Skatteministeriet

26. maj 2015
J. nr. 14-4248559
Plannr. 114-970

Intern Revision

Rapport 2014

Direktørområdet SKAT IT

It-revision af SAP 38 Basis

Modtager
Departementschef Jens Brøchner, Skatteministeriet

Kopi
Direktør Jesper Rønnow Simonsen, SKAT
Direktør Jan Topp Rasmussen, SKAT IT

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

Forord

Skatteministeriets Interne Revision (SIR) har, jævnfør orienteringsbrev af 27. oktober 2014, revideret området for SAP 38 Basis. Den udførte revision er en del af den samlede revision for 2014.

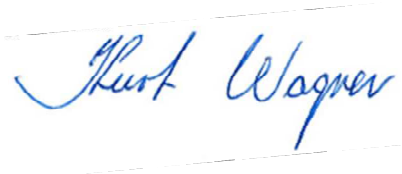
Rapporten indeholder en samlet konklusion omfattende det reviderede område. I konklusionsafsnittet redegør vi for de observationer, som konklusionen i det væsentligste er baseret på. Konklusionsafsnittet indeholder Intern Revisions bedømmelse af det reviderede område samt en beskrivelse af grundlaget for bedømmelsen. Det vil derfor almindeligvis være tilstrækkeligt at læse selve rapporten. Såfremt der ønskes uddybning og detaljering, henvises 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. maj 2015



Kurt Wagner
Revisionschef

Klaus Myssen
Senior Manager

1. Formål

Formålet med revisionen har været at vurdere, hvorvidt interne it-kontroller kan medvirke til at opretholde informationernes integritet og sikkerheden af de data, som SAP 38 behandler.

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

2. Omfang

Revisionen er gennemført i perioden december 2014 til februar 2015 og har omfattet en gennemgang af følgende områder af produktionsmiljøet for SAP 38:

1. Opsætning og anvendelse af SAP
2. Parametre og tabeller
3. Password og login
4. Brugere
5. Profiler i SAP
6. Egenudviklede programmer
7. Væsentlige transaktioner
8. Batchkørsler
9. Ændringsstyring

SAP-specifikke begreber er defineret i bilag 3.

Revisionen er udført i henhold til gældende revisionsstandarder, herunder vejledninger fra Rigsrevisionen. Revisionen er gennemført ved interviews og stikprøvevis gennemgang af foreliggende materiale samt ved egne analyser af data i SAP 38.

Ved revisionen har vi interviewet medarbejdere fra Betalings- og Inddrivelsessystemer.

Revisionen er udført af Klaus Myssen.

3. Konklusion

På baggrund af den udførte revision af de undersøgte områder, er det vores samlede vurdering, at de interne it-kontroller for SAP 38 er på et **ikke helt tilfredsstillende** niveau i relation til opretholdelsen af informationers integritet og sikkerheden af data.

Denne konklusion baserer vi på følgende forhold:

- Vi har konstateret, at 39 dialogbrugere har adgang til at ændre i klient afhængige tabeller. Fx i tabellen vedrørende opsætning af det finansielle regnskab. En del af disse brugere er placeret i Departementet og SIR og har ikke et arbejdsbetinget behov for disse rettigheder.

- Vi har undersøgt standardbrugerne og kan se, at der er en bruger (DDIC) som har tildelt profilerne "SAP_ALL" og "SAP_NEW". Samtidig er det konstateret, at brugeren ikke er låst.

- Vi har ved vores gennemgang identificeret et antal dialogbrugere-id som ikke er personhenførbare. Dermed kan man ikke se, hvilken medarbejdere som har udført de enkelte transaktioner.

- Vi har konstateret 3.029 egenudviklede programmer som starter med ”Z” og 3 egenudviklede programmer som starter med ”Y”. Ingen af disse har tilknyttet nogen transaktionskode.

- Vi har i lighed med tidligere år konstateret et stort antal egenudviklede programmer som ikke indeholder autorisationscheck, hvilket øger risikoen for uautoriserede afvikling.

- Vi har konstateret 22 dialogbrugere (NNIT-XBASIS) som har adgang til at importere transporter i SAP 38. Samtidig har vi fået oplyst, at det kun er Systemejere i Betalings- og Inddrivelsessystemer, som skal have disse rettigheder.

- Vores opfølgning på anbefalingerne fra tidligere år viser, at SKAT har fulgt 13 af vores anbefalinger, hvorfor disse er lukket. Samtidig er der 15 anbefalinger i relation til SAP 38, der fortsat er åbne. Vi har fået oplyst, at SKAT fortsat arbejder med disse anbefalinger, hvorfor vi følger op på disse til næste år.

Vi har prioriteret de observerede forhold således:

Revisionsområde	**Prioritet 1** *Kritisk for forretningen*	**Prioritet 2** *Væsentlig for forretningen*	**Prioritet 3** *Mindre betydning for forretningen*	**2014 I alt**	**2013 I alt**
1. Opsætning og anvendelse	**0**	**1**	**0**	**1**	**2**
2. Parametre og tabeller	**0**	**2**	**0**	**2**	**3**
3. Password og login	**0**	**1**	**0**	**1**	**3**
4. Brugere	**0**	**2**	**1**	**3**	**3**
5. Profiler i SAP	**0**	**0**	**0**	**0**	**4**
6. Egenudviklede programmer	**0**	**2**	**0**	**2**	**3**
7. Væsentlige transaktioner	**0**	**2**	**1**	**3**	**6**
8. Batchkørsler	**0**	**0**	**1**	**1**	**1**
9. Ændringsstyring	**0**	**2**	**0**	**2**	**3**
I alt	**0**	**12**	**3**	**15**	**28**

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

Observationer		Risici	Anbefalinger
1.	**Opsætning og anvendelse**		
1.1. 2013 Prio. 3	<u>Patching af MSSQL</u> SAP38 operativsystemet er baseret på Windows NT med en MSSQL database. Databasen afvikles på en SQL Server 2008 R2 med Service Packs 2 svarende til release 10.50.4000. Via SAP's hjemmeside er det konstateret, at der er frigivet en "Samle pakke 7 for SQL server 2008 R2 SP2" (release 10.50.4286.0) frigivet den 17. Juni 2013 indeholdende 12 hotfixes som er udarbejdet efter SP2. **Status 2014:** Vi har foretaget en ny gennemgang som viser, at seneste frigivet release 10.50.6000 for SQL server 2008 R2 er implementeret i PROD. **Vi anser punktet for lukket.**	Manglende regelmæssig implementering af væsentlige opdateringer, herunder sikkerhedsopdateringer og support pakker, øger risikoen for at kendte sårbarheder og svagheder i ERP systemet kan misbruges.	Vi anbefaler, at der løbende foretages en vurdering af frigivet systemopdateringer, og at der sker implementering af væsentlige opdateringer.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Opgradering sker periodisk og den nævnte patch er kommet umiddelbart efter den gennemførte opgradering i maj 2013. Betalings- og Inddrivelsessystemer vil sammen med vores driftsleverandør sikre at opgradering sker oftere, når patchen indeholder sikkerhedsopgradering.		

Observationer		Risici	Anbefalinger
1.2. 2013 Prio. 2	<u>Patching af SAP38</u> Vi har foretaget en gennemgang af "OCS Package Directory" via S_tcode: SPAM og kan se, at der er en del service patch som ikke er implementeret. **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der fortsat er en del service patch som ikke er implementeret. Samtidig har vi fået oplyst, at området er uændret, og at IT afventer afslutningen af transitionen, hvorefter opdateringen vil blive udført i henhold til årshjulet. **Vi anser fortsat punktet for åbent.**	Manglende implementering af service patch, øger risikoen for misbrug af kendte sårbarheder.	Vi anbefaler, at frigivet service patch' implementeres løbende.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. For at mindske risikoen for at påvirke datoen for implementering af EFI og Skattekontoen, blev det på direktørniveau mellem forretningen og IT besluttet, at udskyde opgradering af SAP38. Database og kernel er opgraderet i maj 2013 og Betalings- og Inddrivelsessystemer har fokus på opgradering til nyeste version inklusive servicepatch, når EFI og Skattekontoen er i stabil drift. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. Betalings- og Inddrivelseskontoret afsluttede transitionen fra Atos til NNIT i december 2014. I løbet af 2015, vil gennemføre patchning af SAP38.		
2	**Parametre og tabeller**		

Observationer		Risici	Anbefalinger
2.1. 2013 Prio. 2	<u>Ændring af system parametre</u> Vi har konstateret, at 48 dialogbrugere har rettigheder til at ændre systemparametre via S_tcode: RZ10. Vi har fra SKAT fået oplyst, at dette skyldes rollen "AD_Regnskab_7" som er tildelt et stort antal medarbejdere i Regnskab, og at SKAT er i proces med at begrænse adgangen. **Status 2014:** Vi har konstateret, at 13 systemejere fra SKAT og 20 NNIT konsulenter (alle dialogbrugere) har rettigheder til at ændre systemparametre via S_tcode: RZ10. Vi har samtidig fået oplyst, at de alle har et arbejdsbetinget behov, hvorfor vi lukker anbefalingen. **Vi anser punktet for lukket.**	Adgang til disse rettigheder for medarbejdere, som ikke har et arbejdsbetinget behov, øger risikoen for fejl og uautoriseret ændringer i systemparametre.	Vi anbefaler, at rettigheder til at foretage ændringer af systemparameter begrænses mest muligt og kun til personer med arbejdsbetinget behov.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. I forbindelse med at Betalings- og Inddrivelsessystemer i december 2013, har ændret rollekonceptet for SAP 38, er det alene brugere med et arbejdsbetinget behov der har rettigheder til at ændre systemparametre. Dette omfatter også driftsleverandørens driftspersonale og systemejere i Betalings- og Inddrivelsessystemer.		
2.2. 2013	<u>Ændring af klient afhængige tabeller</u> Vi har konstateret, at 39 dialogbrugere har adgang til at ændre i klient afhængige tabeller. Fx i tabellen "TVARVC" opsætning af det finansielle regnskab. En del af disse	Adgang til disse rettigheder for medarbejdere, som ikke har et arbejdsbetinget behov,	Vi anbefaler, at rettighederne til at kunne foretage ændringer af klient afhængige tabeller begrænses mest muligt og kun til personer med arbejdsbetinget behov.

Observationer		Risici	Anbefalinger
Prio. 2	brugere er placeret i Departementet og SIR og har ikke et arbejdsbetinget behov for disse rettigheder. **Status 2014:** Vi har fået oplyst, at status er uændret, og at der arbejdes på en løsning mht. gruppering af brugerne, som forventes afsluttet i marts 2015. **Vi anser fortsat punktet for åbent.**	øger risikoen for fejl og uautoriseret ændringer.	
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Betalings- og Inddrivelsessystemer har i december 2013 implementeret et nyt rollekoncept i SAP38. Antallet af adgange til ændring i tabeller er minimeret. Betalings- og Inddrivelseskontoret vil sammen med procesejer gennemgå de arbejdsbetingede behov og tilrette adgangen yderligere i løbet af første kvartal 2014. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. Betalings- og Inddrivelsessystemer vil inden 30. september 2015, sammen med procesejer, sikre at det er alene er medarbejdere med arbejdsbetinget behov der har adgang til at ændre i klient afhængige tabeller.		
2.3. 2013 Prio. 2	<u>Ændringer af klient uafhængige tabeller</u> Vi har konstateret, at 519 dialogbrugere har adgang til at ændre i klient uafhængige tabeller. En del af disse brugere er placeret i Departementet og SIR og har ikke et arbejdsbetinget behov for disse rettigheder. **Status 2014:** Vi har fået oplyst, at der er sket en reduktion i antallet af dialogbrugere, men at der fortsat arbejdes på en løsning	Adgang til disse rettigheder for medarbejdere, som ikke har et arbejdsbetinget behov, øger risikoen for fejl og uautoriseret ændringer.	Vi anbefaler, at rettighederne til at kunne foretage ændringer af klient uafhængige tabeller begrænses mest muligt og kun til personer med arbejdsbetinget behov.

Observationer		Risici	Anbefalinger
	mht. gruppering af brugerne, som forventes afsluttet i marts 2015. **Vi anser fortsat punktet for åbent.**		
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Betalings- og Inddrivelsessystemer har i december 2013 implementeret nyt rollekoncept i SAP38. Antallet af adgange til ændring i tabeller er minimeret. Betalings- og Inddrivelseskontoret vil sammen med procesejer gennemgå de arbejdsbetingede behov og tilrette adgangen yderligere i løbet af første kvartal 2014. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. Betalings- og Inddrivelsessystemer vil inden 30. september 2015, sammen med procesejer, sikre at det er alene er medarbejdere med arbejdsbetinget behov der har adgang til at ændre i klient uafhængige tabeller.		
3	**Password og login**		
3.1. 2013 Prio. 2	<u>Regelmæssigt skift af password</u> Vi har konstateret, at der sker password synkronisering mellem Active Directory og SAP38. Vi har foretaget en gennemgang af samtlige dialogbrugere og har konstateret, at der er 27 gyldige dialogbrugere, som ikke har skiftet password som forventet inden for 90 dage, jf. kravet fra informationsikkehed. 19 af disse dialogbrugere er ATOS brugere. **Status 2014:** Vi har foretaget en ny gennemgang af samtlige dialogbrugere og har konstateret, at der er 132 gyldige dialogbrugere, som ikke har skiftet password som	Manglende regelmæssigt password skift øger risikoen for uautoriseret adgang.	Vi anbefaler, at alle gyldige dialogbrugere skifter password i henhold til password reglerne.

Observationer		Risici	Anbefalinger
	forventet inden for 90 dage. Jf. kravet fra informationssikkerhed. **Vi anser fortsat punktet for åbent.**		
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen og vil fjerne en del af de inaktive brugere i SAP 38, bl.a. dem som mangler skift af password. Derudover vil inaktive eksterne konsulenter bliver fjernet. Oprydningen forventes afsluttet i første kvartal 2014. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. Betalings- og Inddrivelsessystemer gennemgår anvendelsen af autorisationerne for at sikre at password skiftes inden for 90 dage. Opgaven har været nedprioriteret i forbindelse med transitionen i slutningen af 2014. Punktet anses for værende afsluttet		
4	**Brugere**		
4.1. 2013 Prio. 1	<u>Rettigheder til ikke personhenførbare brugere</u> Vi har konstateret, at de ikke personhenførbar brugere: SIESMC og SIESMC1 har fået tildelt "SAP_ALL" profilen og "S_A.Develop" profilen. **Status 2014:** Vi har foretaget en ny gennemgang af "SAP_ALL" og "S_A.Develop" profilen. Vores gennemgang viser, at ingen dialogbrugere har tilknyttet disse profiler. **Vi anser punktet for lukket.**	Øger risikoen for uautoriserede ændringer.	Vi anbefaler, at adgangen til disse brugere spærres, eller at brugerne får frataget deres rettigheder.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Brugerne er ændret til systembrugere.		

Observationer		Risici	Anbefalinger
4.2. 2013 Prio. 3	<u>Gennemgang af oprettede brugere, som ikke har været logget på.</u> Vi har foretaget en gennemgang pr. 12/8-2013 som viser, at der er 825 brugere, som ikke har været logget på SAP38 siden 9/5-2013. Enkelte af disse brugere har ikke været logget på SAP38 siden 2003. **Status 2014:** Vi har foretaget en ny gennemgang og har konstateret, at der er 655 dialogbrugere som ikke har været logget på siden 20/9-2014. Vi har endvidere fået oplyst, at der i marts og december måned 2014 er foretaget oprydning i inaktive brugere. Vi har set dokumentation for, at der er foretaget oprydning i inaktive brugere i 2014, men dokumentationen specificerer ikke hvornår oprydningen er udført. Vi følger op herpå til næste år. **Vi anser fortsat punktet for åbent.**	Oprettede brugere, som ikke benytter sin adgang, øger risikoen for uautoriseret adgang.	Vi anbefaler, at der foretages en revurdering af oprettede brugere, som ikke har været logget på SAP38 siden 2012 eller tidligere for en vurdering af, om de fortsat har et arbejdsbetinget behov for adgang.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Betalings- og Inddrivelsessystemer gennemgår normalt inaktive brugere, med henblik på oprydning to gange årligt. Gennemgangen blev sidst foretaget i foråret 2013. Oprydningen gennemføres sammen med autorisationsgruppen i IT, for at sikre sammenhængen med BRAS, Oprydningen i efteråret 2013 er på grund af opgradering af rollekonceptet i SAP38 blevet udskudt til januar 2014. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er ikke enig i at der ikke har været fulgt op på bemærkningen fra revisionsrapporten fra 2013. Opgaven har i forbindelse med transitionen i slutningen af 2014 været nedprioriteret. Betalings- og Inddrivelsessystemer har senest i april 2015 gennemgået anvendelsen af autorisationer. Opgaven indgår i housekeepingopgaverne og vil fremadrettet blive dokumentet, så det fremgår hvornår vurderingen af den enkelt bruger er foretaget. Forventes udført inden årets udgang.		

Observationer		Risici	Anbefalinger
4.3. 2013 Prio. 2	<u>Systembrugeren DDIC</u> Vi har undersøgt DDIC brugeren, og kan se, at brugeren har tildelt profilerne "SAP_ALL" og "SAP_NEW" samtidig er det konstateret, at brugeren ikke er låst. Systembrugeren DDIC bruges i forbindelse med installation og opgradering af SAP38. **Status 2014:** Vi har konstateret, at systembrugeren DDIC forsat har tildelt profilerne ”SAP_ALL” og ”SAP_NEW” og fortsat ikke holdes låst. **Vi anser fortsat punktet for åbent.**	Manglende låsning af brugeren eller fjernelse af rettigheder til DDIC brugeren i produktion øger risikoen for uautoriserede ændringer.	Vi anbefaler, at DDIC brugeren får fjernet sine privilegerede rettigheder alternativt, at brugeren holdes låst og kun åbnes, når der er behov for det.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen og har ændret brugeren ”DDIC2” til systembruger og password bliver opbevaret af SKAT i tilfælde af, der skulle opstå et behov for at brugerne skal benyttes. Sikringen vurderes dermed til at være optimal. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig i observationen og accepterer risikoen, jf. bemærkningen fra revisionsrapporten fra 2013. Risikoen minimeres ved at der føres kompenserende kontroller, når SAP_ALL bliver tildelt.		

Observationer		Risici	Anbefalinger
4.4. 2013 Prio. 2	<u>Adgang til SU01 – Ændring af UMR</u> Vi har undersøgt antallet af dialogbrugere, som via SU01 har adgang til at udfører følgende i relation til "User Master Record"(UMR): - Create or change UMR - Delete UMR - Add profiles to UMR Vores gennemgang viser, at der er 40 dialogbrugere, som har adgang til at udføre ovenstående handlinger. **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der nu er 9 dialogbrugere som har adgang til at ændre UMR. Disse medarbejdere er placeret i Servicedesk samt en enkelt systemejer. Det er vores vurdering, at disse medarbejdere har et arbejdsbetinget behov. **Vi anser punktet for lukket.**	Et stort antal brugere øger risikoen for uautoriserede ændringer.	Vi anbefaler, at kun brugere med et arbejdsbetinget behov, får autorisationer til SU01.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen, og har i december 2013 ændret rollekonceptet for SAP38, hvor antallet af adgange til ændring i UMR er minimeret.		
4.5. 2013 Prio. 2	<u>Brug af ikke personhenførbare brugere</u> Vi har foretaget en gennemgang af oprettede dialogbrugere for at se, hvorvidt der er oprettet, ikke personhenførbare bruger-id. Ved vores gennemgang har	Anvendelse af bruger-ideer som ikke er personhenførbar, bevirker, at man ikke kan følge transaktionen til den bruger som har initieret transaktionen i SAP.	Vi anbefaler, at der kun oprettes og anvendes personhenførbare bruger-id i SAP.

Observationer		Risici	Anbefalinger
	vi identificeret følgende dialogbruger-id som ikke er personhenførbare: w04ankomst, wbs02, whavnen, wvist01, wkyst04, wnrakas, zpc_dia, default, fejlret_bet, fejlret_rc, kasse_manuel. **Status 2014:** Vores opfølgning viser, at dialogbrugerne ”fejlret_bet”, ”fejlret_rc” og ”wvist01” er slettet og at ”wbs02”, ”zpc_dia”, ”kasse_manual” og ”Default” er ændret til systembrugere. Ligeledes er det set, at ”w04ankomst”, ”whavnen”, ”wkyst04” og ”wnrakas” er ændret til servicebruger. Dermed er de ikke personhenførbare brugere fra sidste år afklaret. Vi har foretaget en ny gennemgang, og har identificeret følgende dialogbruger-id som ikke er personhenførbare: ”SAP38-ESSTAM”, ”SAPSUP”, ”SAPSUPPORT”, hvor de to sidstnævnte er låst af administrator. **Vi anser fortsat punktet for åbent.**		
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Betalings- og Inddrivelsessystemer har lukket brugerne ”fejlret_bet” og ”fejlret_rc” og ændret ”wbs02”, ”zpc_dia”, default og ”kasse_manuel”. Disse brugere kan ikke længere logges på. De øvrige brugere er ændret til servicebruger ud fra et forretningsmæssigt krav. Betalings- og Inddrivelsessystemer vil gå i samarbejde med procesejer for at se på mulighederne for at ændre disse brugere i løbet af 2014. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:		

Observationer		Risici	Anbefalinger
	Der er tale om nye observationer. ”SAPSUP”, ”SAPSUPPORT” anvendes at SAP, når der skal fejlsøges i systemet. Brugerne holdes låst og bliver kun åbnet ved fejlsøgning af SAP. Betalings- og Inddrivelsessystemer vil inden 31. oktober 2015, se på muligheden for at ændre på brugeren ”SAP38-ESSTAM”.		
5	**Profiler i SAP**		
5.1. 2013 Prio. 2	<u>Adgang til profilgeneratoren (PFCG)</u> Vores gennemgang viser, at 30 dialogbrugere har adgang til at oprette eller ændre roller via profilgeneratoren PFCG, herunder personer fra SIR, som ikke bør have adgang. **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der nu kun er 2 dialogbrugere som har adgang til profilgeneratoren. Vi har foretaget en gennemgang af de to brugere og det er vores vurdering, at disse har et arbejdsbetinget behov, hvorfor vi lukker anbefalingen. **Vi anser anbefalingen for lukket.**	Adgang til profil generatoren øger risikoen for uautoriserede ændringer	Vi anbefaler, at adgangen til profilgeneratoren (PFCG) begrænses mest muligt, og kun til personer med arbejdsbetinget behov.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Betalings- og Inddrivelsessystemer har i december 2013 implementeret nyt rollekoncept i SAP38. Rollen er tildelt relevante systemejere i Betalings- og Inddrivelsessystemer.		
5.2. 2012	<u>Kritiske roller SA38/SE38</u> Der er i Fort Consult-rapporten fra oktober 2012 identificeret områder, der er kategoriseret som kritiske	Adgang til transaktionskoderne SA38 og SE38 øger risikoen for	SIR anbefaler, at ingen medarbejdere har adgang til SA38/SE38 i produktionsmiljøet, da transaktionskoderne er forbeholdt

Observationer		Risici	Anbefalinger
Prio. 1	relateret til transaktionskoderne SA38 og SE38 i produktionsmiljøerne, da disse giver adgang til at ændre i idriftsatte SAP-programmer. SIR har udtrukket en liste over brugere med adgang til SA38 og SE38 og identificeret medarbejdere hos SKAT med adgang til at ændre i idriftsatte SAP-programmer: • 48 brugere med w-numre har adgang til transaktionskode SA38 i SAP38 • 42 brugere med w-numre har adgang til transaktionskode SE38 i SAP38 Der er endvidere identificeret andre områder i rapporten fra Fort Consult, hvor risikoen er kategoriseret som høj, som SIR mener er væsentlige for SKAT at tage stilling til i forhold til sikkerheden i SAP Intern og SAP38. **Status 2013:** SIR har fået oplyst, fra "Betalings- og Inddrivelsessystemer", at det for medarbejdere, ud over system- og platformsejere i Betalings- og Inddrivelsessystemer, er planlagt at begrænse adgangen i forbindelse med design af nye roller på SAP38.	uautoriserede ændringer i produktionsmiljøet. Ændring af SAP-programmer i produktion kan medføre fejl i finansielle data. Andre identificerede områder i rapporten, hvor risikoen er kategoriseret som høj, kan medføre uautoriseret adgang til finansielle data, hvilket kan påvirke integriteten af regnskabet dvs. risiko for, at der med eller uden forsæt kan foretages ændringer af finansielle data i SAP og dermed medføre fejl i regnskabet.	udviklere. Eventuelle ændringer eller tilpasninger af programmer bør ske i udviklingsmiljøer og følge de formelle udrulningsprocedurer. Det er endvidere SIRs anbefaling, at der tages stilling til andre områder i rapporten, hvor risikoen er kategoriseret som høj, således at der via en handlingsplan rettes op på områder, som SKAT vurderer væsentlige for forretningen.

Observationer	Risici	Anbefalinger
SIR har foretaget en ny gennemgang som viser, at der fortsat er: • 40 dialogbrugere, som har adgang til transaktionskode SA38 i SAP38 • 51 dialogbrugere, som har adgang til transaktionskode SE38 i SAP38 **Status 2014:** Sir har foretaget en ny gennemgang som viser, at • 44 dialogbrugere har adgang til transaktionskode SA38 i SAP 38, heraf er 21 NNIT brugere og 13 er systemejere fra SKAT. • 47 dialogbrugere har adgang til transaktionskode SE38 i SAP 38, heraf er 34 NNIT brugere og 13 er systemejere fra SKAT. SIR har fået oplyst, at disse brugere har et arbejdsbetinget behov for adgang til disse transaktionskoder. SIR er enig heri, og lukker anbefalingen. **Vi anser punktet for lukket.**		
Høringssvar fra SKAT: Adgangen til SA38 og SE38 er begrænset til udvalgte superbrugere, konsulenter og medarbejdere i Betalings- og Økonomisystemer. De udvalgte superbrugere anvender adgangen til afvikling af programmer ud fra et forretningsmæssigt behov. Øvrige anvender adgangen til fejlsøgninger. Det er desuden besluttet på Forum for SAP Sikkerhed, at der i løbet af foråret 2013 udarbejdes en procesbeskrivelse på proceduren for sikkerhedsscanning, inklusive den efterfølgende opfølgningsprocedure, så der bliver fulgt op på findings i rapporten, herunder begrænsning af adgange til SA38 og SE38. **Bemærkninger fra SKAT, herunder planlagte handlinger til at håndtere risikoen:** Betalings- og Inddrivelsessystemer er enig i anbefalingen. Betalings- og Inddrivelsessystemer har i december 2013 implementeret nyt rollekoncept i SAP38, hvor antallet af brugere med adgang til SA38/SE38 er minimeret.Der iværksættes en proces for at skifte fra		

Observationer		Risici	Anbefalinger
	programeksekvering i SA38/SE38 til at benytte transaktionskoder i stedet for. Processen er afhængig af, at der er den fornødne forretningsdeltagelse. Betalings- og Inddrivelsessystemer tilstræber at afslutte opgaven medio 2014.		
5.3. 2012 Prio. 2	<u>Design af nye roller på SAP38</u> SIR har fået oplyst, at SKAT er i gang med at designe nye roller på SAP38, da nuværende roller er for brede. SIR har foretaget en stikprøvekontrol og identificeret svagheder i relation til kritiske autorisationer (SA38/SE38). SIR kan herved bekræfte, at der er behov for at designe nye roller. **Status 2013:** SIR har fået oplyst, at der nu foreligger en plan for ændringen af rollerne i SAP38, der minimere procesejers opgave mest muligt, og at planen er vedtaget. **Status 2014:** SIR har fået oplyst, at designet af nye roller (som starter med "Z") er færdig, og at de nye roller nu anvendes i relation til SAP opgaverne. Vi har modtaget kopi af rolle og funktionsadskillelse beskrivelsen og kan se, at der er taget højde for funktionsadskillelsen i blandt andet regnskabsfunktionen. **Vi anser punktet for lukket.**	Roller, der er for brede, kan medføre uautoriseret adgang til finansielle data i SAP og dermed påvirke integriteten af regnskabet.	SIR anbefaler, at det nye design af roller færdiggøres og anvendes. Endvidere anbefaler SIR, at det nye design understøtter funktionsadskillelse beskrevet i Regnskabsinstruks for Skatteministeriets Koncern, § 38.
	Høringssvar fra SKAT: På grund af opgavemængden og manglende ressourcer i Regnskab1, var det ikke muligt at få færdiggjort nyt rollekoncept på SAP38 i 2012. Opgaven forventes gennemført i foråret 2013. **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:** Betalings- og Inddrivelsessystemer er enig i anbefalingen, og har implementeret nyt rollekoncept i december 2013.		

Observationer		Risici	Anbefalinger
5.4. 2013 Prio. 2	<u>Profilen "SAP NEW"</u> Vores gennemgang viser, at der er en dialogbruger, som har profilen "SAP_NEW". Det er brugeren "SIESMC". **Status 2014:** Vi har foretaget en ny gennemgang, og har konstateret, at ingen dialogbrugere har profilen "SAP_NEW". **Vi anser punktet for lukket.**	Anvendelse af profilen SAP_NEW i produktionsmiljøet øger risikoen for uautoriseret ændringer. Da profilen indeholder udvidede rettigheder til brug for opgraderinger i SAP.	Vi anbefaler, at ingen dialogbrugere i produktionsmiljøet tildeles profilen SAP_NEW. SAP_NEW profilen bør kun tildeles midlertidigt til systembrugere i forbindelse med opgradering af SAP, og profilen bør fratages når opgraderingen er udført.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen, og har ændret brugeren "SIESMC" til en systembruger.		
6.	**Egenudviklede programmer**		
6.1. 2013 Prio. 2	<u>Tilknyttet S_tcode til egenudviklede programmer.</u> Vi har via SE16 og tabel "TSTC" konstateret, at der kun er 215 egenudviklede Z-programmer ud af 2.550 som har tilknyttet en transaktionskode. Dvs. kun 215 egen udviklede programmer kan startes via en transaktionskode, resten skal afvikles via SA38. **Status 2014:** Vi har foretaget en ny gennemgang som viser: • at der nu findes 3 egenudviklede Y-programmer, og ingen af disse har tilknyttet en transaktionskode. • at der nu findes 3.029 egenudviklede Z-programmer, og kun 477 af disse har tilknyttet en transaktionskode. **Vi anser fortsat punktet for åbent.**	Manglende tilknytning af S_tcode til egenudviklede programmer, øger risikoen for uautoriserede afvikling.	Vi anbefaler, at SAP "Best Practice" på området følges, og at der etableres transaktionskoder (S_tcode) med kald til installerede/importerede programmer.

Observationer		Risici	Anbefalinger
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Betalings- og Inddrivelsessystemer vil tilknytte en S_tcode til programeksekvering for alle programmer, der stadig anvendes. Processen er afhængig af, den fornødne forretningsdeltagelse. Betalings- og Inddrivelsessystemer tilstræber at afslutte opgaven medio 2014. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er ikke enig i, at der ikke har været fulgt op på bemærkningen fra revisionsrapporten fra 2013. SKAT accepterer risikoen for de egenudviklede programmer, som ikke længere anvendes. Betalings- og Inddrivelsessystemer vil inden den 30. juni 2015 indskærpe overfor leverandøren at der ved nyudvikling skal tilknyttes en S_tcode.		
6.2. 2013 Prio. 2	<u>Autorisationscheck i ABAP</u> Vi har via TU02 konstateret, at parameteren ”auth/system_access_check_off” frem til 8/6-2013 har haft værdien "0", hvilket betyder, at der indtil 8/6-2013 er udført autorisationscheck. Efter den 8/6-2013 er parameteren gjort ”Inaktiv”. **Status 2014:** Vi har foretaget en ny gennemgang af parameteren og kan se, at den haft værdien ”0” siden den 11/12-2013, hvilket betyder at der sker autorisationscheck i ABAP, for de programmer som har autorisationscheck indbygget. **Vi anser punktet for lukket.**	Manglende system autorisationscheck øger risikoen for uautoriseret programstart.	Vi anbefaler, at parameteren gøres aktiv, med værdien "0", således at der fortsat sker autorisationscheck ved opstart af programmer.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Det er uvist hvorfor parameteren er ændret. Betalings- og Inddrivelsessystemer har i december 2013, rettet parameteren så den igen er aktiv.		

Observationer		Risici	Anbefalinger
6.3. 2013 Prio. 2	<u>Autorisationscheck i Z-programmer</u> Vi har simpelt tilfældigt udtaget 28 z-programmer ud af 2.550 som er undersøgt for, om de indeholder autorisationscheck. Ved vores gennemgang har vi identificeret, at kun 3 z-programmer ud af 28 indeholdte autorisationscheck. **Status 2014:** Vi har ikke haft adgang til SE38 og har dermed ikke haft mulighed for at verificere hvorvidt der nu sker autorisationscheck i alle egenudviklede programmer. Samtidig har vi heller ikke modtaget dokumentation som viser, at anbefalingen følges. **Vi anser fortsat punktet for åbent.**	Manglende autorisationscheck til egenudviklede programmer, øger risikoen for uautoriseret afvikling.	Vi anbefaler, at SAP "best Practice" på området følges, og at der etableres autorisationscheck i egenudviklede programmer.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen. Der er ikke tidligere indsat autorisationscheck i egenudviklede programmer. Ved alt fremtidig nyudvikling, vil der blive indsat autorisationscheck. Betalings- og Inddrivelsessystemer vil undersøge, hvordan tidligere udviklede programmer kan få indbygget et autorisationscheck. Viser undersøgelsen at det ikke giver udfordringer, vil dette blive gennemført i første halvår 2014. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. Betalings- og Inddrivelsessystemer accepterer risikoen. For nyudvikling og ved ændring af eksisterende programmer vil Betalings- og Inddrivelsessystemer stille krav til leverandøren om der skal være autorisationscheck i egenudviklede programmer. Kravet vil bliver beskrevet i en proces inden den 30. juni 2015.		

Observationer		Risici	Anbefalinger
7.	**Væsentlige transaktioner**		
7.1. 2013 Prio. 2	<u>Adgang til SU02 og PFCG</u> Vi har undersøgt antallet af dialogbrugere, som via SU02 eller PFCG har adgang til at udfører: - Create or change Profiles - Delete Profiles - Activate Profiles - Add authorisation to Profiles Vores gennemgang viser, at der er 30 dialogbrugere, som har adgang til at udføre ovenstående handlinger. **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der nu kun er en dialogbruger som har adgang via SU02 eller PFCG. Det er vores vurdering, at denne dialogbruger har et arbejdsbetinget behov. **Vi anser punktet for lukket.**	Et stort antal brugere øger risikoen for uautoriserede ændringer.	Vi anbefaler, at kun brugere med et arbejdsbetinget behov, får autorisationer til SU02 eller PFCG.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen, og har i december 2013 ændret rollekonceptet for SAP38. Ændring i PFCG er omfattet af en rolle der er tildelt relevante systemejere i Betalings- og Inddrivelsessystemer.		

Observationer		Risici	Anbefalinger
7.2. 2013 Prio. 2	<u>Adgang til SU03 og PFCG</u> Vi har undersøgt antallet af dialogbrugere, som via SU03 eller PFCG har adgang til at udføre: - Create Authorisation - Delete Authorisation - Activate Authorisation Vores gennemgang viser, at der er 30 dialogbrugere, som har adgang til at udføre ovenstående handlinger. **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der nu kun er en dialogbruger som har adgang SU03 eller PFCG. Det er vores vurdering, at denne dialogbruger har et arbejdsbetinget behov. **Vi anser punktet for lukket.**	Et stort antal brugere øger risikoen for uautoriserede ændringer.	Vi anbefaler, at kun brugere med et arbejdsbetinget behov, får adgang til at udføre disse handlinger via SU03 eller PFCG.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen, og har i december 2013 ændret rollekonceptet for SAP38. Ændring i PFCG er omfattet af en rolle der er tildelt relevante systemejere i Betalings- og Inddrivelsessystemer.		
7.3. 2013 Prio. 2	<u>Adgang til SE06–Transport Organizer</u> Vores gennemgang viser, at der er 56 dialogbrugere, som har adgang til at lave ændringer i produktion via SE06 "Transport Organizer". **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der nu er 12 dialogbrugere fra SKAT (Systemejere) og 23 dialogbrugere fra NNIT (Konsulenter). Det er vores	Et stort antal brugere øger risikoen for uautoriserede ændringer direkte i PROD miljøet uden at ændringen først har været igennem den formelle change management proces.	Vi anbefaler, at kun brugere med et arbejdsbetinget behov, får autorisationer til SE06.

Observationer		Risici	Anbefalinger
	vurdering, at disse dialogbrugere har et arbejdsbetinget behov. **Vi anser punktet for lukket.**		
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen og har i december 2013 ændret rollekonceptet for SAP38. Det er alene driftsleverandørens driftspersonale og systemejere i Betalings- og Inddrivelsessystemer, der efter ændringen har rettigheder til at ændre systemparametre.		
7.4. 2013 Prio. 2	<u>Adgang til SCC4 – Klient ændringer</u> Vores gennemgang viser, at der er 29 dialogbrugere, som har adgang til at ændrer klienter i produktion via transaktionen SCC4. **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der nu er 38 dialogbrugere som har adgang til at ændre klienter i produktion via transaktion SCC4. Heraf er 3 Systemejere fra SKAT og 21 NNIT-XBASIS brugere og 8 NNIT-XKON og 6 NNIT-XPI brugere. NNIT-XKON og NNIT-XPI brugere hos NNIT er udviklingsfolk som ikke burde have adgang til SAP 38 PROD. **Vi anser fortsat punktet for åbent.**	Et stort antal brugere øger risikoen for uautoriserede ændringer.	Vi anbefaler, at kun brugere med et arbejdsbetinget behov, får autorisationer til transaktionen SCC4.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen og har i december 2013 ændret rollekonceptet for SAP38. Det er alene driftsleverandørens driftspersonale og systemejere i Betalings- og Inddrivelsessystemer, der efter ændringen har rettigheder til at ændre systemparametre. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:		

Observationer		Risici	Anbefalinger
	SKAT er ikke enig i at der ikke har været fulgt op på bemærkningen fra revisionsrapporten fra 2013. Der er tale om nye observationer i forbindelse med skift til nye driftsleverandør. Betaling- og Inddrivelsessystemer vil inden 30. november 2015 gennemgå adgangene og sikre at der kun er brugere med arbejdsbetinget behov, der har adgang til SCC4.		
7.5. 2013 Prio. 3	<u>Adgang til SM35, SM36 og SM37 – Baggrundsjob</u> Vores gennemgang viser, at der er • 556 dialogbrugere, som via SM35 kan ”release” og ”delete” batch input. • 3.045 dialogbrugere, som via SM36 kan ”release” og ”delete” schedulerede baggrund job. • 2.995 dialogbrugere, som via SM37 kan ”release” og ”delete” baggrundsjob (Batch job) **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der er • 709 dialogbrugere, som via SM35 kan ”release” og ”delete” batch input. • 342 dialogbrugere, som via SM36 kan ”release” og ”delete” schedulerede baggrund job. • 342 dialogbrugere, som via SM37 kan ”release” og ”delete” baggrundsjob (Batch job) Det er vores vurdering, at der fortsat er et stort antal dialogbrugere som har adgang til at påvirke ”baggrundsjob” via undersøgte transaktionskoder. Vi lukker anbefalingen, når vi har set dokumentation for, at der er foretaget en vurdering af, at de pågældende dialogbrugere har behov for disse adgange. **Vi anser fortsat punktet for åbent.**	Et stort antal brugere øger risikoen for uautoriserede ændringer.	Vi anbefaler, at kun brugere med et arbejdsbetinget behov, får autorisationer til transaktionerne SM35, SM36 og SM37.

Observationer		Risici	Anbefalinger
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen og har i december 2013 ændret rollekonceptet for SAP38, hvor adgangen til SM35, SM36 og SM37 er minimeret. Betalings- og Inddrivelsessystemer vil vurdere mulighederne for at mindske antallet af brugere yderligere, ud fra et forretningsmæssigt behov. Vurderingen skal ske sammen med procesejer. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. Betalings- og Inddrivelsessystemer vil inden udgangen af året, sammen med procesejer, vurdere mulighederne for at mindske antallet af brugere yderligere, ud fra et forretningsmæssigt behov.		
7.6. 2013 Prio. 2	<u>Adgang til STMS – Importere transporter</u> Vores gennemgang viser, at der er 55 dialogbrugere, som har adgang til at importere transporter via transaktionen STMS **Status 2014:** Vi har foretaget en ny gennemgang som viser, at der nu er 27 dialogbrugere som har adgang til at importere transporter via transaktionen STMS. 22 NNIT-XBASIS dialogbrugere og 5 W-brugere er fra Betalings- og Inddrivelsessystemer. Dermed er der fortsat brugere som ikke bør have adgang til at importere transporter via STMS. **Vi anser fortsat punktet for åbent.**	Et stort antal brugere øger risikoen for uautoriserede ændringer.	Vi anbefaler, at kun brugere med et arbejdsbetinget behov, herunder SAP-driftsfolk, får authorisationer til transaktionen STMS.
	Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen: Betalings- og Inddrivelsessystemer er enig i anbefalingen og har i december 2013 ændret rollekonceptet for SAP38, hvor efter det kun er systemejere i Betalings- og Inddrivelsessystemer, der har rettigheder til at importere transporter. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:		

Observationer		Risici	Anbefalinger
	SKAT er enig. Ved indgåelsen af nye kontrakt er det leverandørens ansvar at importere transporter, hvorfor en række brugere fra leverandøren har fået adgangen. Betalings- og Inddrivelsessystemer vil inden 30. september 2015, sammen med leverandøren, sikre at det er alene er medarbejdere med arbejdsbetinget behov der har adgang til at importere transporter.		
8	**Batchkørsler**		
8.1. 2012 Prio. 3	<u>Kontobroer</u> Vi har i 2012 konstateret, at kontobroen til overførsel af informationer fra DMR systemet til bogføringen i SAP38 er dokumenteret. SIR har gennemgået dokumentationen og vurderet, at den er retvisende og vil sikre, at finansielle transaktioner fra DMR bliver korrekt bogført i SAP38. Gennemgangen af dokumentationen for de 4 kontobroer har dog vist, at dokumentationen ikke er samlet og ikke er let tilgængelig. **Status 2013:** Vi har set dokumentation som viser, at "Betalings- og Inddrivelsessystemer" har beskrevet en fremtidig proces. Samtidig er det oplyst, at processen endnu ikke er implementeret. Implementeringen afventer idriftsættelse	Manglende overblik over dokumentation af kontobroer kan betyde, at vedligeholdelsen af kontobroer vanskeliggøres, og at det ikke er muligt at skabe et samlet overblik over, hvorfra transaktioner i SAP38 stammer.	SIR anbefaler, at dokumentation for kontobroer bliver dokumenteret ensartet og opbevaret samlet, så de er let tilgængelige, således at transaktionssporet kan følges.

Observationer		Risici	Anbefalinger
	af SAP PS og Skattekontoen. Opgaven med at ajourføre kontobroerne ligger i Regnskab 1. Vi har gennemgået materialet, og det er vores vurdering, at dette er dækkende. Vi lukker anbefalingen, når vi har set dokumentation for, at den er implementeret i driften. **Status 2014:** Området er uændret. Vi har fået oplyst, at der i 2015 vil blive oprettet et projekt, som har til formål at dokumentere alle kontobroer i SAP. **Vi anser fortsat punktet for åbent.**		
	Høringssvar fra SKAT: Betalings- og Økonomisystemer er enig i anbefalingen. **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:** Betalings- og Inddrivelsessystemer er enig i anbefalingen. Betalings- og Inddrivelsessystemer er sammen med forretningen i gang med at implementere retningslinjerne for dokumentation af kontobroerne. Implementeringen forventes gennemført ultimo januar 2014. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. Betalings- og Inddrivelsessystemer er i gang med, sammen med forretningen, at sikre ens retningslinjer for dokumentation af kontorbroerne. Opgaven er udvidet til at omfatte flere systemområder. Opgaven forventes afsluttet inden den 30. september 2015.		
9	**Ændringsstyring**		
9.1. 2012	<u>Test og godkendelse af ændringer</u> SIRs gennemgang viser, at ændringerne i SAP38 er initieret af SKAT, ligesom dokumentationen indikerer en	Manglende godkendelse af ændringer til udvikling og til idriftsættelse bevirker, at der	SIR anbefaler, at alle ændringer godkendes til udvikling og idriftsættelse med tydelig angivelse af, hvem som har godkendt

Observationer		Risici	Anbefalinger
Prio. 2	godkendelse. Der blev fundet to sager, der ikke tydeligt er blevet godkendt til udvikling og en ændring, som ikke tydeligt er godkendt til idriftsættelse. Ydermere er der et mindre antal transporter, der er idriftsat, men sagerne er ikke afsluttet i Remedy. **Status 2013:** SIR har fået oplyst, at "Betalings- og Inddrivelsessystemer" har aftalt en procedure, hvor hver team-ansvarlig en gang i kvartalet kontrollerer, at ændringerne er testet og dokumentet. Seneste gennemgang er blevet foretaget i september/oktober måned 2013 SIR har via stikprøve foretaget en ny gennemgang af ændringerne i SAP38. Gennemgangen viser, at der fortsat er ændringer, hvor det ikke tydeligt fremgår, at ejer/godkender accepterer det fremsatte løsningsforslag, ligesom der ikke i alle tilfælde er identificeret dokumentation for udført test. **Status 2014:** SIR har ikke haft adgang til STMS og har dermed ikke kunne efterprøve om der sker test og godkendelse af ændringer. SIR har dog modtaget dokumentation som viser, at der foretages kontrol i forbindelse med de enkelte "Request for Changes" (RQC). Den udførte kontrol viser, at der fortsat ikke i alle tilfælde udarbejdes tilfredsstillende dokumentation i forbindelse med ændringer. **Vi anser fortsat punktet for åbent.**	kan opstå tvivl om, hvorvidt en ændring er godkendt.	ændringen og hvornår. Ydermere anbefaler vi, at det af dokumentationen tydeligt fremgår, hvilken transport som testes og godkendes.

Observationer		Risici	Anbefalinger
	Høringssvar fra SKAT: Betalings- og økonomisystemer er enig i anbefalingen. **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:** Betalings- og Inddrivelsessystemer er enig i anbefalingen. Det er procesejers ansvar at gennemføre den fornødne funktionelle test og godkende testen. Procesejer har i alle tilfælde truffet beslutning om at ændringen skal sættes i produktion. Da der i nogle tilfælde ikke er dokumentation i ITSM på at der er gennemført test, vil Betalings- og Inddrivelsessystemer indskærpe overfor procesejer at der skal i forbindelse med godkendelsen til produktion også skal godkende den gennemførte test. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. I forbindelse med indgåelsen af en nye drifts- og vedligeholdelseskontrakt fra januar 2015 stilles der andre krav til dokumentation og godkendelse af test af ændringer. Opgaven betragtes som værende afsluttet.		
9.2. 2012 Prio. 2	<u>Funktionsadskillelse i ændringsstyring</u> Ved SIRs gennemgang af SAP38 har SIR identificeret en udvikler fra Atos (JSP og SBS-JSP), som også har benyttet sin adgang til produktionsmiljøet. Det er således konstateret, at 3 af 6 ændringer fra stikprøvekontrollen er blevet udviklet og idriftsat af samme person hos Atos. **Status 2013:** "Betalings- og Inddrivelsessystemer" har opsat en funktionalitet i SAP, der gør at ingen transporter kan gennemføres uden sagsnummer. Herudover er adgangen til STMS frataget konsulenter. SIR har foretaget en ny gennemgang af oprettede udviklingsbrugere, og kan konstatere at ATOS_JSP,	Når udviklere har adgang til produktionsmiljøet øges risikoen for omgåelse af eksisterende procedurer for ændringsstyring herunder utilstrækkelig test og godkendelse, hvilket kan påvirke integriteten af finansielle data, dvs. at regnskabsdata ikke ændres bevidst eller ubevidst i forbindelse med ændringsstyring.	SIR anbefaler, at der etableres en effektiv funktionsadskillelse mellem udvikling og drift, således at ingen udviklere har adgang til at idriftsætte ændringer. En formel procedure for ændringsstyring bør sikre funktionsadskillelse mellem udvikling og drift, for at minimere risikoen for utilstrækkelig autorisation, test og godkendelse af ændringer.

Observationer		Risici	Anbefalinger
	SIESMC og SIESMC1 har været logget på SAP38 i maj og september måned 2013. **Status 2014:** Vi har foretaget en ny gennemgang og konstateret, at der er 6 NNIT brugere tilhørende "NNIT-XPI" gruppen. Vi har gennemgået brugernes rolle (ZBCA_DISPLAY_DRIFT-KONS_GUL) og set, at rollen ikke giver adgang til at foretage ændringer via STMS. **Vi anser punktet for lukket.**		
	Høringssvar fra SKAT: Efter overtagelsen af DMR(SAP38 delen) til drift og vedligeholdelse har Betalings- og Økonomisystemer indskærpet proceduren over for konsulenter, så det alene er medarbejdere i Betalings- og Økonomisystemer, der overfører ændringer til produktion. Ændringer transporteres via STMS. **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:** Betalings- og Inddrivelsessystemer er enig i anbefalingen. Udviklerne har kun en kiggeadgang til transaktionen i produktion, da dette opfyldte deres forretningsmæssige behov. Der er ikke adgang til at implementere transporter i det produktive miljø. Brugerne "SIESMC" og "SIESMC1" er i december 2013 ændret til systembrugere, så der ikke kan logges på disse brugere.		
9.3. 2012 Prio. 2	<u>Transporter udenom STMS</u> SIRs gennemgang viser, at der i løbet af 2012 er idriftsat 5 transporter uden om STMS. SIR har fået oplyst, at disse 5 transporter vedrører DMR-projektet og er ikke dokumenteret som sager i Remedy. **Status 2013:** SIR har fået oplyst, at "Betalings- og Inddrivelsessystemer" har opsat en funktionalitet i SAP,	Manglende anvendelse af etablerede processer og procedurer i forbindelse med transporter, øger risikoen for uautoriserede ændringer, hvilket kan medføre fejl i finansielle data.	SIR anbefaler, at alle transporter, hvis muligt, idriftsættes via STMS. Hvis der skal udføres SAP transporter uden om STMS, bør der udarbejdes en begrundelse for afvigelsen, som dokumenteres i Remedy.

Observationer		Risici	Anbefalinger
	der gør at ingen transporter kan gennemføres uden sagsnummer. SIR har i 2013 foretaget en fornyet gennemgang som viser, at der i 2013 er idriftsat 4 transporter uden om STMS. 3 af disse transporter vedrører konvertering af DMO-data, der ikke kunne udføres i test, og 1 transport, hvor seneste version af "TSP" er lagt i produktion uden om STMS. SIR fastholder sin anbefaling. **Status 2014:** SIR har ikke haft adgang til STMS og har dermed ikke kunne efterprøve om der sker transporter udenom STMS. Ligeledes har SIR ikke modtaget dokumentation for, at der ikke sker transporter udenom STMS, hvorfor punktet fortsat er åbent. **Vi anser fortsat punktet for åbent.**		
	Høringssvar fra SKAT: Som nævnt, blev transporterne gennemført under DMR- projektet. Betalings.- og økonomisystemer er enig i anbefalingen. **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:** Betalings- og Inddrivelsessystemer er enige i, at der ikke må gennemføres transporter uden om STMS, men der kan opstå situationer, hvor der kan være en undtagelse. I de konkrete tilfælde er der tale om en konvertering af data fra SAP38 til SAP PS. Der har været tale om en styret proces, som er beskrevet i konverteringsloggen. Ingen af transporterne indeholder ændringer i programmer. **Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: SKAT er enig. I forbindelse med indgåelsen af en nye drifts- og vedligeholdelseskontrakt fra januar 2015 er det leverandørens ansvar at overføre transporter. Leverandøren er bekendt med kravet. Opgaven betragtes som værende afsluttet.		

Observationer		Risici	Anbefalinger
	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.

Bilag 3: Definition af SAP-specifikke begreber

Begreb	Definition
Autorisationer	Defineres pr. bruger og omfatter rettigheder i SAP fx til at læse og/eller ændre data. Brugere tildeles typisk profiler/roller, som består af en række autorisationer.
Autorisationstjek	Verificerer om en bruger har de relevante autorisationer/rettigheder til at udføre en given handling fx afvikle et program.
Batchkørsler	Er programmer, der kører automatisk i baggrunden og behandler typisk store datamængder i bestemte intervaller fx import eller eksport af data mellem systemer.
Dialogbrugere	Er en fysisk person med eget brugernavn og adgangskode. Brugere tildeles roller.
Klientafhængige tabeller	Er tabeller, som vedrører en enkelt klient fx test (QST) eller produktion (PRD).
Klientuafhængige tabeller	Er tabeller, som vedrører flere klienter fx test (QST) og produktion (PRD).
Profiler	Indeholder rettigheder, som bevirker, at brugerne opnår en række autorisationer til at benytte SAP systemet. En profil kan indeholde en eller flere roller.
Programmer	Omfatter funktionalitet udviklet i programmeringssproget ABAP, som kan afvikles i SAP til fx at fremvise, ændre og/eller slette data.
Roller	Indeholder rettigheder, som bevirker, at brugeren opnår en række autorisationer til at benytte SAP systemet.
SA38	Transaktionskoden giver mulighed for at afvikle programmer eller rapporter.
SAP_ALL	Profilen har alle eksisterende autorisationer i SAP og således ubegrænsede rettigheder i systemet.
SAP_NEW	Profilen har relevante autorisationer til opgradering af SAP miljøet
SE38	Transaktionskoden giver mulighed for at oprette, ændre og afvikle programmer eller rapporter.
Standardbrugere	Brugere, som SAP er født med og kan tilgås af fysiske personer, såfremt adgangskoden er kendt.
Systemparametre	Omfatter sikkerhedsindstillinger, der kan anvendes til at konfigurere systemet.
Transaktionskoder	”s_tcode” omfatter kommandoer, der giver adgang til skærmbilleder i SAP.
Transporter	Omfatter ændringer til SAP.
Udviklingsprofiler	Er en profil, der giver mulighed for at ændre SAP.
User Master Record	UMR er en liste/tabel, som indeholder alle oplysninger om alle brugere i SAP, herunder, hvilke roller brugerne har.