Skatteministeriet

25. februar 2015
J. nr. 14-0049141
Plannr. 11422

Intern Revision

Rapport 2014

Direktørområdet SKAT IT

It-revision af systemopdateringer (patching)

Modtager
Departementschef Jens Brøchner

Kopi
Direktør Jesper Rønnow Simonsen
Direktør Karsten Juncher, Økonomi
Direktør Jan Topp Rasmussen, SKAT IT

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

Forord

Skatteministeriets Interne Revision (SIR) har jævnfør orienteringsbrev af 22. januar 2014 revideret SKATs styring af systemopdateringer (patching). Den udførte revision er en del af den samlede revision for 2014.

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 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 prioriteter, 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 tilsikre, at Intern Revision og den reviderede enhed har en ensartet opfattelse af de observerede forhold. SKAT har efterfølgende udarbejdet handleplaner.

København, den 25. februar 2015

Kurt Wagner
Revisionschef

Aliriza Özden
Manager

1. Formål

Formålet med revisionen er at efterprøve, om SKAT i 2014 har sikret en korrekt og betryggende opdatering af systemer for at undgå uautoriserede ændringer, fejl, mangler og driftsforstyrrelser i forbindelse med opdatering af SKATs it-systemer.

Systemopdatering definerer vi som patching, hotfixes, service packs, maintenance releases til applikationer, styresystemer og databaser, der kan forbedre ydeevne samt begrænse risikoen for driftsforstyrrelser og uautoriserede adgange til SKATs data. Dette omfatter ikke funktionelle ændringer i programmer. Programændringer er omfattet af en særskilt revision i 2014.

På baggrund af revisionens observationer, er eventuelle afledte risici vurderet.

2. Omfang

Revisionen er gennemført i perioden april til oktober 2014 og har omfattet en efterprøvning af:

1) om der er udarbejdet formelle regler og procedurer for systemopdatering
2) om regler og procedurer for systemopdatering bliver fulgt af SKAT
3) om underleverandører følger SKATs regler for systemopdatering
4) om der er kontroller, der sikrer, at systemer bliver opdateret som forventet
5) om der eksisterer regler og procedurer for versionsstyring

Der har været fokus på følgende applikationer samt tilhørende styresystemer og databaser:

- SAP PS – Punktafgifter og selskabsskat
- DMR – Motorregistret
- Vareførsel I - Toldsystemer
- Administrativ IT – SKATs interne systemer

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

Ved revisionen har vi interviewet medarbejdere fra følgende afdelinger i SKAT:

- Betalings- og Inddrivelsessystemer (SAP PS)
- ESDH- og Toldsystemer (DMR)
- Platforme (Vareførsel I)
- It-service og Teknologi (Administrativ IT)

3. Konklusion

Det er vores vurdering, at kontrolmiljøet for styring af processen for systemopdateringer kan karakteriseres som værende "**ikke helt tilfredsstillende**".

Denne konklusion baserer vi på følgende forhold:

- SKAT har ikke klare regler for opdatering af systemer. Dette øger risikoen for, at SKAT ikke stiller de nødvendige krav – også overfor eksterne serviceleverandører. Dette vanskeliggør samt øger risikoen for en tidskrævende opfølgning på, hvordan og hvor ofte systemer skal opdateres.

- Det er ikke muligt for SKAT at følge op på, hvilke systemopdateringer der er tilgængelige, og hvilke den eksterne serviceleverandør har vurderet kritiske og installeret disse i tide. Kritiske opdateringer, der ikke installeres eller ikke installeres i tide af eksterne serviceleverandører, øger risikoen for driftsforstyrrelser og/eller uautoriserede adgange til SKATs data.

- SKATs administrative systemer er ikke opdateret periodisk. Dette øger risikoen for driftsforstyrrelser og/eller uautoriserede adgange.

- Grundet manglende funktionsadskillelse kan samme medarbejder i SKAT installere systemopdateringer til SAP-systemerne på alle it-miljøer uden tilstrækkelig afprøvning og godkendelse, hvilket øger risikoen for uautoriserede opdateringer.

Vi har prioriteret de observerede forhold således:

Revisionsområde	**Prioritet 1** *Kritisk for forretningen*	**Prioritet 2** *Væsentlig for forretningen*	**Prioritet 3** *Mindre betydning for forretningen*	**I alt**
1) Generelt	0	2	0	**2**
2) SAP PS	0	1	2	**3**
3) DMR	0	0	0	**0**
4) Vareførsel I	0	0	0	**0**
5) Administrativ IT	1	0	2	**3**
I alt	**1**	**3**	**4**	**8**

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 kan medvirke til en reduktion af de vurderede risici.

Bilag 1: Observationer, risici og anbefalinger

Nr.	Observationer	Risici	Anbefalinger
1	**Generelt**		
1.1 2014 P2	**Regler for systemopdatering** Af afsnit 10 i sikkerhedspolitikken version 4 dateret 1. juli 2013 fremgår det, at der skal være klare regler for opdatering af systemer, men disse eksisterer ikke. Uanset at systemerne bliver driftet og opdateret af eksterne serviceleverandører, bør SKAT have klare regler for opfølgning, omfang, hyppighed mv.	Manglende implementering af klare regler for styring af opdateringer øger risikoen for, at SKAT ikke stiller de nødvendige krav overfor eksterne serviceleverandører. Dette vanskeliggør samt øger risikoen for en tidskrævende opfølgning på, hvordan og hvor ofte leverandører opdaterer SKATs systemer.	SKAT bør opstille klare regler for styring af systemopdateringer herunder patches, hotfixes, service packs, maintenance releases for blandt andet styresystemer, databaser samt egen udviklede og købte applikationer. Reglerne bør som minimum omfatte omfang, hyppighed, hvornår og hvem der bør opdatere - også for systemer placeret hos eksterne serviceleverandører.
	Handleplan fra SKAT *Jeanette Sporleder Ebbesen, Sikkerhed*: SKAT er enig i observationen. Sikkerhed har udarbejdet en håndbog for risikoejere (system- og procesejere). Håndbogen fastlægger regler for efterlevelse af informationssikkerhedskravene og indeholder også en række konkrete og indirekte krav til systemopdateringer. De konkrete krav til systemopdateringer fremgår af håndbog for risikoejere afsnit 22 og 31. Ved udførelsen af en systemopdatering skal risikoejer ligeledes iagttage de krav, der stilles generelt i håndbogen, og særligt afsnit 25 samt 46 (indirekte krav). • Konkrete krav: o Afsnit 22. Beskyttelse af malware: a) Sikkerhedsopdateringer bliver installeret straks, dog først efter en test og konsekvensvurdering (max. 2 dage) e) Antivirus software og firewall er opdateret g) Sikkerhedssoftware opdateres og vedligeholdes j) Der er procedurer for sikkerhedsopdateringer		

Nr.	Observationer	Risici	Anbefalinger
	m) Sikkerhedsopdateringer testes jf. procedure o Afsnit 31. Styring af leverandørydelser: b) Er ansvarsfordelingen for ændringsstyring og Patch Management beskrevet? c) Er leverandørens modenhedsniveau for ændringsstyring og Patch Management tilfredsstillende? • Indirekte krav: o Afsnit 25. Styring af driftssoftware (Release Management) o Afsnit 46. ITIL (Release Management)		
1.2 2014 P2	**Opfølgning på systemopdatering** Vurdering og installation af systemopdateringer er styret af leverandører jf. eksisterende aftaler. Det fremgår dog ikke af driftsrapporter, hvilke opdateringer der er tilgængelige, og hvilke den eksterne serviceleverandør har vurderet kritiske. Det er således ikke muligt for SKAT at vurdere, om kritiske opdateringer er installeret i tide.	Sikkerhedsbrister eller fejlbehæftede systemer, der ikke opdateres eller opdateres for sent, påvirker ydeevne, øger risikoen for driftsforstyrrelser og/eller uautoriserede adgange til SKATs systemer.	SKAT bør periodisk følge op på, om væsentlige systemer fra fx Microsoft (Windows, Office, Exchange, MS SQL), Oracle (Java, Oracle DB), Adobe (Reader, Flash), Apple (Quicktime), SAP, Citrix mv. er opdaterede i tide.
	Handleplan fra SKAT *Martin Wood, It-service og Teknologi*: Bemærkning: Området henhører under Platforme – Johnni Jensen IT Service og Teknologi, har ekstern driftsleverandør på Citrix området. Her fremgår systemopdateringer, versioner, patchniveauer og driftsleverandørens anbefalinger af den månedlige driftsrapport. *Platforme, Johnni E Mandrup Jensen:* SKAT er delvis enig i observationen samt risikoen. I samarbejde med udbudsfabrikken, og evt. leverandører m.fl., skal der bl.a. opstilles krav til rapporteringer i driftsrapporterne.		

Nr.	Observationer	Risici	Anbefalinger
	I forhold til sikkerhedspatches på operativniveau (Windows, Linux, MVS m.fl), databaser (Oracle, MSSQL m.fl) og øvrige middelwareprodukter er det aftalt, at leverandøren kontakter SKAT om kritikaliteten, og om nødvendigheden af at etablere et "haste" servicevindue. Såfremt der ikke er tale om sikkerhedspatchning, vurderes systemopdateringer i hvert enkelt tilfælde. Her kan nævnes, at Oracle suiten ikke er opgraderet til nyeste versioner, fordi det kræver store udviklingsomkostninger fx at flytte fra Oracle Portal Server til Oracle Webcenter (SKATs portaler). Strategien for dette er en afklaring med Innovation og Arkitektur.		
2	**SAP PS**		
2.1 2014 P3	**Formaliseret proces**: Processen for styring af systemopdateringer, herunder enhancement (EHP) og support packages (SP) for SAP, er ikke nedskrevet og formaliseret. Der er ikke en entydig beskrivelse af ansvarsfordelingen mellem eksterne serviceleverandører og SKAT, herunder hvem der har ansvaret for EHP og SP, samt i hvilket omfang.	En uformel proces kan medføre en uensartet styring af opdateringer til SAP, hvilket ikke kan påvirke kvaliteten men forøge processens tidsanvendelse.	En nedskrevet og formaliseret proces for systemopdateringer bør udarbejdes, kommunikeres ud internt i SKAT og aftales med relevante eksterne serviceleverandører. Endvidere bør det via periodisk overvågning af processen for opdatering af systemer sikres, at den aftalte proces følges.
	Handleplan fra SKAT *Bente Kristensen, Betalings- og Inddrivelsessystemer*: SKAT er enig i observationen. Pr. 1. januar 2015 er SAP PS overgået til drift hos NNIT. I forhold til denne kontrakt er det leverandøren, der har ansvaret for implementeringen af processen. Processen bliver beskrevet i en ændringsanmodning, som skal godkendes i CAB, hvor både leverandøren og SKATs systemejere og platformsejere er med.		

Nr.	Observationer	Risici	Anbefalinger
2.2 2014 P2	**Funktionsadskillelse:** En og samme medarbejder i SKAT har mulighed for at installere support packages på både udviklings-, test- og produktionsmiljø uden opdagende kontroller.	Manglende funktionsadskillelse øger risikoen for uautoriserede opdateringer til SAP, idet det er muligt at idriftsætte support packages uden forudgående tilstrækkelig afprøvning og godkendelse.	Funktionsadskillelse bør etableres for at sikre, at samme medarbejder ikke kan installere opdateringer på både udviklings-, test- og produktionsmiljø. Dette bør sikres på alle SAP-løsninger, selvom de er placeret hos forskellige eksterne serviceleverandører.
	Handleplan fra SKAT *Bente Kristensen, Betalings- og Inddrivelsessystemer*: SKAT er enig i observationen. Det er systemejere, der pt. har muligheden. For at sikre funktionsadskillelsen, vil rollekonceptet inden 30. juni 2015 blive opdateret, hvor systemejer-rollen ikke længere har adgang til at installere support packages på udviklings-, test- og produktionsmiljøerne.		
2.3 2014 P3	**Interval for systemopdatering:** Support packages for SAP har været installeret en gang på to år af SKAT.	Risikoen, for uautoriserede adgange til SKATs systemer, øges ved, at eventuelle sikkerhedsbrister eller fejl i SAP rettes for sent.	SKAT bør ud fra en risikovurdering overveje et hyppigere interval for opdatering af SAP. Risikovurderingen bør både omfatte enhancement packs og support packages for at sikre, at også leverandøren installerer opdateringer i tide.
	Handleplan fra SKAT *Bente Kristensen, Betalings- og Inddrivelsessystemer*: SKAT er enig i observationen. Support packages installation har bl.a. på grund af transition været udskudt. SKAT vil sammen med NNIT i løbet af 2015 vurdere behovet for support packages på SAP.		
3	**DMR**		
	Ingen særskilte observationer.		

Nr.	Observationer	Risici	Anbefalinger
4	**Vareførsel I**		
	Ingen særskilte observationer.		
5	**Administrativ IT**		
5.1 2014 P3	**Formaliseret proces**: Processen for styring af systemopdateringer for interne systemer er ikke nedskrevet og formaliseret.	En uformel proces kan medføre en uensartet styring af systemopdateringer til interne systemer, hvilket ikke kan påvirke kvaliteten men forøge processens tidsanvendelse.	En nedskrevet og formaliseret proces for opdatering af administrative systemer bør udarbejdes, kommunikeres ud internt i SKAT og aftales med relevante samarbejdspartnere. Endvidere bør det via periodisk overvågning af processen for systemopdatering sikres, at den aftalte proces følges.
	Handleplan fra SKAT *Martin Wood, It-service og Teknologi*: SKAT er enig i observationen, og vil formalisere processen. En nedskrevet formaliseret proces forventes at kunne være klar 30-06-2015.		
5.2 2014 P3	**Dokumentation for afprøvning**: Det er konstateret, at dokumentationen for afprøvning af softwarepakker er mangelfuld, da det af dokumentationen ikke fremgår, i hvilket omfang de har været afprøvet og godkendt.	Mangelfuld dokumentation for afprøvning medfører et reduceret overblik over testomfang og testresultat. Dette kan forøge processens tidsanvendelse, men ikke påvirke kvaliteten af gennemførte opdateringer.	Det bør sikres, at systemopdateringer bliver idriftsat med dokumentation for tilstrækkelig afprøvning og godkendelse. Dokumentationen bør bl.a. indeholde oplysninger om testomfang, testresultat, godkendelse af drift, tidspunkt og involverede personer.

Nr.	Observationer	Risici	Anbefalinger
	Handleplan fra SKAT *Martin Wood, It-service og Teknologi*: SKAT er enig i observationen. Afprøvning og test dokumentation, er en del af Change processen, som er ved at blive implementeret. Softwarepakker testes i den almindelige test proces, der udføres af systemejer/projekter, testdokumentationen er derfor en del af test proces, og bør gennemføres af testmanager. Change proces med forøget test dokumentation forventes at kunne være klar 30-06-2015.		
5.3 2014 P1	**Opdatering af administrative systemer:** Kritisk software som Java, Flash, Reader, Shockwave, Silverlight og Microsoft-produkter bliver ikke opdateret periodisk. It-service og Teknologi informerer, at en arbejdsgang for periodisk opdatering af Administrativ IT skal igangsættes indenfor kort tid, men denne har ligget stille grundet frozen zone, der blev etableret for at sikre, at udvikling, afprøvning og idriftsættelse af nye systemer, såsom Skattekontoen, blev påvirket mindst muligt.	Software der ikke opdateres periodisk, øger risikoen for driftsforstyrrelser, ydeevne og/eller uautoriserede adgange til SKATs administrative systemer.	SKAT bør sikre, at software til administrative systemer opdateres periodisk (jf. anbefaling 1.2). Kritiske softwareopdateringer bør også installeres i frozen zone perioder baseret på en business impact analyse.
	Handleplan fra SKAT *Martin Wood, It-service og Teknologi*: SKAT er enig i observationen. Som IT Service og Teknologi beskrev overfor Revisionen, har SKAT vurderet, at hensynet til idriftsættelse af bl.a. Skattekontoren og EFI i en frozen zone periode ikke måtte forstyrres af versionsopdateringer og patchninger af standardsoftware. SKAT har derfor foretaget en risikovurdering og udsat de periodiske opdateringer i frozen perioden. SKAT er ikke uenig i at software skal opdateres periodisk, og som udgangspunkt foretages sikkerhedspatchning i forhold til uautoriserede adgange til SKATs systemer altid så hurtigt som muligt.		

Nr.	Observationer	Risici	Anbefalinger
	SKAT kan dog ikke altid opdatere og patche software, da der ofte er en lang række bindinger til SKATs forretningssoftware, der ved opdatering/patchning ikke ville kunne anvendes eller give driftsforstyrrelser, og som derfor kræver et længere varende test forløb for at kunne fungere efter en opdatering/patchning. Opdateringerne vil således også have ganske betydelige økonomiske konsekvenser i forhold til den vedligeholdelse af legacy applikationer, der så må foretages. SKAT har i forhold til de interne IT miljøer foretaget en lang række beskyttende foranstaltninger, der er med til at sikre at opdateringer i forhold til sikkerhed IKKE er helt så tidskritiske. Således er der etableret Firewalls, Proxy servere, Web scanning, mail scanning i flere niveauer, Antivirus og ikke mindst ”Whitelisting”, som beskytter de interne systemer mod anvendelse af ikke autoriseret software. SKAT vil i forbindelse med formalisering af proces jf. 5.1 beskrive, hvorledes de periodiske opdateringer og patchning skal ske, samt beskrive hvorledes ”Business Impact Analyse” skal dokumenteres i forhold til de områder, hvor periodiske opdateringer som følge heraf udelades. Iværksættelse af den formaliserede proces forventes at kunne implementeres 30-09-2015.		

Bilag 2: Anvendte skala

Ved vurderingen i konklusionen er følgende skala anvendt:	
Meget tilfredsstillende	Intern Revision har ikke konstateret svagheder i de forretningsgange og processer, der understøtter de reviderede område. Samtlige observationer kan henføres til prioritet 3. Prioritet 1: Ingen observationer Prioritet 2: Ingen observationer Prioritet 3: Samtlige observationer
Tilfredsstillende	Intern Revision har observeret enkelte svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationerne er omfattet af prioritet 3. Enkelte observationer med prioritet 2 kan dog forekomme. Samlet set udgør de implementerede forretningsgange et "tilfredsstillende" grundlag for administration af området. Prioritet 1: Ingen observationer Prioritet 2: Enkelte observationer Prioritet 3: Hovedparten af observationer
Ikke helt tilfredsstillende	Intern Revision har observeret flere svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationer er omfattet af prioritet 2 eller 3 med hovedvægten på prioritet 2. Enkelte observationer i prioritet 1 kan dog forekomme. Samlet set medfører svaghederne, at de implementerede forretningsgange udgør "et ikke helt tilfredsstillende" grundlag for administration af området. Der er som følge heraf en forøget risiko for • Væsentlig fejlinformation i regnskaber og ledelsesrapportering • Manglende overholdelse af gældende lovgivning • Manglende overholdelse af interne regler og retningslinjer • Manglende overholdelse af overordnede politikker • Manglende iagttagelse af "skyldige økonomiske hensyn" Prioritet 1: Enkelte observationer Prioritet 2: Hovedparten af observationer Prioritet 3: Et mindre antal observationer
Ikke tilfredsstillende	Intern Revision har observeret flere væsentlige svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationerne er omfattet af prioritet 1 eller 2 med hovedvægten på prioritet 1. Enkelte observationer i prioritet 3 kan forekomme. Samlet set medfører svaghederne, at de implementerede forretningsgange udgør et "ikke tilfredsstillende grundlag" for administration af området. Der er som følge heraf en væsentlig forøget risiko for: • Væsentlig fejlinformation i regnskaber og ledelsesrapportering • Manglende overholdelse af gældende lovgivning • Manglende overholdelse af interne regler og retningslinjer • Manglende overholdelse af overordnede politikker • Manglende iagttagelse af "skyldige økonomiske hensyn" • Manglende realisering af forretningsmålene for det reviderede område. Prioritet 1: Hovedparten af observationer Prioritet 2: Et mindre antal observationer Prioritet 3: Enkelte observationer

Prioritet skal ses i forhold til det reviderede område og er defineret således:

1. ***Kritisk for forretningen:*** Væsentlig svaghed i de etablerede forretningsgange/processer. Svagheden kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Der er en væsentlig forøget risiko for, at processens målopfyldelse ikke realiseres som følge af den konstaterede svaghed. Der bør straks iværksættes foranstaltninger med henblik på at udbedre de observerede svagheder.

2. ***Væsentlig for forretningen:*** Svaghed i de etablerede forretningsgange/processer. Svagheden kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Der er forøget risiko for, at processens målopfyldelse ikke realiseres i fuldt omfang som følge af den konstaterede svaghed. Der bør iværksættes foranstaltninger med henblik på at udbedre de observerede svagheder.

3. ***Mindre betydning for forretningen:*** Ingen væsentlige svagheder i de etablerede forretningsgange/processer. Det er dog muligt at designe de enkelte processer på en mere hensigtsmæssig måde, således at eksekveringen forbedres.