Skatteministeriet

28. april 2016
J. nr. 15-0956796
Plannr. 115-004

Intern Revision

Rapport 2015

Økonomi og IT

It-revision af driftssikkerhed

Modtager
Direktør Jesper Rønnow Simonsen, SKAT

Kopi
Direktør Karsten Juncher, Økonomi og IT
Departementet
Rigsrevisionen

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

Forord

Intern Revision (IR) har, jævnfør orienteringsbrev af 17. marts 2015, revideret driftssikkerhed. 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 28. april 2016

Kurt Wagner
Revisionschef

Aliriza Özden
Manager

1. Formål

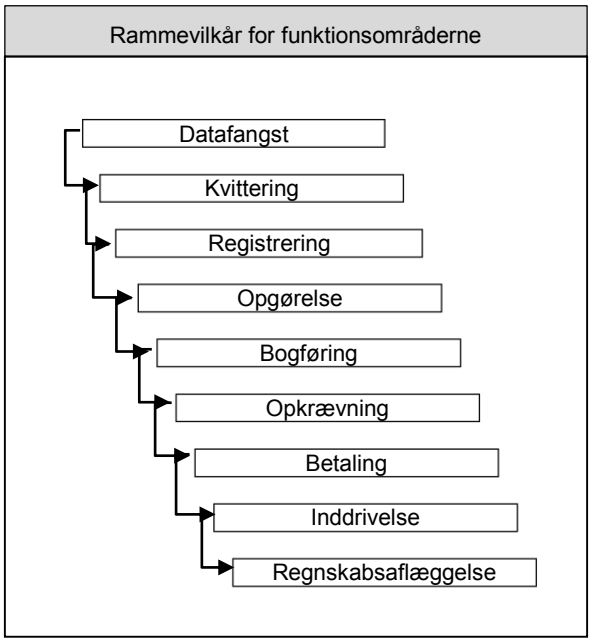
Formålet med revisionen af driftssikkerhed er at undersøge og vurdere, hvorvidt interne it-kontroller medvirker til at opretholde informationers integritet og sikkerheden af data. Mangelfuld implementering af krav til driftssikkerhed kan påvirke ydeevnen og øge risikoen for datatab samt medføre driftsforstyrrelser i SKATs it-systemer.

2. Omfang

Revisionen er udført i perioderne april til december 2015 med udgangspunkt i ISO 27001:2013 og har omhandlet emne ”A.12 Driftssikkerhed” med følgende hovedområder:

1) A.12.1 Driftsprocedurer og ansvarsområder
2) A.12.2 Beskyttelse mod malware (skadelige programmer, fx virus)
3) A.12.3 Backup
4) A.12.4 Logning og overvågning
5) A.12.5 Styring af driftssoftware
6) A.12.6 Sårbarhedsstyring
7) A.12.7 Audit af informationssystemer

SIR anvender følgende model til operationel beskrivelse og kategorisering af aktiviteterne i SKAT:



I forbindelse med denne revision har vi revideret driftssikkerhed, som udgør en del af ”Rammevilkår for funktionsområderne”.

Revisionen har omfattet leverandørerne CSC (TastSelv, SLUT, 3S, DMO mv.), NetCompany (Motor) og NNIT (SAP 38, SAP Intern mv.), som drifter en stor del af SKATs væsentlige og risikofyldte it-systemer, der understøtter processen for aflæggelse af § 9 og § 38 regnskaberne.

Revisionen er udført af Aliriza Özden i henhold til gældende revisionsstandarder, herunder vejledninger fra Rigsrevisionen. Revisionen er gennemført ved interviews, og stikprøvevis gennemgang af foreliggende materiale med medarbejdere fra IT og Økonomi.

3. Konklusion

Det er vores vurdering, at der **i mindre omfang er behov** for ændringer i de reviderede processer i relation til ISO-standarden benævnt "A.12 Driftssikkerhed".

Denne vurdering baserer vi på følgende forhold:

- Formålet med hovedområde "A.12.1 Driftsprocedurer og ansvarsområder" er at undersøge, om der er implementeret kontroller som sikrer korrekt og sikker drift af informationsbehandlingsfaciliteter. Det er vores vurdering, at **formålet ikke er opnået**, da driftsrapporter og generelle revisorerklæringer ikke giver høj sikkerhed for, at driftssikkerheden for SKATs systemer håndteres betryggende.

Det er vores vurdering, at **formålet** for nedenstående områder fra ISO-standarden **delvist er opnået**:

- "A.12.2 Beskyttelse mod malware" - om der er implementeret kontroller som sikrer, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.
- "A.12.3 Backup" - om der er implementeret kontroller, som beskytter mod tab af data.
- "A.12.4 Logning og overvågning" - om der er implementeret kontroller som registrerer hændelser og tilvejebringer bevis.
- "A.12.5 Styring af driftssoftware" - om der er implementeret kontroller, som sikrer integriteten af driftssystemer.
- "A.12.6 Sårbarhedsstyring" - om der er implementeret kontroller, som forhindrer, at tekniske sårbarheder udnyttes.
- "A.12.7 Audit af informationssystemer" - om der er implementeret kontroller, som minimerer virkningen af auditaktiviteter på driftssystemer.

Vi har i bilag 1 udarbejdet en samlet anbefaling til styrkelse af driftssikkerheden. Observationen er følgende:

- CSC drifter flere kritiske systemer og SKAT modtager månedlige driftsrapporter og årlige generelle revisorerklæringer for "CSC Classic" systemer. Det er vores vurdering, at driftsrapporter og generelle revisorerklæringer ikke giver sikkerhed for, at driftssikkerheden er

tilstrækkelig specifikt for SKATs systemer. Dette er beskrevet nærmere i bilag 1.

Vi har prioriteret de observerede forhold således:

Revisionsemne	**Prioritet 1** *Høj risiko*	**Prioritet 2** *Middel risiko*	**Prioritet 3/4** *Lille risiko*	**I alt**
1) Driftsprocedurer og ansvarsområder	**1**	**0**	**1**	**2**
2) Beskyttelse mod malware	**0**	**0**	**1**	**1**
3) Backup	**0**	**0**	**1**	**1**
4) Logning og overvågning	**0**	**0**	**4**	**4**
5) Styring af driftssoftware	**0**	**0**	**1**	**1**
6) Sårbarhedsstyring	**0**	**0**	**2**	**2**
7) Audit af informationssystemer	**0**	**0**	**1**	**1**
I alt	**1**	**0**	**11**	**12**

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

Vi har modtaget handleplaner fra det/de reviderede direktørområde/ 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: Driftsprocedurer og ansvarsområder**		**Funktionsområde: Rammevilkår**
1.1 2015 Prio. 1	**<u>Driftssikkerhed for "CSC Classic" systemer</u>** SKAT modtager månedlige driftsrapporter og årlige generelle revisorerklæringer for "CSC Classic" systemer. Driftsrapporterne og de generelle revisorerklæringer indeholder ikke tilstrækkeligt specifikke konklusioner om følgende områder: • Dokumenterede driftsprocedurer • Kapacitetsstyring • Kontroller mod malware • Backup af information • Hændelseslogning • Beskyttelse af log-oplysninger • Administrator- og operatørlogge • Tidssynkronisering • Softwareinstallation i driftssystemer • Styring af tekniske sårbarheder • Begrænsninger på softwareinstallation • Kontroller i forbindelse med audit af informationssystemer	Der er en forøget risiko for, at SKAT ikke løbende får sikkerhed for, at driftssikkerheden er tilfredsstillende for nogle af SKATs væsentligste og mest risikofyldte systemer under "CSC Classic" aftalen.	Vi anbefaler, at SKAT, for "CSC Classic" systemer outsourcet til CSC, rekvirerer systemspecifikke revisorerklæringer af typen ISAE 3402 type 2, som også omfatter følgende områder: • Dokumenterede driftsprocedurer • Kapacitetsstyring • Kontroller mod malware • Backup af information • Hændelseslogning • Beskyttelse af log-oplysninger • Administrator- og operatørlogge • Tidssynkronisering • Softwareinstallation i driftssystemer • Styring af tekniske sårbarheder • Begrænsninger på softwareinstallation • Kontroller i forbindelse med audit af informationssystemer

Nr.	Observationer	Risici	Anbefalinger
	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: Beskyttelse mod malware**		**Funktionsområde: Rammevilkår**
Området er omfattet af observation 1.1.			
3	**Revisionsemne: Backup**		**Funktionsområde: Rammevilkår**
Området er omfattet af observation 1.1.			
4	**Revisionsemne: Logning og overvågning**		**Funktionsområde: Rammevilkår**
Området er omfattet af observation 1.1.			

Nr.	Observationer	Risici	Anbefalinger
5	**Revisionsemne: Styring af driftssoftware**		**Funktionsområde: Rammevilkår**
Området er omfattet af observation 1.1.			
6	**Revisionsemne: Sårbarhedsstyring**		**Funktionsområde: Rammevilkår**
Området er omfattet af observation 1.1.			
7	**Revisionsemne: Audit af informationssystemer**		**Funktionsområde: Rammevilkår**
Området er omfattet af observation 1.1.			

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.