DIGITALISERINGSSTYRELSEN

Vejledning i etablering og drift af et ledelsessystem for informationssikkerhed (ISMS) med udgangspunkt i ISO 27001

August 2021

2021

Indholdsfortegnelse

Formålet med denne vejledning er at give et overblik over de elementer, der bør indgå i et ledelsessystem for informationssikkerhed (ISMS) i følge ISO 27001-standarden.

Vejledningen er til dig, der har ansvaret for at implementere og vedligeholde et ledelsessystem for informationssikkerhed (ISMS) baseret på ISO 27001. Du kunne fx være informationssikkerhedskoordinator, leder med ansvar for informationssikkerhed eller medarbejder på sikkerhedsområdet.

Her kan du læse mere: Vejledning i planlægning af sikkerhedsarbejdet. Se desuden https://sikkerdigital.dk/myndighed/vejledninger-og-skabeloner for vejledninger og skabeloner til alle væsentlige delaktiviteter i arbejdet med at implementere ISO 27001.

1. ISMS med udgangspunkt i ISO 27001-standarden

Et ledelsessystem for informationssikkerhed – ofte benævnt 'ISMS' (Information Security Management System) – indeholder alle de politikker, procedurer, retningslinjer og tilhørende ressourcer og aktiviteter, som en organisation administrerer for at beskytte sine informationsaktiver. Sagt lidt mere mundret, er et ISMS summen af de instrumenter, man anvender med det formål at styre informationssikkerheden.

Hovedværdien af at organisere styringen af informationssikkerhed med udgangspunkt i et ISMS som fx det, ISO 27001 tilbyder, er, at det kan bidrage til at skabe systematik i styringen af informationssikkerheden. Desuden kan det forventes at efterlevelse af en best practice-standard som ISO 27001, vil medføre et højt niveau af informationssikkerhed. Endelig besluttedes det i den nationale strategi for cyber- og informationssikkerhed 2015-2016 – en beslutning fastholdt i senere nationale strategier for cyber- og informationssikkerhed - at statslige myndigheder skal implementere standarden. Regionerne skal efterleve standarden og kommunerne er pålagt følge principperne i standarden.

ISO 27001 giver et bud på, hvad et velfungerende ISMS bør indeholde, eller i det mindste bør indeholde for at være i overensstemmelse med standarden. Formålet med nærværende vejledning er at give et overblik over de elementer, der bør indgå i et ISMS i følge ISO 27001. Vejledningen kan anvendes på flere måder, men én måde at bruge vejledningen på er som fortolkningsstøtte til ISO 27001-teksten. Som hjælp hertil er det i de følgende afsnit angivet hvilke dele af standarden, afsnittet behandler.

Desuden indeholder vejledningen praktiske spørgsmål, som kan bruges til at tjekke, om man får det væsentligste med i sin implementering af standardens enkelte elementer. Den samlede tjekliste findes bagerst i materialet.

Nogle af kapitlerne i ISO 27001 og de aktiviteter, de beskriver, behandles mere dybdegående i andet vejledningsmateriale, som Digitaliseringsstyrelsen tilbyder. For de afsnit af nærværende vejledning hvor dette gør sig gældende, er der indsat referencer til det mere dækkende materiale. Denne vejlednings primære funktion er således at skabe et overblik over indholdet af ISO 27001 i modsætning til at udlægge alle standardens elementer i detaljen.

2. Krav til et ISMS baseret på ISO 27001-standarden

I ISO 27001's kapitel 4-10 beskrives en række krav, der er obligatoriske at implementere, såfremt man vil kunne sige, at man efterlever standarden. Disse krav beskrives og uddybes i de følgende afsnit.

ISO 27001 anvender den såkaldte "Plan-Do-Check-Act"-model (se grafik nedenfor) som overordnet ramme for styring af informationssikkerhed. Denne model anviser fire faser, som man typisk gennemløber i forbindelse med informationssikkerhedsstyringen. Modellen kan med fordel tænkes ind i arbejdet med at implementere ISO 27001's krav.

Modellen kan anses som strukturerende for arbejdet for ISO 27001 på to måder:

For det første kan dele af standarden ses som naturligt hjemmehørende i forskellige faser i modellen. De indledende kapitler i standarden omhandlende eksempelvis etablering af forretningsoverblik, udarbejdelse af politikker og risikovurderingen kan ses som hjemmehørende i "plan"-fasen. Tilsvarende kan kravene der findes senere i standarden omhandlende eksempelvis evaluering og forbedring, naturligt ses som hjemmehørende i modellens "check" og "act"-faser. På denne måde kan man sige, at ISO 27001 indebærer krav, der sikrer, at alle faser af PDCA-modellen gennemgås i praksis.

For det andet kan modellen anvendes som en generel rettesnor for, hvordan man skal arbejde med ISO 27001's enkelte krav. Selvom man meningsfuldt kan sige – som det blev ovenfor – at arbejdet med eksempelvis evaluering og forbedring hører hjemme i "check" og "act"-faserne, forholder det sig også således, at eksempelvis en konkret evaluering i praksis bør gennemløbe alle modellens faser: En evaluering skal planlægges (fase 1), udføres i praksis (fase to), evalueres (fase tre) og det skal sluttelig overvejes, om der er grundlag for forbedring af evalueringen (fase fire). På samme måde skal en politik for informationssikkerhed – som vi ovenfor placerede i "plan"-fasen" – også implementeres i praksis ligesom det skal løbende overvejes, om politikken er passende eller skal forbedres.

Figur 1
Plan-do-check-act-modellen

Kilde: egen grafik med udgangspunkt i ISO 27001

2.1 Etablering af forretningsoverblik[1]

En væsentlig forudsætning for at styringen af informationssikkerheden bliver en succes, er først at skabe et forretningsoverblik. Formålet med denne aktivitet er at afklare hvilke krav, der skal stilles til informationssikkerheden i organisationen.

Etablering af forretningsoverblik udgør en grundlæggende aktivitet for arbejdet med ISO 27001-standarden. Resultatet af denne proces leverer blandt andet input til flere af de efterfølgende processer, der beskrives nedenfor. Eksempelvis giver det ikke mening at påbegynde risikovurdering uden først at have dannet sig et overblik over den forretning og de aktiver, der skal underkastes risikovurdering.

Følgende elementer skal indgå i forretningsoverblikket i følge ISO 27001:

- Interne forhold og interne interessenter

[1] Afsnittet baserer sig på ISO 27001 afsnit 4.

- Eksterne forhold og eksterne interessenter[2]
- Omfang af ledelsessystemet for informationssikkerhed

Interne forhold og interne interessenter
Det mest centrale interne forhold at identificere er organisationens formål. For offentlige myndigheder kunne dette eksempelvis være politikudvikling, retsdannelse og afgørelse af sager. Ofte kan formålet findes beskrevet i en vision, et strategipapir, en resultatkontrakt eller lignende. Heraf kan det udledes, hvilke opgaver organisationen skal løse, og hvilke informationer, kompetencer og andre ressourcer som er nødvendige for at nå målene.

Med udgangspunkt i en forståelse af organisationens formål kan man påbegynde arbejdet med at identificere organisationens forretningskritiske informationer, systemer, medarbejderkompetencer og processer. Noget er forretningskritisk, hvis det er afgørende for, at organisationen kan opfylde sit formål på en tilfredsstillende måde. Det er imidlertid kun forretningskritiske forhold, der har relevans *i relation til informationssikkerhed*, der skal indgå i forretningsoverblikket. Eksempelvis vil der typisk være en lang række medarbejderkompetencer, der er forretningskritiske, men i nærværende sammenhæng er der kun grund til at danne sig et overblik over de kompetencer, der er forretningskritiske i forhold til at sikre informationers fortrolighed, integritet og tilgængelighed, så organisationen kan opfylde sit formål.

Overblikket kan tage udgangspunkt i nogle af, eller alle, de følgende punkter:

- Formål
- Forretningskritiske processer (fx arbejdsgange)
- Forretningskritiske informationer
- Forretningskritiske it-systemer (fx sagsbehandlingssystemer)
- Forretningskritiske medarbejderkompetencer
- Interne interessenter

Desuden bør man identificere interne interessenter. Disse er typisk organisationens medarbejdere, og er interessenter i den relevante forstand, fordi det kan udgøre en risiko for organisationens overlevelse ikke at imødekomme deres behov og forventninger. Eksempelvis vil de fleste medarbejdere have legitime krav og forventninger til informationssikkerheden, fordi de ønsker at de oplysninger, organisationen behandler om dem (fx i regi af HR og personalehåndtering), behandles forsvarligt.

[2] I følge ISO 31000 er et forhold *internt* hvis det er under organisationens direkte kontrol, og *eksternt* såfremt organisationen ikke har direkte kontrol over forholdet (men i stedet kan anticipere og tilpasse sig det).

Interne forhold og interessenter vil typisk have betydning for, hvilke krav der skal stilles til informationssikkerheden, hvorfor forretningsoverblikket har relevans for det videre arbejde med at styre informationssikkerheden. Eksempelvis vil en organisationen, der behandler mange og følsomme oplysninger for at kunne levere sin kerneydelse typisk stille større krav til informationssikkerheden end en organisation, der behandler få og ikke-følsomme oplysninger.

Eksterne forhold og eksterne interessenter
De eksterne forhold angår alt det, der findes uden for organisationen, og som er afgørende for organisationens opgaveløsning. Det kunne eksempelvis være organisationens kontraktlige forpligtelser, lovkrav, leverandøraftaler og/eller internationale aftaler.

Typiske eksterne interessenter er kunder eller borgere, som modtager organisationens produkt og samarbejdspartnere, myndigheder og leverandører, der indgår i opgaveløsningen. Ofte vil det være sådan, at man i arbejdet med at fastlægge organisationens formål (behandlet i forrige afsnit) kan identificere en række centrale eksterne interessenter.

Organisationens eksterne forhold og interessenter kan have betydning for krav til informationssikkerheden. Et godt eksempel herpå er lovkrav til informationssikkerhed, der udgør et eksternt forhold, som organisationen må tilrette sin informationssikkerhedsstyring efter.

Omfang af ledelsessystemet for informationssikkerhed
En del af opgaven med at etablere forretningsoverblik består i at beslutte og dokumentere det omfang, ISMS'et skal have.

Omfanget kan specificeres på en række forskellige måder og eksempelvis på baggrund af informationstyper, organisationsstruktur og/eller forretningsgange. Bemærk at ISMS'et ikke nødvendigvis behøver dække hele organisationen.

Her kan du læse mere: Hent vejledning i etablering af forretningsoverblik

Tjekliste til forretningsoverblik:

- ✓ Har du identificeret og dokumenteret: i) organisationens formål, ii) forretningskritiske processer, iii) forretningskritiske informationer, iv) forretningskritiske systemer, v) forretningskritiske medarbejderkompetencer og vi) interne interessenter?
- ✓ Identificér og dokumentér hvilke krav punkterne i-vi stiller til informationssikkerheden i din organisation
- ✓ Har du identificeret og dokumenteret eksterne forhold og eksterne interessenter?

- ✓ Identificér og dokumentér hvilke krav eksterne forhold og eksterne interessenter stiller til informationssikkerheden i din organisation
- ✓ Har du defineret omfanget af din organisations ISMS?
- ✓ Ud fra hvilke kriterier er grænserne for din organisations ISMS draget?

2.2 Ledelsesforankring[3]

Ifølge ISO 27001 er informationssikkerhed et ledelsesansvar ligesom økonomistyring, arbejdsmiljø, service eller borgerbetjening. Den ledelsesforankring der er nødvendig på informationssikkerhedsområdet, adskiller sig dermed ikke fra det engagement, ledelsen skal vise på alle andre væsentlige styringsområder. Forankringen af informationssikkerhed skal konkret komme til udtryk i:

- *Målfastsættelse*: Ledelsen skal fastlægge niveauet for sikkerhed i organisationen, herunder acceptere risici
- *Organisering*: Ledelsen skal tage stilling til den praktiske organisering af informationssikkerhedsarbejdet
- *Ressourceallokering og prioritering*: Ledelsen skal afsætte de nødvendige ressourcer til at drive informationssikkerhedsarbejdet
- *Kommunikation*: Ledelsen skal, ved passende lejligheder, kommunikere vigtigheden af informationssikkerhedsarbejdet
- *Fastsættelse af politikker og strategier*: Ledelsen skal fastlægge en informationssikkerhedspolitik og strategi
- *Fastsættelse af roller og ansvar*: ledelsen skal uddelegere det ansvar til medarbejdere, der er relevant for informationssikkerhedsarbejdets udførelse
- *Opfølgning og forbedring af ISMS'et*: Ledelsen skal understøtte løbende evaluering of forbedring af ISMS'et

Flere af ovennævnte aktiviteter behandles mere dybdegående i denne vejlednings følgende afsnit, og behandles desuden særskilt og mere fyldestgørende i ISO 27001's øvrige kapitler.

Den øverste ledelse vil i mange tilfælde etablere en enhed til koordinering af informationssikkerhedsarbejdet (fx et sikkerhedsudvalg). Enheden igangsætter aktiviteter, følger op på implementering af politikker og retningslinjer, måler effekt og rapporterer tilbage til ledelsen

Her kan du læse mere: Hent vejledning i informationssikkerhedspolitik

Her kan du læse mere: Læs mere om hvordan du beskriver og fordeler roller og ansvar for informationssikkerhedsarbejdet her

[3] Afsnittet baserer sig på ISO 27001 afsnit 5.

Styring af informationssikkerhed i koncerner

For informationssikkerhedsstyringen i de statslige myndigheder gælder det, at disse er underlagt departementets tilsyn og indgår som sådan i den samlede koncernstyring. Tilsynet skal være reelt og aktivt. Rigsrevisionen påser dette.

Den enkelte myndighed er dog selv ansvarlig for at beskytte sine informationsaktiver. Dette ansvar kan hverken uddelegeres til en leverandør eller til et departement. Med ISO 27001 er der dog gode muligheder for at skalere indsatsen, så den er proportionel med organisationens størrelse, kompleksiteten af it- anvendelsen.

Tjekliste:

- ✓ Forholder din organisations ledelse sig med passende interval til de emner, der er oplistet i starten af afsnittet?
- ✓ Er der indlagt aktiviteter i årshjulet og årsplanerne og/eller oprettet udvalg, der sikrer, at ledelsen forholder sig til de emner, der er oplistet i starten af afsnittet?
- ✓ Foreligger der en ledelsesgodkendt politik for informationssikkerhed?
- ✓ Foreligger der en ledelsesgodkendt liste over roller og ansvar i forbindelse med sikkerhedsarbejdet

2.3 Risikostyring[4]

For at kunne implementere et velfungerende ISMS er det af afgørende betydning, at man skaber et overblik over risikobilledet for organisationens informationer (med hensyn til deres fortrolighed, integritet og tilgængelighed) og i lyset deraf træffer beslutninger om, hvordan de identificerede risici skal håndteres. Dette kaldes *risikostyring* (se også ISO 27005). For at kunne påbegynde arbejdet med at identificere, vurdere og styre i lyset af relevante risici, må man have et overblik over sin forretning og dens kontekst. Hvordan man skaber dette overblik blev omtalt i afsnit 2.1.

Her kan du læse mere: Vejledning –til risikostyring inden for informationssikkerhed.

[4] Afsnittet baserer sig på ISO 27001 afsnit 6.

Som en del af risikostyringen skal organisationen desuden udarbejde et såkaldt *Statement of Applicability* (SoA). Det er et dokument, der skal beskrive og begrunde de sikringsforanstaltninger, organisationen har til- og fravalgt.[5]

Her kan du læse mere: Hent guide til SoA-dokumentet

Tjekliste:

- ✓ Er der udarbejdet risikovurderinger?
- ✓ Baserer informationssikkerhedsarbejdet og valget af sikringsforanstaltninger sig på risikovurderingerne, og er til- og fravalg af sikringsforanstaltninger dokumenteret i et SoA-dokument

2.4 Ressourcer[6]

Organisationen skal sikre, at der er allokeret tilstrækkelige ressourcer til at de sikkerhedsmål, der er defineret af ledelsen, kan opnås. Det betyder, at der skal være nok ressourcer til, at informationssikkerhedsindsatsen i praksis er egnet til at understøtte organisationens opgavevaretagelse. Endvidere skal der være ressourcer nok til at sikre, at sikringsforanstaltningerne kan implementeres korrekt.

Korrekt implementering betyder, at foranstaltningerne er dokumenterede, at krævede aktiviteter rent faktisk udføres, og at status på arbejdet rapporteres til ledelsen og relevante interessenter.

Ressourcer bør være afsat i budgetter på linje med alle andre omkostninger i organisationen.

Tjekliste:

- ✓ Er der afsat tilstrækkelige ressourcer til at de informationssikkerhedsmål, der er fastsat af ledelsen, kan opfyldes?

2.5 Kompetencer[7]

Organisationen skal sikre, at den råder over de nødvendige kompetencer til at styre informationssikkerheden. Det indebærer, at et passende antal medarbejdere har den rette uddannelsesmæssige baggrund og erfaring til opgaven med realisering af sikkerhedsmålene. Jo mere kompleks en organisation og it-system er, jo større vil kravene til medarbejdere og ledelse være.

---

[5] I november 2021 udkommer en ny og revideret version af ISO 27002. ISO 27002 uddyber ISO 27001's såkaldte anneks A. Eftersom sikkerhedsforanstaltninger til SoA-dokumentet vælges fra Anneks A og ISO 27002, kan revisionen af ISO 27002 give anledning til at genbesøge sit SoA-dokument, da revisionen både indebærer en ny struktur samt introduktion af en række nye sikkerhedsforanstaltninger.
[6] Afsnittet baserer sig på ISO 27001 afsnit 7.1.
[7] Afsnittet baserer sig på ISO 27001 afsnit 7.2.

Kompetencekravet betyder desuden, at organisationen skal vedligeholde og opbygge kompetencer i takt med, at organisationen, risikolandskabet og truslerne udvikler sig.

Tjekliste:

- ✓ Har organisationen overblik over sikkerhedskompetencebehovet?
- ✓ Besidder organisationen de påkrævede sikkerhedskompetencer?
- ✓ Er der etableret processer, der sikrer løbende opkvalificering af medarbejdere, såfremt der findes et behov?

2.6 Awareness (bevidsthed)[8]

Awareness-aktiviteter skal sikre, at organisationens medarbejdere har kendskab til og forstår, hvordan de skal agere for at minimere risikoen for sikkerhedshændelser. Aktiviteterne afhænger af den enkelte organisationsenheds kontekst og vigtigste risikoprioriteter, men som udgangspunkt skal indholdet af informationssikkerhedsretningslinjerne og basale adfærdsnormer, der gælder for organisationens medarbejdere formidles. Det gælder typisk processen for rapportering af hændelser, håndtering af fysisk og digital information, procedurer ved distancearbejde og lignende. Det er her væsentligt at nævne, at organisationens opgave med at sørge for, at ansatte i organisationen har den hensigtsmæssige sikkerhedsadfærd ikke stopper ved awareness-aktiviteter. Viden er sjældent nok til, at den rette adfærd faktisk udføres. I *Metode til adfærdsindsatser* samt tilhørende bilag findes en samlet guide til, hvordan en organisation kan arbejde med indsatser, der påvirker ansattes sikkerhedsadfærd.

Her kan du læse mere: Metode til at arbejde med adfærdsindsatser indenfor cyber- og informationssikkerhed

Tjekliste:

- ✓ Foreligger der en politik for, hvordan medarbejdere bør agere for at minimere risikoen for sikkerhedshændelser?
- ✓ Er medarbejderne i organisationen bevidste om, hvordan de agerer på en måde, der minimerer risikoen for en sikkerhedshændelse?
- ✓ Er der iværksat aktiviteter, der sikrer, at medarbejder løbende mindes om, hvordan de agerer på måder, der minimerer risikoen for sikkerhedshændelser?

[8] Afsnittet baserer sig på ISO 27001 afsnit 7.3.

2.7 Kommunikation[9]

Kommunikation er væsentlige bestanddele i den daglige drift af ISMS'et. *Ekstern kommunikation* i relation til informationssikkerhed skal styres stramt, og der bør være præcise retningslinjer på området. Oplysninger om informationssikkerheden vil nemlig som regel være af fortrolig karakter, hvor sårbarheder og information om, hvordan sikringsforanstaltninger i øvrigt er tilrettelagt, kan afsløres. De situationer der nødvendiggør ekstern kommunikation kan være:

- Udveksling af oplysninger med eksterne serviceleverandører
- Information til borgere og samarbejdspartnere om brud på fortroligheden omkring personoplysninger og andre fortrolige oplysninger
- Information til borgere og samarbejdspartnere om beredskabssituationer, der påvirker den almindelige opgavevaretagelse

Intern kommunikation om informationssikkerhed dækker først og fremmest over det rapporteringskredsløb, der skal være til stede, for at ledelsen kan udøve sine beføjelser på et rettidigt og oplyst grundlag.

Rapportering til ledelsen bør ske via de eksisterende kanaler for kommunikation af ledelsesinformation. Hvis organisationen har etableret et dedikeret informationssikkerhedsudvalg, skal kommunikationen tilrettelægges, så alle væsentlige oplysninger tilgår dette udvalg.

Kommunikation er endvidere en central del af risikostyringsprocessen, og det skal sikres, at repræsentanter for forretningen både høres om forretningsmæssige konsekvenser ved brud på informationssikkerheden og informeres om resultatet af risikovurderinger og de besluttede handlingsplaner.

Der kan også være behov for intern kommunikation i relation til medarbejderstaben. Det er som regel i forbindelse med orientering om sikkerhedshændelser, eller hvis der er behov for, at der udvises en bestemt adfærd eller agtpågivenhed i forhold til fx en ny trussel.

Fælles for kommunikationen gælder, at følgende skal være besluttet og dokumenteret:

- Hvad skal kommunikeres?
- Hvornår?
- Til hvem?
- Af hvem?
- Og ad hvilke kommunikationskanaler?

[9] Afsnittet baserer sig på ISO 27001 afsnit 7.4.

Tjekliste:

- ✓ Er der vedtaget retningslinjer for intern og ekstern kommunikation?
- ✓ Er ansvar for kommunikation fordelt og kommunikeret til de ansvarlige?

2.8 Dokumentation[10]

Dokumentation af ISMS'et er et centralt element i dets etablering og drift. Nogle dokumenter er ifølge ISO 27001 påkrævede at udarbejde. Dokumentationskrav der står opskrevet i ISO 27001s afsnit 4-10, har denne obligatoriske karakter.

Desuden konstaterer ISO 27001, at dokumentationsbehovet afhænger af den konkrete organisations størrelse, typer af aktiviteter, kompleksitet og modenhed. Dette indebærer tre ting:

1. **Tilpasselig**: For ethvert dokumentationskrav i ISO 27001 gælder, at dokumentations omfang bør tilpasses organisationens karakter. Eksempelvis vil en organisation med mange systemer, aktiver og processer alt andet lige skulle producere og dokumentere en mere omfattende risikovurdering end en organisation med kun få systemer, aktiver og processer.
2. **Valgfrihed**: Der er i et begrænset omfang mulighed for at vælge hvilke retningslinjer for dokumentation, man vil implementere. Denne valgfrihed gør sig gældende for retningslinjerne indeholdt i ISO 27001's såkaldte Anneks A og ISO 27002. For Anneks A's retningslinjer gælder specifikt, at en organisation kan undlade at implementere en given retningslinje, såfremt en sådan undladelse er velbegrundet. Det er velbegrundet ikke at implementere en given retningslinje, hvis det er tilfældet, at ingen ekstern bindende standard (fx lovkrav eller kontrakt) kræver, at retningslinjen følges, og organisationens risikovurdering for øvrigt viser, at retningslinjen er unødvendig for at behandle risici. Sådanne valg skal dokumenteres i SoA-dokumentet.
3. **Dokumentationsbehov der ikke er beskrevet i ISO 27001, Anneks A eller ISO 27002**: Der kan i princippet være dokumentation, der er nødvendig for at sikre et effektivt ISMS,

[10] Krav til form og proces for dokumentationen baserer sig på ISO 27001 afsnit 7.5. Hvad der skal/kan dokumenteres, følger af flere afsnit såvel som dele af det såkaldte Anneks A.

men som ikke eksplicit fremgår af ISO-standarden og tilhørende dokumenter (jf. ISO 27001 afsnit 7.5.1b).

Obligatorisk dokumentation

Omfang af ISMS'et (scope)	4.3
En informationssikkerhedspolitik der indeholder målsætninger for informationssikkerhedsstyringen	5.2e og 6.2
Dokument der beskriver organisationens risikovurderingsproces	6.1.2
Dokument der beskriver organisationens risikohåndteringsproces	6.1.3
SoA-dokument	6.1.3d
Dokumentation af uddannelse, evner, erfaring og kvalifikationer	7.2d
Resultater af risikovurderingsproces og risikohåndteringsproces	8.2, 8.3
Procesbeskrivelse for evaluering af informationssikkerheden og resultaterne af disse evalueringer	9.1
Procesbeskrivelse for interne audits og resultaterne af disse	9.2g
Dokumentation af ledelsen gennemgang af evaluering af informationssikkerheden og effekten af ISMS, afvigelser og opfølgende handlinger	9.3
Oversigt over informationssikkerhedshændelser (afvigelser), korrigerende handlinger, og resultatet af de korrigerende handlinger	10.1

Valgfri dokumentation relevante; 'A' henviser til 'Anneks A')[11]

Roller og ansvarsområder for informationssikkerhed	ISO 27002 6.1.1
Kontrakter med medarbejdere og øvrige kontrahenter skal beskrive ansvar for informationssikkerhed	A.7.1.2
Fortegnelse over aktiver, inkl. ejerskab	A.8.1.1
Klassifikation af information samt politik for håndtering af klassificeret information	A.8.2.1, A.8.2.2, A.8.2.3
Politik for adgangsstyring	A.9.1.1
Driftsprocedurer	A.12.1.1
Hændelseslogs	A.12.4.1
Administrator- og operatørlog	A.12.4.3
Krav til fortroligheds- og hemmeligholdelsesaftaler	A 13.2.4
Procedurer for styring af systemændringer	A.14.2.2
Principper for udvikling af sikre systemer	A 14.2.5
Informationssikkerhedspolitik for leverandørforhold	A.15.1.1
Proces for håndtering af informationssikkerhedsbrud	A.16.1.5
Implementering af informationssikkerhedskontinuitet (dokumentation af beredskab)	A.17.1.2

[11] Det bemærkes, at ISO 27002, der har til formål at uddybe ISO 27001's anneks A, nævner en række yderligere dokumentationsforanstaltninger, der ikke nævnes i anneks A. Disse kan til- og fravælges efter behov.

Roller og ansvarsområder for informationssikkerhed	ISO 27002 6.1.1
Identifikation af gældende lovgivning og kontraktkrav	A.18.1.1

Ovennævnte krav er alle krav til *indholdet* af dokumentationen. Følgende *formkrav* gælder desuden for dokumentationen:

- Der skal fastsættes en navngivningsstandard, formatstandard (fx sprog og grafik), mediestandard (fx papir og/eller elektronisk dokument), tages beslutning om dokument-metadata og accepterede filformater.

Dokumentationen skal endvidere være styret efter følgende krav:

- Det skal være nemt tilgængeligt for autoriserede brugere
- Det skal beskyttes mod tab af fortrolighed og integritet
- Lagringssted, -medier og -metode skal besluttes for såvel digital som papirbåren dokumentation
- Opbevaringsperiode og sletteprocedurer skal være fastlagt
- Der skal være en proces for review og godkendelse af dokumentationen
- Der skal være et revisionsspor for ændringer

Tjekliste:

- ✓ Har organisationen udarbejdet obligatorisk dokumentation?
- ✓ Har organisationen taget stilling til hvilke af de valgfri dokumentationstyper, organisationen har behov for, og er tilvalg/fravalg begrundet i SoA-dokumentet?
- ✓ Har organisationen taget stilling til formkrav til dokumentation?
- ✓ Er der etableret en proces for dokumentstyring (fx mht. dokumentationens beskyttelse, slettefrister mm.)

2.9 Drift og evaluering[12]

Driften af ISMS'et omfatter det daglige informationssikkerhedsarbejde. Når alle de ovenfor nævnte elementer er etableret, bliver det muligt at styre informationssikkerheden på en dag-til-dag-basis. Standarden fremhæver eksplicit tre aktiviteter, der bør indgå i driften, ud over det ikke nærmere specificerede sæt af driftsaktiviteter, der er nødvendige for at opfylde informationssikkerhedsmålsætningerne for organisationen:

[12] Dette afsnit baserer sig på ISO 27001 kapitel 8-10.

- Hændelseshåndtering
- Styring af leverandører for så vidt angår de risici, hvor organisationen har valgt at outsource risikohåndteringen
- Løbende (re)vurdering af informationssikkerhedsrisici

Hvor den første aktivitet må forventes at have en ad hoc karakter, og er afhængig af de sikkerhedshændelser organisationen oplever, kan de to øvrige aktiviteter med fordel styres ved at indlægge dem i årshjul og årsplaner. Indplacering i årshjul kan være med til at sikre, at emnerne systematisk genbesøges med et passende interval. Dette betyder imidlertid ikke, at styring af leverandører og risikovurdering kun skal foretages på de i årshjulet indlagte tidspunkter. Eksempelvis kan ændringer i trusselsbilledet eller risikolandskabet give anledning til leverandørstyring og risikovurdering på ad hoc basis.

Her kan du læse mere om leverandørstyring: https://sikkerdigital.dk/myndighed/vejledninger-og-skabeloner

ISO 27001 stiller desuden krav om, at der løbende følges op på informationssikkerhedsstyringen. Organisationen bør iværksætte følgende typer opfølgning:

Overvågning og måling
Organisationens informationssikkerhedsfunktion skal selv udføre overvågnings- og målingsaktiviteter. Der skal være dokumenterede retningslinjer på området, som beskriver metoder, frekvens og genstande ('hvem' eller 'hvad') for kontrollen. Et element i egenkontrollen kunne være et egentligt måleprogram, hvor en række foruddefinerede målbare indikatorer for informationssikkerhed beregnes og rapporteres i henhold til en fastlagt plan. Sådanne målinger kan blandt andet bidrage til at fastslå det aktuelle sikkerhedsniveau, og over tid anvendes som indikatorer for udviklingen af modenheden af informationssikkerhedsstyringen.

Intern audit
Periodisk gennemførelse af intern audit er ligeledes et krav ifølge ISO 27001. De fleste offentlige organisationer råder ikke over en egentlig intern revision eller audit-funktion, hvilket dog ikke er afgørende for at opfylde kravet. Hensynet bag kravet kan opfyldes ved at lade en uafhængig ekstern part gennemgå ISMS'et med et passende interval. Det tilsyn en central enhed skal føre med underliggende institutioner, kan efter omstændighederne også udgøre den interne audit.

Gennemgangen skal tage udgangspunkt i en auditplan, som organisationen har ansvaret for at vedligeholde. Gennemgangens omfang skal fastlægges, så det bliver undersøgt, om styringen af informationssikkerheden lever op til organisationens egne krav til sikkerhedsniveauet såvel som ISO 27001-standarden.

Den interne audits observationer og anbefalinger skal dokumenteres til organisationens interne brug (se også forrige afsnit om dokumentationskrav).

Ledelsesmæssig opfølgning
Den sidste type opfølgning er ledelsens egen opfølgning. Først og fremmest skal ledelsen følge op på:

- Resultat fra egenkontrollen, tendens i de væsentligste målinger af informationssikkerheden, overskridelse af vedtagne tærskelværdier
- Observationer og anbefalinger i auditrapporter

Herudover er ledelsesopfølgning påkrævet ved:

- Status på handlingsplaner, som ledelsen har iværksat til udbedring af konstaterede sårbarheder
- Ændringer i det generelle trusselsbillede, som organisationen agerer under

Tjekliste:

- ✓ Foreligger der en plan for løbende egen evaluering ISMS'et?
- ✓ Foreligger der en plan for intern audit?
- ✓ Foreligger der en plan for hvordan ledelsen involveres i opfølgningen på ISMS's kvalitet

2.10 Forbedring

Ifølge ISO 27001's kapitel 10 skal organisationen løbende søge at forbedre informationssikkerheden og styringen heraf. Dette bør ske på de to følgende måder:

- Forbedring foranlediget af sikkerhedshændelser
- Løbende forbedring af ISMS'et

Forbedring foranlediget af sikkerhedshændelser
Hvis der opstår en sikkerhedshændelse, der medfører en afvigelse[13], bør organisationen iværksætte en undersøgelse af, om ISMS'et kan forbedres, så en lignende afgivelse ikke opstår igen. Sådanne undersøgelser skal omfatte en identifikation af årsager samt en vurdering af potentialet for gentagelse af hændelser og afvigelser. Undersøgelserne skal følges op af handleplaner. På denne måde giver faktiske sikkerhedshændelser anledning til læring og forbedring af organisationens informationssikkerhed.

[13] En 'afvigelse' er i følge ISO 27000 enhver manglende opfyldelse af standardens krav. Bemærk at en 'hændelse' ifølge ISO 27001 også kan henvise til et skift i organisationens omgivelser såsom trusselslandskabet.

Løbende forbedring af ISMS'et
Desuden bør man løbende og uafhængigt af faktiske hændelser, søge at forbedre ISMS'et. Eksempelvis ved at optimere organisering, informationsflow, dokumentationskvalitet, forretningsgange.

Der vil for det meste være en klar sammenhæng mellem organisationens informationssikkerhedsmæssige modenhed, og de kræfter, den har brugt på løbende forbedring af ISMS'et.

Her kan du læse mere: Vejledning i evaluering og opfølgning

Tjekliste:

- ✓ Foreligger der procedurer i organisationen, der sikrer, at sikkerhedshændelser underkastes nærmere analyse med henblik på at identificere forbedringspotentiale?

3. Tjekliste

Forretningsoverblik	• Har du identificeret og dokumenteret: i) organisationens formål, ii) forretningskritiske processer, iii) forretningskritiske informationer, iv) forretningskritiske systemer, v) forretningskritiske medarbejderkompetencer og vi) interne interessenter? • Identificér og dokumentér hvilke krav punkterne i-vi stiller til informationssikkerheden i din organisation • Har du identificeret og dokumenteret eksterne forhold og eksterne interessenter? • Identificér og dokumentér hvilke krav eksterne forhold og eksterne interessenter stiller til informationssikkerheden i din organisation • Har du defineret omfanget af din organisations ISMS? • Ud fra hvilke kriterier er grænserne for din organisations ISMS draget?
Ledelsesforankring	• Forholder din organisations ledelse sig med passende interval til de emner, der er oplistet i starten af afsnittet? • Er der indlagt aktiviteter i årshjulet og årsplanerne og/eller oprettet udvalg, der sikrer, at ledelsen forholder sig til de emner, der er oplistet i starten af afsnittet? • Foreligger der en ledelsesgodkendt politik for informationssikkerhed? • Foreligger der en ledelsesgodkendt liste over roller og ansvar i forbindelse med sikkerhedsarbejdet?
Risikostyring	• Er der udarbejdet risikovurderinger af forretningskritiske aktiver, processer og systemer? • Baserer informationssikkerhedsarbejdet og valget af sikringsforanstaltninger sig på risikovurderingerne, og er til- og fravalg af sikringsforanstaltninger dokumenteret i et SoA-dokument?
Ressourcer, kompetencer, awareness	• Er der afsat tilstrækkelige ressourcer til at de informationssikkerhedsmål, der er fastsat af ledelsen, kan opfyldes? • Har organisationen overblik over sikkerhedskompetencebehovet? • Besidder organisationen de påkrævede sikkerhedskompetencer? • Er der etableret processer, der sikrer løbende opkvalificering af medarbejdere, såfremt der findes et behov? • Foreligger der en politik for, hvordan medarbejdere bør agere for at minimere risikoen for sikkerhedshændelser? • Er medarbejderne i organisationen bevidste om, hvordan de agerer på en måde, der minimerer risikoen for en sikkerhedshændelse? • Er der iværksat aktiviteter, der sikrer, at medarbejder løbende mindes om, hvordan de agerer på måder, der minimerer risikoen for sikkerhedshændelser?
Kommunikation	• Er der vedtaget retningslinjer for intern og ekstern kommunikation? • Er ansvar for kommunikation fordelt og kommunikeret til de ansvarlige?
Dokumentation	• Har organisationen udarbejdet obligatorisk dokumentation? • Har organisationen taget stilling til hvilke af de valgfri dokumentationstyper, organisationen har behov for, og er tilvalg/fravalg begrundet i SoA-dokumentet? • Har organisationen taget stilling til formkrav til dokumentation? • Er der etableret en proces for dokumentstyring (fx mht. dokumentationens beskyttelse, slettefrister mm.)
Evaluering og forbedring	• Foreligger der en plan for løbende egenevaluering ISMS'et? • Foreligger der en plan for intern audit? • Foreligger der en plan for hvordan ledelsen involveres i opfølgningen på ISMS's kvalitet?

	• Foreligger der en plan for hvordan ledelsen involveres i opfølgningen på ISMS's kvalitet? • Foreligger der procedurer i organisationen, der sikrer, at sikkerhedshændelser underkastes nærmere analyse med henblik på at identificere forbedringspotentiale?

Vejledning til etablering og drift af et ledelsessystem for informationssikkerhed (ISMS) med udgangspunkt i ISO 27001
Udgivet august 2021
Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
www.sikkerdigital.dk.

Foto Colourbox

ISBN 978-87-93073-40-1