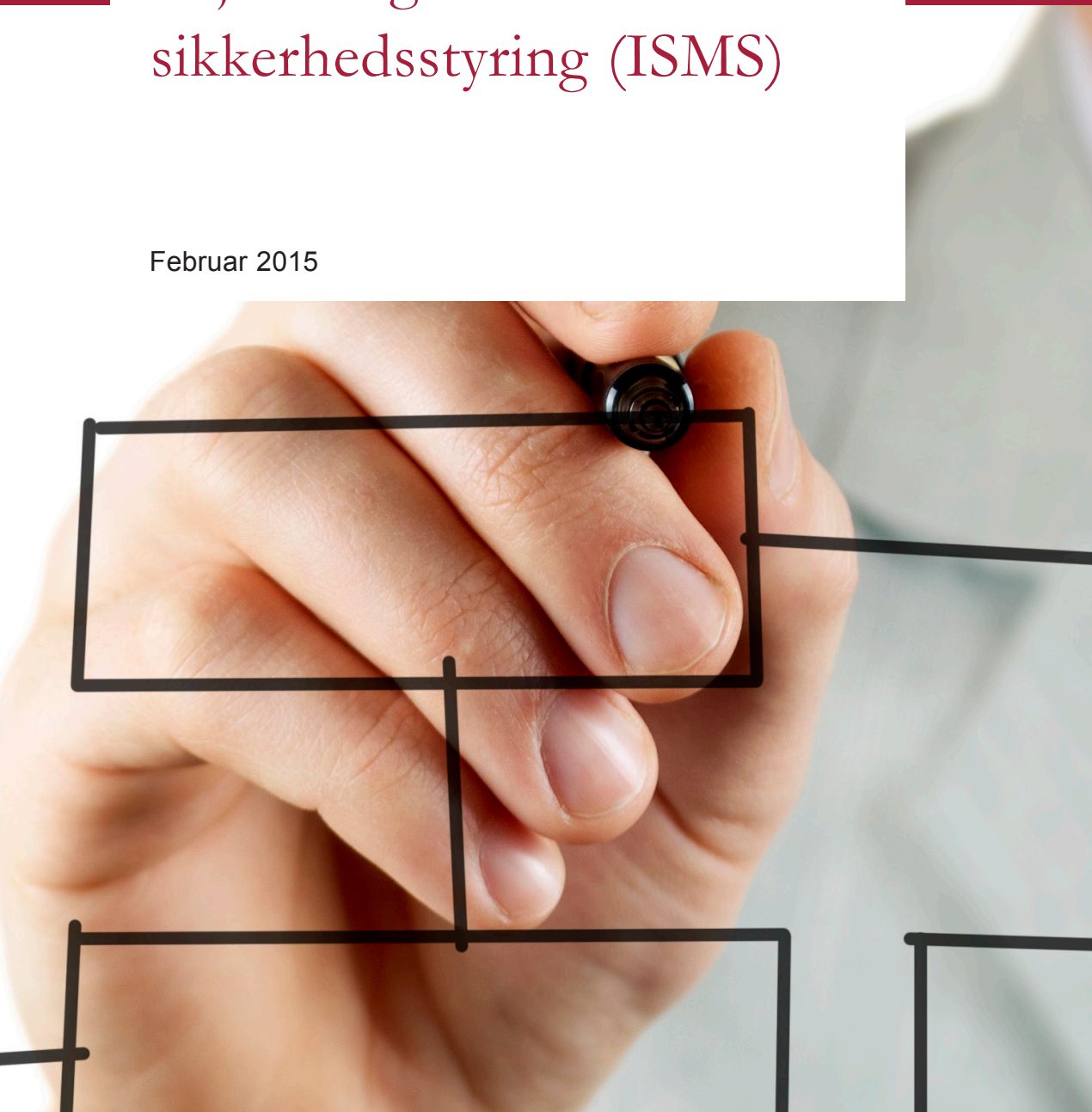
DIGITALISERINGSSTYRELSEN

Vejledning i informations-sikkerhedsstyring (ISMS)

Februar 2015



Vejledning i informationssikkerhedsstyring (ISMS)

Udgivet februar 2015

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
Digitaliseringsstyrelsens hjemmeside
www.digst.dk.

Foto Colourbox

Elektronisk publikation
ISBN 978-87-93073-11-1

Indhold

1. ISO27001

Denne vejledning giver et overblik over de elementer og koncepter, der bør indgå i et ledelses- og styringssystem for informationssikkerhed (ISMS). Samtidig giver vejledningen et bud på, hvordan det kan kombineres i en styringsmodel, der sikrer, at organisationen opnår det ønskede sikkerhedsniveau ved hjælp af kontroller, opfølgning og rapportering.

Vejledningen er skrevet til sikkerhedskoordinatorer og sikkerhedsansvarlige, som har opgaven med implementering af ISO27001[1]. Den primære målgruppe er den statslige sektor, men både regioner, kommuner og private virksomheder kan bruge materialet.

ISMS'et er tænkt som en del af det samlede ledelsessystem i organisationen, der sikrer opnåelse af mål og hensigtsmæssig brug af ressourcer. Med udgangspunkt i forretningsmæssige risici dækker ISMS'et etablering, implementering, drift, overvågning, gennemgang, vedligeholdelse og forbedring af informationssikkerheden.

> ISMS'et er et samlet udtryk for de politikker, procedurer, processer, organisatoriske beslutningsgange og aktiviteter, som udgør komponenterne i organisationens styring af informationssikkerhed.

Organisationens kontekst

ISO27001 stiller krav om, at en række styringsaktiviteter er til stede for at kunne lykkes med styringen af informationssikkerhed. Når der i en organisation er skabt et samspil mellem styringsaktiviteterne, er det i realiteten udtryk for, at der er implementeret et fungerende ISMS.

Organisationen skal stræbe efter at forstå egne informationsaktivers forretningsmæssige betydning, og hvordan grænseflader til omverdenen kan påvirke denne betydning.

Forståelsen kan opnås igennem en overordnet vurdering af, hvordan risikobilledet i forhold til informationsaktiver er påvirket af:

- Typen af organisationsudøvelse (politikudvikling, retsdannelse, afgørelse af sager, "faktisk forvaltning")
- Organisationens formål og mål

[1] Med den danske udgivelse af ISO27001:2013 i januar 2014 er der nu krav om implementering af standarden i den statslige sektor. I denne vejledning bruges ISO27001 som betegnelse for ISO27001:2013.

- Organisationens opbygning
- Den geografiske placering
- Teknologianvendelsen.

Et andet væsentligt element er *omverdenen*: Hvem er organisationens væsentligste interessenter? Og hvilke af disse kan have en interesse i, hvordan organisationen beskytter sine informationsaktiver? Er der deciderede krav til tilgængelighed, fortrolighed eller integritet af data?

Eksempler på interessenter, der kan have en sådan interesse er:

- Borgere, der har overladt (personlige) oplysninger til organisationen
- Politiske aktører, der medvirker i det lovforberedende arbejde
- Andre organisationer, med hvem der udveksles oplysninger
- Leverandører, der behandler oplysninger på vegne af organisationen

Endelig skal *scopet* fastlægges for informationssikkerhedsstyringen:

- Er hele ministerområdet omfattet af alle dele af ISMS'et, eller differentieres der fx på forretnings- eller organisationsområder?
- Er alle geografiske lokationer omfattet?

Certificering: Værd af gå efter?

Virksomheder og organisationer, der implementerer ledelsessystemer efter ISO27001, kan vælge at lade sig certificere for at demonstrere, at styringen er implementeret og effektiv.

Der er fra statslig side ikke krav om, at offentlige organisationer lader sig certificere. I de tilfælde, hvor organisationen indtager en rolle som *it-serviceleverandør* i forhold til andre organisationer, borgere eller virksomheder, kan det være en god måde at skabe en grundlæggende tillid med en certificering.

Værdien af en certificering er bl.a. øget professionalisering i arbejdet med sikkerhed, og samtidig forbedres mulighederne for at etablere et tilstrækkeligt sikkerhedsniveau. I samarbejdsrelationer er mange spørgsmål også lettere at svare på, da dokumentationen er udarbejdet og opdateret. Selve processen frem mod certificering er dog ret omfattende og kostbar, og det anbefales, at der udarbejdes en business case om spørgsmålet, inden arbejdet igangsættes.

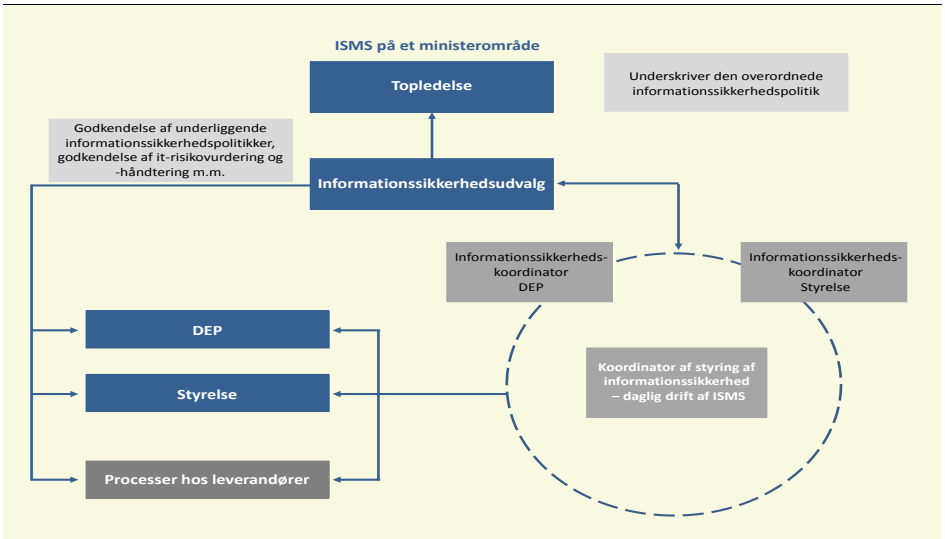
Ledelse

Informationssikkerhed er et ledelsesansvar ligesom økonomistyring, arbejdsmiljø, service eller borgerbetjening. Ledelsesforankring har alle dage været anerkendt som en væsentlig forudsætning for at kunne drive et effektivt ISMS.

Den ledelsesforankring, der er nødvendig på informationssikkerhedsområdet, adskiller sig ikke fra det engagement, ledelsen skal vise på alle andre væsentlige styringsområder. Forankringen skal konkret komme til udtryk i:

- Målfastsættelse: Ledelsen skal fastlægge niveauet for sikkerhed i organisationen, herunder acceptere risici
- Organisering: Der skal både tages stilling til organiseringen internt i den enkelte organisation og organiseringen som sådan:
  - Ressourceallokering
  - Definering af politikker og strategier
  - Definering af roller og ansvar
  - Aktiv opfølgning på den løbende rapportering.

Den øverste ledelse skal etablere en organisation til koordinering af informationssikkerhedsarbejdet. Organisationen igangsætter aktiviteter, følger op på implementering af politikker og retningslinjer, måler effekt og rapporterer tilbage til ledelsen.



En velfungerende implementering af ISO27001 baserer sig på en risikobaseret og ledelsesforankret tilgang. En tilgang, hvor arbejdet med informationssikkerhed vurderes i forhold til betydningen for forretningen, og hvor prioriteringen af indsatsen derfor flyttes ud af it-afdelingen og fra it-leverandøren og over til forretningen.

En beskrivelse af risikostyringsprocessen findes i *Vejledning i risikostyring og -vurdering*.

Som en del af risikohåndteringsarbejdet skal organisationen udarbejde et Statement of Applicability (SoA). Det er et dokument, der skal beskrive og begrunde de kontroller, organisationen har tilvalgt og fravalgt. SoA-dokumentet er således et arbejdsdokument, som til enhver

tid skal indeholde et overblik over kontrollerne og status herpå. SoA-dokumentet er nærmere beskrevet i *Guide til SoA-dokumentet*.

Styring af informationssikkerhed på et ministerområde

Informationssikkerhedsstyringen i de enkelte organisationer er underlagt departementets tilsyn og indgår som sådan i den samlede koncernstyring. Tilsynet skal være reelt og aktivt. Rigsrevisionen påser dette.

Den enkelte organisation er dog selv ansvarlig for at beskytte sine informationsaktiver. Dette ansvar kan hverken uddelegeres til en leverandør eller til et departement. Med ISO27001 er der dog gode muligheder for at skalere indsatsen, så den er proportional med organisationens størrelse og kompleksiteten af it-anvendelsen.

2. Virkemidler

Virkemidler forstås i denne sammenhæng som alle de forudsætninger i form af processer, materialer, beslutninger, der skal være til stede for at sikre et velfungerende ISMS. I det følgende nævnes de væsentligste:

Ressourcer

Organisationen skal sikre, at der er allokeret tilstrækkeligt med ressourcer til, at de *af ledelsen definerede* informationssikkerhedsmæssige mål kan nås. Det betyder bl.a., at der skal være nok ressourcer til stede til, at informationssikkerhedsindsatsen i praksis er egnet til at understøtte organisationens opgavevaretagelse. Endvidere skal der være ressourcer nok til at sikre, at kontrollerne kan implementeres.

Implementering betyder, at kontrollerne er dokumenteret, at krævede aktiviteter rent faktisk udføres, og at status rapporteres.

Ressourcer bør være eksplicit afsat i budgetter mv. på linje med alle andre omkostninger i organisationen. Dermed bliver det også synliggjort, hvad organisationen bruger på informationssikkerhed.

Kompetencer

Organisationen skal sikre, at den råder over de nødvendige informationssikkerhedsfaglige kompetencer i relation til at styre informationssikkerhed. Det indebærer, at et passende antal medarbejdere skal have den rette uddannelsesmæssige baggrund og erfaring til opgaven med realisering af ledelsens mål for informationssikkerheden. *Jo mere kompleks en organisation og it-anvendelse er, jo større vil kravene til medarbejdere og ledelse være.*

Den samlede pulje af kompetencer, der er til rådighed på et ministerområde vil kunne have betydning for de kompetencer, den enkelte organisation under ministerområdet skal råde over. Det er ikke alle organisationer, som i dag har en it-sikkerhedskoordinator på fuld tid, og nogle af opgaverne kan være fordelt på flere. Det endelige ansvar for en organisations informationsaktiver er dog altid forankret hos ledelsen af organisationen.

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

Awareness og bevidsthed

Awarenessaktiviteter skal sikre, at organisationens medarbejdere har kendskab til og forstår, hvordan de skal agere for at minimere risikoen for sikkerhedshændelser. Det vil sige, at der skal være en bevidsthed omkring beskyttelse af data i organisationen, og at arbejdet med informationssikkerhed prioriteres på alle niveauer.

Aktiviteterne afhænger af den enkelte institution, men som udgangspunkt skal indholdet af informationssikkerhedspolitikken og basale adfærdsnormer i forhold til medarbejdernes omgang med informationsaktiver, herunder it-udstyr, formidles til medarbejderen. Det gælder fx også proces for rapportering af hændelser og sanktionsmuligheder ved overtrædelse af informationssikkerhedspolitikken.

Awarenessaktiviteterne kan med fordel kombineres med interne kurser og lign. Fx kan informationssikkerhed indgå som en fast del af et introduktionsforløb for nye medarbejdere. På Digitaliseringsstyrelsens hjemmeside findes *Guide til awareness om informationssikkerhed*, der giver vejledning i, hvordan man kan udføre awarenessaktiviteterne.

Kommunikation

Kommunikation både internt i organisationen og eksternt til samarbejdspartnere og andre interessenter er væsentlige bestanddele i den daglige drift af ISMS'et. Kommunikation med eksterne parter skal styres stramt, og der bør være præcise retningslinjer på området. Oplysninger om området vil som regel være af fortrolig karakter, som kan afsløre sårbarheder og information om, hvordan kontroller i øvrigt er tilrettelagt. De situationer, der nødvendiggør kommunikation med eksterne parter, 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.

Kommunikation internt i organisationen om informationssikkerhed er awarenessaktiviteter. Derudover skal der etableres rapporteringsprocedurer, så der er tilstrækkelig information til stede, for at ledelsen kan udøve sine beføjelser på et rettidigt og oplyst grundlag.

Rapporteringen bør ske via de eksisterende kanaler for kommunikation af ledelsesinformation. Hvis organisationen har etableret et dedikeret informationssikkerhedsudvalg, skal kommunikationen selvfølgelig 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 kommunikation til medarbejderne. Det er som regel aktuelt ved sikkerhedshændelser, eller hvis der er behov for ændring af en bestemt adfærd eller agtpågivenhed i forhold til fx en ny trussel.

Endelig er der også ledelsens generelle kommunikation til medarbejderne om informationssikkerhed som et vigtigt led i forankringen.

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

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

Dokumentation

Dokumentationen af ISMS'et er et centralt element i dets etablering og drift, om end ikke alt behøver at skulle dokumenteres.

ISO27001 angiver dels, hvilke konkrete dokumenter, der skal være udarbejdet om informationssikkerhedsstyringen, og dels konstaterer ISO27001, at dokumentationsbehovet afhænger af den konkrete organisations størrelse, typer af aktiviteter, kompleksitet og modenhed.

Bruttolisten kan bruges som en nyttig krydsreference, som organisationen kan holde sin informationssikkerhedsdokumentation op imod:

- En dokumenteret informationssikkerhedspolitik, der indeholder målsætninger for informationssikkerhed
- En dokumenteret scoping af ISMS'et
- Dokumenterede retningslinjer for kontroller
- En beskrivelse af risikovurderingsprocessen
- En risikovurderingsrapport
- En plan for håndtering af risici – risikohåndteringsplan
- Procedurer for måling af sikringsforanstaltningers effektivitet
- Et "Statement of Applicability" (SoA)
- Programmer for interne audits
- Rapportering til ledelsen om evaluering af informationssikkerheden og effekten af ISMS, afvigelser og opfølgende handlinger

Følgende form- og proceskrav gælder for dokumentationen:

- Oprettelse og opdatering af dokumenter skal være styret. Det indebærer, at der skal fastsættes en navngivningsstandard, tages beslutning om dokument-metadata og accepterede filformater.
- Der skal være en proces for review og godkendelse af dokumentationen.
- Der skal være et revisionsspor for ændringer.

Dokumentationen skal endvidere være kontrolleret, hvilket betyder:

- Det skal være nemt tilgængeligt for autoriserede brugere
- Det skal beskyttes mod uautoriserede brugere
- Lagringssted, -medier og -metode skal besluttes for såvel digital som papirbåren dokumentation
- Opbevaringsperiode og sletteprocedurer skal være fastlagt.

3. Drift og opfølgning

Driften af ISMS'et omfatter primært det daglige informationssikkerhedsarbejde. Når alle forudsætninger er på plads i form af ledelsesforankring og virkemidler, bliver det muligt at styre informationssikkerheden på en dag-til-dag-basis. Nogle aktiviteter har en særligt fremtrædende plads i denne fase:

- Risikohåndtering, særligt af de risici, som organisationen har valgt selv at kontrollere
- Styring af leverandører, for så vidt angår de risici, hvor organisationen har valgt at flytte (outsource) risikohåndteringen
- Overvågning af alle ændringer (planlagte og ikke planlagte) i omverdenen i bred forstand, der kunne have uønskede konsekvenser for informationssikkerheden.

Standarden stiller endvidere krav om, at der løbende følges op på informationssikkerhedsstyringen.

Organisationen bør derfor iværksætte følgende typer af 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 (metriker) for informationssikkerhed beregnes og rapporteres i henhold til en fastlagt plan. Sådanne målinger kan bl.a. bidrage til at fastslå det aktuelle sikkerhedsniveau, der over tid anvendes som indikatorer for udviklingen af modenheden af informationssikkerhedsstyringen.

Intern audit

Periodisk gennemførelse af intern audit er ligeledes et krav i ISO27001. Mange offentlige organisationer råder ikke over en egentlig intern revision eller auditfunktion, hvilket dog ikke er afgørende. Hensynet bag kravet kan opfyldes ved at lade en uafhængig ekstern part gennemgå ISMS'et med et passende interval. Det tilsyn, departementet 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 scope skal fastlægges, så det bliver undersøgt, om styringen af informationssikkerheden lever op til organisationens egne krav til sikkerhedsniveauet.

Den interne audits observationer og anbefalinger skal dokumenteres til organisationens interne brug.

Ledelsesmæssig opfølgning

Den sidste type 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
- Opfølgning på 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.

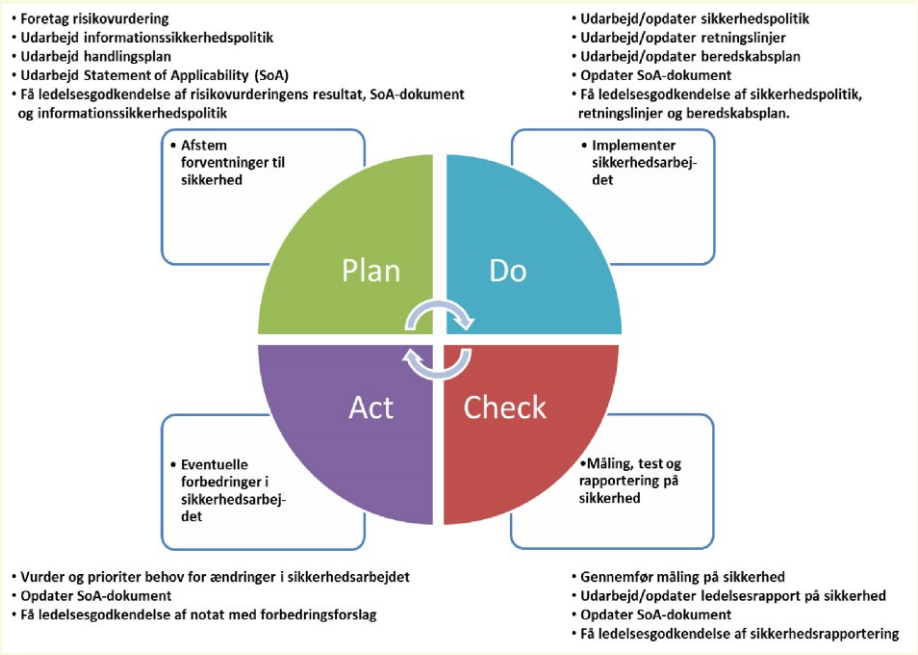
4. Forbedring

Der er primært to områder for forbedring, som organisationen skal fokusere på:

- Den øjeblikkelige håndtering af hændelser og afvigelser, der skyldes svigt i kontroller eller nyopståede trusler og sårbarheder
- Den løbende forbedring af ISMS'et for at optimere organisering, informationsflow, dokumentationskvalitet, forretningsgange mv.

Organisationens håndtering af hændelser og afvigelser skal omfatte en identifikation af årsager og en vurdering af potentialet for gentagelse. Dette skal følges op af handlingsplaner med løbende opfølgning, bl.a. baseret på styring og opfølgning på hændelser.

Figuren illustrerer procesmodellen med referencer til styringsaktiviteterne i standarden.



Den løbende forbedring af selve ISMS'et omfatter alle aktiviteter, der kan optimere arbejdsgange, kommunikation, ressourceforbrug, kvalitet i rapportering osv. 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.

Et velfungerende ISMS er helt overordnet et udtryk for, at der er skabt et samspil mellem styringsaktiviteterne. En ofte benyttet – og effektiv – måde at illustrere en sådan styringsmodel er at sammenholde informationssikkerhedsstyringens væsentligste aktiviteter og leverancer i forhold til en *Plan-Do-Check-Act* procesmodel. Pjecen *Ledelsesforankret Informationssikkerhed* beskriver de væsentligste aktiviteter og udfordringer i hver af disse faser.