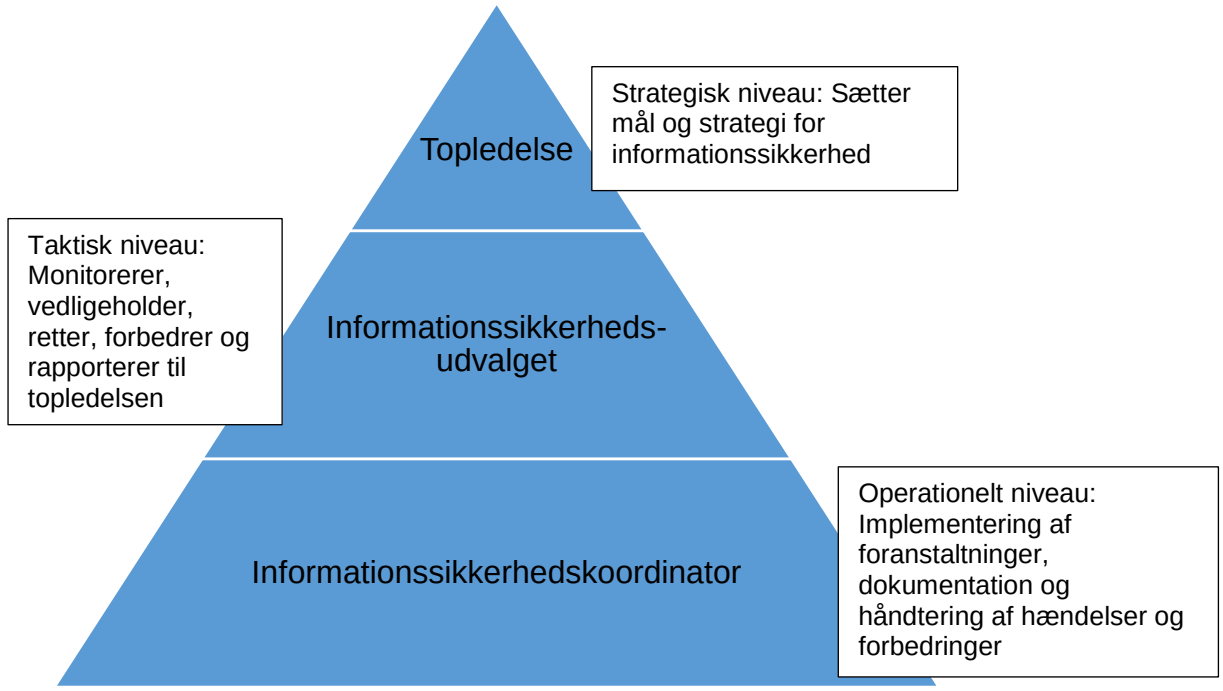
# Informationssikkerhedsudvalget

Det overordnede ansvar for informationssikkerheden ligger hos topledelsen, men det er Informationssikkerhedsudvalget, der konkret arbejder med informationssikkerheden og sørger for, at den realiseres og efterleves i organisationen.
Informationssikkerhedsudvalget udmønter og igangsætter tiltag, indsatser og forbedringer, som tilgodeser sikkerhedsstrategien og gennemfører de mål, som topledelsen har fastlagt.

Informationssikkerhedsudvalget bør arbejde ud fra et godkendt kommissorium. Afholdelsen af møder kan dog eventuelt falde ind i en eksisterende møderække, hvor deltagerne i informationssikkerhedsudvalget mødes i anden sammenhæng.




**Organisering**

Organisationen bør overveje informationssikkerhedsudvalgets sammensætning nøje, således at organisationen er bedst muligt repræsenteret, samtidig med, at de nødvendige kompetencer er til stede i udvalget i forhold til de opgaver, der skal løses.

Det anbefales, at kommunaldirektøren eller et andet medlem af direktionen indgår i udvalget med det formål at skabe en ledelsesforankring på højt niveau i organisationen samt for at sikre beslutningsdygtighed.

Lederne af de væsentligste forretningsområder bør også være repræsenteret i informationssikkerheds-udvalget, da disse ledere definerer, hvilke data der er vitale og kritiske for driften.
Endelig bør Databeskyttelsesrådgiveren (DPO'en) indgå som rådgiver for informationssikkerhedsudvalget.

**Sammenspil med organisationen**

Organisationens informationssikkerhedskoordinator, eller en anden person med tilsvarende ansvar for informationssikkerheden, har til opgave at koordinere de planlagte (og uforudsete) aktiviteter som informationssikkerhedsudvalget igangsætter og fungerer typisk også som sekretærfunktion for informationssikkerhedsudvalget.
Input til og output fra informationssikkerhedsudvalget behandles af informationssikkerhedskoordinatoren, som i praksis koordinerer og iværksætter opgaverne i organisationen.

Informationssikkerhedskoordinatoren vurderer i samarbejde med formanden for udvalget, hvilket materiale der er relevant at forelægge til behandling i informationssikkerhedsudvalget, men informationssikkerhedsudvalget kan også efterspørge bestemt materiale til behandling.
Det er også informationssikkerhedskoordinatoren, der informerer relevante parter i organisationen om informationssikkerhedsudvalgets beslutninger og sikrer, at organisationen udfører opgaver om informationssikkerhed.

**Eksempler på input til informationssikkerhedsudvalget**

Elementer fra årshjulet

- Status på risikovurderinger
    - Hvilke områder er der foretaget risikovurderinger på siden sidst?
    - Er der fundet områder med høj risiko og er der besluttet mitigerende handlinger?
    - Planlagte risikovurderinger det næste kvartal
- Trusselsbillede og mulige forbedringer
- Resultater fra interne audits
- Politikker til godkendelse
- Resultat af beredskabstest

Elementer fra årsplanen

- Status på sikkerhedsarbejdet/sikkerhedsprojekter, herunder løbende forbedringer og status på tekniske foranstaltninger ift. cybersikkerhed (kan være udvalgte områder, så som antivirus, firewall, antispam og -phishing filtre, kryptering, netværkssikkerhed, fysisk sikkerhed.)
- Status på uddannelse/awareness
- Status på gennemførte risikovurderinger

Elementer fra daglig drift

- Hændelsesrapportering
    - Sikkerhedshændelser
        - Omfang
        - Type
        - Konsekvens
    - Status på udbedring
    - Forebyggende foranstaltninger

Input fra eksterne

- Bemærkninger og tilsynsplaner fra Datatilsynet
- Alerts/varslinger/ændringer i trusselsbillede
- Bemærkninger fra it-revisionen

Informationssikkerhedsudvalget vurderer inputtet fra informationssikkerhedskoordinatoren og træffer en overordnet beslutning om, hvorledes og af hvem relevante aktiviteter skal udføres.

Udvalget godkender politikker, overordnede procedurer samt risikovurderingens resultater og risikohåndteringsplaner.

**Rapportering til direktionen**

Informationssikkerhedsudvalget gennemgår status, rapporteringer og resultater og evaluerer disse. Evalueringen dokumenteres i en ledelsesrapport, og der udarbejdes en indstilling til direktionen, som kan omfatte forslag til forbedringer og ændringer af organisationens ledelsessystem for informationssikkerhed.

Eksempel på rapporteringen:

- Væsentlige ændringer i sikkerhedspolitik og sikkerhedsregler
- Status på opfyldelse af målsætninger for informationssikkerhed
- Status på audit, it-revision og tilsyn (årligt)
- Testrapport fra beredskabstest (årligt)
- Status på risikovurderinger med høj risiko
- Status på sikkerhedshændelser siden sidste status opgjort pr. kvartal eller måned.
    - Typer
    - Antal, herunder antal med konsekvenser for borgerne
    - Konsekvenser
    - Forebyggende foranstaltninger
- Status på uddannelse i informationssikkerhed (Awareness)
    - Hvilke fagforvaltninger har gennemført uddannelse
    - Antal medarbejdere der har gennemført
    - Antal medarbejdere der har undladt at gennemføre
- Eventuel indstilling til forbedring af informationssikkerheden med beskrivelse af omkostninger og konsekvens