Skatteministeriet

24. juni 2016
J. nr. 16-0284527
Plannr. 116-011

Intern Revision

Rapport 2016

Økonomi

Informationssikkerhedspolitikker

Modtager
Direktør Jesper Rønnow Simonsen

Kopi
Direktør Karsten Juncher
Departementet
Rigsrevisionen

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

Forord

Intern Revision (IR) har, jævnfør orienteringsbrev af 7. marts 2016, revideret området for ”Informationssikkerhedspolitikker”. Den udførte revision er en del af den samlede revision for 2016.

Rapporten indeholder en samlet konklusion omfattende det reviderede område. I konklusionsafsnittet redegør vi for de observationer, som konklusionen i det væsentligste er baseret på. Konklusionsafsnittet indeholder Intern Revisions bedømmelse af det reviderede område samt en beskrivelse af grundlaget for bedømmelsen. Det vil derfor almindeligvis være tilstrækkeligt at læse selve rapporten. Såfremt der ønskes uddybning og detaljering, henvises der til bilagene.

Rapportens bilag 1 indeholder en systematisk fremstilling af de observationer, som den udførte revision har givet anledning til. Bilaget indeholder tillige en vurdering af de tilknyttede risici samt Intern Revisions forslag til anbefalinger, der kan formindske de vurderede risici. Med udgangspunkt i risikovurderingerne har SKAT udarbejdet handleplaner med henblik på at formindske de vurderede risici.
Intern Revisions anbefalinger har været anvendt som inspiration ved udarbejdelse af handleplaner. Vi vil løbende vurdere implementeringen af SKATs handleplaner.

Rapportens bilag 2 indeholder en beskrivelse af de prioriteringer, der er anvendt ved klassifikationen af de enkelte observationer. Bilaget indeholder herudover en beskrivelse af koblingen mellem observationernes prioriteringer og den samlede overordnede konklusion.

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 24. juni 2016.

Kurt Wagner
Revisionschef

Annette Kirstine Skov Pedersen
Manager

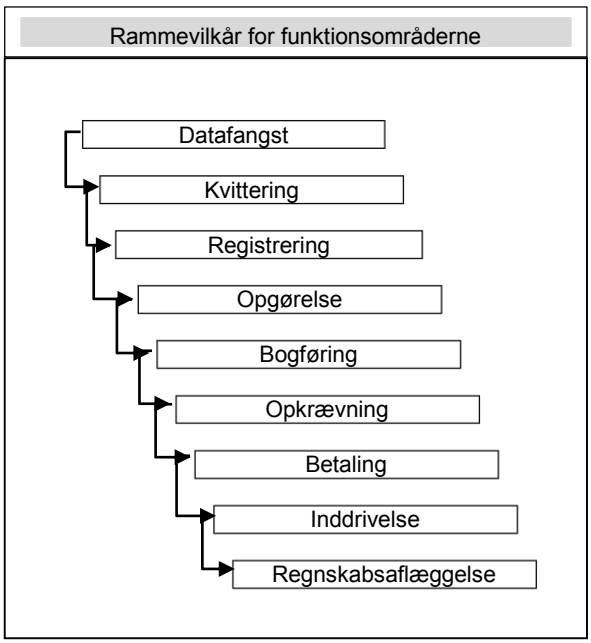
1. Formål

Formålet med revisionen har været at undersøge og vurdere, om SKAT har tilrettelagt politikker og retningslinjer for informationssikkerheden, og om de er i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

2. Omfang

Revisionen er udført i perioden marts til april 2016 med udgangspunkt i ISO standarden 27001 og har omfattet emnet "A.5 Informationssikkerhedspolitikker" med følgende hovedområde:

- A.5.1 Retningslinjer for styring af informationssikkerhed



SIR anvender denne model til operationel beskrivelse og kategorisering af aktiviteterne i SKAT. I forbindelse med denne revision har vi revideret følgende funktionsområde:

- Rammevilkår for funktionsområderne

I de enkelte observationer har vi henvist til, hvilket funktionsområde, som observationen vedrører.

ISO 27001 standarden for informationssikkerhed har været obligatorisk for statslige myndigheder siden starten 2014 og skulle være implementeret primo 2016. Departementet er bekendt med, at SKATs implementering af ISO 27001 først vil være gennemført ved udgangen af 2016 (j.nr. 15-1528730).

Revisionen er udført i henhold til gældende revisionsstandarder, herunder vejledninger fra Rigsrevisionen. Revisionen er gennemført ved interviews, og stikprøvevis gennemgang af foreliggende materiale.

Ved revisionen har vi interviewet medarbejdere fra Informationssikkerhed.

Revisionen er udført af Annette Kirstine Skov Pedersen og Klaus Friis Myssen.

3. Konklusion

Det er vores vurdering, at der **i mindre omfang er behov** for ændringer i de reviderede processer i relation til " A.5 Informationssikkerhedspolitikker".

Denne vurdering baserer vi på følgende forhold:

- Sikkerhed har udarbejdet regelsæt for SKAT (håndbog for ledere og håndbog for medarbejdere) til understøttelse af ministeriets informationssikkerhedspolitik, men dette arbejde ikke er baseret på en samlet overordnet risikovurdering.

Vi har udarbejdet et antal anbefalinger til styrkelse af de enkelte hovedområder. Samtlige anbefalinger fremgår af bilag 1. Den væsentligste anbefaling er følgende:

- Vi har konstateret, at SKAT ikke har udarbejdet en samlet, overordnet risikovurdering som grundlag for udarbejdelse af informationssikkerheds-politik og regelsæt (se evt. anbefaling A.5.1.1.3. i bilag 1).

Vi har prioriteret de observerede forhold således:

Nr.	Emne/Område/Kontrolmål	Prio. 1	Prio. 2	Prio. 3	Prio. 4	I alt
A.5.1	Retningslinjer for styring af informationssikkerhed					
A.5.1.1	Politikker for informationssikkerhed	0	2	0	1	**3**
A.5.1.2	Gennemgang af politikker for informationssikkerhed	0	0	0	1	**1**
I alt		**0**	**2**	**0**	**2**	**4**

Prioriteterne skal ses i forhold til det reviderede område og er nærmere defineret i bilag 2.

Vi har modtaget handleplaner fra det reviderede direktørområde. Det er vores vurdering, at implementeringen af de udarbejdede handleplaner vil medvirke til en reduktion af de vurderede risici.

Bilag 1: Observationer, risici og anbefalinger

Nr.	Observationer	Risici	Anbefalinger
A.5.1	**Kontrolmål:** **Retningslinjer for styring af informationssikkerhed.**		**Funktionsområde:** **Rammevilkår for funktionsområderne**
A.5.1.1	**Politikker for informationssikkerhed**		
A.5.1.1.1 **Prio. 4**	Overordnet politik for informationssikkerhed Vi har konstateret, at der foreligger en overordnet politik for informationssikkerhed, som er godkendt af ledelsen og offentliggjort på intranettet. Vi har gennemgået politikken og finder den anvendelig til at styrke informationssikkerheden i SKAT.		
A.5.1.1.2 **Prio. 2**	Understøttelse af informationssikkerhed med retningslinjer SKAT har udarbejdet håndbog for ledere og håndbog for medarbejdere, som udgør regelsættet til den overordnede informationssikkerhedspolitik. Håndbøgerne er godkendt af SKATs direktion d. 17. december 2014. I februar 2015 udsatte Skatteministeriets departement implementeringen, så håndbøgerne kunne	Den korte tidsfrist til implementeringen af håndbøgerne og ISO 27001 medfører øget risiko for, at implementering af alle væsentlige områder ikke kan nås.	Vi anbefaler, at SKAT øger deres fokus på implementeringen af ISO 27001 og eventuel udarbejder og følger en overordnet plan for implementeringen af alle væsentlige områder for at understøtte det ønskede sikkerhedsniveau i SKAT.

Nr.	Observationer	Risici	Anbefalinger
	tilpasses og blive godkendt i ministeriets samarbejdsfora inden implementeringen. Håndbog for medarbejdere er godkendt d. 31. marts 2016 af SKATs ledelse, hvorimod godkendelse af håndbog for ledere udestår. Regelsættet i håndbøgerne skal være implementeret inden 31. december 2016 som en del af ISO 27001 implementeringen.		
	Handleplan: SKAT har i samarbejde med departementet ultimo maj 2016 lagt en ny handlingsplan for at komme i mål med implementeringen af ISO 27001. Handlingsplanen har følgende trin: 1) Nyt ISMS-dokument udarbejdes efter departementets skabelon og forelægges direktionen (30. juni 2016) 2) Tilpasning af modenhedsanalysen, så den passer til ISO27001 (30. juni 2016) 3) Risikovurdering gennemført i SKATs forretning (30. juni 2016) 4) Regelsæt for SKAT tilpasses og kontrolkatalog udarbejdes og lægges i ControlManager (31. august 2016) 5) På baggrund af modenhedsanalysen og den netop afsluttede risikovurdering udarbejdes en opdateret SOA op mod den kvalitetssikrede/gennemarbejdede Håndbog for Ledere og/eller ISO27001 i ControlManager (30. september 2016) 6) Håndbog for ledere forelægges direktionen (30. september 2016) 7) Modenhedsanalyse, risikovurdering og SOA, samt forslag til handlingsplan og awareness forelægges SKATs direktion til godkendelse (31. oktober 2016) 8) Kontroller og aktiviteter kan herefter iværksættes og køre i et årshjul. Tidsplan: 31.12.2016 Ansvarlig person: Jeanette Sporleder Ebbesen		

Nr.	Observationer	Risici	Anbefalinger
A.5.1.1.3 **Prio. 2**	<u>Risikovurdering som grundlag for fastlæggelse af informationssikkerheds-niveauet</u> Vi har konstateret, at vi ikke har fået forelagt dokumentation som viser, at SKAT har udarbejdet sikkerhedshåndbøger, som er baseret på en overordnet risikovurdering af SKATs samlede forretning.	Manglende identifikation og vurdering af forretningsmæssige risici medfører øget risiko for, at håndbøgerne for informationssikkerhed i SKAT ikke afspejler et sikkerhedsniveau, som er tilpasset de konkrete trusler og risici.	Vi anbefaler, at håndbøgerne for informationssikkerhed udarbejdes med udgangspunkt i en samlet vurdering af forretningsmæssige risici, der viser, hvilke konkrete trusler og risici, som SKAT bør behandle.
	<u>Handleplan:</u> Der er pr. juni 2016 udarbejdet en samlet risikovurdering i forretningen. Denne vil fremover danne udgangspunkt for kvalitetssikring af kontroller og håndbog for ledere. Risikoanalysen vil fremover blive foretaget en gang årligt. Frist: 31.12.2016 Ansvarlig person: Jeanette Sporleder Ebbesen		
A.5.1.2	**Gennemgang af politikker for informationssikkerhed**		
A.5.1.2.1 **Prio. 4**	<u>Gennemgang af retningslinjer for informationssikkerhed</u> Vi har konstateret, at ejerskabet til informationssikkerhedspolitik og regelsæt er fastlagt, og at der regelmæssigt foretages gennemgang af politikken og regelsættet. Vi har gennemgået regelsættet i Sikkerhedshåndbøgerne og finder dem		

Nr.	Observationer	Risici	Anbefalinger
	anvendelige til at styrke informationssikkerheden i SKAT.		
	SLUT		

Bilag 2: Anvendt skala

Ved udarbejdelsen af konklusionen er følgende skala anvendt:	
Intet behov for procesændringer	Intern Revision har ikke observeret svagheder i de forretningsgange og processer, der understøtter det reviderede område. Prioritet 1: Ingen observationer Prioritet 2: Ingen observationer
Behov for procesændringer i mindre omfang	Intern Revision har observeret enkelte svagheder i de forretningsgange og processer, der understøtter det reviderede område. Prioritet 1: Ingen observationer Prioritet 2: Enkelte observationer
Behov for procesændringer i større omfang	Intern Revision har observeret flere svagheder i de forretningsgange og processer, der understøtter det reviderede område. Observationerne er hovedsageligt omfattet af prioritet 1 og 2 med flest observationer i prioritet 2. Prioritet 1: Flere observationer Prioritet 2: Flest observationer
Behov for procesændringer i væsentligt omfang	Intern Revision har observeret flere svagheder i de forretningsgange og processer, der understøtter det reviderede område. Observationerne er hovedsageligt omfattet af prioritet 1 eller 2 med flest observationer i prioritet 1. Prioritet 1: Flest observationer Prioritet 2: Flere observationer

Det skal bemærkes, at ovenstående beskrivelse, med hensyn til antal observationer pr. prioritet, er vejledende i forhold til vores samlede vurdering af konklusionen.

Prioritering af de enkelte observationer:

Prioritet 1: Høj Risiko for manglende målopfyldelse:
Væsentlige svagheder i den etablerede forretningsgang/proces. Svaghederne kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Som følge heraf er der en væsentlig øget risiko for, at processens formål ikke realiseres. Manglende opfyldelse af processens formål vil have store konsekvenser for virksomheden. Der bør snarest muligt iværksættes foranstaltninger med henblik på at udbedre de observerede svagheder.

Prioritet 2: Middel risiko for manglende målopfyldelse:
Svagheder i den etablerede forretningsgang/proces. Svaghederne kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Som følge heraf er der en øget risiko for, at processens målopfyldelse ikke fuldtud realiseres. Manglende opfyldelse af processens formål vil have store konsekvenser for virksomheden. Der bør iværksættes foranstaltninger med henblik på at udbedre den observerede svaghed.

Prioritet 3: Lille risiko for manglende målopfyldelse:
Ingen svagheder i den etablerede forretningsgang/proces. Som følge heraf er der ikke en øget risiko for, at processens formål ikke realiseres. Den reviderede proces kan dog designes med henblik på at forbedre eksekveringen af processen. Processen vil dog være omfattet af den risiko, der, uanset styrken af de interne kontroller, altid vil være til stede.

Prioritet 4: Lille risiko for manglende målopfyldelse:
Ingen svagheder i den etablerede forretningsgang/proces. Som følge heraf er der ikke en øget risiko for, at processens formål ikke realiseres. Processen vil dog være omfattet af den risiko, der, uanset styrken af de interne kontroller, altid vil være til stede.