Skatteministeriet

6. februar 2015
J. nr. 14-4162205
Plannr. 114-340

Intern Revision

Rapport 2014

Direktørområde Inddrivelse

Opfølgningsrapport på afgivne anbefalinger vedrørende generelle it-kontroller i relation til D/R-systemet

Modtager
Departementschef Jens Brøchner

Kopi
Direktør Jesper Rønnow Simonsen, SKAT
Direktør Jens Sørensen, Inddrivelse, SKAT
Direktør Jan Topp Rasmussen, IT, SKAT

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

Forord

Skatteministeriets Interne Revision (SIR) har, jævnfør orienteringsbrev af 12. september 2014, udført opfølgningsrevision af D/R systemet. 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 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 tilsikre, at Intern Revision og den reviderede enhed har en ensartet opfattelse af de observerede forhold. SKAT har efterfølgende udarbejdet handleplaner.

København, den 6. februar 2015

Kurt Wagner
Revisionschef

Klaus Myssen
Senior Manager

1. Formål

Skatteministeriets Interne Revision (SIR) har i september og oktober måned 2014 fulgt op på tidligere afgivne anbefalinger i relation til generelle it-kontroller for D/R-systemet.

Ved opfølgningen har vi vurderet i hvilket omfang SKAT har implementeret afgivne anbefalinger fra rapporten "It-revision af generelle it-kontroller i relation til D/R-systemet" (j.nr. 13-5399723) og på den måde styrket it-sikkerheden i og omkring D/R-systemet.

2. Omfang

Vi har fulgt op på 8 anbefalinger, som har omfattet følgende områder:

- Drift af datacentre og netværk
- Anskaffelse, ændringer og vedligeholdelse af systemsoftware
- Anskaffelse, udvikling og vedligeholdelse af applikationssystemer
- Adgangssikkerhed.

Vi har ved opfølgningen, gennemgået den fysiske sikkerhed i relation til anvendte serverrum for D/R-systemet.

Opfølgningen er foretaget ved interviews, og ved indsamling og stikprøvevis gennemgang af foreliggende materiale samt ved fysisk observation. Ved revisionen er medarbejdere fra afdelingen it-drift interviewet.

Revisionen er udført af Klaus Myssen.

Denne opfølgning er udført parallelt med opfølgningen afgivne anbefalinger i relation til applikationskontroller i relation til D/R-systemet med selvstændig rapportering.

3. Konklusion

På baggrund af årets opfølgning og revision er det fortsat vores samlede vurdering, at de generelle it-kontroller i relation til D/R-systemet er på et **ikke-tilfredsstillende niveau**.

Denne konklusion er baseret på følgende forhold:

• Vores opfølgning viser, at SKAT har implementeret 4 af vores anbefalinger fra tidligere år, hvorfor disse er afsluttet.

• SKAT arbejder fortsat på, at få omlagt HVX-delen af D/R-systemet til en webbaseret grænseflade, med det formål, at kunne udskifte det "gamle" udstyr. (se evt. anbefaling 1.1.)

• SKAT har tilkendegivet, at der er 3 observationer, som de ikke ønsker at implementere. SKAT har dermed valgt at acceptere risikoen og ikke implementere anbefalingen:

1. Observationen vedrører "manglende benyttelse af AntiVirus-software", hvilket øger risikoen for, uautoriseret/skadelig kode med risiko for påvirkning af tilgængeligheden (anbefaling 1.3 i bilag 1).
2. Observationen vedrører "manglende anvendelse af personhenførbare bruger-id i relation til administrator-konti", hvilket øger risikoen for, at man ikke kan konstatere, hvilken medarbejder, som har benyttet disse konti (anbefaling 4.1 i bilag 1).
3. Observationen vedrører "Manglende patching". Der er ikke foretaget sikkerhedsopdatering af anvendt styresystem (AIX 4.21 GCOS6) siden 1997. De kørende versioner er endvidere udgået af support i 2001, hvilket øger risikoen for misbrug af kendte sårbarheder, hvilket kan påvirke system-, data- og driftssikkerhed. (se evt. anbefaling 2.1).

De afgivne anbefalinger fremgår af nedenstående oversigt (se bilag 1):

Revisionsemne	**Prioritet 1** *Kritisk for forretningen*	**Prioritet 2** *Væsentlig for forretningen*	**Prioritet 3** *Mindre betydning for forretningen*	**I alt**
Drifts af datacentre og netværk	**1**	**1**	**0**	**2**
Anskaffelse, ændringer og vedligeholdelse af system-software	**1**	**0**	**0**	**1**
Anskaffelse, udvikling og vedligeholdelse af ap-plikationssystemer	**0**	**0**	**0**	**0**
Adgangssikkerhed	**1**	**0**	**0**	**1**
I alt 2014	**3**	**1**	**0**	**4**
I alt 2013	**6**	**1**	**1**	**8**

Prioriteringerne 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 som er indarbejdet i bilag 1. 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

Observationer		Risici	Anbefalinger
1.	**Drifts af datacentre og netværk**		
1.1. Prioritet 1 Overført anbefaling 12-04906 fra 2012	<u>Gammelt udstyr</u> Intern Revision har i forbindelse med tidligere revision nr. 12- 053 "Fysisk Sikkerhed", udført i 2012, observeret, at D/R-systemet benytter ældre BULL AIX udstyr. Udstyret kan ikke genanskaffes på grund af alder. SKAT har i forbindelse med en omorganisering fået 20-25 maskiner til overs, som nu anvendes til reservedele. Intern Revision har fået oplyst, at SKAT har valgt at lade udstyret stå i maskinstuen i Østbanegade med den begrundelse, at systemet er under udfasning, og at der ikke er sikkerhed for kontinuerlig drift efter en evt. flytning. **Status 2013:** Vi har fået oplyst, at DR-systemejer er ved at undersøge muligheden for, at det resterende D/R skal overføres til en SAP-løsning eller videreføres i en moderniseret stand, herunder en afvikling af frontenden. **Status 2014:** Systemet er endnu ikke udskiftet. Analysen af HVX-delen af D/R-systemet er afsluttet og grundet chefskifte udestår fortsat en stillingtagen til systemets	Manglende vedligeholdelse og opdatering af anvendt it-materiel, øger risikoen for, øgede driftsproblemer, hvilket kan påvirke tilgængeligheden.	Intern Revision anbefaler, at SKAT udskifter det forældede udstyr med henblik på, at sikre en kontinuerlig og acceptabel tilgængelighed af D/R-systemet. Alternativt bør SKAT overveje, at migrere nuværende funktionalitet til nyere plaform, hvilket muliggør en fremtidig support.

Observationer		Risici	Anbefalinger
	fremtid. En stillingtagen forventes at foreligge primo 2015. Vi har i forbindelse med revisionen fået kendskab til at den HW-tekniker, som SKAT benytter hos Steria fylder 65 år i august 2015 og forventes at stoppe umiddelbart efter. Det vil ikke være muligt for SKAT at få HW support til de kørende Escala-serverne, efter teknikeren fratrædelse. **Vi anser fortsat punktet for åbent.**		
	Høringssvar fra SKAT: SKAT vil jf. SIR's anbefaling, undersøge muligheden for udskiftning af udstyret. Det er dog samtidig SKAT's indtryk, at "rød prioritet 1 væsentlig mangel" er for "hårdt dømt", idet der er reservedele til flere år. Se endvidere handleplanens punkt 11 Ansvarlig; DR systemejer. **Høringssvar fra SKAT 2013:** I efteråret 2013 har IT-Drift påbegyndt en analyse af HVX-delen af D/R-systemet. Som følge af nogle organisatoriske ændringer ligger opgaven p.t. stille. IT-Drift forventer analysen færdiggjort i 2014. **Høringssvar fra SKAT 2014:** SKAT har januar 2015 iværksat en proces med at få omlagt HVX-delen af D/R systemet til en webbaseret grænseflade. Forventes afsluttet 3. kvartal 2015, hvilket betyder, at alt det gamle udstyr kan "skrottes".		
1.3. 2013 Prioritet 2	<u>Benyttelse af AntiVirus-software</u> Vi har fået oplyst, at der ikke er installeret antivirus beskyttelse på nogle af Escala-serverne, som drifter D/R- systemet. **Status 2014:** Vi har fået oplyst, at netværksgruppen har undersøgt muligheden for virusscanning af datatrafikken til og fra Escala-serverne. Grundet anvendelse af forskellige kommunikationsprotokoller	Manglende AntiVirus software øger risikoen for uautoriseret/skadelig kode med risiko for påvirkningen af tilgængelighed.	Vi anbefaler, at der installeres AntiVirus-software på de pågældende servere, og at AntiVirus-softwaren opdateres løbende. Alternativt vil vi anbefale, at der etableres anden foranstaltning til beskyttelse mod skadelig kode på D/R- serverne.

Observationer		Risici	Anbefalinger
	er en virusscanning ikke mulig. SKAT er bekendt med, og har valgt at leve med risikoen. **Vi anser fortsat punktet for åbent.**		
	Høringssvar fra SKAT: Der findes ikke AntiVirus-software til de gamle HVX-maskiner. Netværksgruppen undersøger mulighederne for en eventuel scanning af datatrafikken til og fra HVX-maskinerne. Tidshorisont: 1. halvår 2014.		
1.4. 2013 Prior itet 3	<u>Gamle Backup-bånd</u> Ved vores gennemgang af brandskabe med backupbånd er der identificeret en del backup bånd fra tidligere servere samt backups, som nu er omfattet af backuprutinerne hos Interxion/Steria. Vi kunne ikke af båndene se, hvor lang tid disse skulle opbevares, inden de skulle overskrives eller destrueres. **Status 2014:** Vi har konstateret, at der er foretaget oprydning i anvendte brandskab, og at det nu er noteret, hvornår de eksisterende bånd skal kasseres. **Vi anser punktet for lukket.**	Manglende kendskab til anvendte backupbånds rotationsplan øger risikoen for unødig opbevaring af gamle data.	Vi anbefaler, at det undersøges, hvorvidt backupbånd fra tidligere servere fortsat er relevante at opbevare, samt at det noteres, hvornår de pågældende bånd kan genanvendes eller destrueres.
	Høringssvar fra SKAT: Der er taget initiativ til oprydning/kassation og konvertering til en backup-robot hos Interxion. Tidshorisont: 1. halvår 2014. Backup-rutinerne omkring HVX-maskinerne er ok.		
1.5.	<u>Nød- og beredskabsplaner</u>	Manglende nød- og	Vi anbefaler, at SKAT på baggrund af en risikoanalyse

Observationer		Risici	Anbefalinger
2013 Prioritet 1	Vi har fået oplyst, at SKAT i relation til D/R-systemet ikke har udarbejdet nød- og beredskabsplaner for de regionale systemer, som er placeret i Østbanegade og i Haderslev. **Status 2014:** Vi har modtaget kopi af udarbejdet "nødprocedure" af 7.maj 2014, som omhandler hvornår og hvordan, der skal ske reetablering af backup-server ES46. Samtidig er det oplyst, at de har foretaget test af reetableringen, og at denne test forløb tilfredsstillende. Det er vores vurdering, at dette er tilstrækkeligt. **Vi anser punktet for lukket.**	beredskabsplaner øger risikoen for, at SKAT, i tilfælde af en nød- eller katastrofesituation, ikke vil kunne reetablere de regionale systemer inden for den tidshorisont, som ledelsen forventer, hvilket kan blive kritisk for SKAT	udarbejder en skriftlig nød- og beredskabsplan, der godkendes af ledelsen. Nød- og beredskabsplanen skal tage højde for SKAT' afhængighed i relation til tilgængeligheden af D/R-systemet. Endvidere anbefaler vi, at nødplanen testes årligt.
	Høringssvar fra SKAT: Punktet er undersøgt, og der findes p.t. ingen nød- og beredskabsplan, hverken i Haderslev eller i Østbanegade. Der skal udarbejdes en plan. Dette vil ske i 1. halvår 2014.		
2.	**Anskaffelse, ændringer og vedligeholdelse af systemsoftware**		
2.1. 2013 Prioritet 1	<u>Manglende patching</u> Vi har fået oplyst, at der ikke er sket patching af AIX 4.21 GCOS6 siden 1997. De kørende versioner er endvidere udgået af support i 2001. **Status 2014:** Området er uændret og skal ses i sammenhænge	Manglende patching, øger risikoen for misbrug af kendte sårbarheder.	Vi anbefaler, at der sker opgradering til en AIX version, som supporteres. Alternativt anbefaler vi, at løsningen flyttes til et nyere it-miljø.

Observationer		Risici	Anbefalinger
	med den manglende stillingtagen til HVX-delen. De af brugerne anvendte applikationer er kodet så de kun kan afvikles under styresystemet GCOS6 med tilhørende software DM6TP (disse komponenter udgik af support omkring 2003). I 1995 blev GCOS6 virtualiseret med softwarekomponenten hvx(version B30.0). Denne hvx version kan kun afvikles på aix servere med AIX 4.2.1. (AIX 4.2.1 udgik af support omkring 2003). Der er derfor ikke foretaget sikkerhedsopdatering af anvendt styresystem (AIX 4.2.1, GCOS6, DM6TP mm) idet dette ikke længere leveres. SKAT er bekendt med, og har valgt at leve med risikoen. **Vi anser fortsat punktet for åbent.**		
	Høringssvar fra SKAT: Da udstyret er meget gammelt, er der ikke mulighed for patchning.		
3.	**Anskaffelse, udvikling og vedligeholdelse af applikationssystemer**		
3.1. 2013 Prior itet 1	<u>Ændringsstyring</u> Vi har fået oplyst, at der ikke er udarbejdet nogen formel change management proces for, hvordan ændringer i D/R-systemet skal udvikles og håndteres. **Status 2014:**	Manglende formelle change management processer øger risikoen for uautoriserede ændringer.	Vi anbefaler, at der bliver udarbejdet en tilpasset change management proces for D/R-systemet, som sikrer, at kun testede og godkendte ændringer flyttes til driftsmiljøet.

Observationer		Risici	Anbefalinger
	Vi har modtaget kopi af dokumentet "Ændrings- og versionsstyring" og finder dokumentet anvendelig i relation til change processen. **Vi anser punktet for lukket.**		
	Høringssvar fra SKAT: IT-Drift udarbejder en change management procesbeskrivelse. Tidshorisont: 1. kvartal 2014.		
3.2. 2013 Prioritet 1	<u>Versionsstyring</u> Vi har fået oplyst, at der ikke er udarbejdet nogen formel proces for versionsstyringen af programkoden i forhold til D/R-systemet. **Status 2014:** Vi har til skærm set, at der sker versionsstyring direkte i kildekoden. Vi har endvidere set, at dette beskrives i dokumentet "Ændrings- og versionsstyring". Det er vores vurdering, at dette er tilstrækkeligt og anvendeligt. **Vi anser punktet for lukket.**	Manglende formel versionsstyring øger risikoen for, at kendskabet til, hvilke ændringer, der er udført, fortabes.	Vi anbefaler, at der bliver udarbejdet en formel proces, som sikrer fastholdelse og kendskab til, hvilke ændringer der er udført og i hvilke versioner i kildekoden til DR-systemet.
	Høringssvar fra SKAT: IT-Drift udarbejder en change management procesbeskrivelse. Tidshorisont: 1. kvartal 2014.		
4.	**Adgangssikkerhed**		
4.1. 2013 Prioritet 1	<u>Manglende anvendelse af personhenførbare bruger-id i relation til admin-konti.</u> Vi har fået oplyst, at der benyttes 3 brugerkonti med	Manglende anvendelse af personhenførbare bruger-id i forbindelse	Vi anbefaler, at der oprettes personhenførbar bruger-id til de pågældende medarbejdere med administrator rettigheder, hvis de har et arbejdsbetinget behov for disse rettigheder.

Observationer		Risici	Anbefalinger
	administrator rettigheder. Det er ROOT, ADMINX og BOOSSX. Det er samtidig oplyst, at der er personer, der benytter disse admin-konti til administration og styring af D/R systemet. **Status 2014:** Området er uændret. SKAT har tilkendegivet, at de ikke ønsker at ændre ved disse brugerkonti. SKAT er bekendt med, og har valgt at leve med risikoen. **Vi anser fortsat punktet for åbent.**	med admin-konti øger risikoen for, at man ikke kan se, hvilken medarbejder, som har udført hvilke ændringer.	
	Høringssvar fra SKAT 2013: Der findes ikke tilstrækkelig viden til sikkert at kunne udføre opgaven. Der er stor risiko for, at der kan opstå uforudsigelige konsekvenser ved at foretage ændringer, herunder stor risiko for at man ikke kan genskabe adgangen til disse administrator konti. Det er derfor IT-Drifts opfattelse, at det er for risikofyldt at forsøge at foretage ændringer i det eksisterende set-up.		
	SLUT		

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.