DIGITALISERINGSSTYRELSEN

Vejledning i planlægning af sikkerhedsarbejdet

August 2021

2021

Indholdsfortegnelse

Formålet med denne vejledning er, at beskrive hvordan du kan planlægge arbejdet med at styre informationssikkerheden i din organisation. Vejledningen gennemgår:

- Hvordan du skaber ledelsesforankring af informationssikkerhedsindsatsen
- Hvordan du sikrer, at sikkerheden koordineres på tværs af organisationen
- Hvordan du fordeler roller og ansvar i forhold til sikkerhedsarbejdet
- Hvordan du systematiserer arbejdet med informationssikkerhedsstyringen i et årshjul

Vejledningen er til dig, der har til opgave at koordinere og styre informationssikkerheden i din organisation. Du kan fx være leder med ansvar for Informationssikkerhed, informationssikkerhedskoordinator eller databeskyttelsesrådgiver (DPO).

Her kan du læse mere: Hent rejsefortælling om funktioner roller og ledelse i informationssikkerhed; 'Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed.

1. Indledning

At etablere et ledelsessystem for informationssikkerhed (ISMS), fx gennem implementering af ISO 27001-standarden, er et omfattende arbejde. Undervejs går det op for de fleste, at arbejdet ikke stopper, når ledelsessystemet er etableret. Efter etableringen kommer den løbende implementering, evaluering og forbedring af ledelsessystemet for informationssikkerhed og derigennem informationssikkerheden som sådan.

Formålet med denne vejledning er derfor at beskrive, hvordan du kan planlægge det daglige arbejde med at styre informationssikkerheden i din organisation. Vejledningen gennemgår:

- Hvordan du skaber ledelsesforankring af informationssikkerhedsindsatsen
- Hvordan du sikrer, at sikkerheden koordineres på tværs af organisationen
- Hvordan du fordeler roller og ansvar i forhold til sikkerhedsarbejdet
- Hvordan du systematiserer arbejdet med informationssikkerhedsstyringen i et årshjul

2. Ledelsesforankring

At implementere et ledelsessystem for informationssikkerhed kræver solid ledelsesforankring. Ledelsen skal tydeligt støtte arbejdet med informationssikkerheden ved for eksempel at:

- Etablere en organisatorisk struktur, hvor informationssikkerhed behandles på ledelsesniveau
- Ved passende lejligheder udtrykke vigtigheden af, at organisationen arbejder seriøst med informationssikkerhed
- Tilføre de nødvendige ressourcer til arbejdet med informationssikkerheden i form af økonomi og personale med de påkrævede sikkerhedskompetencer
- Skabe grundlaget for processer som tilgodeser, at informationssikkerhed indarbejdes i analyse, design, udvikling, anskaffelse, implementering og anvendelse af informationsaktiver på tværs af organisationen
- Gå forrest med gode eksempler på, hvordan informationssikkerheden udføres i praksis.

Organisering
Det praktiske arbejde med informationssikkerheden uddelegeres til medarbejdere i organisationen. Disse arbejder ud fra retningslinjer og instrukser udstukket af ledelsen. Nedenfor ses en oversigt over de væsentligste roller i informationssikkerhedsstyringen:

Eksempler på rollefordeling i sikkerhedsarbejdet

Informationssikkerhedsfunktionen - Udfører det praktiske og rammesættende sikkerhedsarbejde såsom at udføre risikovurderinger, udvælge sikkerhedsforanstaltninger til SoA-dokumentet, rådgive om sikkerhed, igangsætte awareness-aktiviteter og sikre compliance. Informationssikkerhedsfunktionen har desuden til opgave at beslutte, hvilke input der skal forelægges informationssikkerhedsudvalget. Input, der vurderes relevante, forelægges informationssikkerhedsudvalget, og den efterfølgende beslutning dokumenteres. Det er også informationssikkerhedsfunktionen, der informerer relevante funktioner om informations-sikkerhedsudvalgets 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 input 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.

Ledelsens indsats i forbindelse med informationssikkerheden behøver ikke foregå som en aktivitet, der udføres isoleret fra de øvrige aktivitet, som bør have ledelsens opmærksomhed. Tværtimod er det ofte meningsfyldt og fremmende for informationssikkerhedsarbejdet at tage udgangspunkt i den eksisterende organisering og forretningsgange. Man kan fx oprette et særligt udvalg, hvor lederne kun behandler informationssikkerhed. Alternativt kan det i nogle situationer vise sig mere praktisk at få informationssikkerhed på dagsordenen i et eksisterende udvalg eller mødeforum, hvor lederne alligevel er samlet. På denne måde bringes informationssikkerhed op på niveau med alle andre emner, som ledelsen behandler.

Informationssikkerhedsudvalget, eller den gruppe ledere, 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 mødeække, hvor deltagerne i informationssikkerhedsudvalget mødes i anden sammenhæng.

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

Eksempel på kommissorium og dagsorden for informationssikkerhedsudvalgsmøder

Kommissorium
Baggrund
Informationssikkerhedsudvalgets medlemmer
Ansvar og opgaver
Rapportering
Møder i informationssikkerhedsudvalget
Frekvens
Dagsorden
Varetagelse af sekretariatsfunktion

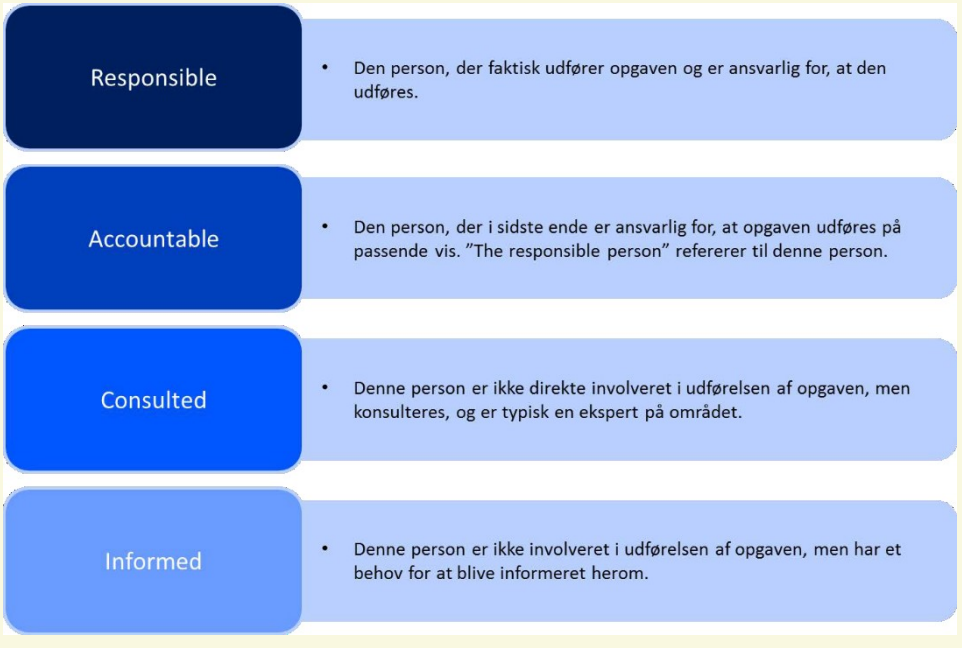
Dagsorden
Godkendelse af dagsorden
Godkendelse af referat fra sidste møde

Status på igangværende arbejder
Opfølgning på informationssikkerhedshændelser siden sidst
Håndterede afvigelser siden sidst
Nye afvigelser
Ændringer i trusselsbilledet
Godkendelse af nye eller opdaterede politikker
Eventuelt

Informationssikkerhedsudvalgets input og output 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.

Det bør defineres hvem der har hvilke roller i styringen af informationssikkerheden. Her kan eksempelvis den såkaldte RACI-model være til hjælp, da den bidrager til at skabe overblik over rolle- og ansvarsfordeling:

Figur 1
RACI-model



I vejledningen *'Rejsefortælling om funktioner, roller og ledelse i informationssikkerhed'*, der findes på sikkerdigital.dk, findes mere information om netop RACI-modellen samt roller og ansvar i arbejdet med informationssikkerhed.

Det anbefales, at organisationen beskriver, godkender og dokumenterer ledelses-systemets roller og ansvarsområder i overensstemmelse med ISO 27001's krav 5.3 og kontrollen A.6.1.1 i ISO 27001 Anneks A.

3. Informationssikkerhedsarbejdets relation til øvrige forretningsområder

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

Informationssikkerhed 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 informationssikkerhedsmæssige krav i udbud. Størstedelen af det praktiske arbejde med informationssikkerhed udføres således ikke af hverken ledelsen eller informationssikkerhedsfunktionen, men af de medarbejdere i funktioner og afdelinger, der hver eneste dag bidrager til at skabe et passende informationssikkerhedsniveau i organisationen.

Medarbejdernes rolle
Medarbejderne skal uddannes og vejledes i de regler for informationssikkerhed, der gælder for organisationen.

Derudover skal medarbejderne vide, hvordan de observerer og håndterer brud på informationssikkerheden, og de skal informeres om nye relevante regler og tiltag.

Viden og bevidsthed er dog ikke altid tilstrækkeligt til at opnå en god sikkerhedsadfærd blandt ledere og medarbejdere. I 'Metode til at arbejde med adfærdsindsatser indenfor cyber- og informationssikkerhed' findes mere hjælp til, hvordan organisationen kan tilrettelægge indsatser, der ikke blot skaber bevidsthed, men også skaber efterlevelse.

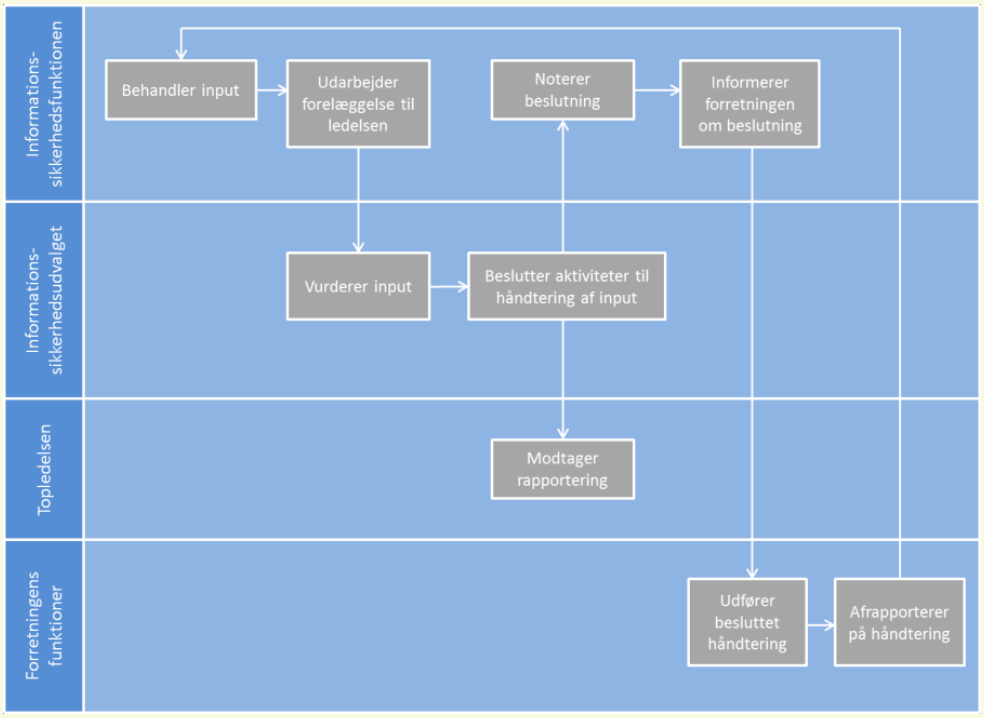
4. Skab overblik over ansvar og aktiviteter med et proces-flow

Formålet med at implementere et ledelsessystem for informationssikkerhed er at gøre organisationen i stand til systematisk at udføre eller håndtere:

- Risikovurderinger
- Forskellige typer af afvigelser, herunder bl.a. sikkerhedshændelser
- Korrigerende handlinger
- Opfølgning på informationssikkerheden
- Løbende forbedringer og prioritering af ressourcer

Hvordan skaber man overblik over, hvem der gør hvad i gennemførelsen af disse aktiviteter? En mulighed er at kortlægge sine aktiviteter ved hjælp af såkaldte *proces-flows*. Nedenfor vises et eksempel herpå. Her optræder rollerne "Topledelsen", "Informationssikkerhedsudvalget", "Informationssikkerhedsfunktionen" og "Forretningens funktioner" (som defineret i afsnit 2). Rollen "Forretningens funktioner" er bredt defineret, og indfanger alle de dele af organisationen, der arbejder med informationer, eller på anden måde kan påvirke informationssikkerheden. Valget af roller og deres beskrivelse (se nedenfor) er ment som inspiration, og kan tilpasses organisationen.

Figur 2
Eksempel på proces-flow



Kilde: Digitaliseringsstyrelsen

Værdien af at opstille et proces-flow består i, at man kan danne sig et ret detaljeret overblik over, hvordan organisationen skal forholde sig til et givent input i forhold til: hvilke aktiviteter der skal igangsættes, hvordan disse aktiviteter spiller sammen, og hvem der besidder ansvaret for at afvikle aktiviteterne.

Nedenfor findes en liste med input, som kan danne grundlag for at opstille proces-flow med delaktiviteter og ansvarsfordeling. Listen er tænkt som inspiration, og udgør ikke en fuldstændig tjekliste.

Eksempler på input til proces-flow

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.

5. Årshjul og årsplan

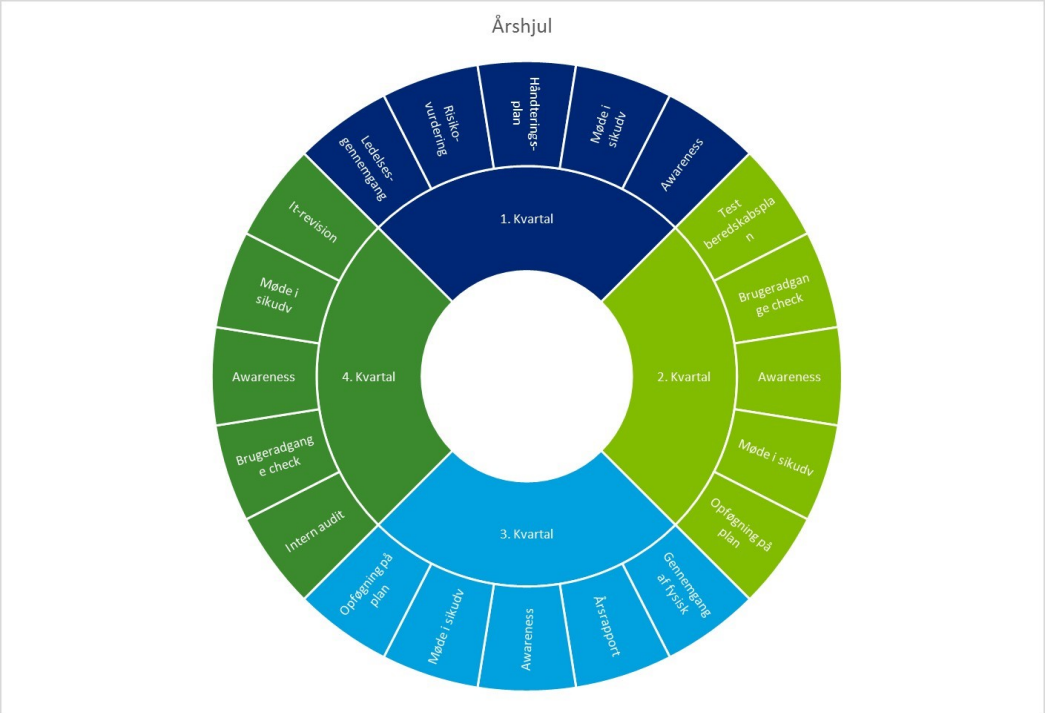
For at styre informationssikkerheden og for at sikre, at ledelsen har de rette styringsværktøjer, gentages en række aktiviteter løbende år efter år. Aktiviteter der gentages, kan placeres i et årshjul med det formål at illustrere årets aktiviteter overskueligt. Nedenfor vises et eksempel på et årshjul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

Årshjul - Indeholder aktiviteter, der skal gentages med passende tidsintervaller. Disse aktiviteter har ofte karakter af opfølgning, evaluering, møder eller lignende. Dette er 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.

Årsplan - 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 fx tre eller fem år. Årsplanen og risikohåndteringsplanen kan med fordel slås sammen. Årsplanen har typisk en mere konkret og detaljeret karakter end årshjulet, og identificerer også de medarbejdere, der er ansvarlige for at løse opgaverne i planen.

Nedenfor er vist et eksempel på en skabelon til et årshjul samt inspiration til elementer, der kan indgå.

Figur 3
Eksempel på årshjul



Kilde: Digitaliseringsstyrelsen

- **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 og om det har givet det ønskede resultat.

- **Opfølgning på målinger**. 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.

- **Ledelsesgennemgang af ledelsessystem for informationssikkerhed** ('møde i sik(kerheds)udv(alg)' i årshjulet). 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** ('årsrapport' i årshjulet). Informationssikkerhedsmedarbejderne skal med planlagte mellemrum rapportere om sikkerhedstilstanden i organisationen.

- **Medarbejderadfærd og –uddannelse** ('awareness' i årshjulet). Den ønskede sikkerhedsadfærd, medarbejderne skal have i dagligdagen, skal holdes ved lige. Det kan med fordel gøres ved planlagte aktiviteter gennem året.

- **Adgangsstyring**. Det skal løbende verificeres, at kun autoriserede brugere har adgang til systemer ('brugeradgange check' i årshjulet).

- **Test af beredskab**. Beredskabet skal testes med passende mellerum ('test beredskabsplan' i årshjulet).

Vejledning i planlægning af sikkerhedsarbejdet
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: 978-87-93073-39-5