Skatteministeriet

17. maj 2016
J. nr. 15-2368547
Plannr. 115-010

Intern Revision

Rapport 2015

SKAT Kundeservice og Økonomi

Revisorerklæringer for it-systemer outsourcet til serviceleverandører

Modtager
Direktør Jesper Rønnow Simonsen, SKAT

Kopi
Direktør Merete Agergaard, Kundeservice
Direktør Karsten Juncher, Økonomi
Departementet
Rigsrevisionen

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

Forord

Intern Revision (IR) har, jævnfør orienteringsbrev af 14. september 2015 revideret revisorerklæringer for it-systemer outsourcet til serviceleverandører. Den udførte revision er 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.

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.

København, den 17. maj 2016

Kurt Wagner
Revisionschef

Aliriza Özden
Manager

1. Formål

Formålet med revisionen er at undersøge og vurdere, hvorvidt SKAT rekvirerer revisorerklæringer for alle væsentlige og risikofyldte it-systemer, som er outsourcet til it-serviceleverandører.

2. Omfang

Revisionen har omfattet væsentlige og risikofyldte it-systemer, der understøtter processen for aflæggelse af § 9 og § 38 regnskaberne. Revisionen, der er udført i perioden medio september – medio november 2015, har omfattet interview med en række nøglemedarbejdere, og har bl.a. bestået af følgende aktiviteter:

1) Identifikation af væsentlige og risikofyldte it-systemer: 3S, BE, CKR-K, COR, CPS, CSR komplekset, CWB, D-COR, DIAS, DMI, DMO, DMR, DR, ECS, EFI, e-indkomst komplekset, EMCS, EROS, ES, Forskud, ICS, KOBRA, KR-L, NTSE, PAF, PAL, Quota, R75, RCO, SAP38, SAPIntern, SLS komplekset, SLUT komplekset

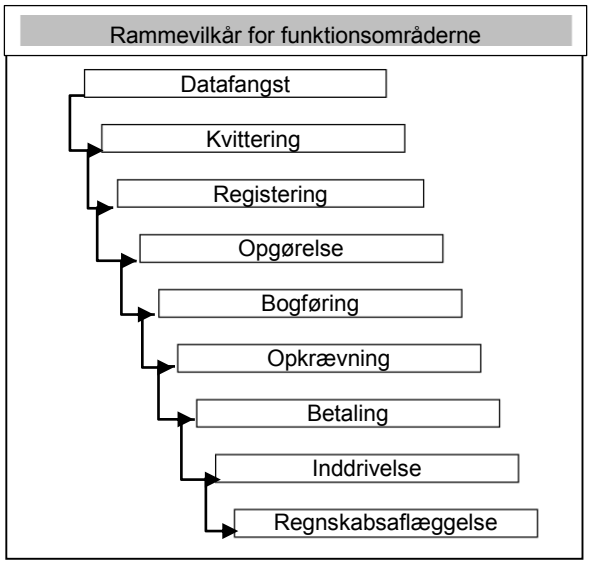
2) Identifikation af It-serviceleverandører, som drifter væsentlige og risikofyldte systemer: CSC, CGI, Systematic, Netcompany, Konsortiet (KMD, Cap. Affecto), IBM, European Dynamics, KMD og NNIT

3) Rekvirering og gennemgang af revisorerklæringer

4) Vurdering af type og periode for revisorerklæringer

5) Udarbejdelse af observationer, risici og anbefalinger

I forbindelse med revisionen anvendes nedenstående model, som opdeler processen i en række funktionsområder. Vi har i forbindelse med nærværende revision revideret rammevilkår for funktionsområderne. Det reviderede område er fremhævet med gråt i figuren:



Revisionen er udført af Henrik Friis-Pedersen og Aliriza Özden ved interviews, og stikprøvevis gennemgang af foreliggende materiale i samarbejde med medarbejdere fra Kundeservice og Økonomi/IT.

3. Konklusion

Det er vores vurdering, at der **i væsentligt omfang er behov** for ændringer i de reviderede processer. Denne vurdering baserer vi på følgende forhold:

- SKAT rekvirerer ikke revisorerklæringer, som giver specifik sikkerhed for alle væsentlige og risikofyldte it-systemer, der er outsourcet til it-serviceleverandører.

Vi har prioriteret de observerede forhold således:

Revisionsemne	**Prioritet 1** *Høj risiko*	**Prioritet 2** *Middel risiko*	**Prioritet 3/4** *Lille risiko*	**I alt**
1. Sikkerhed gennem systemspecifikke revisorerklæringer	**2**	**0**	**0**	**2**
2. Risikovurdering af væsentlige it-systemer	**0**	**1**	**0**	**1**
3. Overblik over revisorerklæringer	**0**	**1**	**0**	**1**
I alt	**2**	**2**	**0**	**4**

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

Vi har modtaget handleplaner fra de reviderede direktørområder. 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
1	**Revisionsemne: Sikkerhed gennem systemspecifikke revisorerklæringer**		**Rammevilkår for funktionsområderne**
1.1 2015 Prio. 1	**<u>Rekvirering af revisorerklæringer</u>** Vi har konstateret, at SKAT ikke rekvirerer revisorerklæringer, som giver specifik sikkerhed for it-driften af alle væsentlige og risikofyldte it-systemer, som er outsourcet til it-serviceleverandører. Det er vores vurdering, at løbende møder vedr. drift og informationssikkerhed samt månedlige driftsrapporter ikke giver tilstrækkelig sikkerhed for driften af SKATs it-systemer.	Manglende revisorerklæringer medfører en forøget risiko for, at SKAT ikke får mulighed for at iværksætte kompenserende handlinger, såfremt de væsentligste og mest risikofyldte systemer ikke håndteres forsvarligt og i overensstemmelse med: • Aftalegrundlaget mellem SKAT og it-serviceleverandør • Regnskabsinstruksens afsnit 3.5 Drift, vedrørende rekvirering af revisorerklæringer Dette medfører en afledt risiko for en mindre grad af sikkerhed på it-området.	Vi anbefaler, at SKAT for de væsentlige og risikofyldte it-systemer outsourcet til serviceleverandører, rekvirerer systemspecifikke revisorerklæringer af typen ”ISAE 3402, type 2”. I disse revisorerklæringer erklærer serviceleverandørens revisor sig om, hvorvidt en række væsentlige kontroller rettet specifikt mod SKATs it-systemer hos serviceleverandøren, har fungeret tilfredsstillende i en given periode. Revisorerklæringer bør således kombineres med løbende driftsmøder og månedlige driftsrapporter.
	Handleplan fra Claus Middelboe Andersen – Økonomi, IT Services: I 2011 fravalgte Direktionen at indhente en revisorerklæring fra CSC. Dette blev besluttet af følgende årsager: - Revisorerklæringer på alle de systemer CSC drifter, ville medføre omkostninger i millionklassen. - Etablering af sikkerhedsfora og månedlige driftsmøder med leverandører blev vurderet til, at ville give en direkte kontakt og i højere grad give en løbende føling med, om leverandøren lever op til sikkerhedskravene - En årlig ”temperaturmåling” i form af en revisorerklæring giver kun i begrænset omfang indsigt i leverandørens daglige håndtering af sikkerhedsspørgsmål. - Leverandøren udleverer endvidere kopi af diverse erklæringer, certificeringer m.v., som allerede foreligger. På drifts- og sikkerhedsmøderne rapporteres om sikkerhedsrelaterede incidents og changes, fremadrettede forbedringer af it sikkerheden, adgangsrettigheder, dataintegritet (gennemgang af adgangslogs), samt sikkerhedsangreb. Da ovenstående direktionsbeslutning har nogle år bag sig, har Direktør Karsten Juncher anmodet om, at der foretages en fornyet vurdering af beslutning. Dette arbejde blev igangsat medio marts og forventes afsluttet inden sommerferien (ultimo juni 2016). Flemming Gert Poulsen er tovholder og med i arbejdsgruppen sammen med Kundeservice.		

Nr.	Observationer	Risici	Anbefalinger
Nr.	Observationer	Risici	Anbefalinger
1	**Revisionsemne: Sikkerhed gennem systemspecifikke revisorerklæringer**		**Rammevilkår for funktionsområderne**
1.2 2015 Prio. 1	**Revisorerklæringer for CSC Classic systemer** Vi har konstateret, at SKAT ikke rekvirerer specifikke revisorerklæringer vedr. CSC Classic systemer fra it-serviceleverandøren CSC, som drifter mere end 20 væsentlige og risikofyldte systemer.	Risikoen er, at SKAT ikke opnår tilstrækkelig sikkerhed for, om it-driften af væsentlige og risikofyldte systemer håndteres forsvarligt og i overensstemmelse med aftalegrundlaget mellem SKAT og CSC.	Vi anbefaler, at SKAT for alle væsentlige og risikofyldte CSC Classic systemer outsourcet til CSC, rekvirerer systemspecifikke revisorerklæringer af typen ISAE 3402 type 2.
	Handleplan fra Claus Middelboe Andersen – Økonomi, IT Services: I 2011 fravalgte Direktionen at indhente en revisorerklæring fra CSC. Dette blev besluttet af følgende årsager: - Revisorerklæringer på alle de systemer CSC drifter, ville medføre omkostninger i millionklassen. - Etablering af sikkerhedsfora og månedlige driftsmøder med leverandører blev vurderet til, at ville give en direkte kontakt og i højere grad give en løbende føling med, om leverandøren lever op til sikkerhedskravene - En årlig "temperaturmåling" i form af en revisorerklæring giver kun i begrænset omfang indsigt i leverandørens daglige håndtering af sikkerhedsspørgsmål. - Leverandøren udleverer endvidere kopi af diverse erklæringer, certificeringer m.v., som allerede foreligger. På drifts- og sikkerhedsmøderne rapporteres om sikkerhedsrelaterede incidents og changes, fremadrettede forbedringer af it sikkerheden, adgangsrettigheder, dataintegritet (gennemgang af adgangslogs), samt sikkerhedsangreb. Da ovenstående direktionsbeslutning har nogle år bag sig, har Direktør Karsten Juncher anmodet om, at der foretages en fornyet vurdering af beslutning. Dette arbejde blev igangsat medio marts og forventes afsluttet inden sommerferien (ultimo juni 2016). Flemming Gert Poulsen er tovholder og med i arbejdsgruppen sammen med Kundeservice.		

Nr.	Observationer	Risici	Anbefalinger
2	**Revisionsemne: Risikovurdering af væsentlige it-systemer**		**Rammevilkår for funktionsområderne**
2.1 2015	**Manglende risikovurderinger** Vi har konstateret, at der ikke er udarbejdet risikovurdering for følgende væsentlige og risikofyldte it-system Digitalisering af	Risikoen er, at SKAT ikke har et samlet overblik over risici for alle væsentlige og risikofyldte it-systemer, og at dette øger risikoen for utilstrækkelig fokus på kritiske	Vi anbefaler, at SKAT indfører en proces, der sikrer en systematisk risikovurdering af alle SKATs it-systemer, inden hele it-systemer eller væsentlige dele af it-systemer idriftsættes.

Nr.	Observationer	Risici	Anbefalinger
Prio. 2	Selskabsskat (DIAS), inden dele af systemet blev idriftsat. Vi har dog noteret os, at der foreligger en udfyldt risikotjekliste anvendt i projektet. Risikotjeklisten vurderer dog ikke systemet på samme parametre som SKATs standardiserede risikovurderinger gør i RISK-systemet.	systemer både ved normal it-drift, og i tilfælde af it-driftsnedbrud m.m.	
	Handleplan fra Anna Sofie Bahnson Witzgall – Kundeservice, Digital udvikling, Projektledelse: Metode tager initiativ til et møde mellem procesejer (Sikkerhed) og kompetenceejer for projektledere i IT (Projekt- og programledelse), hvor det kan aftales, hvordan procesejer kan implementere og følge op på processen, herunder hvilke krav projektlederne skal opfylde. Mødet finder sted i Q1 2016.		
Nr.	**Observationer**	**Risici**	**Anbefalinger**
3	**Revisionsemne: Overblik over revisorerklæringer**		**Rammevilkår for funktionsområderne**
3.1 2015 **Prio. 2**	**<u>Manglende overblik over revisorerklæringer</u>** Vi har konstateret, at SKAT ikke har etableret et samlet overblik over de revisorerklæringer, der rekvireres, og at der ikke er placeret et entydigt ansvar for processen med rekvirering af revisorerklæringer. Vi har fået oplyst, at SKAT fremadrettet vil indarbejde oplysninger fra revisorerklæringer i "Systemoverblik".	Risikoen er, at SKAT ikke opnår et samlet overblik over revisorerklæringerne, hvilket kan medføre, at der ikke løbende følges op på eventuelle bemærkninger i erklæringerne.	Vi anbefaler, at SKAT indfører en proces, der sikrer en systematisk løbende: • opfølgning på, at alle revisorerklæringer indhentes • opfølgning på eventuelle bemærkninger i revisorerklæringerne.
	Handleplan fra Jacob Krause Schütz - Kundeservice, Digital udvikling, Projekt- og Porteføljestyring: Projekt- og Porteføljestyring tager initiativ til et møde med Underdirektør for Forretningsprocesser og Underdirektør for Digital Udvikling, hvor der kan aftales en proces for etablering af overblik og opfølgning på indhentede revisorerklæringer samt en fremtidig ansvarsfordeling af opgaven. Mødet finder sted i Q2 2016.		

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.