DIGITALISERINGSSTYRELSEN

Vejledning i evaluering og opfølgning

Juni 2016

2016

Indhold

Indledning

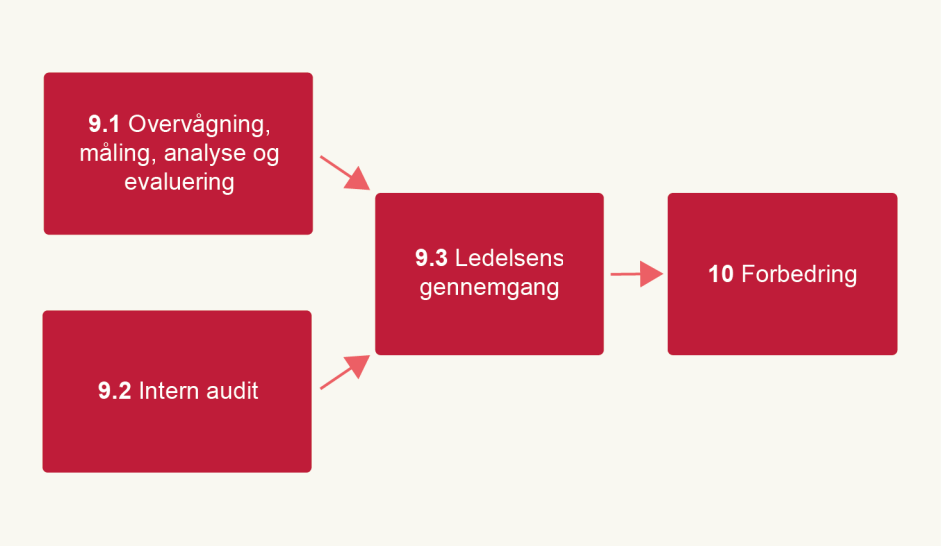
Denne vejledning tager udgangspunkt i Guide til implementering af ISO27001, udgivet af Digitaliseringsstyrelsen i september 2015, og har til formål at give en vejledning i en struktureret tilgang til arbejdet med evaluering og opfølgning af implementeringen af ISO27001

Det er målet med denne vejledning at give læseren metoder og understøttende værktøjer til at kunne evaluere organisationens styring af informationssikkerhed, vurdere værdien af arbejdet med ISO27001 og give input til, hvordan organisationen kan arbejde med forbedringer og opfølgninger på de besluttede aktiviteter.

Vejledningen er inddelt i tre områder:

- Metoder og værktøjer til overvågning, måling, analyse og evaluering
- Metode til gennemførelse af intern audit i organisationen
- Metode til gennemførelse af ledelsens gennemgang.

De to første aktiviteter, måling og audit, genererer input til ledelsens gennemgang.



Alle disse aktiviteter skal danne grundlag for de løbende forbedring af ledelsessystemet for informationssikkerhed. Det er bl.a. gennem disse aktiviteter, at organisationen får fulgt op på de handlingsplaner, der er udarbejdet.[1]

[1] Se vejledning i planlægning af sikkerhedsarbejdet, udgivet af Digitaliseringsstyrelsen i 2016 på digst dk

1. Metoder og værktøjer til overvågning, måling, analyse og evaluering

1.1 Formålet med overvågning, måling, analyse og evaluering

Overvågning, måling, analyse og evaluering af informationssikkerheden er et krav i ISO27001 i forbindelse med evaluering af organisationens ledelsessystem for informationssikkerhed. Formålet er at vurdere, om de implementerede politikker, processer og kontrolforanstaltninger til sikring af organisationens informationer og systemer er effektive i forhold til at opnå de planlagte resultater.

1.2 Overvågning og måling af ledelsessystemet for informationssikkerhed

Organisationen skal fastlægge, hvad værdien og det ønskede resultat skal være af overvågning og måling af ledelsessystemet for informationssikkerhed. Ledelsen spiller en vigtig rolle i at definere værdien af overvågning, målinger og succeskriterierne for de valgte målepunkter, da ledelsen i sin gennemgang af ledelsessystemet for informationssikkerhed skal bruge resultatet til at evaluere styringen af informationssikkerheden i organisationen.

Der kan være stor forskel på, hvad der kan måles, og hvilke muligheder der er for at gennemføre en måling. For en organisation, som er umoden i sin it-understøttelse af informationssikkerheden, kan det være svært og omfangsrigt at implementere og følge op på mange målepunkter. For en moden it-understøttet organisation kan indhentning af måledata automatiseres, og det vil derfor være mere overskueligt at have et større måleprogram. Det er væsentlig at vurdere, hvilket modenhedsniveau organisationen er på, når omfanget af overvågning og målinger bestemmes, således at måleprogrammet bliver tilrettelagt bedst muligt fra starten. Organisationens modenhedsniveau kan for eksempel vurderes ud fra CoBIT's seks modenhedsniveauer[2].

1.3 Tilrettelæggelsen af et måleprogram

Organisationen skal tilrettelægge et måleprogram, som opfylder kravene i ISO27001. Omfanget af måleprogrammet bør bestemmes ud fra organisationens muligheder for at evaluere informationssikkerheden og effekten af ledelsessy-

[2] ISACA's Control Objectives for Information and Related Technology (COBIT)

stemet. Nedenfor gennemgås en række krav, som skal fastlægges og tilrettelægges i det samlede måleprogram.

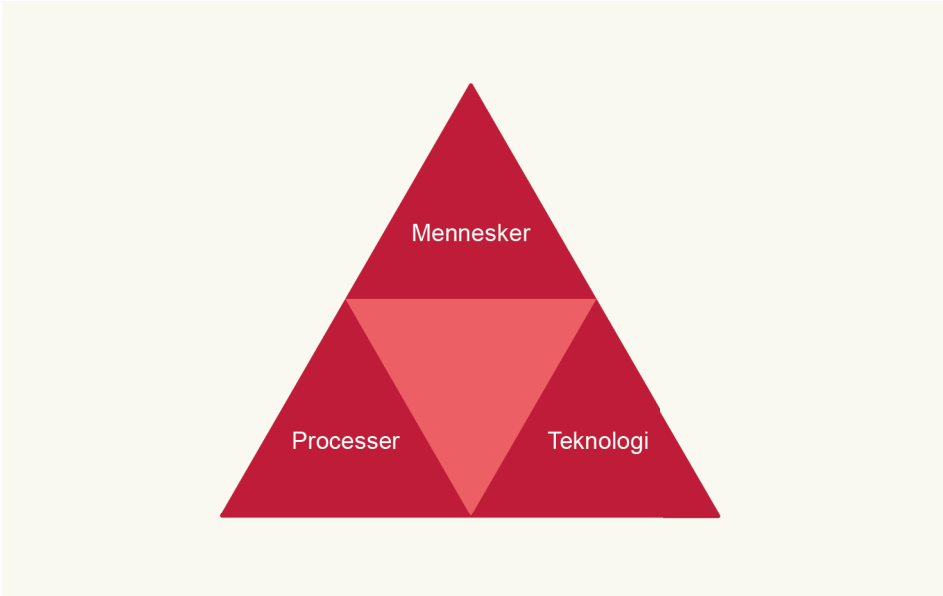
Hvad skal overvåges og måles, og hvilke metoder skal anvendes?

Organisationen skal identificere de områder, som er vigtigst at overvåge for at vurdere effektiviteten af ledelsessystemet. Her er det væsentlig at tage udgangspunkt i de vigtigste forretningsprocesser og identificere disse processers kritiske succesfaktorer.

Hvis beskyttelse af informationers fortrolighed er vigtigt for organisationen, kan en succesfaktor være, at der ingen sikkerhedshændelser har været, som har medført brud på fortroligheden. Der kan således måles på antallet af sikkerhedshændelser i organisationen, der har medført lækage af informationer. Der kan også måles på antallet af medarbejdere, der har gennemført organisationens awarenesstræning med en korrekt besvarelsesprocent på mindst 85 pct. på testspørgsmål om reglerne for informationssikkerhed. I bilag 1 er vist et eksempel på en uddybet beskrivelse af et målepunkts forudsætninger, opbygning og værdi.

Målepunkter kan inddeles i tre kategorier:

- Mennesker
- Processer
- Teknologi



Målepunkter i mennesker kategorien skal sige noget om effektiviteten af de kontrolforanstaltninger, målingen er afhængig af:

- Aktiviteter, der kræver en menneskelig indsats
- En bestemt menneskelig adfærd
- Bestemte menneskers/medarbejderes holdning eller opfattelse
- Virksomhedens kultur

Målepunkter i processer-kategorien skal sige noget om effektiviteten af de kontrolforanstaltninger, der er afhængige af, at bestemte retningslinjer, procedurer eller instrukser beskrives eller udføres.

Målepunkter i teknologi-kategorien skal sige noget om effektiviteten af de kontrolforanstaltninger, der er afhængige af en form for teknologisk understøttelse.

Kilde: Målerpunkter for informationssikkerhed, Center for Cybersikkerhed

Center for Cybersikkerhed har udgivet vejledningen Målepunkter for informationssikkerhed, som organisationen kan tage udgangspunkt i i tilrettelæggelsen og udarbejdelsen af målepunkter.

Hvornår skal overvågningen og målingen udføres, og hvem skal gøre det?

Organisationens årshjul for styring af informationssikkerhed skal indeholde aktiviteter for, hvornår overvågning og målinger skal gennemføres. Frekvensen kan være forskellig, alt efter hvilke målepunkter der identificeres.

Nedenfor ses eksempler på, hvornår målepunkter kan overvåges og måles.

Målepunkt	**Frekvens**
Opdatering af organisationens politikker er sket rettidigt	Årligt
Antallet af sikkerhedsændringer	Månedligt
Antallet af medarbejdere, som har gennemført awareness-træning	Kvartalsvist

Organisationen bør udpege ansvarlige medarbejdere, som skal indsamle måleresultater. I praksis kan det være medarbejdere, som har det daglige driftsansvar for de processer, som organisationen har implementeret for at kunne opfylde kravene til informationssikkerhed. Målingerne afrapporteres til organisationens informationssikkerhedsfunktion, som analyserer og evaluerer målingen og overvågningen.

Funktionsadskillelse skal altid overvejes i denne sammenhæng. Hvis informationssikkerhedsfunktionen har det daglige driftsansvar for processer, der overvåges og måles på, skal organisationen overveje, om der er andre, som enten skal udføre processerne eller alternativt foretage målingerne.

Hvornår skal resultaterne fra overvågningen og målingen analyseres og evalueres, og hvem skal gøre det?

Resultaterne skal løbende analyseres og evalueres i organisationens informationssikkerhedsudvalg. Dette bør være en fast aktivitet på informationssikkerhedsudvalgets agenda, og en del af den faste afrapportering til organisationens topledelse, jf. ISO27001's krav om ledelsens gennemgang.

Resultatet af overvågninger og målinger skal analyseres og evalueres i forhold til de definerede succeskriterier. I praksis kan informationssikkerhedsfunktionen

være ansvarlige for at analysere og evaluere resultaterne, baseret på en fastlagt måleproces.

Måleprocessen kan tilrettelægges i følgende faser, hvor følgende aktiviteter indgår:

1. Fastlæg målepunkter, som skal udgøre måleprogrammet i organisationens ledelsessystem. Informationssikkerhedsfunktionen fastlægger målepunkterne, og deres tærskelværdier bestemmes, baseret på organisationens succesfaktorer. Datagrundlaget for målepunkterne skal være til stede, og succeskriteriet skal være opnåeligt. Hvor teknologi er krævet til at fremskaffe måledata, skal denne være implementeret.
2. Indhent måledata. Informationssikkerhedsfunktionen får indrapporteret måledata. Det er kun data, der er nødvendige for målingen, som skal indhentes. Beregningsmodeller skal være defineret på forhånd i forbindelse med fastlæggelsen af målepunkter. Målingerne kan for eksempel samles i et regneark, som giver det samlede billede af målepunkterne, eventuelle underliggende målepunkter og selve måleresultaterne.
3. Analyser resultatet. Resultaterne analyseres i forhold til de definerede succeskriterier. For hvert målepunkt beregnes resultatet, baseret på beregningsmodellerne, og de definerede tærskelværdier. Resultaterne kan for eksempel rapporteres i værdierne grøn, gul og rød:
   3.1. GRØN: Måleresultatet er over tærskelværdien for accepteret, hvilket indikerer, at processen afvikles som forventet.
   3.2. GUL: Måleresultatet er under tærskelværdien for accepteret, og processen skal overvåges tættere, men det er ikke kritisk for forretningen. Årsagen skal analyseres og evalueres.
   3.3. RØD: Måleresultatet er under tærskelværdien for accepteret, og resultatet indikerer en risiko for forretningen, som skal vurderes og afrapporteres til ledelsen.
4. Rapporter resultatet løbende til organisationens ledelsessystem. Informationssikkerhedsfunktionen skal sikre, at rapportering sker på en genkendelig måde i organisationen, for eksempel ved brug af grønne, gule og røde farver. Rapporteringen skal endvidere indikere, om det går bedre fremad i en positiv retning eller dårligere, eller om situationen er uforandret.

Husk at organisationen skal opbevare hensigtsmæssig, dokumenteret information som bevis for overvågningen og målingen og rapportering af resultatet til organisationens ledelse.

2. Metoder og værktøjer til intern audit

2.1 Formålet med intern audit

Intern audit gennemføres for at identificere, om der er en rød tråd igennem organisationens ledelsessystem for informationssikkerhed, gående fra organisationens risikobillede, topledelsens beslutninger og den overordnede informationssikkerhedspolitik, til de underliggende informationssikkerhedspolitikker og processer, som skal opfylde informationssikkerhedskravene og til de implementerede kontroller. Intern audit skal også afdække, om organisationens ledelsessystem for informationssikkerhed lever op til organisationens egne krav samt kravene i standarden.

Intern audit er en systematisk, uafhængig og dokumenteret proces, som har til formål at fremskaffe beviser eller auditvidnesbyrd, og evaluere disse objektivt for at bestemme, i hvilket omfang auditkriterierne er opfyldt.

Intern audit er ikke at forveksle med revision. En revisor vil stille krav til en meget høj grad af overbevisning og dermed tage mange stikprøver og indsamle megen dokumentation. En it-revisor har fokus på kontroller, der understøtter den finansielle revision. Intern audit er i den sammenhæng mere en review-proces, hvor auditor følger politikker, processer og kontroller til ende og konstaterer, om de er implementeret i organisation og fungerer. Ud over audit og revision, vil der i nogle organisationer ligeledes blive gennemført tilsyn af forskellig slags. Et tilsyn kan have et bestemt emne eller periode, som der er fokus på, og vil i sin natur nok ligne et review mere end en traditionel it-revision.

2.2 Tilrettelæggelse af et auditprogram og en audit plan

Auditprogrammet tilrettelægges efter en struktur, hvor følgende områder er fastlagt:

- Omfanget af den interne audit bestemmes, baseret på ledelsessystemet for informationssikkerhed og kontroller på udvalgte områder
- Identifikation og evaluering af risici for auditprogrammet. Der gennemføres en risikovurdering af, om programmet kan gennemføres som planlagt
- Estimeret timeantal og eventuelt budget for de nødvendige ressourcer
- Målet for den interne audit, omfang og kriterier for hver enkelt audit
- Auditmetoder og sammensætning af auditteamet.

Den interne audit skal planlægges ind i årshjulet for styring af informationssikkerheden. Her kan eksterne audits, it-revisioner og tilsyn tages i betragtning, når planlægningen gennemføres.

Der skal med udgangspunkt i auditprogrammet udarbejdes en auditplan for den konkrete audit.

- Auditplanen skal tage hensyn til status på og vigtigheden af de processer og områder, der skal auditeres, og til resultaterne af tidligere audits.
- Auditplanen bør planlægges i samarbejde med informationssikkerhedsfunktionen og andre relevante interne interessenter i organisationen og godkendes i informationssikkerhedsudvalget.
- Auditplanen skal indeholde målepunkter, som kan give en indikation af, hvorvidt organisationens krav til informationssikkerhed efterleves.
- Den interne audit skal planlægges i god tid, og de involverede ledere, funktioner og områder skal ligeledes orienteres i god tid om auditplanen.
- Auditøren skal, som en del af auditplanen, lave opfølgning på tidligere afvigelser.
- Auditøren skal sende auditplanen til godkendelse i organisationens ledelse.

2.3 Den interne auditors rolle

Den interne auditors rolle er at gennemgå organisationens ledelsessystem for informationssikkerhed med henblik på at identificere, om der er uoverensstemmelser mellem ISO27001-standardens krav og organisationens egne krav på den ene side, og organisationens reelle efterlevelse på den anden side. Rollen omfatter blandt andet, at:

- Finde og løse problemer og afvigelser, inden kunden/borgeren/klienten/brugeren gør det
- Give input til forbedringer af organisationens informationssikkerhed
- Overvåge efterlevelsen af internationale standarder
- Overvåge efterlevelse af kravene til ledelsessystemet for informationssikkerhed.

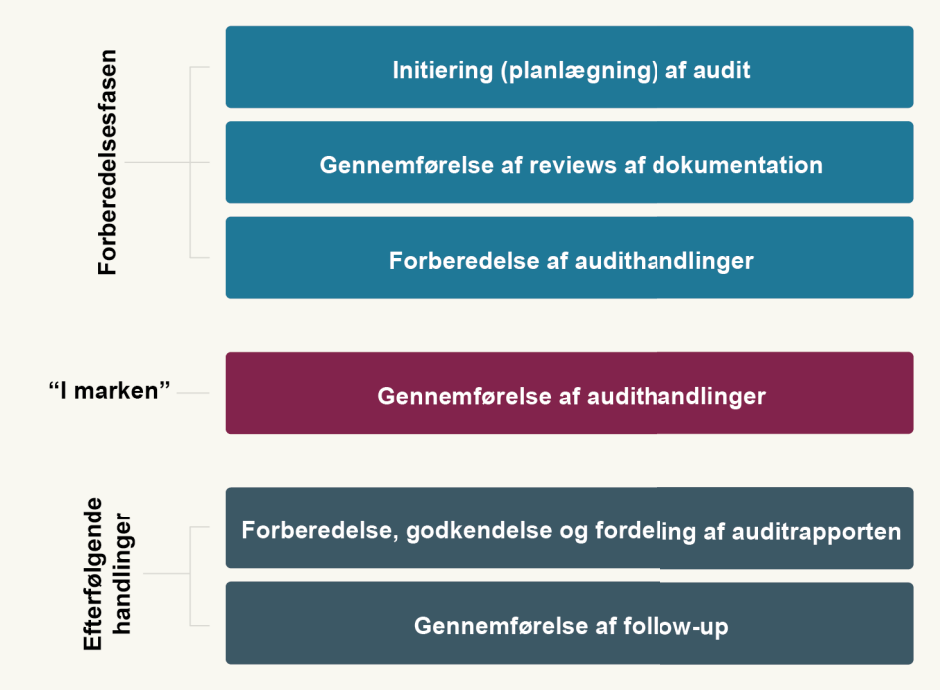
2.4 Hvem kan auditere og hvordan?

Organisationen har et ansvar for at udpege de medarbejdere, som skal gennemføre den interne audit og dermed føre kontrol med, om ledelsessystemet for informationssikkerhed er i overensstemmelse med organisationens egne krav og kravene i ISO27001 og at systemet er effektivt implementeret og bliver vedligeholdt.

De udvalgte medarbejdere skal være uafhængige, dvs. de må ikke lave audit på eget arbejde eller ansvarsområde, eller på anden måde være forhindret i objektiv

og upartisk bedømmelse. De udvalgte medarbejdere skal have god indsigt i organisationens krav til informationssikkerhed, processer, ISO27001 og fokus på forbedringsmuligheder.

Den interne audit kan gennemføres efter følgende proces:



Den interne audit kan udføres og dokumenteres i auditskemaet vist i bilag 2.

2.5 Rapportering til organisationens ledelse

Rapporteringen til organisationens ledelse skal indeholde en samlet analyse og evaluering af den gennemførte audit. Den interne auditor er ansvarlig for, at analysen og evalueringen gennemføres. Afvigelser af særlig kritisk karakter bør rapporteres direkte til ledelsen efter aftale med denne. Auditrapporteringen skal formelt dokumenteres og godkendes af ledelsen.

Informationssikkerhedsfunktionen kan få uddelegeret opgaven med at sikre, at resultaterne af den interne audit rapporteres til organisationens ledelse. Rapporteringen af auditresultater indgår som en del af grundlaget for ledelsens gennemgang af ledelsessystemet for informationssikkerhed.

2.6 Opfølgning på konstaterede afvigelser

Informationssikkerhedsfunktionen er ansvarlig for at initiere en handlingsplan for håndtering af afvigelser og løbende forbedringer, som skal godkendes af Informationssikkerhedsudvalget. Handlingsplanen indgår i ledelsens gennemgang af ledelsessystemet for informationssikkerhed. Handlingsplanen bør indeholde

veldefineret deadline og angivelse af ansvar for udførelse, samt de kriterier, som skal være opfyldt, for at afvigelsen er håndteret. Derudover bør eventuelle behov for økonomiske ressourcer vurderes.

5 gode råd til en intern audit

- Stil åbne spørgsmål og lad auditee tale.
- Vurderer du, at metoden/processen kan følges i praksis?
- Kan auditee dokumentere, at processen er fulgt?
- Kan du, som intern auditor, identificere den røde tråd fra informationssikkerhedspolitikken til metoden/processen?
- Er de højest prioriterede risici fulgt op af en risikohåndteringsplan?

Den interne audit

Politikker, processer og procedurer skal være:

- Designet - hvad gør de?
- Implementeret - hvordan gør de det?
- Operationel effektive - gør de det, de siger, de gør?

3. Metoder og værktøjer for ledelsens gennemgang

3.1 Formålet med ledelsens gennemgang

Ledelsens gennemgang er et krav i ISO27001, og beskrevet i kapitel 9.3 Ledelsens gennemgang. Gennemgangen er en central aktivitet i organisationens sikring af, at implementeringen og driften af ledelsessystemet for informationssikkerhed til stadighed er egnet tilstrækkeligt og effektivt i forhold til organisationens egne målsætninger og kravene i ISO27001.

Formålet med at gennemføre en ledelsesgennemgang er, at topledelsen løbende gennemgår og evaluerer, om organisationens ledelsessystem for informationssikkerhed er effektivt i forhold til de målsætninger for informationssikkerhed, som organisationen har fastsat. Topledelsens gennemgang skal resultere i beslutninger for forbedring af systemet og processernes effektivitet og opgaveløsningen og nødvendige ressourcer. Evalueringen skal ske på baggrund af organisationens målsætninger for informationssikkerhed, interne auditresultater, sikkerhedshændelser, revisionsbemærkninger, afvigelser og korrigerende handlinger, risiko vurderinger og -håndteringsplaner.

Faktaboks

Formålet med ledelsens gennemgang er at gøre topledelsen i stand til at evaluere, om organisationens styring af informationssikkerhed er effektiv og implementere forbedringer. Det kan f.eks. være et ændret risikobillede som følge af et ændret trusselsbillede.

3.2 Hvem har ansvaret?

Det er organisationens topledelse, som har ansvaret for at gennemføre ledelsens gennemgang af ledelsessystem for informationssikkerhed. Ansvaret ligger hos topledelsen, fordi der er tale om et ledelsessystem, som kan have en konsekvens for organisationens formål, hvis dennes informationsaktiver ikke er tilstrækkeligt og effektivt beskyttet mod brud på fortrolighed, integritet og tilgængelighed.

I gennemgangen skal indgå ledelsens evaluering af, hvordan eventuelle ændringer i eksterne og interne forhold vil påvirke ledelsessystemet, herunder et eventuelt ændret trusselsbillede. Derudover om eksterne forhold i form af væsentlige samarbejdspartnere og interessenter, ændringer af lovgivning og i leverandørforhold, kan betyde ændringer i ledelsessystemet for informationssikkerhed. Interne forhold kan ligeledes påvirke informationssikkerheden i form af f.eks. organisationsændringer, ændret medarbejdersammensætning eller økonomiske prioriteringer.

Topledelsen er organisationens øverste ledelse inden for omfanget af ledelsessystemet for informationssikkerhed og vil kunne være direktionen, bestyrelsen, departementschefen mv.

Topledelsen kan uddelegere aktiviteter i forbindelse med gennemgangen til underliggende afdelinger eller områder i organisationen. Afdelinger, som varetager den daglige drift af informationssikkerhed, kan få ansvaret for at indsamle grundlaget for ledelsens gennemgang, supportere gennemførelsen og sikre, at dokumentation foreligger. Ydermere at medvirke til, at handlinger på baggrund af ledelsens beslutning igangsættes. Organisationens informationssikkerhedsudvalg kan gennemføre en rapportering af igangværende aktiviteter i form af organisationens risikohåndteringsplan, auditresultater, styringen af afvigelser og resultater af overvågning og måling og afrapportere konklusioner til topledelsen.

Topledelsens ansvar er at foretage den overordnede evaluering af ledelsessystemet for informationssikkerhed på baggrund af informationssikkerhedsudvalgets evaluering.

Det anbefales, at organisationen beskriver, godkender og dokumenterer ledelsessystemets roller og ansvarsområder i overensstemmelse med ISO27001's krav 5.3 og kontrollen A.6.1.1 i ISO27001 Anneks A.

Organisationen bør overveje informationssikkerhedsudvalgets sammensætning nøje, således at organisationen er bedst muligt repræsenteret, samtidig med at de nødvendige kompetencer er til stede i udvalget til de opgaver, der skal løses. Ligeledes bør det overvejes, at en af organisationens direktører indgår i udvalget med det formål at skabe en ledelsesforankring på højt niveau i organisationen.

3.3 Hvor ofte skal ledelsen gennemgå organisationens ledelsessystem?

Ledelsens gennemgang skal ske løbende og være i overensstemmelse med organisationens behov og organisering af informationssikkerhed. Planlægningen af gennemgangen bør indgå i organisationens samlede styring af informationssikkerhed, som kan udmøntes i et årshjul. Organisationen anbefales at beskrive organisationens organisering af styringen af informationssikkerhed og definere behovet for evaluering af ledelsessystemet for informationssikkerhed. Behovet kan være forskelligt fra organisation til organisation. For eksempel kan der i forbindelse med implementering af ISO27001 i en organisation være et øget behov for rapporteringer til ledelsen om implementeringens fremdrift og omfang, som ledelsen kan evaluere på baggrund af.

3.4 Proces for ledelsens gennemgang

Organisationens informationssikkerhedsfunktion kan i praksis få uddelegeret ansvaret for at supportere processen for ledelsens gennemgang.

En organisation kan tilrettelægge sine aktiviteter i forbindelse med ledelsens gennemgang således:

Proces for ledelsens gennemgang af ledelsessystem for informationssikkerhed

Informationssikkerhedsfunktionen indkalder til ledelsens gennemgang af ledelsessystemet for informationssikkerhed. Funktionen sikrer, at grundlaget for ledelsens gennemgang er til stede i form af:

a. Status på igangværende tiltag vedrørende informationssikkerhed
b. Ændringer i interne og eksterne påvirkninger og tilbagemelding fra interessenter
c. Afrapportering af afvigelser
d. Resultater af målinger og overvågning
e. Resultater af audits, revisions- og tilsynsrapporter mv.

f. Opnåelse af målsætninger og opdateret GAP-analyse
g. Status på risikovurdering og -håndteringsplan
h. Opdateret trusselsbillede og mulige forbedringer.

Informationssikkerhedsudvalget gennemgår status, rapporteringer, målinger og resultater og evaluerer disse. Evalueringen dokumenteres i en rapportering, og der udarbejdes en indstilling til organisationens topledelse, som omfatter forslag til løbende forbedringer og ændringer af organisationens ledelsessystem for informationssikkerhed. Beslutninger, som bliver truffet på baggrund af ledelsens gennemgang af ledelsessystemet for informationssikkerhed, skal dokumenteres.

Beslutninger skal omfatte følgende:

- Løbende forbedringsmuligheder
- Behov for ændringer i ledelsessystemet for informationssikkerhed
- Ressourcer og kompetencer til styring af informationssikkerhed og drift af ledelsessystemet.

Resultatet af ledelsens gennemgang skal kommunikeres til relevante parter i organisationen. I praksis kan informationssikkerhedsfunktionen være ansvarlig for at sikre, at beslutninger er dokumenteret og bliver kommunikeret til relevante parter. Organisationen skal sikre, at beslutningerne bliver udmøntet i konkrete handlinger, som har ledelsens fokus og opbakning. Det er et krav, at ledelsens gennemgange dokumenteres og godkendes.

3.5 Indholdet af ledelsens gennemgang

Ledelsen skal i sin gennemgang af ledelsessystemet for informationssikkerhed overveje og betragte igangværende tiltag og resultater.

Nedenstående punkter kan udgøre en dagsorden for gennemgangen:

1. Status for handlinger fra tidligere gennemgange
2. Gennemgå ændringer i eksterne og interne spørgsmål, som påvirker ledelsessystemet for informationssikkerhed
3. Status på afvigelser og korrigerende handlinger
4. Status på resultater af overvågning og måling
5. Status på audit-, tilsyns- og revisionsresultater
6. Status på opfyldelse af målsætninger for informationssikkerhed
7. Tilbagemelding fra interessenter
8. Resultater af risikovurderingen og status på risikohåndteringsplanen
9. Muligheder for løbende forbedringer.

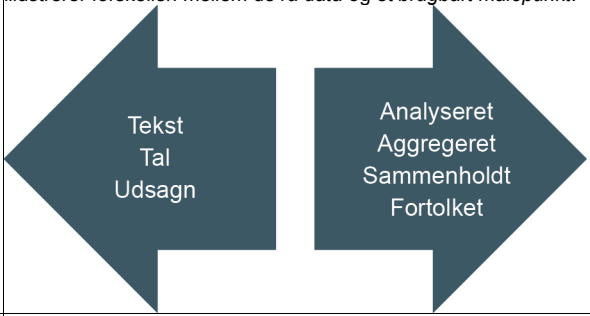
I bilaget bagerst i vejledningen er gengivet et eksempel på et skema, der kan anvendes til ledelsens gennemgang.

Kernespørgsmål for ledelsen kan være

- Er informationssikkerhedspolitikken stadig relevant i relation til det, vi udfører?
- Er roller og ansvar klargjort og giver de mening?
- Tildeles der hensigtsmæssige ressourcer?
- Overholder vi lovpligtige krav?
- Er procedurer klare og hensigtsmæssige? Har vi brug for andre/flere? Skulle vi afskaffe nogle?
- Hvad betyder teknologiske/organisatoriske forandringer for vores ISMS og dets effektivitet?
- Betyder lovgivningsmæssige ændringer, at vi skal ændre noget i vores ISMS?
- Hvilke interessentovervejelser er blevet fremsat siden sidste gennemgang?
- Er der andre måder at gøre tingene på - hvad kan vi ellers gøre for at forbedre ISMS?

Bilag 1. Skabelon for beskrivelse af målepunkter til inspiration

Målepunktsdefinition

Betegnelse for målepunkt	Kort beskrivelse af målepunktet
Roller og ansvar for målepunkt	For hvert målepunkt, virksomheden vælger at anvende, bør det fastlægges, "hvem der gør hvad" i forhold til målingen. Dette kan f.eks. angives i et RACI-paradigme (alternativt I-D O, Informed, Decision, Ownership). (R)esponsible har ansvar for målepunktsbeskrivelsen, herunder fastsættelse af aflæsnings- og rapporteringsfrekvens samt tærskelværdier. R har endvidere det udførende ansvar i forhold til, at målingen udføres. (A)ccountable er sponsor, som skal allokere ressourcer, til at målingen kan udføres, og for at der følges op med korrigerende handlinger, hvis målingen falder uden for tærskelværdierne. Det vil ofte være CIO/it-chef. (C)onsulted er alle de involverede medarbejdere, der bidrager til datagrundlaget for målingen. (I)nformed er alle de medarbejdere, der modtager rapportering omkring målingen. I defineringen af de 22 indikatorer er I som eksempel både tildelt bestemte rolleindehavere (f.eks. CEO) og organisatoriske strukturer (f.eks. "it-sikkerhedsudvalget"). Den enkelte virksomhed skal overveje dette på baggrund af sin organisatoriske opbygning.
Type måling	- Objektiv måling - baseret direkte på en observeret værdi (målbar). - Subjektiv måling - udtryk for en menneskelig (subjektiv) vurdering af observationens betydning.
COBIT proces, som målepunktet vedrører	Henvisning til relevant COBIT-proces.
Sikkerhedsområde fra ISO/IEC 27002:2013, som målepunktet vedrører	Henvisning til relevant sikkerhedsområde fra ISO/IEC 27002:2013
Register / database / fortegnelse / person, hvorfra målingen skal aflæses	Her angives kilden(erne), som indeholder datagrundlaget til at generere målepunktet. Datagrundlaget kan være genereret løbende, men kan også være resultatet fra punktvise aktiviteter (f.eks. resultat fra awareness-kampagne).
Værdi/attribut, der skal trækkes fra systemerne og eventuel beregningsmetodik	En mere præcis angivelse af, hvilke specifikke data, der skal trækkes fra systemerne, samt eventuelt en angivelse af, hvorledes data skal behandles for at nå frem til den endelige måling. Følgende nøgleord illustrerer forskellen mellem de *rå data* og et *brugbart målepunkt*. 
Frekvens for aflæsning	Her angives aflæsningsfrekvens for data.
Ønsket tendens	Her angives, om målingen bør være stigende, faldende eller stabil over

	tid. Hvis der er en target-værdi (mål), angives denne også.
Tærskelværdier	Angivelse af tærskler over eller under hvilke, der bør iværksættes korrigerende handlinger.
Frekvens for rapportering	Data er ikke nødvendigvis sammenfaldende med aflæsnings frekvens. Det angives, hvem der rapporteres til i henhold til RACI.

Bilag 2. Auditskema til inspiration

Auditskema

Dato for gennemførelse	dd.mm.åååå
Auditør	[Indsæt navn]
Referent	[Indsæt navn]

Kontrol eller proces	A xx.xx.xx
Ansvarlig forretningsfunktion	[Indsæt funktionens navn]
Reference til krav	[Indsæt reference til ISO eller lign.]

Beskriv formål Eksempelvis: Formålet med denne audit er, at vurdere hvorvidt processen er i overensstemmelse med organisationens egne krav til sit ledelsessystem for informationssikkerhed (ISMS), kravene i ISO270001:2013 samt om processen er effektivt implementeret og vedligeholdt.

Konklusion [Her beskrives kort den samlede vurdering inkl. placeringen på den anvendte skala. Eksempelvis: ”Det vurderes, at processen forvaltes på en ***tilfredsstillende*** måde. I vedlagte bilag dokumenteres hvorledes processen er styret.”]

Vurderingsskema

Auditspørgsmål ***Styring og ressourcer***	**Ja/Nej**	**Bemærkninger og referat til dokumentation**
Er processen formelt beskrevet?		
Er processen formelt godkendt?		
Er ledelsens roller og ansvar formelt beskrevet og forankret?		
Er medarbejdernes roller og ansvar formelt beskrevet og forankret?		
Er opgaven formelt budgetteret, her- under er der afsat økonomi og ressourcer til løsning af opgaven?		
Del vurdering		**<J = Tilfredsstillende** **<N = Ikke tilfredsstillende**

Implementering og drift

Lever kontrolforanstaltningen op til kravene i ISMS'et?		
Lever processen op til kravene i ISO27001:2013?		
Er de nødvendige processer og instrukser beskrevet og opdateres disse som beskrevet i ISMS'et?		
Kan der påvises en tilstrækkelig implementering, eksempelvis afholdelse af workshops for medarbejdere og ledelse?		
Har processen en tilstrækkelig kvalitet?		
Vurderer auditee, at medarbejderne har de tilstrækkelige kompetencer til at løse opgaven?		
Del vurdering		**<J = Tilfredsstillinde** **<N = Ikke tilfredsstillende**

Efterlevelse og rapportering

Kender ledelsen og medarbejderne politikken, processen og instrukser?		
Følges politikken, processen og instrukser?		
Kan væsentlige aktiviteter dokumenteres?		
Bygger dokumentation på tilstrækkelige registreringer (bevisførelse) for efterlevelsen?		
Rapporteres indsats og resultat til ledelse og/eller andre interessenter, som beskrevet i ISMS'et?		
Del vurdering		
Samlet vurdering		**<J = Tilfredsstillende** **<N = Ikke tilfredsstillende**

Ansvarlig funktionsleder		[Indsæt navn]	
I forhold til ovenstående vurdering er jeg:			
Meget enig	**Enig**	**Uenig**	**Meget uenig**

Bemærkninger hvis funktionslederen er enig/uenig
[Indsæt bemærkninger]

Auditørens anbefalinger
[Indsæt anbefaling]

Bilag 3. Ledelsens gennemgang – skema til inspiration

<table>
<tr><td colspan="3">Ledelsens gennemgang af [Indsæt organisationens navn] ledelsessystem for informationssikkerhed</td></tr>
<tr><td colspan="3">Dagsorden
1. Status for handlinger fra tidligere gennemgange
2. Gennemgå ændringer i eksterne og interne spørgsmål, som påvirker ledelsessystemet for informationssikkerhed Status på afvigelser og korrigerende handlinger
3. Status på resultater af overvågning og måling
4. Status på audit-, tilsyn- og revisionsresultater
5. Status på opfyldelse af målsætninger for informationssikkerhed
6. Tilbagemelding fra interessenter
7. Resultater af risikovurderingen og status på risikohåndteringsplanen
8. Muligheder for løbende forbedringer</td></tr>
<tr><td colspan="3">Dato</td></tr>
<tr><td>Deltagere
[Indsæt navneliste]</td><td>Deltager
(sæt kryds)</td><td>Deltager ikke
(sæt kryds)</td></tr>
<tr><td rowspan="3">1</td><td colspan="2">Status for handlinger fra tidligere gennemgange</td></tr>
<tr><td colspan="2">Input:
- Tidligere referat fra ledelsens evaluering
- Liste med status over igangværende initiativer i relation til ledelsessystemet for informationssikkerhed</td></tr>
<tr><td colspan="2">Referat:</td></tr>
<tr><td colspan="3">Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:</td></tr>
<tr><td rowspan="3">2</td><td colspan="2">Gennemgå ændringer i eksterne og interne spørgsmål, som påvirker ledelsessystemet for informationssikkerhed</td></tr>
<tr><td colspan="2">Input:
- Ændringer i lovgivning
- Ændringer i leverandørforhold
- Organisatoriske ændringer</td></tr>
<tr><td colspan="2">Referat:</td></tr>
<tr><td colspan="3">Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:</td></tr>
<tr><td rowspan="2">3</td><td colspan="2">Status på afvigelser og korrigerende handlinger</td></tr>
<tr><td colspan="2">Input:</td></tr>
</table>

	- Organisationens risikolog
	Referat:
	Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:
4	**Status på resultater af overvågning og måling**
	Input:
	Referat:
	Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:
5	**Status på audit-, tilsyns- og revisionsresultater**
	Input: - Auditrapport - Tilsynsrapport - Revisionsrapport
	Referat:
	Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:
6	**Status på opfyldelse af målsætninger for informationssikkerhed**
	Input: - Målsætninger for informationssikkerhed (ISO27001 Krav 6.2)
	Referat:
	Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:
7	**Tilbagemelding fra interessenter**
	Input: - Kundedialoger og -klager - Input fra samarbejdspartnere - CFCS, Digitaliseringsstyrelsen vedrørende informationssikkerhed
	Referat:

	Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:
8	**Resultater af risikovurderingen og status på risikohåndteringsplanen**
	Input: - Risikovurderingsrapport - Risikohåndteringsplan - Resultater af risikovurderingen - Status risikohåndteringsplanen
	Referat:
	Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:
9	**Muligheder for løbende forbedringer**
	Input:
	Referat
	Beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ledelsessystemet for informationssikkerhed:

Godkendt (navn og dato)
Version og placering af dokumentet

digst.dk