Skatteministeriet

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

Intern Revision

Rapport 2014

Direktørområde Inddrivelse

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

Modtager
Departementschef Jens Brøchner

Kopi
Direktør Jesper Rønnow Simonsen, SKAT
Direktør Jens Sørensen, Inddrivelsen, 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.

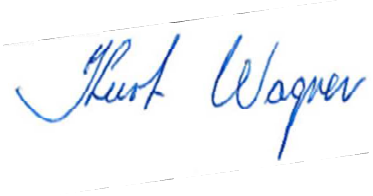
Rapporten indeholder en samlet konklusion omfattende det reviderede område. I konklusionsafsnittet redegør vi for de observationer, som konklusionen i det væsentligste er baseret på. Konklusionsafsnittet indeholder Intern Revisions bedømmelse af det reviderede område samt en beskrivelse af grundlaget 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 applikationskontroller for D/R-systemet.

Ved opfølgningen har vi vurderet i hvilket omfang SKAT har implementeret afgivne anbefalinger fra rapporten "It-revision af applikations 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 12 anbefalinger, som har omfattet følgende områder:

- Systemdokumentation mm.
- Adgangsrettigheder og funktionsadskillelse
- Behandling af inddata
- Proceskontroller
- Behandling af uddata
- Transaktions- og kontrolspor.

Vi har ved opfølgningen, gennemført en fornyet test af nøgle-kontroller i relation til manuelle indtastninger af momsangivelser og A-skat i 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 IT interviewet.

Revisionen er udført af Klaus Myssen.

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

3. Konklusion

På baggrund af årets opfølgning og revision er det vores samlede vurdering, at de interne kontroller i DR-systemet er på et **tilfredsstillende** niveau.

Denne konklusion er baseret på følgende forhold:

- Vores opfølgning viser, at SKAT har implementeret 9 af vores anbefalinger fra tidligere år, hvorfor disse er afsluttet.

- SKAT arbejder fortsat med en anbefaling vedrørende afhængigheden af "Nøglepersoner". Der arbejdes på, at flytte D/R-systemet til anden platform som kan serviceres af flere medarbejdere (anbefaling 2.7 i bilag 1)

- SKAT har tilkendegivet, at der er en observation, som de ikke ønsker at implementere. SKAT har dermed valgt at acceptere risikoen og ikke implementere anbefalingen.
  1. Der er i juni måned 2014 udarbejdet en risikoanalyse for D/R. Det fremgår af risikoanalysen, at DR er sikret godt imod: Hacking, Virus og Hardware-fejl samt at der sker vedligeholdelse af systemet. Vi har kendskab til, at der ikke er installeret antivirus software, at DR afvikles på gammelt hardware, og at der ikke er sket patching af operativsystemet til DR siden 1997 (se evt. anbefaling 1.2.).

- Vi har ud fra væsentlighed og risiko testet udvalgte kontroller i relation til momshåndteringen og A-skat i DR systemet. Vi har i den forbindelse ikke konstateret svagheder i de undersøgte kontroller, hvorfor det fortsat er vores vurdering, at kontrolmiljøet i relation til momshåndteringen og A-skat i DR systemet bidrager til nøjagtigheden af manuelt indtastede data.

Vores revision viser dog også, at SKAT i stort omfang har arbejdet med tidligere konstaterede svagheder i områderne for "adgangsrettigheder og funktionsadskillelse", hvorfor sikkerheden på disse væsentlige områder er forbedret.

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**
Systemdokumentation	**0**	**1**	**0**	**1**
Adgangs-rettigheder og funktionsadskillelse	**0**	**1**	**0**	**1**
Behandling af inddata	**0**	**0**	**0**	**0**
Proceskontroller	**0**	**0**	**0**	**0**
Behandling af uddata	**0**	**0**	**0**	**0**
Transaktions- og kontrolspor	**0**	**0**	**0**	**0**
I alt 2014	**0**	**2**	**0**	**2**
I alt 2013	**6**	**4**	**2**	**12**

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.	**Systemdokumentation**		
1.2. Prioritet 2 Overført anbefaling 12-04907 fra 2012	<u>Risikoanalyse</u> Intern Revision har konstateret, at seneste risikoanalyse for D/R er udarbejdet i 2011. Intern Revision har desuden observeret, at forholdene vedrørende gamle BULL AIX udstyr ikke er omtalt i risikoanalysen. **Status 2013:** Vi har fået oplyst, at risikoanalysen vil blive opdateret årligt og vil blive gennemført i jan-feb. 2014 således, at der følges samme kadence som for øvrige applikationer. Risikovurdering af BULL AIX vil ske i samme opdatering. **Status 2014:** Vi har konstateret, at der i juni måned 2014 er udarbejdet en ny risikoanalyse for D/R. Vi har foretaget en gennemgang af analysen og er ikke enig i den samlede vurdering. Det fremgår blandt andet af risikoanalysen, at DR er sikret godt imod: 1. Hacking og Virus 2. Hardware-fejl 3. Og at der sker "Vedligeholdelse af systemet" Vi har kendskab til, at 1. der ikke er installeret AW-SW eller andet, der beskytter mod skadelig kode 2. DR afvikles på gammelt HW, og at der ikke længere	Manglende analyse af de risici, som it-anvendelse indebærer, kan betyde, at risici ikke er synliggjort, og at der er risici ved it-anvendelsen, der ikke i tilstrækkeligt omfang er afdækket til et niveau, som ledelsen kan acceptere. Det kan endvidere betyde, at der ikke er tilstrækkelig sikkerhed omkring systemer og data og dermed fortrolighed, pålidelighed og tilgængelighed.	Intern Revision anbefaler, at SKAT i lighed med øvrige systemer foretager en årlig opdatering af it-risikoanalysen for D/R-systemet i overensstemmelse med Skatteministeriets koncernpolitik for informationssikkerheds it-regler afsnit 4. Intern Revision anbefaler, at SKAT foretager en revurdering af den udarbejdede risikoanalyse og eventuel uddybe områderne for: • Hacking og Virus • Hardware-fejl • Vedligeholdelse af systemet

Observationer		Risici	Anbefalinger
	kan anskaffes nyt HW 3. der ikke er sket patching af DR siden 1997 SKAT har tilkendegivet, at de ikke ønsker at udføre yderligere på området. SKAT er bekendt med, og har valgt at leve med risikoen. **Vi anser fortsat punktet for åbent.**		
	Høringssvar fra SKAT: SKAT tager SIRs anbefaling til efterretning og vil fremover foretage en årlig opdatering af risikoanalysen. Frist: 1.10.2013 **Høringssvar fra SKAT 2013:** Der pågår p.t. rettelser i risikoanalysesystemet. Når disse rettelser er foretaget, vil der blive foretaget risikoanalyse. Tidshorisont marts/april 2014.		
1.3. 2013 Prior itet 3	<u>Drifts af andre databaser end D/R relaterede</u> Vi har fået oplyst, at der på Escala-serveren (ES14), driftes 33 Oracle databaser, indeholdende statiske regionale bogholderioplysninger fra perioden 1996 til 1999. Vi har samtidig fået oplyst, at ES14 serveren på sigt ønskes udfaset i lighed med de øvrige Escala-servere, på grund af hardware-alder og mindre muligheder for at få reservedele. **Status 2014:** Vi har set dokumentation for, at de Oracle databaser som var placeret på serveren ES14 er slettet. **Vi anser anbefalingen for lukket.**	Risikoen ved at have data liggende på en server, hvortil der ikke længere kan skaffes reservedele, øger risikoen for, at data tabes ved hardware nedbrud.	Vi anbefaler, at det undersøges, om de omtalte databaser kan flyttes til et andet miljø.

Observationer		Risici	Anbefalinger
	Høringssvar fra SKAT 2013: IT-Drift har undersøgt sagen og fundet at serveren kan lukkes/nedtages. Der vil foregå destruktion af serverens data efter gældende retningslinjer for destruktion af data, når serveren nedtages. Tidshorisont: 2014.		
1.4. 2013 Prioritet 3	<u>Drifts af servere, placeret i Østbanegade</u> Vi har fået oplyst, at den medarbejder i SKAT, som supportere Escala serverne i serverrummet i Østbanegade, er fysisk tilhørende i NEG. Det er samtidig oplyst, at medarbejderen dagligt skal foretage skift af backup medie, ligesom andre driftsforstyrrelser kan kræve en fysisk tilstedeværelse i serverrummet, hvilket har givet anledning til flere daglige transporter mellem Østbanegade og NEG. **Status 2014:** It-drift har overvejet forskellig løsningsmuligheder, men finde den nuværende løsning for mest optimal. SIR er enig. **Vi anser anbefalingen for lukket.**	Daglig transport mellem to lokationer er både tids- og ressourcekrævende. Ressourcer som kunne anvendes mere hensigtsmæssigt.	Vi anbefaler, at det overvejes at flytte driften af D/R-systemet til nyere platform, som muliggør fjernstyring af serverne. Alternativt kan medarbejderen som udfører support på Escala serverne, fysisk blive placeret i Østbanegade, eller supporten kan overdrages til en medarbejder i Østbanegade.
	Høringssvar fra SKAT 2013: IT-Drift vil overveje bemærkningen, men finder ikke den eksisterende lokalisering er til hinder for fornuftig drift.		
1.5. 2013 Prioritet 2	<u>Ajourføring af "Systemoverblik"</u> Vi har konstateret, at systemet "Systemoverblik" i relation til D/R-systemet ikke er ajourført med de faktiske systemsammenhænge.	Manglende opdatering af systemoverblik, med relevante	Vi anbefaler, at systemoverblik opdateres med de faktiske informationer i relation til D/R-systemet, herunder en ajourføring af systemsammenhængen.

Observationer		Risici	Anbefalinger
	Vi har kendskab til, at systemejer har udarbejdet en ny systemsammenhæng oversigt, som viser de kørende systemer, herunder integration til DMO, og at oversigten er overdraget til brug for en opdatering af "systemoverblik". **Status 2014:** Vi har foretaget en fornyet gennemgang af "Systemoverblik" i relation til D/R-systemet, og kan se, at beskrivelsen er ajourført med nye systemsammenhænge og en ny beskrivelse af systemet. **Vi anser anbefalingen for lukket.**	informationer, øger risikoen for, at informationer om D/R systemet ikke kan fastholdes.	
	Høringssvar fra SKAT 2013: Ajourført materiale sendt til Arkitektkontoret den 11.12.13. Systemoverblikket er endnu ikke ajourført. Rykket Arkitektkontoret den 14.01.14. Tidshorisont: 1. kvartal 2014.		
2.	**Adgangsrettigheder og funktionsadskillelse**		
2.1. Prioritet 1 Overført anbefalin	<u>Logisk adgangssikkerhed</u> Intern Revision har konstateret, at der i D/R systemet kan anvendes password på ét tegn, ligesom det er muligt at ændre password ved at genbruge det password, man havde i forvejen. Dvs.,at systemet accepterer ændringer af password uden at det reelt gennemføres. **Status 2013:**	Manglende krav til passwords kompleksitet eller jævnlig skift af passwords øger risikoen for uautoriseret adgang til systemer og data.	Intern Revision anbefaler, at SKAT tilpasser D/R-systemet således, at krav til password, som minimum følger Skatteministeriets koncernpolitik for informationssikkerheds it-regler afsnit 11.3 Dvs., at password som minimum skal: - bestå af min. 8 tegn - være en blanding af store og små bogstaver - indeholde minimum ét stort bogstav

Observationer		Risici	Anbefalinger
g 12-049 01 fra 2012	Vi har fået oplyst, at SKAT fortsat arbejder på en løsning omkring opbygningen af password på HVX maskinerne. **Status 2014:** Vi har fået oplyst, at pwd-kvaliteten er hævet, og at der nu kæves min. 8 tegn, store og små bogstaver samt minimum ét tal. Vi har indhentet kopi af kildekoden og kan se, at koden er ændret i marts 2014, og at koden indeholder omtalte pwd-krav. Vi har prøvet at logge på D/R og kan konstatere, at kravet til nye pwd er steget. **Vi anser anbefalingen for lukket**		- indeholde minimum ét tal og/eller ét specialtegn.
	Høringssvar fra SKAT: SKAT er enig i SIRs anbefaling og vil undersøge muligheden for at efterkomme anbefalingen. SKAT vil endvidere undersøge muligheden for at oprette unikke brugernumre, så samme brugernummer ikke eksisterer på forskellige regioner. **Høringssvar fra SKAT 2013:** IT-Drift er i gang med opgaven. Tidshorisont: 1. halvår 2014.		
2.2. Prioritet 2 Overført anbefaling 12-049 02	<u>Vejledning omkring sikkerhedsgrupper</u> Intern Revision har observeret, at "Vejledning til justering af sikkerhedsgrupperne af 15. august 1997" ikke er ajourført siden udgivelsen. Vejledning er på nuværende tidspunkt mangelfuld og tager udgangspunkt i et D/R system og de tilknyttede systemer, som det så ud i 1997. **Status 2013:** Vi har fået oplyst, at der fortsat arbejdes med en gennemgang og ajourføring af vejledningen og efterfølgende effektuering i BRAS.	Manglende retningslinjer for funktionsadskillelse øger risikoen for, at der i systemet tildeles modstridende rettigheder. Manglende funktionsadskillelse øger risikoen for	Intern Revision anbefaler, at SKAT ajourfører vejledningen for sikkerhedsgrupper med udgangspunkt i den nuværende version af D/R systemet, og den måde systemet anvendes på.

Observationer		Risici	Anbefalinger
fra 2012	**Status 2014:** Siden 1/8-2013 har DR systemet kun været anvendt som et angivelsessystem og har således ikke håndteret frigivelser eller udbetalinger. Dermed er der ikke længere en risiko i relation til manglende funktionsadskillelse internt i DR systemet, hvorfor der heller ikke er behov for en ajourføring af omtalte vejledning i relation til DR systemet. **Vi anser punktet for lukket.**	utilsigtede og tilsigtede fejl. Manglende ajourføring af vejledning til opretholdelse af funktionsadskillelse øger risikoen for, at medarbejderne på sigt opnår mulighed for at omgå funktionsadskillelsen og dermed kan udføre handlinger, som ikke var tiltænkt.	
	Høringssvar fra SKAT: Risikoen er jf. handleplanen løst fremadrettet – bl.a. via blokering i BRAS - handleplanen pkt. 9 Vejledningen omkring sikkerhedsgrupper skal ajourføres, som anbefalet af SIR. Ansvarlige: Sikkerhedskontoret og Betalings- og Regnskabskontoret **Bemærkninger fra SKAT 2013:** IT-Drift har påbegyndt opgaven. Tidsestimat: 1. halvår 2014.		
2.3. Prioritet 1 Overført	<u>Tildelte sikkerhedsgrupper</u> Intern Revision har foretaget en gennemgang af oprettede w-numre i DR-systemet pr. 19. november 2012 og deres rettigheder for 6 regioner. I alt er 8.560 w-numre gennemgået, og der er konstateret manglende funktionsadskillelse for 842 w-numre.	Manglende efterlevelse af gældende vejledning på området øger risikoen for manglende	Intern Revision anbefaler, at der foretages en gennemgang og oprydning af de tildelte w-numre, herunder, at w-numrene kun tildeles rettigheder i henhold til arbejdsbetinget behov, og i henhold til gældende vejledning vedr. "Opgaver i Regnskab og BetalingsCentret med snitflader til andre enheder i

<table>
<tr><th colspan="2">Observationer</th><th>Risici</th><th>Anbefalinger</th></tr>
<tr><td>anbefaling fra 12-04903 fra 2012</td><td>Dvs. 842 w-numre har rettigheder, som ikke bør kombineres i henhold til den anvendte vejledning på området: ”Vejledning til justering af sikkerhedsgrupperne af 15. august 1997”.

Specifikation af vores gennemgang.
<table>
<tr><th>Region</th><th>Antal w-numre med konflikter</th><th>Antal w-numre uden konflikter</th></tr>
<tr><td>02</td><td>120</td><td>1.365</td></tr>
<tr><td>03</td><td>51</td><td>1.338</td></tr>
<tr><td>38</td><td>187</td><td>1.018</td></tr>
<tr><td>63</td><td>118</td><td>1.045</td></tr>
<tr><td>97</td><td>82</td><td>872</td></tr>
<tr><td>98</td><td>284</td><td>2.075</td></tr>
<tr><td>I alt</td><td>842</td><td>7.718</td></tr>
</table>

Status 2013:
Efter idriftsætning af DMO og EFI i august/september 2013 er der foretaget en reduktion i antallet af anvendelige menuer i D/R-systemet, hvilket kan påvirke antallet af w-numre med konflikter. Vi har i samarbejde med ”Betalings- og Regnskabskontoret” ajourført oversigten pr. 17. december 2013 med udgangspunkt i reduktionen af anvendelige menuer i D/R-systemet.
<table>
<tr><th>Region</th><th>Antal w-numre med konflikter.</th></tr>
<tr><td>02</td><td>47</td></tr>
</table></td><td>funktionsadskillelse med tilhørende forøget risiko for utilsigtede og tilsigtede fejl i regnskabet.</td><td>SKAT.”</td></tr>
</table>

Observationer	Risici	Anbefalinger

03	16
38	103
63	35
97	26
98	112
I alt	**339**

Ajourføringen viser et markant fald i antallet af konflikter. Samtidig har vi fået oplyst, at "Betalings- og Regnskabskontoret" forventer, med udgangspunkt i ovenstående, at kunne udarbejde en vejledning i løbet af 1. kvartal 2014.

Vi har endvidere i oktober 2013, i samarbejde med "Betalings- og Regnskabskontoret", foretaget en stikprøvevis gennemgang af et antal transaktioner, hvor funktionsadskillelsen ikke har været overholdt. Ved gennemgangen er der ikke konstateret misbrug af den manglende funktionsadskillelse.

Status 2014:

Siden 1/8-2013 har DR systemet kun været anvendt som et angivelsessystem og har således ikke håndteret frigivelser eller udbetalinger. Dermed er der ikke længere en risiko i relation til manglende funktionsadskillelse internt i DR systemet, hvorfor denne anbefaling ikke længere er relevant i relation til DR systemet.

Vi anser punktet for lukket.

Høringssvar fra SKAT:

SKAT tager SIRs anbefaling til efterretning og anbefalingen er efterkommet, jf. handleplanens punkt 9 & 2.

Observationer		Risici	Anbefalinger
	Høringssvar fra SKAT 2013: IT-Drift har påbegyndt opgaven. Tidsestimat; 1. halvår 2014.		
2.4. Prioritet 1 Overført anbefaling fra 12-04904 fra 2012	<u>Brugere uden arbejdsbetinget behov</u> Intern Revision har observeret, at der i D/R – systemet er tildelt opdateringsrettigheder til en række medarbejdere, som ikke er placeret i enten "Betalingscentret" eller i "Udland". Der henvises til gældende vejledning vedr. "Opgaver i Regnskab og Betalingscentret med snitflader til andre enheder i SKAT." **Status 2013:** Vi har fået oplyst, at der arbejdes på at få synkroniseret BRAS med TP-systemet, og at dette arbejde forventes afsluttet i 2013. **Status 2014:** It-drift har pr. 15/8-2014 foretaget en oprydning af brugerne i D/R-systemet. Der er pt. ca. 1.800 brugere, som, efter It-drifts vurdering, har et arbejdsbetinget behov. **Vi anser anbefalingen for lukket.**	Registrering direkte i D/R, foretaget af medarbejdere uden arbejdsbetinget behov, medfører øget risiko for fejl.	Intern Revision anbefaler, at kun medarbejdere med et arbejdsbetinget behov opnår rettigheder til at taste angivelser i D/R-systemet.
	Høringssvar fra SKAT: SKAT tager SIRs anbefaling til efterretning og vil i henhold til handleplanens punkt 6 og 2 foretage det nødvendige herfor. **Bemærkninger fra SKAT 2013:** IT-Drift har påbegyndt opgaven. Tidsestimat. 1. halvår 2014.		
2.5. Prioritet 1 Overført	<u>Fratrådte medarbejdere</u> Intern Revision har konstateret, at der i D/R systemet findes en række aktive brugerkonti, som tilhører fratrådte medarbejdere. **Status 2013:**	Fratrådte medarbejdere med aktive brugerkonti øger risikoen for	Intern Revision anbefaler, at brugerkonti for fratrådte medarbejdere slettes eller spærres i overensstemmelse med Skatteministeriets koncernpolitik for informationssikkerheds it-regler afsnit 11.2.2.

Observationer		Risici	Anbefalinger
anbefaling fra 12-04905 fra 2012	Vi har fået oplyst, at der arbejdes på at få synkroniseret BRAS med TP-systemet, og at dette arbejde forventes afsluttet i 2013. **Status 2014:** It-drift har pr. 15/8-2014 foretaget en oprydning af brugerne i D/R-systemet. Der er pt. ca., 1.800 brugere, som, efter It-drifts vurdering, har et arbejdsbetinget behov. **Vi anser anbefalingen for lukket.**	uautoriseret adgang til systemet.	
	Høringssvar fra SKAT: SKAT tager SIRs anbefaling til efterretning og har truffet de nødvendige beslutninger, jf. handleplanens punkt 9. **Høringssvar fra SKAT 2013:** Der er sket sletning af brugerkonti i D/R-systemet, som tilhører fratrådte medarbejdere.		
2.6. Prioritet 1 Overført anbefaling fra 12-04910 fra 2012	<u>Dobbelte brugerkonti</u> Intern Revision har konstateret, at 231 medarbejdere har to brugerkonti til D/R systemet. De to brugerkonti er typisk identiske i tildelte sikkerhedsgrupper. **Status 2013:** Vi har fået oplyst, at der arbejdes på at få synkroniseret BRAS med TP-systemet, og at dette arbejde forventes afsluttet i 2013. **Status 2014:** Siden 1/8-2013 har DR systemet kun været anvendt som et angivelsessystem og har således ikke håndteret frigivelser eller udbetalinger. Dermed er der ikke længere en risiko i relation til manglende funktionsadskillelse internt i DR systemet, hvorfor denne anbefaling ikke længere er relevant i relation til DR systemet.	Anvendelse af dobbelte brugerkonti øger risikoen for omgåelse af funktionsadskillelsen.	Intern Revision anbefaler, at den enkelte medarbejder kun har en brugerkonto med registreringsrettigheder i D/R-systemet. Er der behov for yderligere brugerkonti, må disse kun have læse rettigheder.

Observationer		Risici	Anbefalinger
	Vi anser punktet for lukket.		
	Høringssvar fra SKAT: SKAT tager SIRs anbefaling til efterretning og vil ændre dobbelte brugerkonti, så den ene brugeradgang kun har læserettigheder. **Høringssvar fra SKAT 2013:** IT-Drift har påbegyndt opgaven. Tidsestimat: 1. halvår 2014.		
2.7. 2013 Prioritet 2	<u>Nøglepersoner</u> Vi har fået oplyst, at der kun er to medarbejdere i SKAT, som kan tilpasse og supportere Escala-serverne. Endvidere findes enkelte medarbejdere hos Steria, som har kendskab til Escala-serverne. **Status 2014:** Vi har fået oplyst, at området er uændret i relation til SKAT. Den medarbejder hos Steria, som yder support på DR, fylder 65 år i august 2015 og forventes at gå på pension umiddelbart efter. **Vi anser fortsat punktet for åbent.**	Personafhængighed i relation til D/R systemet bevirker, at der er risiko for, at den fortsatte drift og tilretning af systemet ikke kan udføres, hvis en eller flere af nøglepersonerne forsvinder.	Vi anbefaler, at der tilføres yderligere personalemæssige ressourcer til styringen og driften af de regionale DR servere, således at SKAT har flere medarbejdere, som kan supportere Escala-serverne og D/R-systemet. Alternativt vil vi anbefale, at SKAT overvejer at flytte D/R systemet til en nyere platform, som kan supporteres af flere medarbejdere i SKAT/Steria.
	Høringssvar fra SKAT 2013: Maskinerne er ikke blevet flyttet til Interxion, da der er stor risiko for, at maskinerne ikke kan genstartes efter en flytning. Endvidere kan telelinjerne ikke umiddelbart flyttes. (manglende kendskab hos TDC). Der skal endvidere skiftes backup-bånd dagligt, og jævnlig genstart af maskinerne finder også sted. Dette er også årsag til, at vi valgte ikke at flytter maskinerne. **Høringssvar fra SKAT 2014:** SKAT arbejder på, at flytter D/R-systemet til anden platform, og på den måde reducerer personafhængigheden. Forventes afsluttet primo 2016.		
2.8. 2013 Prioritet 2	<u>Revurdering af oprettede brugere</u> Vi har ikke kunnet konstatere, hvorvidt der foretages regelmæssig revurdering af oprettede brugere i DR-	Manglende revurdering og spærring af oprettede brugere i DR-	Vi anbefaler, at der som minimum foretages årlige revurdering af brugerne i D/R-systemet, herunder behovet for adgange og behovet for tildelte rettigheder. Hvis en bruger ikke har et arbejdsbetinget behov, bør

Observationer		Risici	Anbefalinger
	systemet. Vi har dog kendskab til, at antallet af daglige brugere efter idriftsættelsen af DMO (én skattekonto) har bevirket, at antallet af daglige brugere i DR-systemet er faldet. **Status 2014:** Vi har set korrespondance, hvoraf det fremgår, at der findes en procedure i relation til regelmæssig oprydning af brugerne i D/R, og at der den 11/8-2014 er foretaget en oprydning blandt TP-brugerne. Samtidig er det oplyst, at der foretages årlige sammenligninger mellem oprettede brugere i HVX og BRAS, og at det er de berørte afdelingsledere der vurderer den enkelte brugers behov for adgang til systemet. **Vi anser punktet for lukket.**	systemet, som ikke har et arbejdsbetinget behov for adgang, øger risikoen for uautoriserede ændringer.	medarbejderen ikke have adgang til DR-systemet
	Høringssvar fra SKAT 2013: Løst/løses ifm. punkterne 2.4. og 2.5.		
3.	**Behandling af inddata**		
3.1.	Gennemgang af området har ikke givet anledning til væsentlige bemærkninger.		
4.	**Proceskontroller**		
4.1.	Gennemgang af området har ikke givet anledning til		

Observationer		Risici	Anbefalinger
	væsentlige bemærkninger.		
5.	**Behandling af uddata**		
5.1.	Gennemgang af området har ikke givet anledning til væsentlige bemærkninger.		
6.	**Transaktions- og kontrolspor**		
6.1.	Gennemgang af området har ikke givet anledning til væsentlige bemærkninger.		
	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.

Anbefalinger med farven "grå" i bilag 1, er anbefalinger, som er lukket i året.