Skatteministeriet

26. januar 2016
J. nr. 15-0376916
Plannr. 115-003

Intern Revision

Rapport 2015

SKAT IT

It-revision af anskaffelse, udvikling og vedligeholdelse af systemer

Modtager
Direktør Jesper Rønnow Simonsen

Kopi
Direktør Karsten Juncher
Departementet
Rigsrevisionen

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

Forord

Intern Revision (IR) har, jævnfør orienteringsbrev af 12. marts 2015, revideret anskaffelse, udvikling og vedligeholdelse af systemer. Den udførte revision er en del af den samlede revision for 2015.

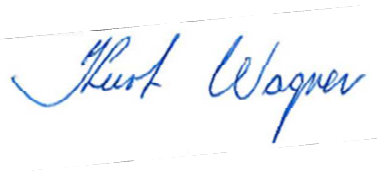
Rapporten indeholder en samlet konklusion omfattende det reviderede område. I konklusionsafsnittet redegør vi for de observationer, som konklusionen i det væsentligste er baseret på. Konklusionsafsnittet indeholder Intern Revisions bedømmelse af det reviderede område samt en beskrivelse af grundlaget 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 26. januar 2016



Kurt Wagner
Revisionschef

Aliriza Özden
Manager

1. Formål

Formålene med revisionen har været at undersøge og vurdere, hvorvidt interne it-kontroller hos SKAT medvirker til at opretholde informationers integritet og sikkerheden af data, herunder:

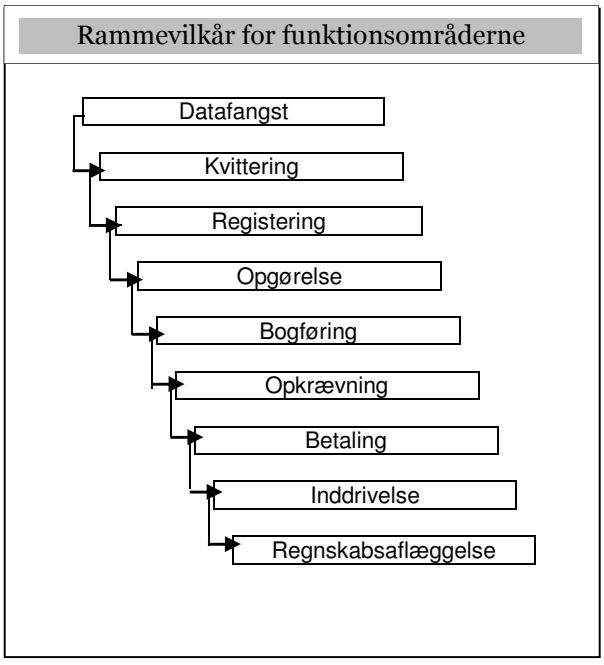
- at informationssikkerhed er en integreret del af informationssystemerne gennem hele livscyklussen,
- at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus,
- at testdata beskyttes.

Manglende eller sen implementering af informationssikkerhedskrav, ved anskaffelse, udvikling og vedligeholdelse af systemer, kan udgøre en risiko for væsentlig fejlinformation, svig samt manglende overholdelse af lovkrav.

2. Omfang

Revisionen er udført i perioden marts til juni 2015 med udgangspunkt i ISO standarden 27001 og har omfattet emne "A.14 Anskaffelse, udvikling og vedligeholdelse af systemer" med følgende hovedområder:

- A.14.1 Sikkerhedskrav til informationssystemer
- A.14.2 Sikkerhed i udviklings- og hjælpeprocesser
- A.14.3 Testdata



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.

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 Arkitektur & Innovation, Metode, Projekt- og programledelse, samt Projektchefer.

Vi har indhentet dokumentation dels fra SKATs digitale værktøjer fx projektportalen og SharePoint, dels fra ressourcepersoner i de respektive afdelinger.

Revisionen er primært udført ved gennemgang og vurdering af dokumentation fra projektet Mini One Stop Shop suppleret med interview af ressourcepersoner for udvalgte projekter vedrørende udvalgte kontroller.

Revisionen er udført af Henrik Stender og Aliriza Özden.

3. Konklusion

Det er vores vurdering, at der er **behov for procesændringer i større omfang** i de reviderede processer i relation "A.14 Anskaffelse, udvikling og vedligeholdelse af systemer".

Denne konklusion baserer vi på følgende forhold:

- Formålet med hovedområde "A.14.1 Sikkerhedskrav til informationssystemer" er, at undersøge om der er kontroller som sikrer, "at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen". Det er vores vurdering, at **formålet ikke er opnået**, hvilket blandt andet skyldes, at der ikke i alle tilfælde sker orientering af SIR ved ændringer af regnskabsrelaterede it-systemer og orientering af "Sikkerhed" ved faseskift.

- Formålet med hovedområde "A.14.2 Sikkerhed i udviklings- og hjælpeprocesser" er at undersøge om der er kontroller som sikrer, "at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus". Det er vores vurdering, at **formålet er opnået**, i relation til beskrivelser af rammedokumenter og anvendte værktøjer i det nuværende setup. Det er dog samtidig konstateret at udviklingsopgaverne i SKAT går i mod en mere agile metoder, hvilket kræver tilpasning af anvendte dokumenter.

- Formålet med hovedområde "A.14.3 Testdata" er at undersøge om der er kontroller som sikrer, "at beskyttelse af data, som anvendes til test". Det er vores vurdering, at **formålet ikke er opnået**, hvilket blandt andet skyldes at rammerne for sikring af testdata – fx brug af driftsdata, personoplysninger samt krav til testmiljøer ikke fremgår af SKATs politik for test.

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

- Manglende implementering af intern vejledning fra Sikkerhed i Metode kontoret bevirker, at Sikkerhed ikke har modtaget de i vejledningen forudsatte tilbagemeldinger i forbindelse med faseskift.

- Rammer for sikring af testdata - fx brug af driftsdata, personoplysninger, samt krav til testmiljøer - indgår ikke i SKATs politik for test eller Rammebeskrivelse for test i SKAT.

- SKATs tilsyn med leverandøren CGI vedrørende projektet Mini One Stop Shop har ikke omfattet en risikovurdering af en ekstern revisorerklæring.

Vi har prioriteret de observerede forhold således:

	Revisionsemne	**Prioritet 1** *Høj risiko*	**Prioritet 2** *Middel risiko*	**Prioritet 3** *Lille risiko*	**I alt**
A.14.1	Sikkerhedskrav til informationssystemer	0	3	1	**4**
A.14.2	Sikkerhed i udviklings- og hjælpeprocesser	0	1	0	**1**
A.14.3	Testdata	0	2	1	**3**
I alt		**0**	**6**	**2**	**8**

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.14.1	**Kontrolmål: Sikkerhedskrav til informationssystemer**		**Funktionsområde: Rammevilkår for funktionsområderne**
A.14.1.3 2015 Prio. 3	Link i projektportalen Projektportalen indeholder en række skabeloner og vejledninger som skal anvendes. Vi har ved vores gennemgang af materialet konstateret, at der er fejl i det anvendte link med teksten "Håndbog for risikoejere". Dokumentet, som der linkes til, er reelt vejledningen "Informations-sikkerhed, Projekter og Risikoregisteret".	Forkert og/eller misvisende navngivning af link udgør en risiko for fejl og uhensigtsmæssig anvendelse af vejledninger og skabeloner.	Vi anbefaler, at SKAT kvalitetssikrer link i projektportalen, hvor Sikkerhedsvejledningen (Informationssikkerhed, Projekter og Risikoregisteret – Informationssikkerhed 25. april 2014) forudsættes anvendt.
	Handleplan fra Kontoret for Projekt og Programledelse: Metode foretager en grundig gennemgang af Projektportalen for at kvalitetssikre links i dokumenter og på sitet. Hvor muligt vil links redigeres således, at der ikke linkes direkte til et dokument, men rettere til Sikkerheds sharepoint med henvisning til rette dokument. På den måde sikres vi, at vi altid henviser til gældende dokument, da dokumentet så skal findes på forfatterkontorets (Sikkerheds) sharepoint. Alle links på Projektportalen er rettet ved udgangen af Q1 2016.		
A.14.1.4 2015 Prio. 2	Orientering af Intern Revision Regnskabsinstruksen (§9 og §38) afsnit 3.4 Systemudvikling og –vedligeholdelse, indeholder krav om, at SIR på tidligst	Sen - eller manglende - inddragelse af Intern Revision udgør en risiko for, at nødvendige kontroller ikke implementeres rettidigt. Intern Revision varetager desuden informationspligten over for	Vi anbefaler, at processen for SKATs orientering af SIR ændres således, at SIR bliver orienteret tidligere i processen og inden nye systemer elle ændringer i systemer anvendes i produktion/drift.

	mulige tidspunkt inddrages i planlægningen og ændringer af regnskabs- og it-systemer. Vi har fået oplyst, at SIR generelt orienteres sent vedrørende planlagte ændringer af regnskabs- og it-systemer. F.eks. har SKAT anvendt "Værdipapirsystemet" (VPS) siden indkomståret 2010, men SIR har først modtaget formel orientering vedrørende "Værdipapir-systemet" i marts 2015. Vi er bekendt med, at overdragelses-dokumentet, der anvendes ved overdragelse af et it—system fra projekt til driftsorganisationen ligeledes indeholder punkter i relation til orientering af Intern Revision. Overgangen fra projekt til driftsorganisation bør ikke være styrende for orientering eller inddragelse af Intern Revision.	Rigsrevisionen. Manglende inddragelse af Intern Revision udgør en risiko for at SKAT ikke lever op til sin forpligtelse om orientering af Rigsrevisionen (som skal have mulighed for at udtale sig jf. Bekendtgørelse om statens regnskaber m.v.).	
	Handleplan fra Kontoret for Projekt og Programledelse: Metode foreslår, at det indskrives i SKATs projektmodel under Specifikationsfasen, at der skal rapporteres ind til SIR. Såfremt SIR har behov for rapportering tidligere i projektets levealder, bedes SIR kontakte Metode. Efterlevelse af kravet om rapportering skal ske i projekterne. Dette ansvar ligger hos Projekt- og Programledelse. SKATs projektmodel opdateres senest i Q2 2016. Kontaktperson: Hans Otto Nielsen.		

A.14.1.5 2015 Prio. 2	Risikostyring og risikoregister Kontoret for Sikkerhed i SKAT har udarbejdet vejledningen ”Informationssikkerhed, Projekter og Risikoregisteret”, som et supplement til Digitaliseringsstyrelsens ”Vejledning om risikostyring og anvendelse af risikoregisteret”. Vejledningen fra Kontoret for Sikkerhed er dateret 24. april 2014 og er publiceret via projektportalen. Et væsentligt element i vejledningen er orientering af Kontoret for ”Sikkerhed” om projekters risici ved projekternes faseskift (se også punkt 1.6). Kontoret for Sikkerhed har i perioden (frem til medio 2015) ikke modtaget de i vejledningen forudsatte tilbagemeldinger. Sammenholdt med interview af projektledere, vurderer vi, at vejledningen fra Kontoret for Sikkerhed ikke anvendes i praksis.	Manglende anvendelse af Kontoret for Sikkerheds vejledning i it-udviklingsprojekter udgør en risiko for at den udførte risikostyring ikke har en tilstrækkelig detaljeringsgrad og dermed en manglende eller sen håndtering af informations-sikkerhedsrisiciene, der er beskrevet i vejledningen.	Vi anbefaler, at SKAT implementerer vejledningen fra ”Sikkerhed” og at der sker orientering af ”Sikkerhed” ved faseskift. Er vejledningen ikke længere i overensstemmelse med SKATs aktuelle behov i it-udviklingsprojekter, bør indholdet ajourføres eller eventuelt slettes fra Projektportalen.
	Handleplan fra Kontoret for Metode: 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 vejledningen, herunder hvilke krav projektlederne skal opfylde. Mødet finder sted i Q1 2016. Kontaktperson: Anna Sofie Bahnson Witzgall Metode sikrer eventuelle konsekvensrettelser i henvisningerne til Sikkerhed i Projektportalen. Alle links på Projektportalen er rettet ved udgangen af Q1 2016.Kontaktperson: Lene Bjærre		

A.14.1.6 2015 Prio. 2	<u>Dialog med Kontoret for Sikkerhed</u> Jf. vejledningen "Informationssikkerhed, Projekter og Risikoregisteret" fra kontoret "Sikkerhed" skal der ske orientering til "Sikkerhed" om sikkerhedsrisici. Orientering skal ske ved projekternes faseskift jf. projektmodellen. Formålet med orienteringen af "Sikkerhed" er grundlaget for en efterfølgende rapportering af sikkerhedsrisici til SKATs direktion. Kontoret for Sikkerhed har oplyst, at de ikke modtager disse orienteringer.	Manglende systematisk orientering af "Sikkerhed" øger risikoen for manglende eller sen reaktion på akkumulerede sikkerhedsrisici.	Vi anbefaler, at behovet for - og forventninger til - projektorganisationernes rapportering afstemmes med kontoret for "Sikkerhed" og at vedtaget vejledning følges.
	Handleplan fra Kontoret for Metode: 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 vejledningen, herunder hvilke krav projektlederne skal opfylde. Mødet finder sted i Q1 2016. Kontaktperson: Anna Sofie Bahnson Witzgall Metode sikrer eventuelle konsekvensrettelser i henvisningerne til Sikkerhed i Projektportalen. Alle links på Projektportalen er rettet ved udgangen af Q1 2016. Kontaktperson: Lene Bjærre		

A.14.2	**Kontrolmål: Sikkerhed i udvikling- og hjælpeprocesser**		**Funktionsområde: Rammevilkår for funktionsområderne**
A.14.2.1 2015 Prio. 2	<u>Sikker udviklingspolitik</u> Arkitektur og Innovation, samt kontoret for "Metode" har beskrevet en lang række rammedokumenter og værktøjer, som understøtter, at informationssikkerhed tilrettelægges og implementeres i den traditionelle udviklingscyklus hos SKAT. F.eks. projektportalen, testpolitik og arkitekturguidelines m.v. I praksis arbejder SKAT i mod mere agil selvudvikling, hvor udviklingsopgaverne i højere grad end tidligere varetages internt. Der findes ikke en samlet politik, som sikrer, at informationssikkerhed tilrettelægges og implementeres ensartet i forskellige it-udviklingsscenarier.	Manglende beskrivelse af rammer og mål i forhold til informationssikkerhed i udviklingslivscyklussen udgør en risiko for et utilsigtet uensartet sikkerhedsniveau i udviklingen af SKATs it-løsninger.	Vi anbefaler, at SKAT beskriver rammerne for sikker udvikling i en samlet politik. Formålet er at sikre, at informations-sikkerhed tilrettelægges og implementeres på et ensartet niveau på trods af forskellige udviklingsscenarier.
	Handleplan fra Kontoret for Arkitektur & Innovation: A&I indkalder til et møde med Sikkerhed med deltagelse fra hhv. Metode, FOD og P&P, hvor en samlet sikkerhedspolitik for udviklingsmetoder drøftes. Mødet finder sted i Q1 2016. Kontaktperson: Jens Holst-Andersen. A&I eller Sikkerhedskontoret udarbejder en sikkerhedspolitik i samarbejde med FOD og Metode. Politikken er godkendt i Q2 2016. Kontaktpersoner: Jens Holst-Andersen, Jeanette Sporleder, Jane Dahl og Anna Sofie Bahnson Witzgall		
A.14.3	**Kontrolmål: Testdata**		**Funktionsområde: Rammevilkår for funktionsområderne**

A.14.3.1 2015 Prio. 3	<u>Løbende ajourføring af SKATs testpolitik</u> SKATs testpolitik er gældende for test af it-systemer i SKAT og forudsættes taget op til revision minimum én gang årligt. Politiken er senest ajourført 15. januar 2014.	Manglende løbende vurdering og ajourføring af SKATs testpolitik udgør en risiko for at regelsættet ikke er i overensstemmelse med SKATs aktuelle behov.	Vi anbefaler, at SKATs testpolitik revurderes/kvalitetssikres minimum 1 gang om året, herunder at revurderingen dokumenteres.
	Handleplan fra Kontoret for Metode: Metode foretager en revision af den gældende testpolitik. Det nuværende regelsæt dikterer, at den reviderede SKAT testpolitik skal godkendes af IT-ledelsen. Metode foreslår, at dette fremover ændres, således at man kun ved væsentlige ændringer i testpolitikken skal fremlægge til IT-ledelsens godkendelse. Revision foretages senest i Q2 2016. Kontaktperson: Hans Otto Nielsen		
A.14.3.2 2015 Prio. 2	<u>Sikring af testdata</u> Rammer for sikring af testdata - fx brug af driftsdata, personoplysninger, samt krav til testmiljøer - indgår ikke i SKATs politik for test eller Rammebeskrivelse for test i SKAT.	Manglende stillingtagen til sikring af testdata udgør en risiko i forhold til fortrolighed (fx Persondatalov) og datatab.	Vi anbefaler, at SKATs testpolitik udvides med beskrivelse af overordnede rammer for sikring af testdata fx brug af driftsdata, personoplysninger, samt krav til testmiljøer.
	Handleplan fra Kontoret for Metode: Metode udvider SKATs testpolitik med beskrivelse af overordnede rammer for sikring af testdata. Politik revideres (og udvides) senest i Q2 2016. Kontaktperson: Hans Otto Nielsen		
A.14.3.3 2015 Prio. 2	<u>Tilsyn med leverandører i it-udviklingsforløb</u> SKATs tilsyn med leverandøren CGI vedrørende projektet Mini One Stop Shop har ikke omfattet en risikovurdering af en ekstern revisorerklæring.	Manglende tilsyn med serviceleverandører i et udviklingsforløb udgør en trussel mod fortrolighed og tilgængelighed af SKATs (test) data og systemer.	Vi anbefaler, at SKAT indhenter eksterne revisorerklæringer fra serviceleverandører, hvor SKAT samarbejder om udviklingsprojekter og hvor sikring af testmiljøer og/eller testdata er relevant.

	Handleplan fra Kontor for Projekt- og Programledelse: Projekt- og programledelse tager initiativ til et møde med IT Styring og Aftaler, hvor det aftales, hvordan processen for indhentning af interne revisorerklæringer inkluderes i udbudsmaterialet, samt hvordan det efterleves i projekterne. Mødet finder sted i Q1. Kontaktperson: Jacob Krause Schütz
	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.