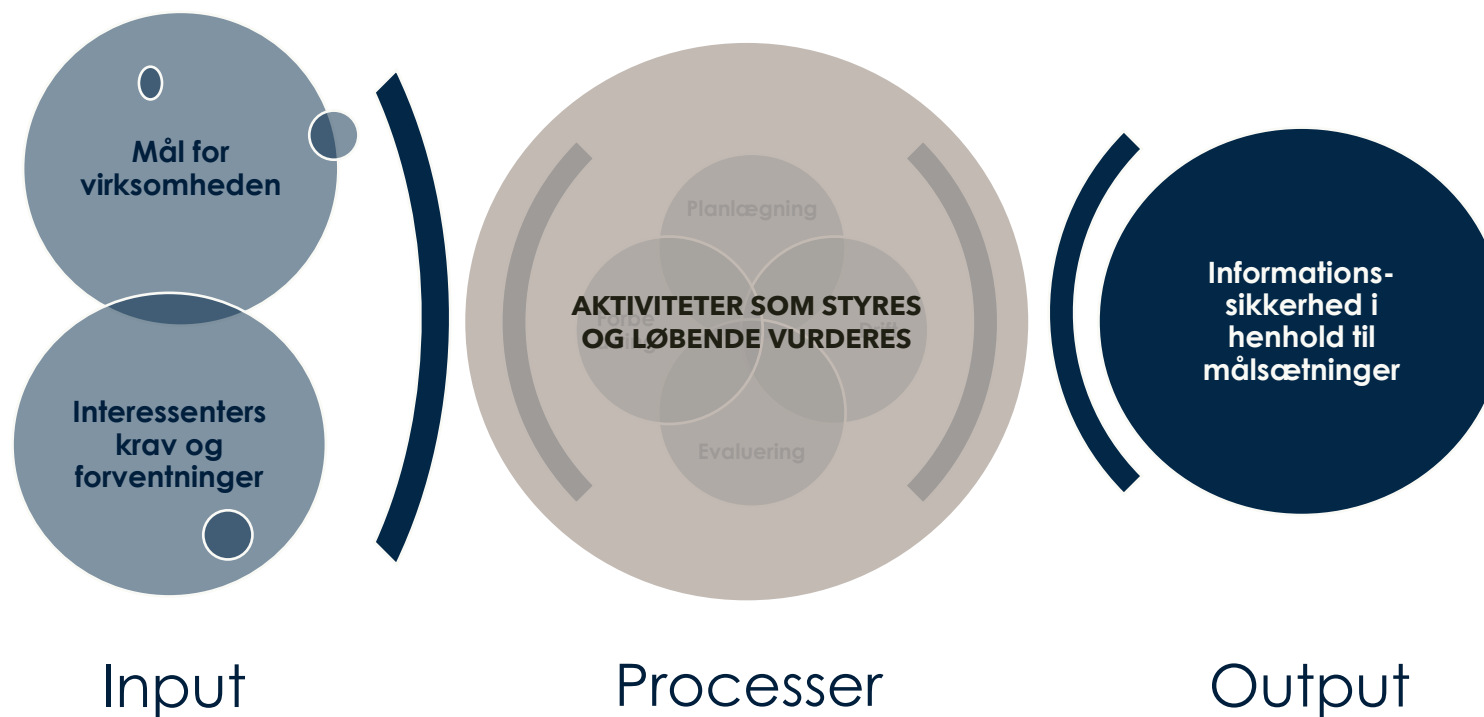


# PDCA i modsætning til brandslukning



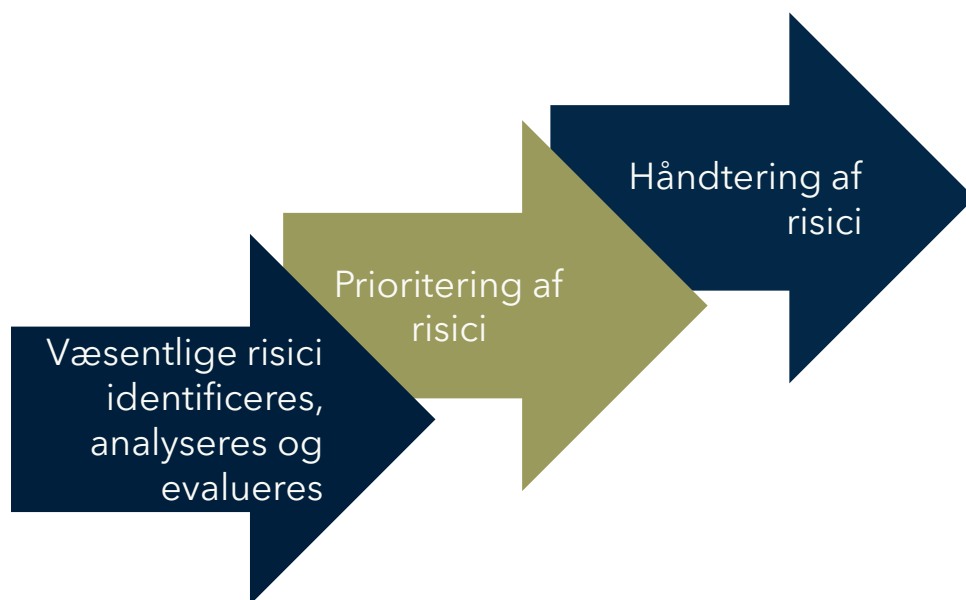


# Procestilgang



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


-

-

-







“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.”

ISO/IEC 27001:2023, 0.1

# Hvad er informationer?

Information er et **aktiv**, der ligesom andre vigtige aktiver i organisationen er af afgørende betydning for organisationens forretning og derfor skal beskyttes.

ISO/IEC 27000 4.2.2

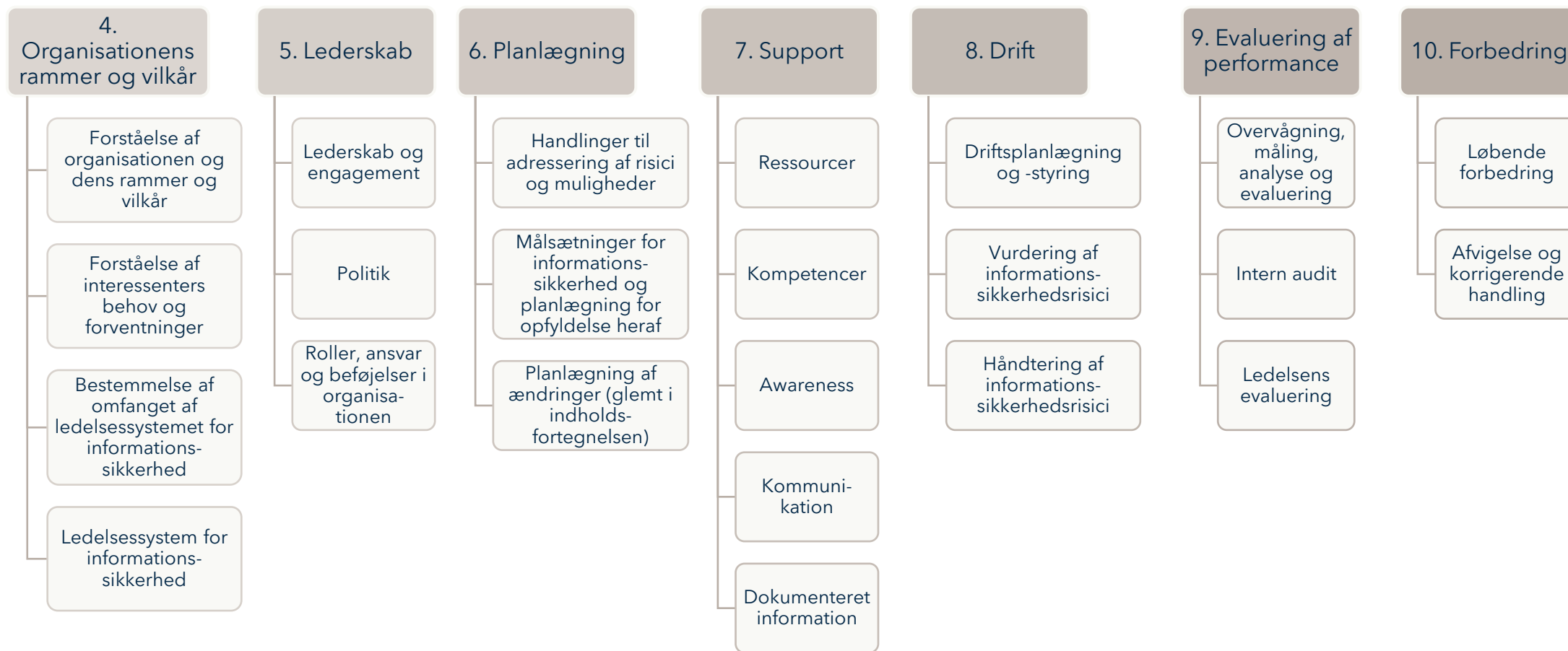




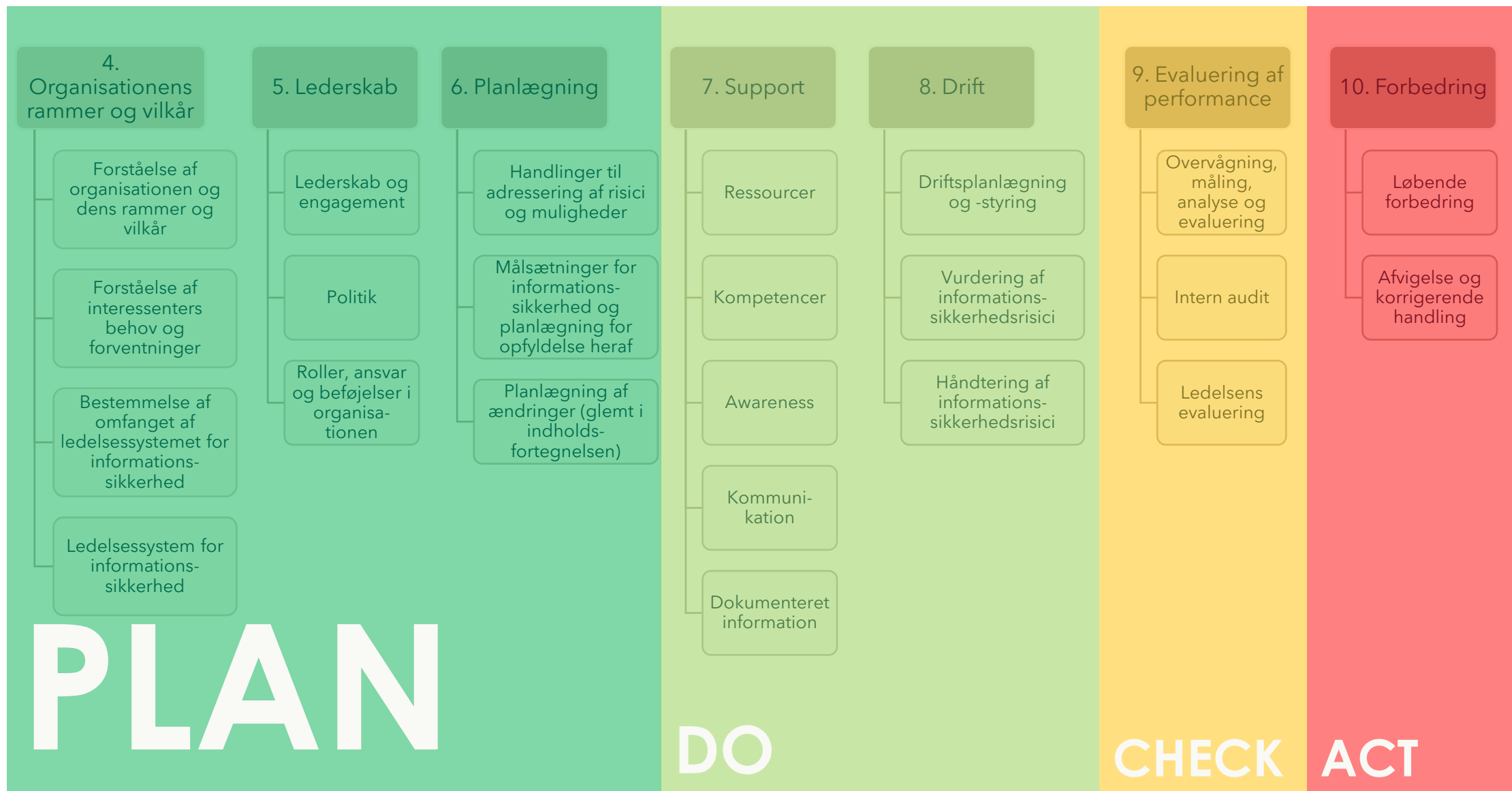
**FORTROLIGHED**

**INTEGRITET**

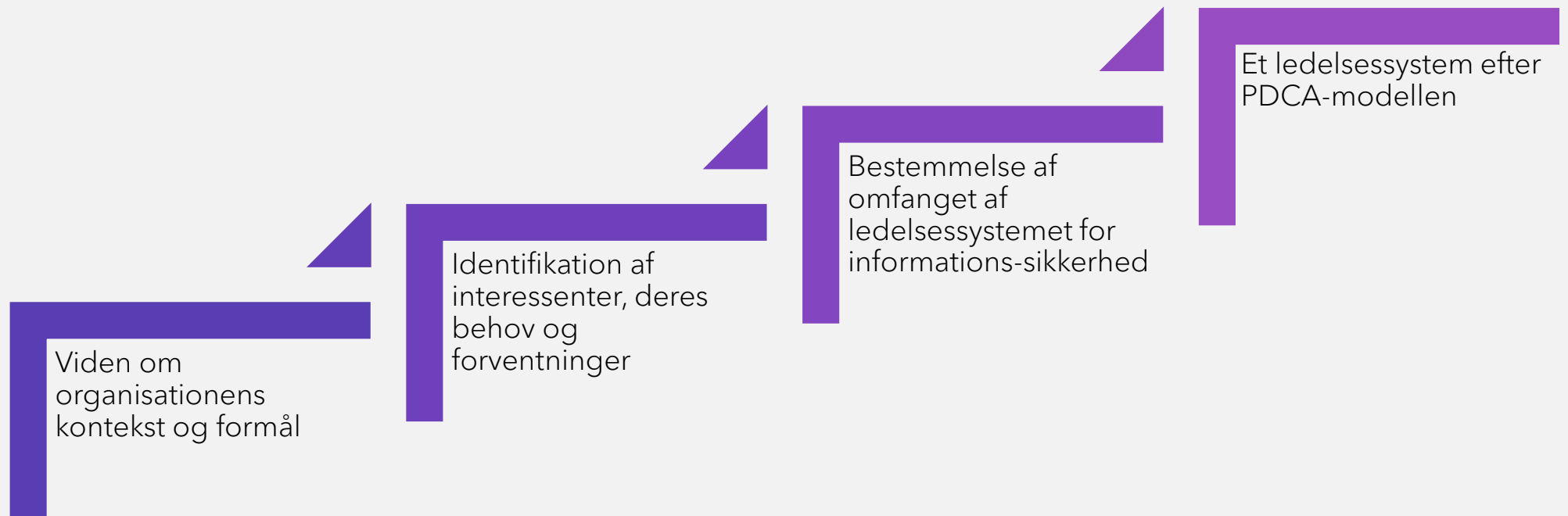
**TILGÆNGELIGHED**





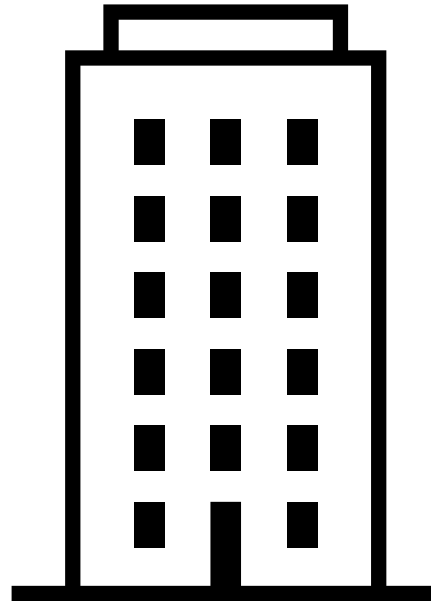


## 4. Organisationens rammer og vilkår



### **Eksterne forhold**

Lovgivning  
Aftaler  
Branchekrav  
Interessenter  
Kulturelle forhold  
Politiske forhold



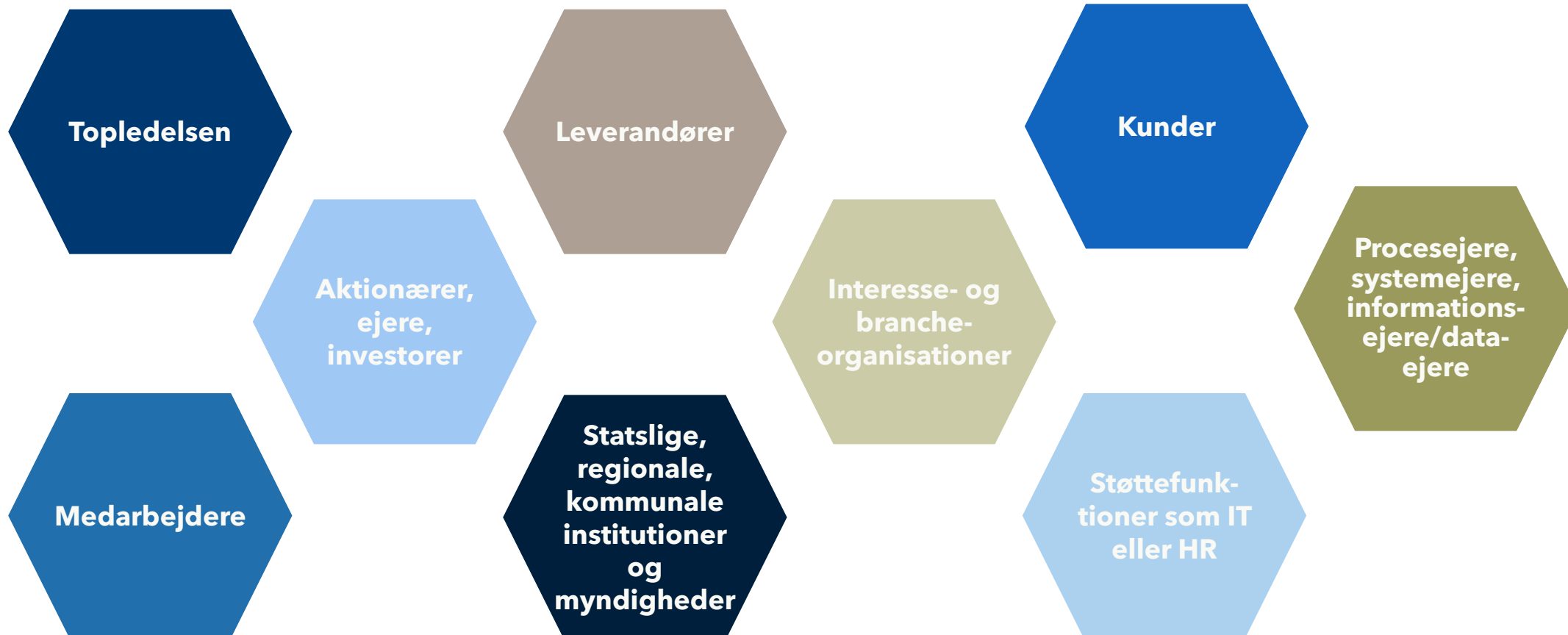
### **Eksterne forhold**

Samfundsmæssige forhold  
Konkurrenter  
Teknologiske forhold  
Miljømæssige forhold  
Konkurrencemæssige forhold

### **Interne forhold**

Organisationens kultur  
Politikker, målsætninger og strategi  
Struktur, roller og ansvarsfordeling  
Processer og procedurer  
Kapabiliteter  
Fysisk infrastruktur og miljø  
Resultater fra audit og risikovurderinger

# Interessenter





## 5. Lederskab

### Lederskab og engagement

- Kommunikation, ressourcetildeling og strategisk forankring

### Politik

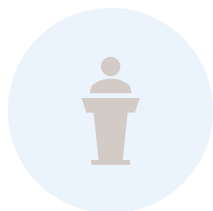
- Fastlæggelse af målsætninger og politikken for informationssikkerhed

### Roller, ansvar og beføjelser i organisationen

- Delegering og kommunikation

# Topledelsens ansvar

Topledelsen skal udvise lederskab og forpligtelse



**UDVISE LEDERSKAB**



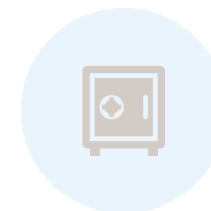
**FASTLÆGGE POLITIK  
OG MÅL**



**SIKRE INTEGRATION  
MED FORRETNINGS-  
PROCESSER**



**KOMMUNIKERE**



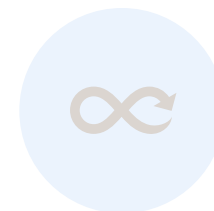
**SIKRE RESSOURCER**



**LEDE OG STØTTE  
MEDARBEJDERE OG  
LEDERE**



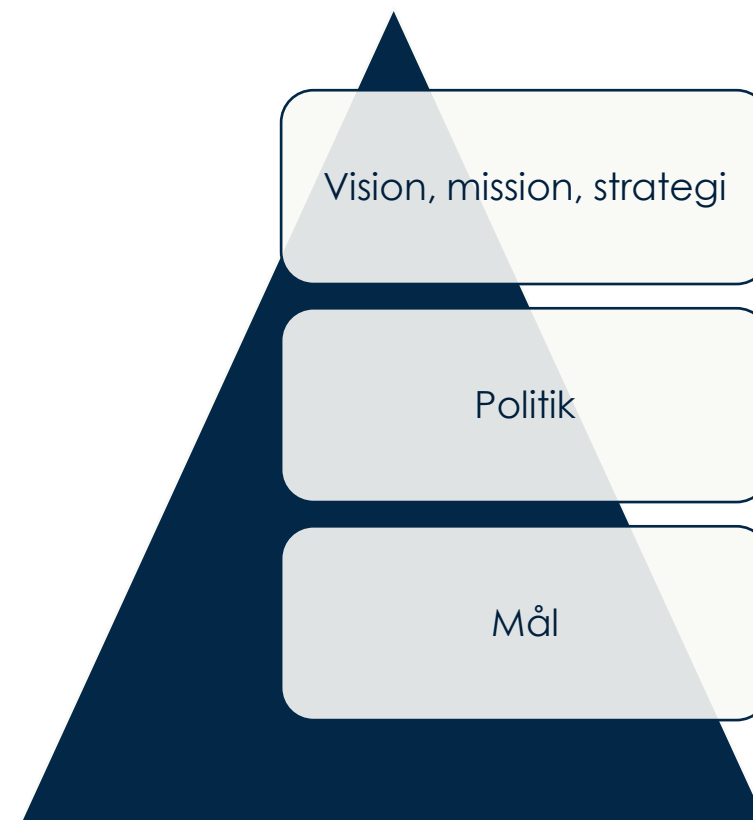
**SIKRE RESULTATER**



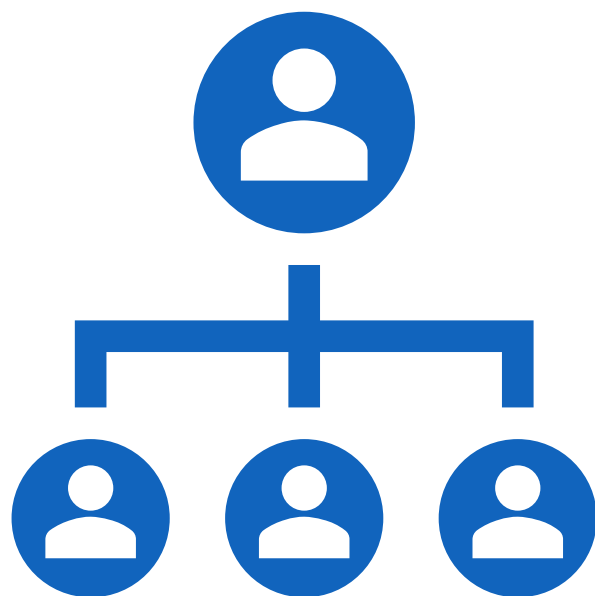
**FREMME LØBENDE  
FORBEDRING**

# Informationssikkerhedspolitik

- Skal være tilpasset til organisationens formål
- Skal indeholde målsætninger for arbejdet med informationssikkerhed eller opstille rammer til at fastlægge dem
- Skal indeholde en forpligtelse til at opfylde relevante krav
- Skal indeholde en forpligtelse til løbende forbedring
- Skal indeholde en forpligtelse til dokumenteret information
- Skal kommunikeres internt i organisationen
- Være tilgængelig for interessenter, hvor det giver mening



# Roller, ansvar og beføjelser

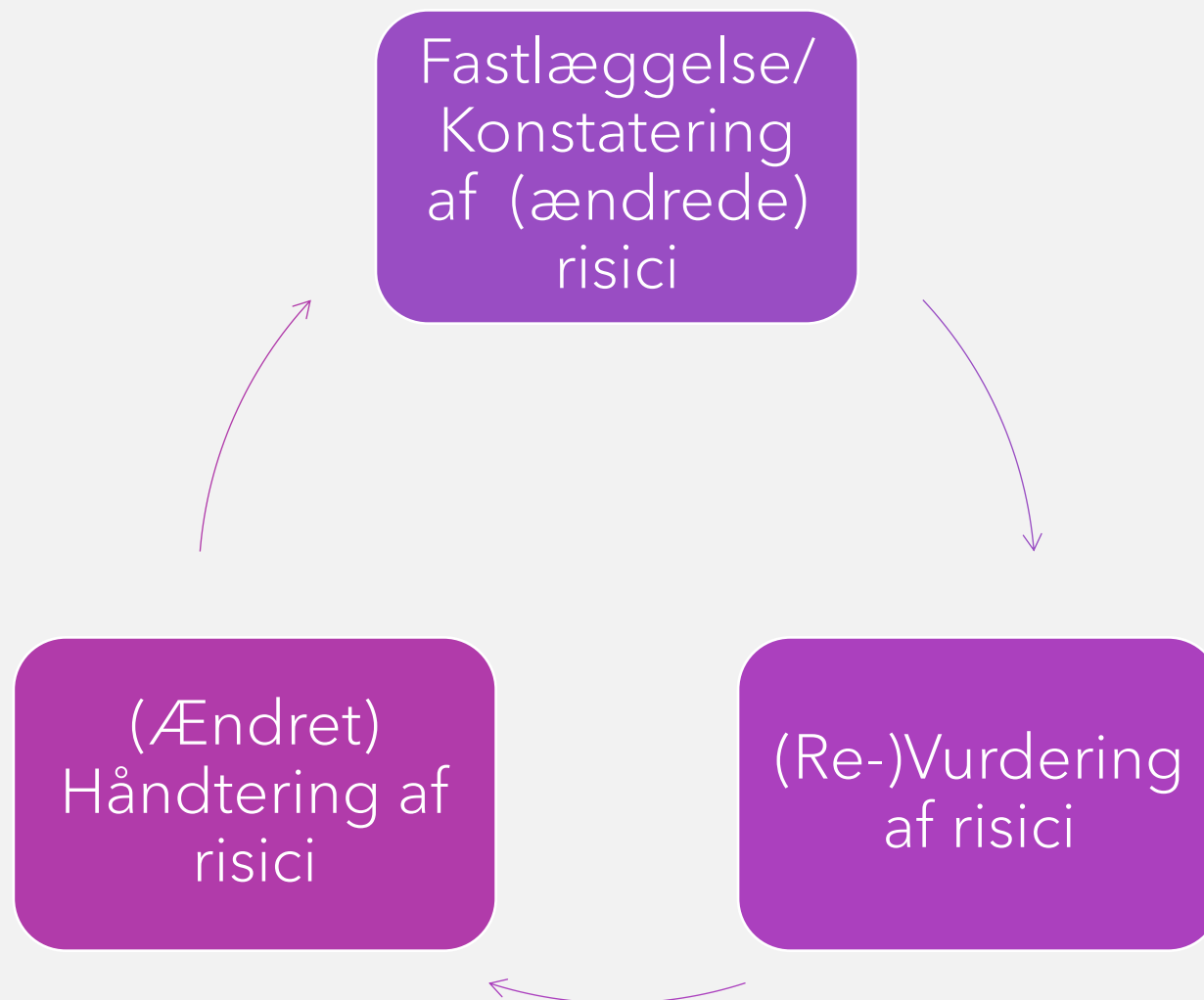


Topledelsen skal sikre, at ansvar og beføjelser er delegeret og kommunikeret i organisationen. Det gøres for at

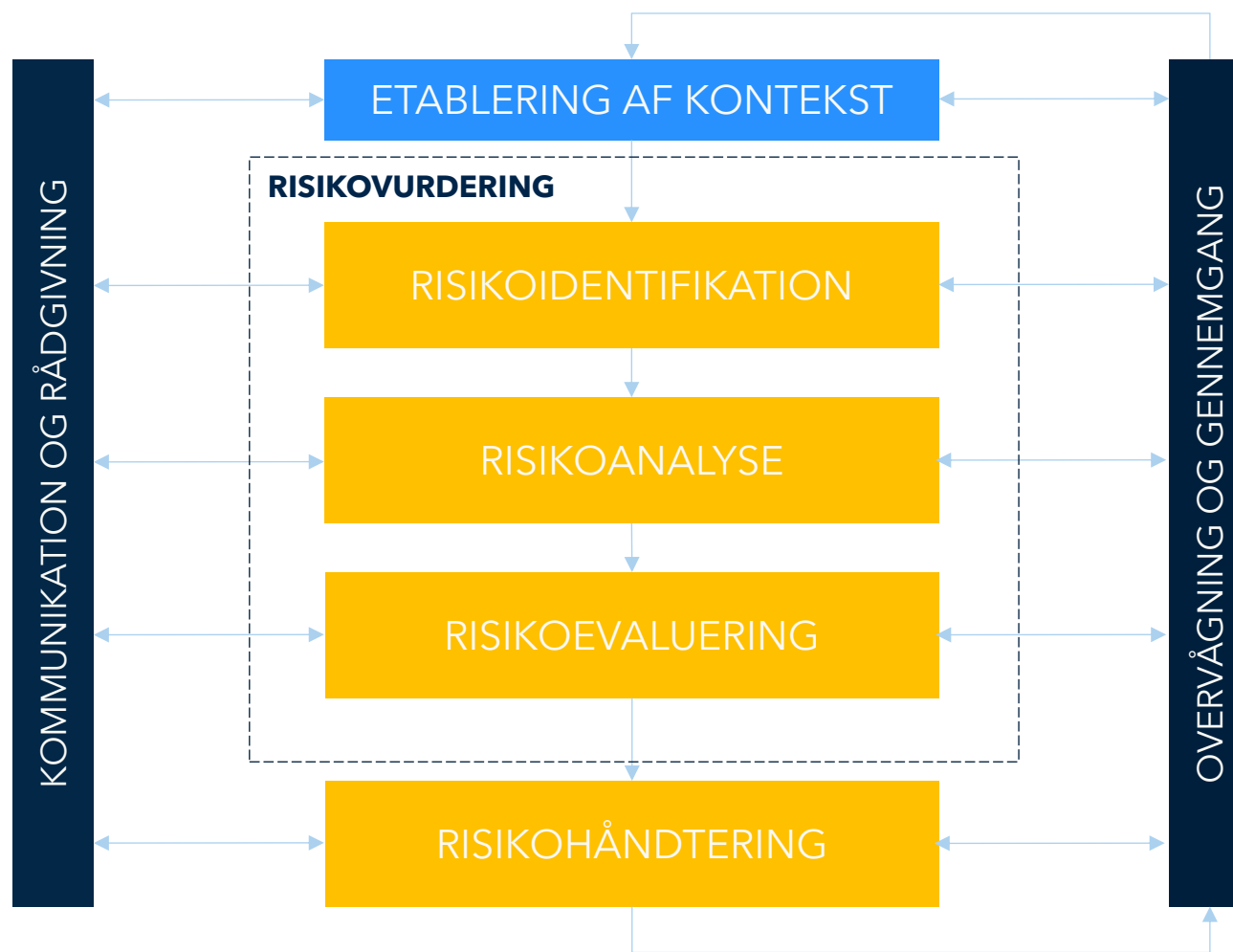
- Sikre at ISMS er i overensstemmelse med kravene i 27001
- Aflægge rapport til topledelsen om effekten af ISMSet

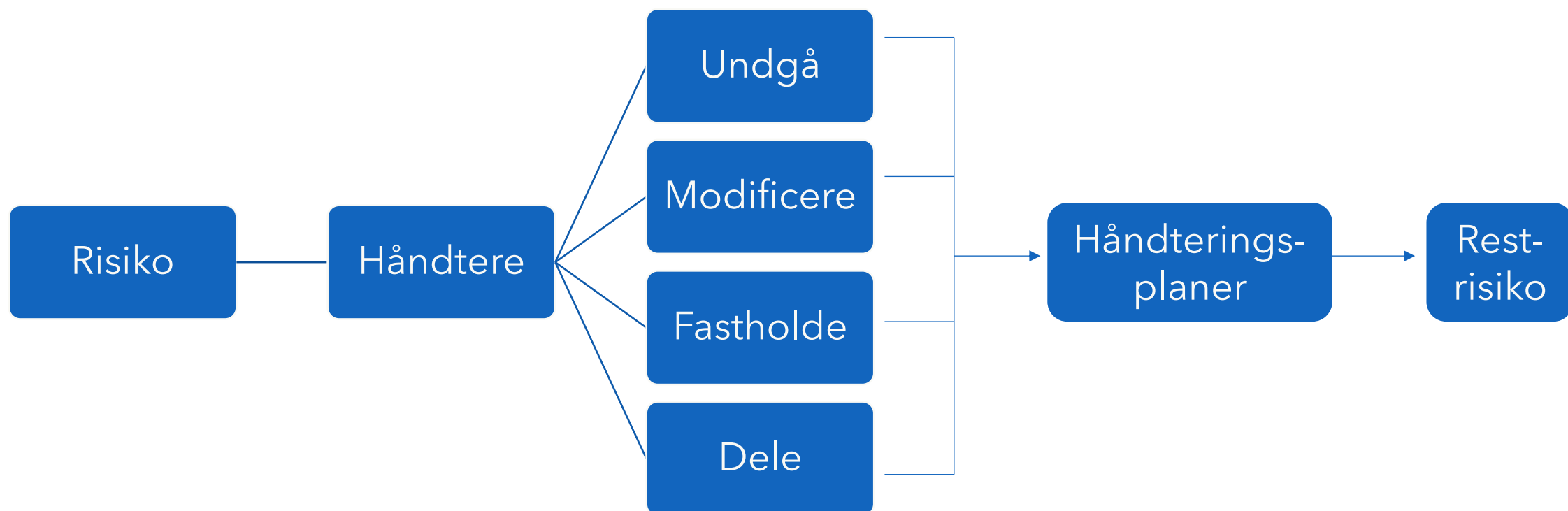


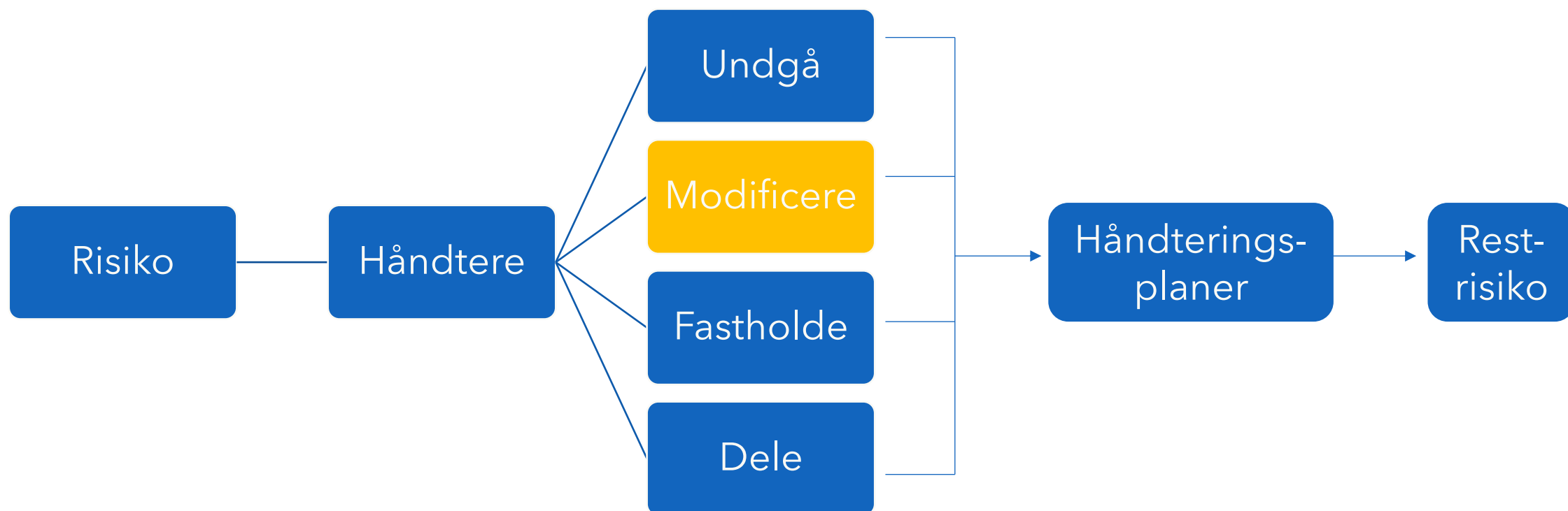
## 6. Planlægning



# Risikostyring, jf. ISO/IEC 27005









# FORANSTALTNING

tiltag, der bevarer og/eller ændrer risiko

ISO/IEC 27005 3.1.16



# Statement of Applicability (SoA)



Et statement of applicability (SoA) skal indeholde

- De nødvendige foranstaltninger (6.1.3 b og c)
- Begrundelse for valget af foranstaltningerne
- Om de er implementeret eller ej
- Begrundelse for hvorfor nogle af foranstaltningerne i Anneks A er fravalgt
- Risikostyring er hovedbegrundelse for til- og fravalg
- Tilføj foranstaltninger ved behov eksempelvis for at leve op til krav fra lovgivning, aftaler og/eller compliance

# 7. Support



Ressourcer



Kompetencer



Awareness

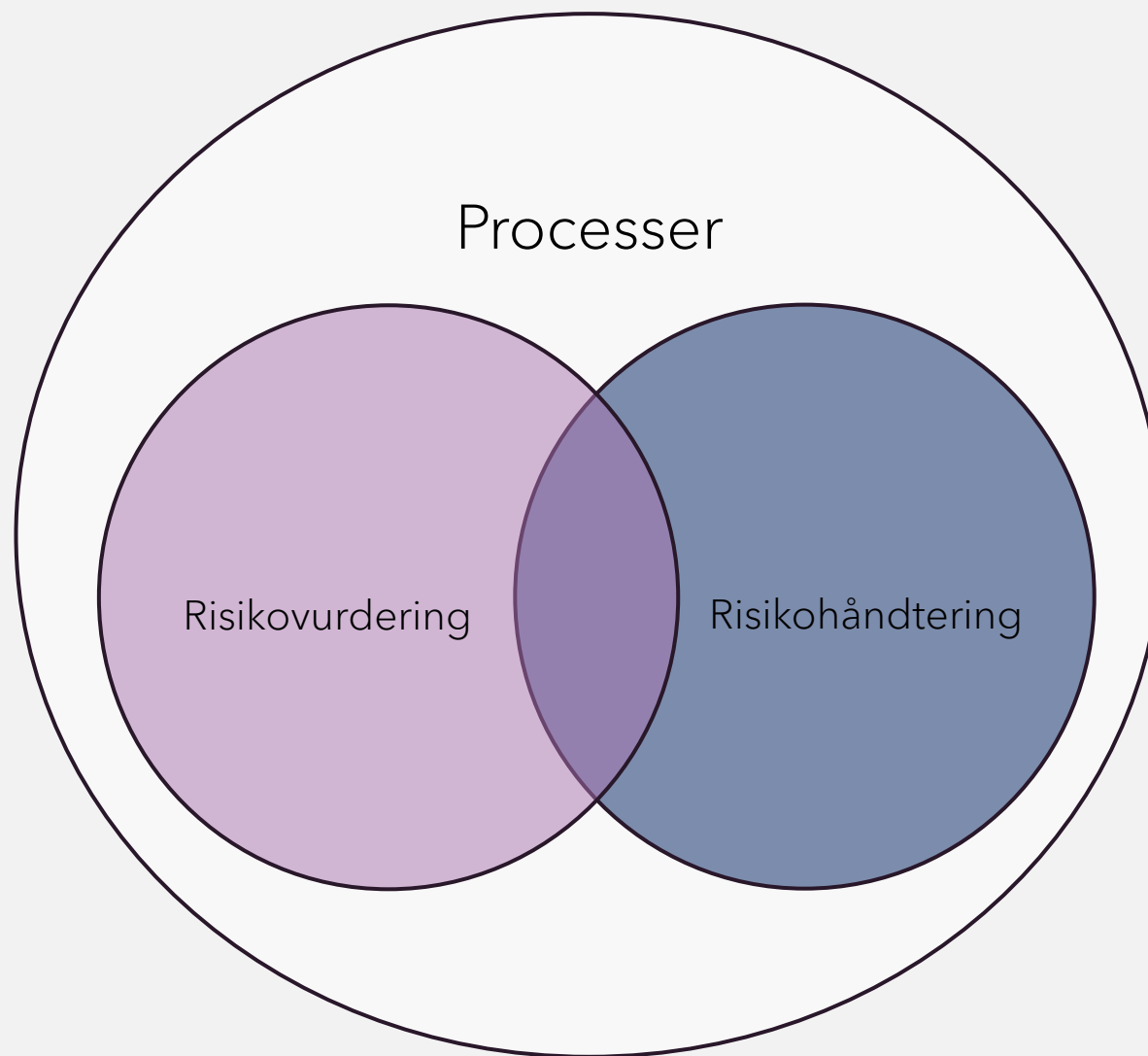


Kommunikation



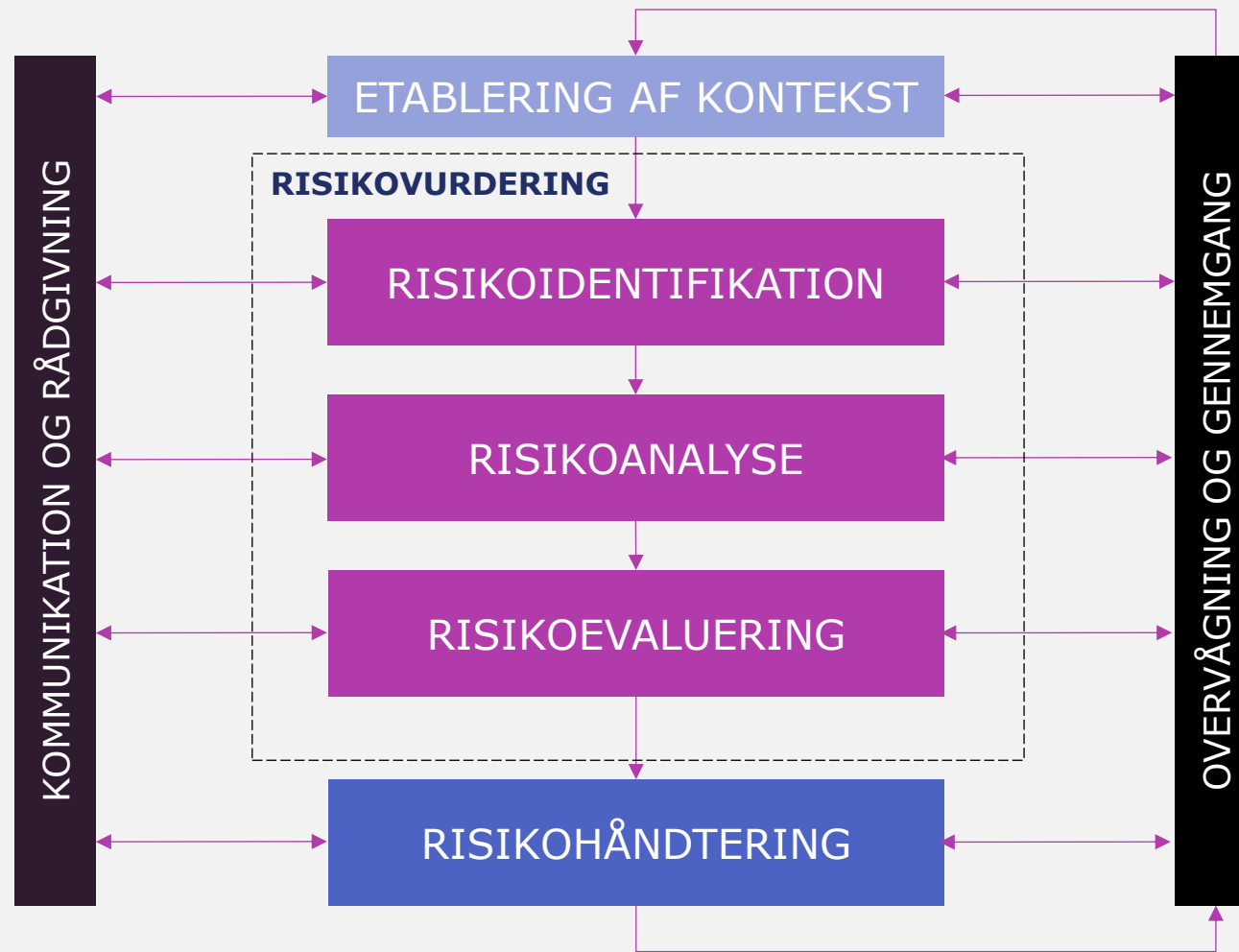
Dokumentation

## 8. Drift

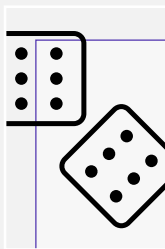




# Risikostyring, jf. ISO/IEC 27005



# Anneks A



Risikovurdering,  
muligheder for  
risikohåndtering og  
kriterier for risikoaccept.



Overholdelse af  
lovgivning, aftaler eller  
brancherelaterede krav.



Effekten af samspillet  
mellem forskellige  
foranstaltninger.

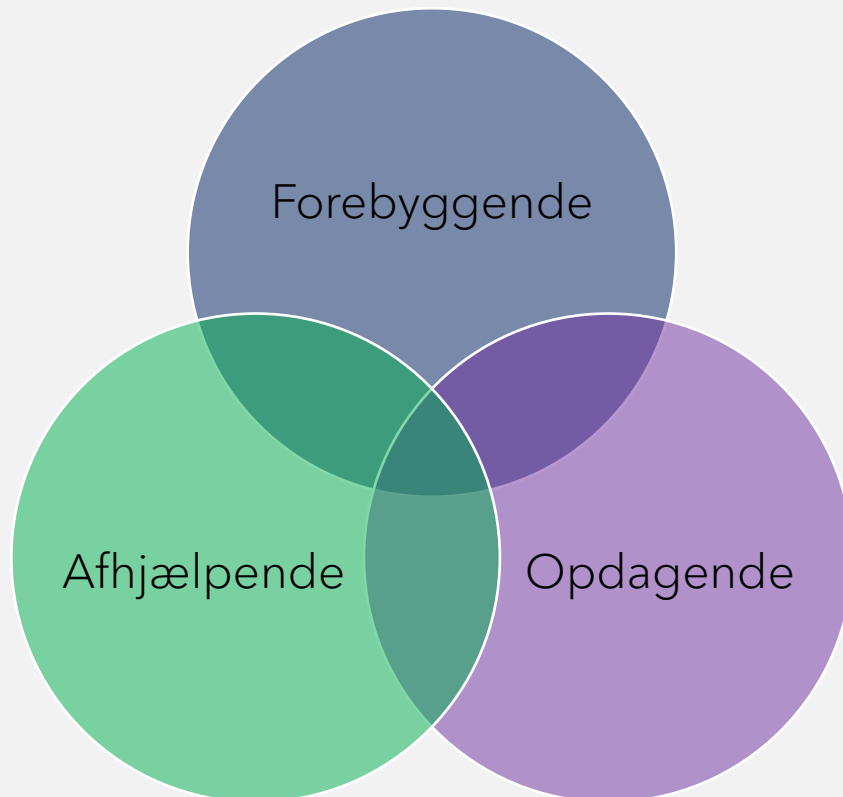
Organisatoriske

Personrelaterede

Fysiske

Teknologiske

# Typer af foranstaltninger



## Forebyggende foranstaltninger

- Foranstaltninger, der forhindrer at en informationssikkerhedshændelse sker

## Opdagende foranstaltninger

- Foranstaltninger, som opdager en informationssikkerhedshændelse

## Afhjælpende foranstaltninger

- Foranstaltninger, som begrænser konsekvenserne af en informationssikkerhedshændelse

## 9. Evaluering

### Overvågning, måling, analyse og evaluering

- Hændelser
- Processers effektivitet
- Risikovurderinger

### Interne audits

- Efterlevelsgrad og udbytte
- Forbedringspotentiale

### 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

## Intern audit ser på efterlevelse af egne og standardens krav

Effektivitet i  
implementering  
og anvendelse  
af systemet

Programmet for interne audits skal omfatte:

En PDCA-  
model

Auditkriterier  
og  
anvendelses-  
område

Roller til sikring  
af objektivitet  
og uafhængig-  
hed

Proces for  
rapportering til  
ledelsen

Dokumentation  
af program og  
resultater



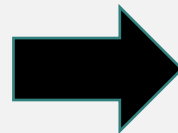
# Ledelsens evaluering

Topledelsen skal med planlagte intervaller evaluere organisationens ISMS for at sikre at det fortsat er egnet, tilstrækkeligt og effektivt

## Input

Skal indeholde informationer om:

- Status fra sidst
- Interne/ eksterne ændringer af relevans for ISMS
- Feedback fra interessenter, resultater og trends
- Internt audit-rapport
- Resultater fra risikovurdering og status på risikohåndteringsplan
- Muligheder for løbende forbedringer



## Output

Beslutninger vedrørende:

- Forbedring af ISMS effektivitet
- Opdatering af risikovurdering og -håndtering
- Ændring af behov for foranstaltninger og procedurer
- Justering af ressourcebehov
- Forslag til forbedringer
- Ændringer af kriterierne til vurderinger af risici eller for accept

# 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
- Foranstaltningerne skal bruges sammen med afsnit 6.1.3 Håndtering af informationssikkerhedsrisici fra ISO/IEC 27001

Tabel A.1 — Foranstaltninger til informationssikkerhed

5	Organisatoriske foranstaltninger	
5.1	Politikker for informationssikkerhed	<b>Foranstaltning</b> Informationssikkerhedspolitik og emnespecifikke politikker skal defineres, godkendes af ledelsen, offentliggøres, kommunikeres til og anerkendes af relevante medarbejdere og relevante interessenter og vurderes med planlagte mellemrum samt hvis der sker væsentlige ændringer.
5.2	Roller og ansvar for informationssikkerhed	<b>Foranstaltning</b> Roller og ansvar for informationssikkerhed skal defineres og allokere i overensstemmelse med organisationens behov.
5.3	Funktionsadskillelse	<b>Foranstaltning</b> Konfliktende opgaver og konfliktende ansvarsområder skal adskilles.
5.4	Ledelsens ansvar	<b>Foranstaltning</b> Ledelsen skal kræve, at alle medarbejdere efterlever informationssikkerhed i overensstemmelse med organisationens fastlagte informationssikkerhedspolitik, emnespecifikke politikker og procedurer.
5.5	Kontakt med myndigheder	<b>Foranstaltning</b> Organisationen skal etablere og vedligeholde kontakt med relevante myndigheder.
5.6	Kontakt med særlige interessegrupper	<b>Foranstaltning</b> Organisationen skal etablere og vedligeholde passende kontakt med særlige interessegrupper eller andre specialistfora omkring sikkerhed og faglige organisationer.
5.7	Underretning om trusler	<b>Foranstaltning</b> Information om informationssikkerhedstrusler skal indsamles og analyseres med henblik på at frembringe underretning om trusler.
5.8	Informationssikkerhed i projekter	<b>Foranstaltning</b> Informationssikkerhed skal integreres i projektstyringen.
5.9	Fortegnelse over information og understøttende aktiver	<b>Foranstaltning</b> Der skal udarbejdes og vedligeholdes en fortegnelse over information og understøttende aktiver, herunder ejere.

# Organisatoriske foranstaltninger

- 5.1 Politikker for informationssikkerhed
- 5.2 Roller og ansvar for informationssikkerhed
- 5.3 Funktionsadskillelse
- 5.4 Ledelsens ansvar
- 5.5 Kontakt med myndigheder
- 5.6 Kontakt med særlige interessegrupper
- 5.7 Underretning om trusler
- 5.8 Informationssikkerhed i projekter
- 5.9 Fortegnelse over information og understøttende aktiver
- 5.10 Acceptabel brug af information og understøttende aktiver
- 5.11 Returnering af aktiver
- 5.12 Klassifikation af information
- 5.13 Mærkning af information
- 5.14 Overførsel af information
- 5.15 Administration af adgang
- 5.16 Styring af identifikation
- 5.17 Autentifikationsoplysninger
- 5.18 Adgangsrettigheder
- 5.19 Informationssikkerhed i leverandørforhold
- 5.20 Håndtering af informationssikkerhed i leverandøraftaler
- 5.21 Styring af informationssikkerhed i IKT-forsyningskæden
- 5.22 Overvågning, vurdering og ændringsstyring af leverandørydelser
- 5.23 Informationssikkerhed ved brug af cloudtjenester
- 5.24 Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents
- 5.25 Vurdering af og beslutning om informationssikkerhedshændelser
- 5.26 Håndtering af informationssikkerhedsincidents
- 5.27 Læring fra informationssikkerhedsincidents
- 5.28 Indsamling af bevismateriale
- 5.29 Informationssikkerhed under driftsforstyrrelse
- 5.30 IKT-parathed til understøttelse af business continuity
- 5.31 Juridiske, lovmæssige, regulatoriske og kontraktlige krav
- 5.32 Intellektuelle ejendomsrettigheder
- 5.33 Beskyttelse af optegnelser
- 5.34 Privatlivsbeskyttelse og beskyttelse af personoplysninger
- 5.35 Uafhængig vurdering af informationssikkerhed
- 5.36 Overensstemmelse med politikker, regler og standarder for informationssikkerhed
- 5.37 Dokumenterede driftsprocedurer



# Personrelaterede og fysiske foranstaltninger

- 6.1 Screening
- 6.2 Ansættelsesvilkår og -betingelser
- 6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed
- 6.4 Sanktioner
- 6.5 Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold
- 6.6 Hemmeligholdelses- og fortrolighedsaftaler
- 6.7 Distancearbejde
- 6.8 Indrapportering af informationssikkerhedshændelser

- 7.1 Fysisk områdesikring
- 7.2 Fysisk adgangskontrol
- 7.3 Sikring af kontorer, lokaler og faciliteter
- 7.4 Fysisk sikkerhedsovervågning
- 7.5 Beskyttelse mod fysiske og miljømæssige trusler
- 7.6 Arbejde i sikrede områder
- 7.7 Ryddeligt skrivebord og låst skærm
- 7.8 Placering og beskyttelse af udstyr
- 7.9 Sikring af aktiver uden for organisationens områder
- 7.10 Lagringsmedier
- 7.11 Forsyningssikkerhed
- 7.12 Sikring af kabler
- 7.13 Vedligeholdelse af udstyr
- 7.14 Sikker bortskaffelse eller genbrug af udstyr

# Teknologiske foranstaltninger

- 8.1 Brugerenheder
- 8.2 Privilegerede adgangsrettigheder
- 8.3 Begrænset adgang til information
- 8.4 Adgang til kildekode
- 8.5 Sikker autentifikation
- 8.6 Kapacitetsstyring
- 8.7 Beskyttelse mod malware
- 8.8 Styring af tekniske sårbarheder
- 8.9 Konfigurationsstyring
- 8.10 Sletning af information
- 8.11 Datamaskering
- 8.12 Forebyggelse af datalækage
- 8.13 Backup af information
- 8.14 Redundans i faciliteter til informationsbehandling
- 8.15 Logning
- 8.16 Overvågning af aktiviteter
- 8.17 Synkronisering af ure
- 8.18 Brug af privilegerede understøttende programmer
- 8.19 Softwareinstallation i test- og produktionssystemer
- 8.20 Netværkssikkerhed
- 8.21 Sikring af netværkstjenester
- 8.22 Segmentering af netværk
- 8.23 Webfiltrering
- 8.24 Brug af kryptografi
- 8.25 Sikker udviklingslivscyklus
- 8.26 Krav til applikationssikkerhed
- 8.27 Sikker systemarkitektur og udviklingsprincipper
- 8.28 Sikker programmering
- 8.29 Sikkerhedstest under udvikling og godkendelse
- 8.30 Outsourcet udvikling
- 8.31 Adskillelse af udviklings-, test- og produktionsmiljøer
- 8.32 Ændringsstyring
- 8.33 Information til brug for test
- 8.34 Beskyttelse af informationssystemer under audit

# Foranstaltninger ISO/IEC 27001 og NIS2



# Foranstaltninger fra artikel 21

Foranstaltningerne skal som minimum omfatte eller tage højde for:

- a) Politikker for risikoanalyse og informationssystemsikkerhed.
- b) Håndtering af hændelser.
- c) Driftskontinuitet, eksempelvis 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 hos enheden, hvor det er relevant.

# Politikker for risikoanalyse og informationssystemssikkerhed

Artikel 21, stk. 2, a: Politikker for risikoanalyse og informationssystemssikkerhed.

ISO/IEC 27001 krav

ISO/IEC 27001 5.2 Politik

ISO/IEC 27001 6.1 Handlinger til håndtering af risici og muligheder

Foranstaltninger fra ISO/IEC 27001 Anneks A

- 5.1 Politikker for informationssystemssikkerhed



# Håndtering af hændelser

Artikel 21, stk. 2, b: Håndtering af hændelser.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- 5.5 Kontakt med myndigheder
- 5.6 Kontakt med særlige interessegrupper
- 5.24 Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents
- 5.25 Vurdering af og beslutning om informationssikkerhedshændelser
- 5.26 Håndtering af informationssikkerhedsincidents
- 5.27 Læring fra informationssikkerhedsincidents
- 5.28 Indsamling af bevismateriale
- 6.8 Indrapportering af informationssikkerhedshændelser



# Driftskontinuitet

Artikel 21, stk. 2, c: Driftskontinuitet, eksempelvis backup-styring og reetablering efter en katastrofe, og krisestyring.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- 5.29 Informationssikkerhed under driftsforstyrrelse
- 5.30 IKT-Parathed til understøttelse af business continuity
- 8.13 Backup af information

# Forsyningskædesikkerhed

Artikel 21, stk. 2, d: Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- 5.7 Underretning om trusler
- 5.19 Informationssikkerhed i leverandørforhold
- 5.20 Håndtering af informationssikkerhed i leverandøraftaler
- 5.21 Styring af informationssikkerhed i IKT-forsyningskæden
- 5.22 Overvågning, vurdering og ændringsstyring af leverandørydelser
- 5.23 Informationssikkerhed ved brug af cloudtjenester

# Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse

Artikel 21, stk. 2, e: Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- 5.7 Underretning om trusler
- 8.20 Netværkssikkerhed
- 8.21 Sikring af netværkstjenester
- 8.25 Sikker udviklingslivscyklus
- 8.26 Krav til applikationssikkerhed
- 8.27 Sikker systemarkitektur og udviklingsprincipper
- 8.28 Sikker programmering
- 8.29 Sikkerhedstest under udvikling og godkendelse



# Effektivitet af foranstaltninger

Artikel 21, stk. 2, f : Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.

ISO/IEC 27001:

- 9.1 Overvågning, måling, analyse og evaluering



# Cyberhygiejnepraksisser og uddannelse

Artikel 21, stk. 2, g: Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- 6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed



# Politikker og procedurer vedrørende brug af kryptografi

Artikel 21, stk. 2, h: Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- 8.24 Brug af kryptografi

# Personalesikkerhed, adgangskontrol og forvaltning af aktiver

Artikel 21, stk. 2, i: Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- Personalesikkerhed
  - 6.1 Screening
  - 6.2 Ansættelsesvilkår og -betingelser
  - 6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed
  - 6.4 Sanktioner
  - 6.5 Ansvar i forbindelse med ophør eller ændring i ansættelsesforhold
  - 6.6 Hemmeligholdelses- og fortrolighedsaftaler
  - 6.7 Distancearbejde
  - 6.8 Indrapportering af informationssikkerhedshændelser

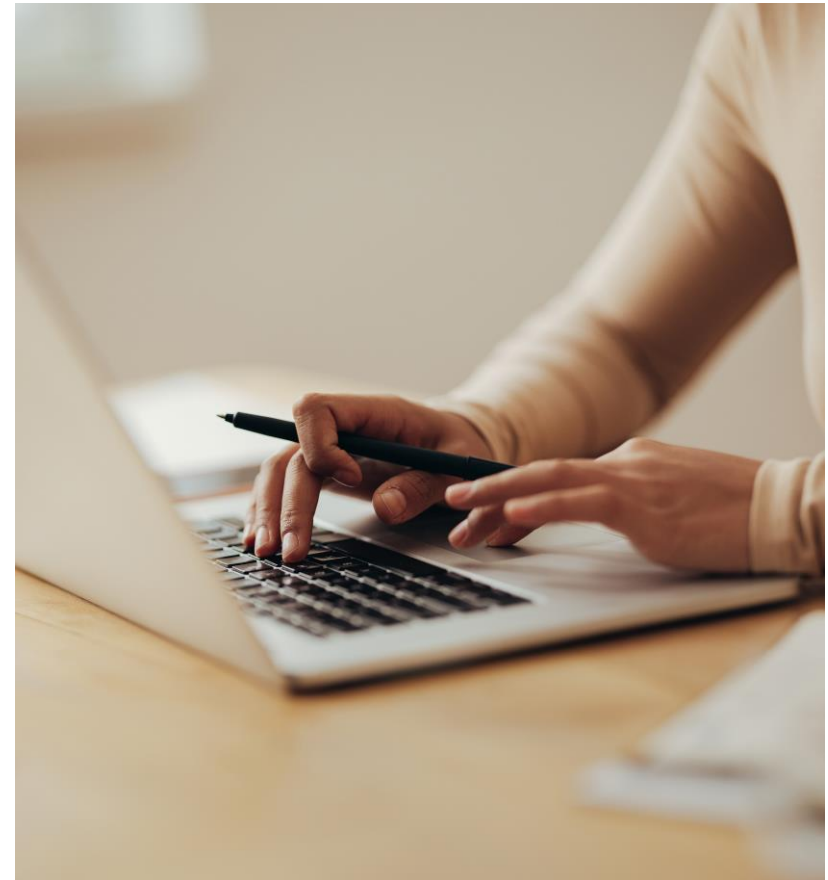


# Personalesikkerhed, adgangskontrol og forvaltning af aktiver

Artikel 21, stk. 2, i: Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- Adgangskontrolpolitikker
  - 5.1 Politikker for informationssikkerhed
  - 5.15 Administration af adgang
  - 5.18 Adgangsrettigheder



# Personalesikkerhed, adgangskontrol og forvaltning af aktiver

Artikel 21, stk. 2, i: Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- Forvaltning af aktiver
  - 5.9 Fortegnelse over information og understøttende aktiver.
  - 5.10 Acceptabel brug af information og understøttende aktiver.
  - 5.11 Returnering af aktiver
  - 8.15 Logning

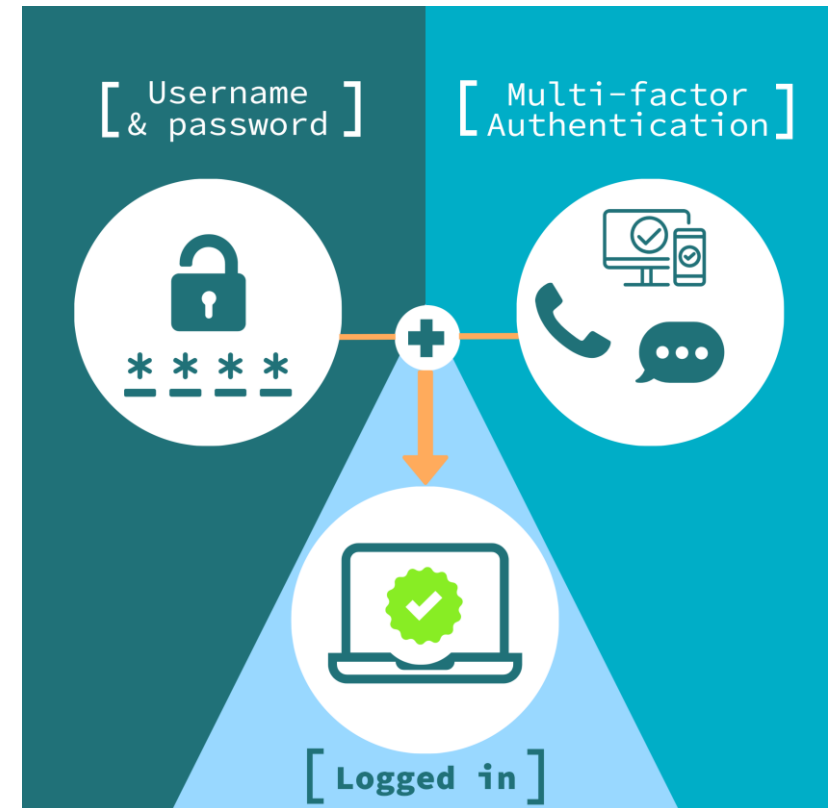


# Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering

Artikel 21, stk. 2, j: Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.

Foranstaltninger fra ISO/IEC 27001 Anneks A

- 5.15 Administration af adgang
- 5.30 IKT parathed til understøttelse af business continuity



Kilde University of Bath

# 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)

## Læs mere

- NIS2 direktivet <https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32022L2555>
- Sikker Digital <https://www.sikkerdigital.dk>
- Center for cybersikkerhed <https://www.cfcs.dk/>
- Dansk Standard om NIS2 <https://www.ds.dk/da/i-fokus/lovgivning/lovgivning-paa-det-digitale-omraade-og-standarder/nis2-direktivet-net-og-informationssikkerhedsdirektivet>

# Tak for den her gang

Mette Krogh Sørensen

Tlf.: 2285 6224

Email: [mks@ds.dk](mailto:mks@ds.dk)