DIGITALISERINGSSTYRELSEN

Vejledning i etablering af forretningsoverblik

Januar 2018

2018

Indhold

Indledning:
Styring af informationssikkerhed ved hjælp af forretningsoverblikket

Vejledning i forretningsoverblik er en af flere vejledninger, som er tiltænkt arbejdet med den internationale standard for styring af informationssikkerhed, ISO 27001. Et af de vigtige skridt i arbejdet med ISO 27001 er at skabe et overblik over den organisation, der skal arbejde med standarden.

En væsentlig forudsætning for, at ledelsens styring af informationssikkerhed[1] bliver en succes, er først at skabe et overblik over organisationens kontekst. Organisationens kontekst omfatter eksterne og interne forhold og interessenter, der er relevante for organisationen og dens formål. Organisationens kontekst nedfældes i forretningsoverblikket.

Ledelsens styring af informationssikkerhed skal understøtte organisationens opgavevaretagelse og samtidig integreres i eksisterende, velfungerende ledelses- og arbejdsprocesser.

Forretningsoverblikket skal tilpasses løbende som organisationens kontekst ændrer sig. Det er på baggrund af dette, at ledelsens styring af informationssikkerheden tilpasses. Alle interne og eksterne forhold og interessenter klarlægges for at sikre, at ledelsessystemet for informationssikkerhed understøtter arbejdet med at imødekomme de forventninger som der er til informationssikkerheden.

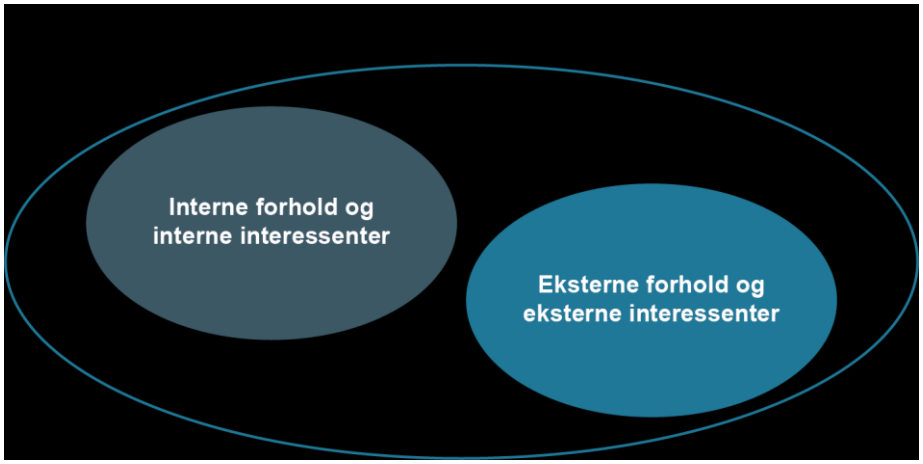
Vejledningen beskriver kort de vigtige elementer i at kortlægge organisationens kontekst og giver et eksempel på hvordan denne kan nedfældes i et forretningsoverblik. Endelig beskrives de processer man med fordel kan inddrage i arbejdet med forretningsoverblikket, samt den nødvendige afgrænsning af arbejdet med ledelsens styring af informationssikkerheden.

[1] Også kaldet ledelsessystemet for informationspolitik (ISMS)

1. Forretningsoverblikket

I ISO 27001 er det beskrevet, at organisationens kontekst omfatter eksterne og interne forhold, samt hvilke eksterne og interne interessenter, der er relevante for organisationen og den formål. Dertil kan man med fordel kortlægge organisationens processer.

Figur 1.1
Forretningsoverblik



Forretningsoverblikket skal kortlægge organisationens kontekst og alt det der skal til for at ledelsens styring af informationssikkerheden fungerer.

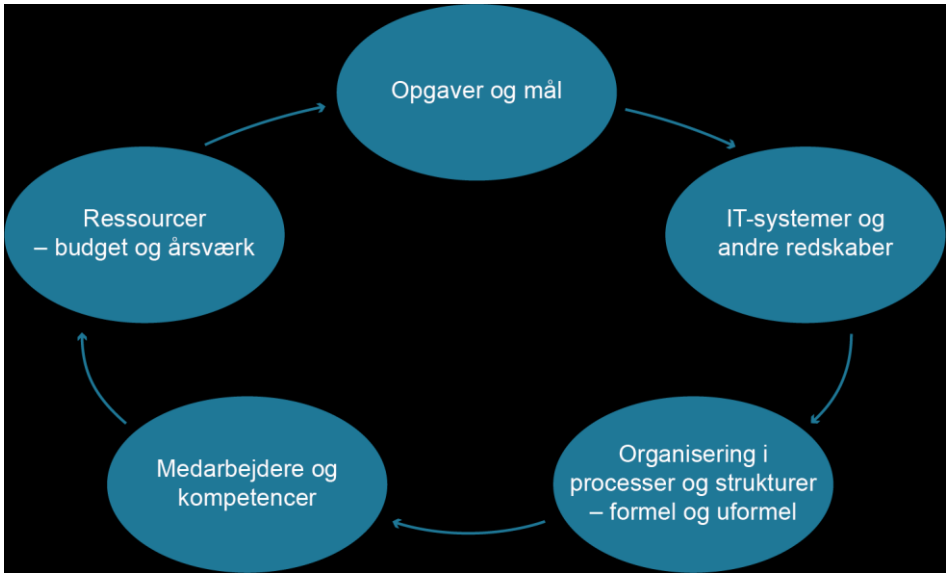
Der skal være et godt overblik over, hvilke informationer, der er vigtige for forretningen, og hvad det kan, få af konsekvenser, hvis der sker en kompromittering af informationernes fortrolighed, integritet eller tilgængelighed.

1.1 De interne forhold og interessenter

Interne forhold omhandler alle de mål, processer, systemer, ressourcer, medarbejdere m.m. som en organisation består af.

Det mest centrale interne forhold er det formål som organisationen er sat i verden for. Ofte vil formålet være beskrevet i en resultatkontrakt, en vision, en strategi 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. Derudover vil modtageren af organisationens ydelser være beskrevet. Det kan være andre organisationer, virksomheder eller borgere. Figuren neden for indeholder eksempler på interne forhold og interessenter.

Figur 1.2
Organisationens interne forhold og interessenter



Blandt de vigtige interne forhold er de processer og systemer der sikre opfyldelse af formålet. Andre vigtige interne forhold er de interne interessenter såsom de medarbejdere, som løser opgaverne, og de kompetencer, de har. Det er vigtigt, at man har medarbejderne med i forretningsoverblikket.

Metode

Læs de vigtigste strategiske dokumenter, gennemfør interview eller afhold workshops med nøglepersoner. Dokumentér overblikket over forretningskritiske aktiver, der skal beskyttes, skriftligt.

1.2 De eksterne forhold og interessenter

De eksterne forhold omhandler fx kontraktlige forpligtelser, lovkrav, leverandøraftaler, internationale aftaler. Ofte er der blandt disse forhold et overlap eller en lighed med de eksterne interessenter, fx leverandører, brugere, myndigheder og interesseorganisationer. Figuren neden for indeholder eksempler på eksterne interessenter.

Figur 1.3
Organisationens eksterne interessenter

Organisationens eksterne forhold og interessenter kan stille krav og behov til informationssikkerheden. Herunder, kunder/borgere, som modtager organisationens opgaveløsning, og samarbejdspartnere, myndigheder og leverandører, der indgår i opgaveløsningen.

Mange organisationer har en meget vigtig ekstern interessent, nemlig deres it-drifts-leverandør. Når hele eller dele af it-driften er outsourcet, stiller det særlige krav til organisationens leverandørstyring.

Metode

Læs de vigtigste dokumenter, fx leverandøraftaler og -kontrakter, regler og love, branchenormer m.m. Gennemfør interview eller afhold workshops med nøglepersoner. Dokumenter overblikket skriftligt.

2. Kortlægning af processer

Som en del af opgaven med at etablere et forretningsoverblik, er det en god ide at få identificeret og dokumenteret organisationens processer. I kraft af digitaliseringen af informationsbehandlingen er flere og flere processer understøttet af et eller flere it-systemer. Det er ofte de systemer, vi behandler, når vi omtaler it-risikovurderinger, it-revision og implementering af it-kontroller.

Man kan med fordel tage udgangspunkt i procesbeskrivelserne eller man kan starte med informationerne eller it-systemerne, fordi dem har organisationen som regel et overblik over. Processer er ikke altid velbeskrevet, men ligger implicit i den måde, det daglige arbejde udføres.

Forretningsmål	Enhver forretning/organisation har et formål med det, de gør. Det kan være at producere varer, at levere serviceydelser, at varetage en myndighedsopgave m.m. Forretningsmålene kan ofte brydes op i delmål eller opgaveområder, men til sammen udgør de den samlede forretning. Undersøg, hvad organisationens mål er.
Forretningsprocesser	For at en forretning eller en organisation skal kunne varetage sine opgaver og nå sine mål, har de etableret en række forretningsprocesser, der omdanner et givet input til et output. Det kan f.eks. være en virksomhed, der omdanner rågummi til bildæk, eller et departement, der omdanner input fra styrelser til ministerbetjening. Klarlæg, hvilke processer der er i organisationen.
Informationer	For at forretningsprocesser kan fungere, kræver det som regel, at der anvendes informationer. Uden de informationer ville processen gå i stå, og hvis informationerne er forkerte, kan output fra processen blive fejlbehæftet. Måske er informationerne forretningshemmeligheder, som er vigtige for organisationen at holde fortrolige. Find ud af, hvilke informationer der er vigtige for organisationen.
It-systemer	Til behandling af de informationer, der understøtter forretningsprocesser, anvender vi i dag it-systemer. Det er bl.a. disse it-systemer, vi prøver at beskytte gennem vores informationssikkerhedsarbejde. Hvad er de vigtigste it-systemer?

Der findes mange forskellige processer i en organisation. Organisationen kan vælge at afgrænse sit ledelsessystem for informationssikkerhed til kun at dække dele af organisationens processer, informationer og it-systemer.

Forretningsprocesser er de processer, der indgår direkte i organisationens kerneopgaver, det er f.eks. mælkeproduktion for et mejeri eller ministerbetjening

for et departement. Støtteprocesser er de processer, der hjælper med at holde forretningsprocesserne i gang. Det er f.eks. HR-processer, der sørger for rekruttering, lønudbetaling m.m., eller serviceprocesser, der sørger for bygningsvedligehold, rengøring m.m. Både forretningsprocesser og støtteprocesser er afhængige af informationer og it-systemer, f.eks. har HR et lønsystem, og service har planer over bygningerne. De dele af organisationen, der ligger uden for ledelsessystemet for informationssikkerhed, betragtes som eksterne leverandører.

3. Afgrænsning af ledelsessystemet for informationssikkerhed

Når en organisation skal definere omfanget af ledelsens styring af informationssikkerhed (ledelsessystemet for informationssikkerhed), skal den, på baggrund af det etablerede forretningsoverblik, bestemme sig for, hvad der skal dækkes af ledelsessystemet.

Afgrænsningen kan foretages i forhold til mange forskellige aspekter og ud fra eksempelvis følgende overvejelser:

- Hvilke dele af organisationen skal indgå? Der kan være en del af en organisation, der med fordel kan udelades, fordi den ikke er informationstung, eller fordi det kan give mening at den etablerer et selvstændigt ledelsessystem.
- Skal alle informationer indgå? Der er måske visse dele af organisationens informationer, der ikke er kritiske for forretningen.
- Skal alle informationsaktiver indgå? Der kan være it-systemer, man ønsker at holde uden for et ledelsessystem for informationssikkerhed, det kan f.eks. være produktionssystemer, der ikke er på netværk eller på anden måde har en beskyttelse i sig selv.
- Ønsker organisationen at starte med en lille del af organisationen, informationerne eller it-systemerne, for så gradvist at udvide omfanget over tid? Som regel er det bedre at starte med en lille del og ikke prøve at få alt med i første omgang. Det giver organisationen mulighed for at drage erfaringer og bringe læring med ind i det fortsatte arbejde, når omfanget af ledelsessystemet udvides.

Grænseflader mellem processer, der udføres af organisationen selv, og processer, der udføres af andre organisationer, kan også have indflydelse på, hvordan ledelsessystemet afgrænses. For mange organisationer med outsourcet it-drift gør det sig gældende, at meget af styringen med informationssikkerheden sker gennem leverandørstyring, og det vil have indflydelse på afgrænsningen.

4. Eksempel på et forretningsoverblik

Neden for ses et eksempel på et forretningsoverblik. Forretningsoverblikket er udarbejdet over finansministeriet.

Finansministeriets forretningskontekst
Juni 2017

Indhold

1.1 Finansministeriets forretningskontekst

Dette notat har til formål at afdække den organisatoriske forretningskontekst som er relevant for Finansministeriets informationssikkerhed.

Finansministeriets koncern består af et departement (DEP) og fem institutioner, Statens Administration (SAM), Digitaliseringsstyrelsen (DIGST), Moderniseringsstyrelsen (MODST), Statens It (SIT), samt Center for Offentlig Innovation (COI).

1.2 Strategisk målsætning/Ansvarsområde

Finansministeriet (FM) spiller en central rolle i forhold til skiftende regeringers økonomiske politik. Ministeriet er blandt andet ansvarlig for at udarbejde de årlige finanslove, men arbejder også med følgende øvrige hovedarbejdsområder: Økonomisk politik, mere effektiv regulering, produktivitet og vækst, EU og international økonomisk politik, offentlige finanser, kommuner og regioner samt statens selskaber.

FM varetager også en række generelle administrative opgaver for staten fx udbetaling af løn, tilskud og pension, udarbejdelse af personalepolitik samt håndtering af it services (gennem Statens It). Endeligt varetager FM flere offentligt rettede løsninger med stor samfundsmæssig relevans, for borgere og virksomheder.

Finansministeriet har en central rolle i staten, hvilket skal afspejles i den måde hvorpå forretningsområderne håndteres. Det er således vigtigt at der udvises effektivitet, kvalitet og korrekthed i håndteringen af opgaver, og at der arbejdes for at understøtte dette gennem organisationen.

1.3 Interessenter

Finansministeriet har et bredt spektrum af interessenter at tage hensyn til. I relation til informationssikkerhedsmæssige spørgsmål vil FM imødekomme disse interessenters forventninger, ved at sikre at relevante love, regler og kontrakter overholdes, samt at medarbejdere handler i overensstemmelse med disse og i øvrigt er bevidste om vigtigheden af informationssikkerhed i samarbejdet.

De centrale interessenter for FM er:

- Folketinget, herunder særligt regeringen
- Øvrige statslige myndigheder
- Regionerne, herunder særligt DR
- Kommunerne, herunder særligt KL
- Borgerer som brugere af offentlige løsninger
- Erhvervslivet som afhængig af flere offentlige tjenester
- Private interesseorganisationer
- Private leverandører

Styring af informationssikkerheden i Finansministeriets ledelsessystem for informationssikkerhed dækker underliggende styrelsers informationer, informationssystemer og andre aktiver til behandling af informationer. Den omfatter endvidere informationer, som ikke tilhører Finansministeriet, men som Finansministeriet kan gøres ansvarlig for. Ledelsessystemet omfatter desuden de fysiske rammer for organisationen. Styringsgrundlaget skal sikre, at indsatsen sker i overensstemmelse med de strategiske mål for koncernen.

Finansministeriet gør stor brug af serviceleverandører og andre myndigheder, som varetager vigtige funktioner i forhold til FM's opgaver. Det er derfor vigtigt at der gennem samarbejdet med disse, arbejdes målrettet med at sikre et passende niveau af informationssikkerhed.

[Indsæt tekst her eller slet (max. 800 anslag)]

digst.dk