DIGITALISERINGSSTYRELSEN

Vejledning i planlægning af sikkerhedsarbejdet

Juni 2016

2016

DIGITALISERINGSSTYRELSEN

Vejledning i planlægning af sikkerhedsarbejdet

Juni 2016

2016

Denne publika ion er udarbejdet af
Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K
Telefon 33 92 52 00
digst@digst dk

Design: Bgraphic
Foto: Colourbox

Elektronisk publikation:
ISBN: 987-87-93073-18-0

Publikationen kan hentes på
Digitaliseringsstyrelsens hjemmeside
www.digst.dk

Indledning

For at sikre, at de rette instrumenter til styring er til stede, er det vigtigt at informationssikkerhedsarbejdet planlægges, og at roller og ansvar for gennemførelse af de planlagte og ikke- planlagte aktiviteter er fordelt.

Formålet med denne vejledning er at give anvisninger på, hvordan denne opgave kan løses, og hvordan arbejdet med styring af informationssikkerheden kan planlægges og integreres i organisationens daglige drift.

Implementeringen af et passende niveau af informationssikkerhed gennem eksempelvis ISO27001 er et stort arbejde[1]. Først undervejs går det op for de fleste, at arbejdet ikke stopper, når implementeringen er gennemført. Det egentlige arbejde med at drive og vedligeholde informationssikkerheden starter faktisk først her. Et arbejde, der kræver styring, indsigt og overblik. Herved skabes grundlaget for at igangsætte aktiviteter de steder, hvor beskyttelsen af aktiverne enten skal korrigeres eller forbedres.

Der kan være situationer, hvor det er helt centralt, at der reageres hurtigt, og arbejdet med informationssikkerheden skal derfor tilrettelægges, så der tages højde for organisationens kontekst. Arbejdet er derfor heller ikke en "engangsforestilling", men derimod en iterativ proces, hvor samme aktiviteter gentages over tid, nye kommer til og andre udgår.

[1] Guide til implementering af ISO27001 Udgivet af Digitaliseringsstyrelsen i september 2015 på digst dk

1. Ledelsesforankring er en forudsætning

At implementere ISO27001 i en organisation er en strategisk beslutning, og for at opnå et passende niveau af informationssikkerhed kræves der en solid ledelsesforankring. Ledelsen skal både være med til at træffe beslutninger af sikkerhedsmæssig karakter og beslutninger om, hvordan selve ledelsessystemet skal drives.

Ledelsen skal tydeligt støtte arbejdet med informationssikkerheden for eksempel ved, at:

- Etablere en organisatorisk struktur, hvor informationssikkerhed behandles på ledelsesniveau
- Offentligt udtrykke vigtigheden af, at organisationen arbejder seriøst med informationssikkerhed
- Tilføre de nødvendige ressourcer til arbejdet med informationssikkerheden i form af økonomi og kompetent personale
- Gå forrest med gode eksempler på, hvordan informationssikkerheden udføres i praksis.

Governancestruktur

En af grundstenene i succesfuld drift af et ledelsessystem for informationssikkerhed, er en organisatorisk struktur, hvor informationssikkerhed behandles på ledelsesniveau. Det praktiske arbejde med informationssikkerheden uddelegeres til kompetente medarbejdere i organisationen, men disse arbejder ud fra retningslinjer, instrukser og konkrete opgaver udstukket af ledelsen.

Med ledelsen forstås en tværorganisatorisk gruppe af ledere, der har kompetencerne til at træffe de nødvendige beslutninger - også når truslerne er alvorlige, og konsekvenserne er store.

Organisering

Ledelsens opbakning til informationssikkerheden og arbejdet hermed fremhæves flere gange i ISO27001. Det er derfor afgørende, at der implementeres en organisering af informationssikkerheden, hvor ledelsen får en central og aktiv rolle.

Det betyder ikke, at ledelsens indsats i forbindelse med informationssikkerheden skal foregå som en særlig og isoleret aktivitet. Tværtimod kan det være meningsfyldt og fremmende for arbejdet at tage udgangspunkt i den eksisterende organisering og forretningsgange.

Der kan oprettes et særligt udvalg, hvor lederne kun behandler informationssikkerhed, men det kan i nogle situationer vise sig mere praktisk at få informationssikkerhed på dagsordenen i et eksisterende udvalg, hvor lederne alligevel er samlet. På denne måde bringes informationssikkerhed op på et niveau med alle andre emner, som ledelsen behandler.

Informationssikkerhedsudvalget, der i det daglige varetager den ledelsesmæssige opgave i forhold til at drive og vedligeholde informationssikkerheden, bør arbejde ud fra et dokumenteret og godkendt kommissorium. Afholdelsen af møder kan dog sagtens falde ind i en eksisterende møderække, hvor deltagerne i informationssikkerhedsudvalget mødes i anden sammenhæng.

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.

Input til og output fra informationssikkerhedsudvalget behandles af organisationens informationssikkerhedsfunktion, som i praksis udfører opgaverne. Denne funktion har til opgave at drive de planlagte (og ikke-planlagte) aktiviteter og fungerer typisk også som en sekretærfunktion i informationssikkerhedsudvalget.

For at forstå, hvem der har hvilke roller og ansvar i en organisering af informationssikkerheden, skal det klart defineres, hvem der gør hvad. Her kan eksempelvis RACI-modellen være en hjælp, da den bidrager til at definere roller og ansvar.

Responsible	• Den person, der faktisk udfører opgaven og er ansvarlig for, at den udføres.
Accountable	• Den person, der i sidste ende er ansvarlig for, at opgaven udføres på passende vis. "The responsible person" refererer til denne person.
Consulted	• Denne person er ikke direkte involveret i udførelsen af opgaven, men konsulteres, og er typisk en ekspert på området.
Informed	• Denne person er ikke involveret i udførelsen af opgaven, men har et behov for at blive informeret herom.

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. Se beskrivelse af roller og ansvar i ledelsessystemet på side 10.

2. Samarbejde med forretningens afdelinger og områder

Det ledelsesmæssige lag i organisationen behandler og afklarer overordnede spørgsmål om informationssikkerheden, mens de underliggende lag håndterer de konkrete aktiviteter på baggrund af ledelsens beslutninger. Det er således ikke informationssikkerhedsfunktionen, der alene udfører det praktiske arbejde.

Informationssikkerheden er en tværgående disciplin, der stort set involverer alle funktioner, der har kontakt med organisationens informationer, lige fra HR-funktionen, der anmoder om adgangsrettigheder til nye medarbejdere, til indkøbsfunktionen, der skal stille informations-sikkerhedsmæssige krav i udbud. Størstedelen af arbejdet med informationssikkerheden udføres således ikke af hverken ledelsen eller informationssikkerhedsfunktionen, men af alle de mange medarbejdere i funktioner og afdelinger, der hver eneste dag bidrager til at fast-holde et passende informationssikkerhedsniveau i organisationen.

I afsnittet ”Aktiviteter i et ledelsessystem for informationssikkerhed” beskrives et eksempel på, hvordan et ledelsessystem for informationssikkerhed kan organiseres, herunder hvordan

relationen mellem ledelse, informationssikkerhedsfunktionen og medarbejdere i forretningen kan koordineres.

Uddannelse og sikkerhedsbevidsthed

Medarbejderne i hele organisationen skal uddannes og vejledes i, hvilke regler for informationssikkerhed der generelt er i organisationen og de regler, der gælder specifikt for deres arbejdsområde.

Derudover skal medarbejderne være vidende om, hvordan de observerer og håndterer mulige brud på informationssikkerheden, og endelig skal de informeres om nye relevante regler og tiltag.

Digitaliseringsstyrelsen har udgivet en guide til awareness om informationssikkerhed, og Statens informationssikkerhedsforum har etableret et bibliotek med awarenessmateriale, der frit kan anvendes af medlemmerne. Guiden findes på www.digst.dk og biblioteket på www.digitaliser.dk.

Endvidere indeholder Statens fælles læringsløsning Campus et kursus i generel informationssikkerhed, der kan gennemføres af alle medarbejdere i staten. Formålet med dette kursus er at skabe awarness omkring informationssikkerhed og medvirke til at styrke de vaner, der understøtter en god informationssikkerhed i en organisation.

3. Aktiviteter i et ledelsessystem for informationssikkerhed

Et ledelsessystem for informationssikkerhed er et ledelsessystem på lige fod med eksempelvis økonomi, produktion og HR, som mange organisationer allerede kender. Ledelsessystem for informationssikkerhed er nærmere defineret i Digitaliseringsstyrelsens "Vejledning i informationssikkerhedsstyring (ISMS) ".

I relation til planlægning af informationssikkerhedsarbejdet er de centrale elementer i et ledelsessystem for informationssikkerhed, at ledelsen bliver i stand til at styre håndteringen af:

- Forskellige typer af afvigelser, herunder bl.a. sikkerhedshændelser
- Korrigerende handlinger
- Opfølgning
- Løbende forbedringer.

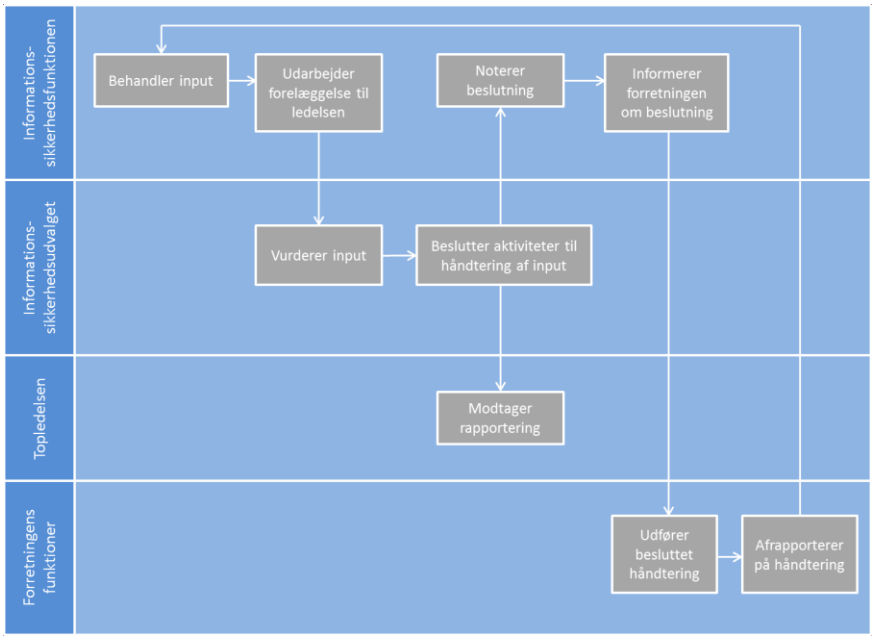
En forudsætning herfor vil være en organisering af arbejdet med informationssikkerheden, der tager højde for den kontekst, organisationen befinder sig i og en styring af både tilbagevendende og enkeltstående aktiviteter.

Ledelsessystem for informationssikkerhed består ikke kun af ledende medarbejdere. I et ledelsessystem for informationssikkerhed inddrages alle funktioner i organisationen, der arbejder med informationer, da disse kommer med input vedrørende afvigelser til informationssikkerhedsudvalgets arbejde, løser opgaver, bidrager med viden mv. Funktionerne i organisationen kan, afhængigt af situationen, derfor både have forskellige roller i forhold til RACI-modellen, mens udvalget og topledelsens roller er mere konstante.

	Responsible	Accountable	Consulted	Informed
Topledelsen		X		
Informationssikkerhedsudvalget		X		
Informationsikkerhedsfunktionen	X		X	X
Funktioner i forretningen	X		X	X

Nedenfor vises et eksempel på et proces-flow i et ledelsessystem for informationssikkerhed. Her optræder rollerne Topledelsen, Informationssikkerhedsudvalget, Informationssikkerhedsfunktionen og funktioner i forretningen. Rollen "funktioner i forretningen" er en bred definition,

der rummer alle de dele af organisationen, der arbejder med informationer eller på anden måde kan påvirke informationssikkerheden.



Som input til proces-flowet er nedenfor en liste, der er opdelt i overordnede kategorier med tilhørende eksempler. Listen er alene at betragte som eksempler, og er ikke at betragte som fuldstændig.

Eksempler på input til ledelsessystem for informationssikkerhed

Elementer fra årshjulet

- Resultater fra risikovurderinger
- Resultater fra interne audits
- Politikker til godkendelse.

Elementer fra årsplanen

- Planlægning og godkendelse af tests
- Planlægning og godkendelse af projekter
- Udarbejdelse af nye metoder.

Eksterne input

- Bemærkninger fra Rigsrevisionen
- Alerts/varslinger
- Ændringer i trusselsbilledet.

Roller og ansvar i ledelsessystemet for informationssikkerhed

Informationssikkerhedsfunktionen – Behandler input og vurderer, om disse er relevante til behandling hos informationssikkerhedsudvalget. Input, der vurderes relevante, forelægges informationssikkerhedsudvalget, og den efterfølgende beslutning dokumenteres. Det er også informationssikkerhedsfunktionen, der informerer relevante funktioner om informationssikkerhedsudvalgets beslutninger. Efter funktionernes behandling af inputtet, modtager informationssikkerhedsfunktionen en tilbagemelding fra funktionen om de gennemførte aktiviteter, omkring i hvilket omfang de har fulgt anvisningen fra informationssikkerhedsudvalget, og om aktiviteten er gennemført succesfuldt.

Informationssikkerhedsudvalget – Vurderer inputtet og træffer en overordnet beslutning om, hvorledes og af hvem, hvilke aktiviteter skal udføres. Udvalget godkender ligeledes politikker, overordnede procedurer samt risikovurderingens resultater og risikohåndteringsplaner.

Forretningens funktioner – Udfører de aktiviteter, som informationssikkerhedsudvalget beslutter, og afrapporterer efterfølgende til informationssikkerhedsfunktionen omkring, om den gennemførte aktivitet har fulgt informationssikkerhedsudvalgets anvisning, og om aktiviteten er gennemført succesfuldt.

Nedenfor er eksempler på elementer i et kommissorium og eksempel på en dagsorden for informationssikkerhedsudvalget.

Kommissorium

- Baggrund
- Informaitonssikkerhedsudvalgets medlemmer
- Ansvar og opgaver
- Rapportering
- Møder i Informaitonss kkerhedsudvalget
  - Frekvens
  - Dagsorden
- Varetagelse af sekretariatsfunktion

Dagsorden

- Godkendelse af dagsorden
- Godkendelse af referat fra sidste møde
- Status på igangværende arbejder
- Opfølgning på informationss kkerhedshændelser siden sidst
- Håndterede afvigelser siden sidst
- Nye afvigelser
- Ændringer i trusselsbilledet
- Godkendelse af nye eller opdaterede politikker
- Eventuelt

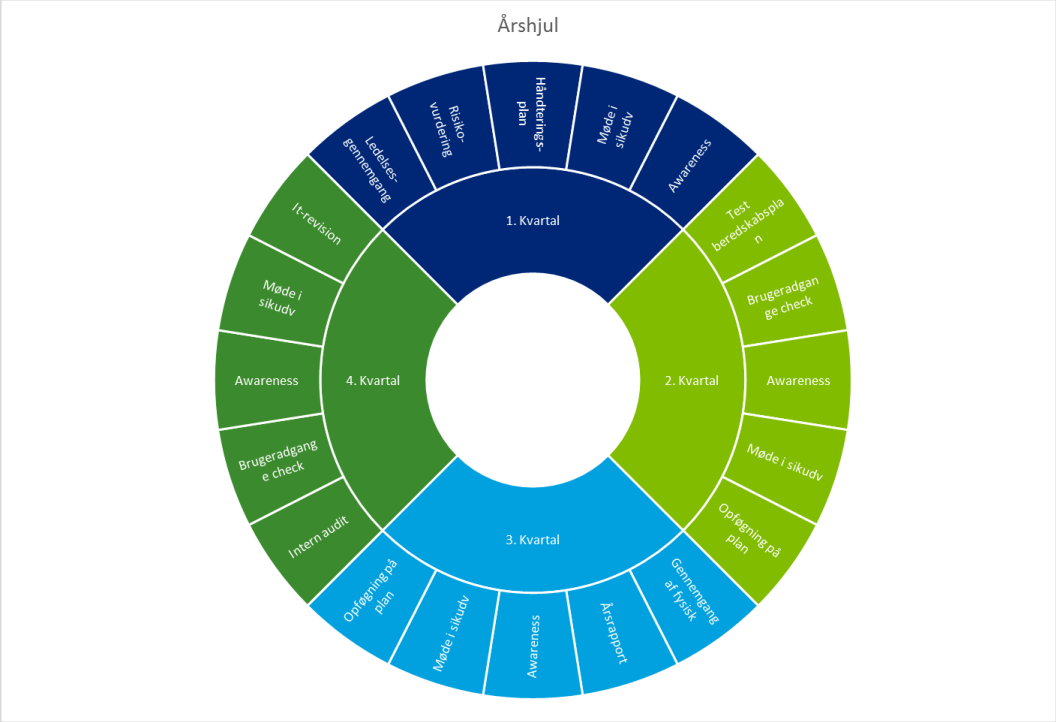
4. Årshjul og årsplan

For at styre informationssikkerheden og for sikre, at ledelsen har de rette styringsværktøjer, gentages en række aktiviteter løbende år efter år, mens andre er enkeltstående aktiviteter. Aktiviteter, der gentages, kan placeres i et årshjul med det formål at illustrere årets aktiviteter simpelt og overskueligt. Nedenfor vises et eksempel på et årshjul og dets indhold. Enkeltstående aktiviteter kan også placeres i årshjulet, hvis de skal gennemføres i indeværende år.

Forskellen på årshjulet og årsplanen:

Årshjulet	Indeholder aktiviteter, der skal gentages med passende tidsintervaller. De er ikke i sig selv en sikkerhedsforanstaltning, men er ofte aktiviteter, der har karakter af opfølgning, evaluering, møder eller lignende. Alt sammen aktiviteter, der skal sikre, at den gennemførte indsats er tilstrækkelig. Det er ofte gennem disse aktiviteter, at der kan identificeres forbedringspotentialer og dermed opgaver til årsplanen eller risikohåndteringsplanen.
Årsplanen	Indeholder aktiviteter til forbedring af ledelsessystemet for informationssikkerhed, kontroller, sikringsforanstaltninger, processer eller lignende. Den indeholder aktiviteter, der afsluttes, og som ikke har behov for at blive gentaget, før der igen er identificeret et forbedringspotentiale. En årsplan behøver ikke kun dække et år, den kan sagtens løbe over f.eks. tre eller fem år. Årsplanen og risikohåndteringsplanen kan med fordel slås sammen.

Nedenfor er vist et eksempel på en skabelon til et årshjul.



Eksempler på aktiviteter, der med fordel kan lægges i årshjulet:

- **Risikovurdering**. Organisationens risikovurdering skal gentages med planlagte mellemrum.
- **Risikohåndteringsplan**. Den periodiske risikovurdering giver anledning til, at risikohåndteringsplanen skal opdateres, som følge af det ændrede risikobillede. Hvis risikobilledet ikke har ændret sig, skal organisationen stadig tage stilling til, om risikohåndteringsplanen stadig er dækkende for at opnå et passende sikkerhedsniveau.
- **Opfølgning på risikohåndteringsplanen**. Organisationen skal følge op på, om der er fremdrift i de indsatser, der er beskrevet i risikohåndteringsplanen.
- **Opfølgning på målinger**[2]. Hvis organisationen har valgt at gennemføre målinger af sikkerheden, skal der følges op på målingerne, for at se, om sikkerhedsniveauet bevæger sig i den ønskede retning.
- **Intern audit**. Der skal gennemføres intern audit med planlagte mellemrum.

[2] For vejledning i måling, audit og ledelsesgennemgang, se Vejledning i evaluering og opfølgning Udgivet af Digitaliseringsstyrelsen 2016 på digst dk

- **Ledelsesgennemgang af ledelsessystem for informationssikkerhed**. Ledelsen skal med planlagte mellemrum gennemgå organisationens ledelsessystem for informationssikkerhed for at vurdere, om det er passende i forhold til forretningsmål, eksterne og interne interessenter, den risiko organisationen står over for, de ressourcer, der anvendes, og andre input fra organisationen. Samtidig skal ledelsen vurdere muligheden for at forbedre ledelsessystemet for informationssikkerhed.

- **Ledelsesrapportering**. Informationssikkerhedsmedarbejderne skal med planlagte mellemrum rapportere om sikkerhedstilstanden i organisationen.

- **Awareness**. Den bevidsthed, medarbejderne skal have om egen rolle i sikkerhedsarbejdet, skal holdes ved lige. Det kan med fordel gøres ved planlagte aktiviteter gennem året.


1
2
3
4
5
digst.dk