Skatteministeriet

22. februar 2016
J. nr. 15-2841741
Plannr. 115-019

Intern Revision

Rapport 2015

Direktørområdet SKAT IT

Intern audit og tilsyn med it-anvendelsen i SKAT

Modtager
Direktør Jesper Rønnow Simonsen, SKAT

Kopi
Direktør Karsten Juncher, SKAT
Departementet
Rigsrevisionen

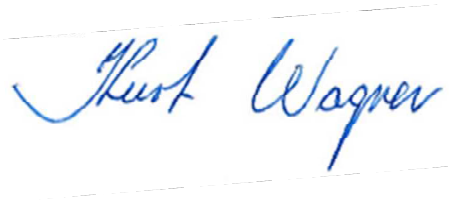
- ✓ **Revision**
- ✓ **Rådgivning**
- ✓ **Rapportering**

Forord

Intern Revision (IR) har, jævnfør orienteringsbrev af 28. september 2015, vurderet SKATs ledelsessystem for informationssikkerhed (ISMS). Opgaven er udført, som en del af den samlede revision for 2015.

Rapporten har været fremsendt i udkast til den reviderede enhed med henblik på at sikre, at Intern Revision og den reviderede enhed har en ensartet opfattelse af de observerede forhold. SKAT har efterfølgende udarbejdet handleplaner.

København, den 22. februar 2016



Kurt Wagner
Revisionschef

Klaus Myssen
Senior manager

1. Formål

Kontoret for ”Sikkerhed” er ansvarlig for implementeringen af ISO27001 i SKAT. ISO 27001 har været obligatorisk for statslige myndigheder siden starten af 2014 og skal være implementeret primo 2016. Departementet er bekendt med, at SKAT er i proces med at implementere ISO 27001 og at implementeringen først forventes gennemført ved udgangen af 2016. (j.nr. 15-1528730)

Intern Revision har ifølge aftale med Departementet i perioden december 2015 til januar 2016 gennemført Intern audit og tilsyn i den underliggende styrelse ”SKAT” for 2015, med henblik på at tilse og vurdere, om styringen af informationssikkerheden i SKAT er tilrettelagt hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt, så informationers fortrolighed, integritet og tilgængelighed sikres i overensstemmelse med det regelgrundlag, institutionen er underlagt.

Intern audit og tilsynet er udført ved at indhente relevant dokumentation, herunder dokumentet ”Ledelsessystem for informationssikkerhed” samt ISO implementeringsplaner med tilhørende handlingsplan. Endvidere er indhentet udfyldt spørgeramme i relation til implementeringen af ISO27001og udfyldt selvevalueringsskema. Vi har foretaget en gennemgang og vurdering af indhentet materiale ligesom der er holdt ad-hoc møder med Sikkerhed og anvendt viden fra tidligere udførte it-revisioner.

2. Afgrænsning

Årets tilsyn omfatter ikke et selvstændigt tilsyn med it-anvendelsen i Spillemyndigheden og Skatteankestyrelsen. Dette begrundes med, at en stor del af it-anvendelsen i spillemyndigheden og skatteankestyrelsen i 2015 har været fælles med SKAT, ligesom disse styrelser i mindre omfang har en selvstændig strategisk, økonomisk eller forretningsmæssig betydning for opgavevaretagelsen på ministerområdet.

3. Omfang – Intern audit

Den interne audit er udført efter kravene i ISO27001 (afsnit 9.2) og har omfattet en vurdering af, hvorvidt ledelsessystemet for informationssikkerhed:

a) er i overensstemmelse med
   1. organisationens egne krav til sit ledelsessystem for informationssikkerhed og
   2. kravene i den internationale standard
b) er effektivt implementeret og bliver vedligeholdt

4. Konklusion – Intern audit

Vi har foretaget en gennemgang af implementeringsplanerne med tilhørende tidsestimater og milepæle. Det er vores vurdering, at planen er anvendelig og realistisk, hvorfor området samlet set vurderes at være **tilfredsstillende**.

Med udgangspunkt i gennemgangen af det fremsendte materiale, har vi følgende bemærkninger i relation til efterlevelse af kravene i ISO 27001:

a.1) Det er konstateret, at Sikkerhed i SKAT har udarbejdet dokumentet "Ledelsessystem for informationssikkerhed". Dokumentet foreligger endnu ikke i en endelig version, men indeholder en klar og anvendelig beskrivelse af organisationens egne krav til et ISMS.

a.2) Det er påset, at dokumentet "Ledelsessystem for informationssikkerhed" følger strukturen og kravene i ISO27001.

b) SKAT er fortsat i gang med at udvikle og implementere et ISMS, hvorfor det ikke kan vurderes, om det er effektivt implementeret og vedligeholdt.

5. Omfang - Tilsyn

Tilsynets omfang og emner er tilrettelagt ud fra en vurdering af væsentlighed og risiko. I dette tilsyn har der været fokus på følgende forhold:

a) Har ledelsen i SKAT tilrettelagt en styring, der sikrer, at informationssikkerheden er fastlagt og håndteret hensigtsmæssigt?
b) Sikrer de generelle it-kontroller i SKAT et, efter institutionens forhold, betryggende sikkerhedsniveau?
c) Foretager SKAT periodiske risikovurderinger af informationssikkerheden for at identificere risiko for tab af fortrolighed, integritet og tilgængelighed?
d) Har SKAT fastlagt politikker og retningslinjer for informationssikkerheden?
e) Har SKAT taget stilling til bemærkninger og anbefalinger fra revisions-og tilsynsmyndigheder?

6. Konklusion - Tilsyn

Tilsynets gennemgang har givet anledning til følgende bemærkninger til de enkelte emner:

a) Udfyldt spørgeramme og selvevalueringsskema som dækker områderne i ISO27001 er gennemgået. Ud fra gennemgangen er det vores vurdering, at SKAT har tilrettelagt en hensigtsmæssig styring af informationssikkerheden, en styring som der fortsat arbejdes med, i forbindelse med implementeringen af ISMS. Ved gennemgangen er vi blevet informeret om, at der endnu ikke foreligger lokale beredskabsplaner samt at der ikke er gennemført test og evaluering af SKATs overordnede beredskabsplan inden for de seneste 12 måneder. Spørgerammen indeholder desuden SKATs stillingtagen til "Cyberforsvar der virker" hvoraf det fremgår, at SKAT har implementeret sikringstiltagene.

b) Intern Revision foretager løbende it-revision af de generelle it-kontroller i SKAT ud fra en 3-årig rotationsplan. Revisionerne viser, at SKAT fortsat har udfordringer på udvalgte områder, hvor kontrolmiljøet karakteriseres som værende "ikke helt tilfredsstillende". I forbindelse med revisionerne er der udarbejdet en række anbefalinger til styrkelse af områderne. Anbefalinger som SKAT arbejder på at følge. Det er vores vurdering, at de generelle it-kontroller i SKAT samlet set, endnu ikke har et betryggende sikkerhedsniveau.

c) Via spørgerammen har SKAT oplyst, at systemejere og projektmedarbejdere udarbejder risikovurderinger og at bevidsthedsniveauet omkring risici i SKAT er højt. SKAT mangler dog at gennemføre en risikoanalyse, som omfatter den fulde organisation, og som inkluderer processer og deres afhængigheder.

d) Vi er bekendt med, at SKAT har udarbejdet en række regelsæt og procedurebeskrivelser, som understøtter sikkerhedspolitikken og sikkerhedshåndbøger for informationssikkerheden.

e) Vi har kendskab til, at SKAT løbende arbejder med, og tager stilling til bemærkninger og anbefalinger fra revisions- og tilsynsmyndigheder.

Tilsynet har ikke givet anledning til yderligere bemærkninger.