Skatteministeriet

2. februar 2016
J. nr. 15-2018836
Plannr. 115-009

Intern Revision

Rapport 2015

Direktørområdet SKAT IT

It-revision af SAP38 Basis

Modtager
Direktør Jesper Rønnow Simonsen, SKAT

Kopi
Direktør Karsten Juncher, SKAT
Departementet
Rigsrevisionen

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

Forord

Skatteministeriets Interne Revision (SIR) har, jævnfør orienteringsbrev af 3. juli 2015, revideret området for SAP38 Basis. Den udførte revision er en del af den samlede revision for 2015.

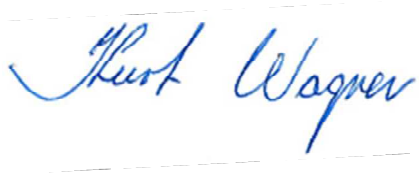
Rapporten indeholder en samlet konklusion omfattende det reviderede område. I konklusionsafsnittet redegør vi for de observationer, som konklusionen i det væsentligste er baseret på. Konklusionsafsnittet indeholder Intern Revisions bedømmelse af det reviderede område samt en beskrivelse af grundlaget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

Rapportens bilag 1 indeholder en systematisk fremstilling af de observationer, som den udførte revision har givet anledning til. Bilaget indeholder tillige en vurdering af de tilknyttede risici samt Intern Revisions forslag til anbefalinger, der kan formindske de vurderede risici. Med udgangspunkt i risikovurderingerne har SKAT udarbejdet handleplaner med henblik på at formindske de vurderede risici.
Intern Revisions anbefalinger har været anvendt som inspiration ved udarbejdelse af handleplaner. Vi vil løbende vurdere implementeringen af SKATs handleplaner.

Rapportens bilag 2 indeholder en beskrivelse af de prioriteringer, der er anvendt ved klassifikationen af de enkelte observationer. Bilaget indeholder herudover en beskrivelse af koblingen mellem observationernes prioriteringer og den samlede overordnede konklusion.

Rapporten har været fremsendt i udkast til den reviderede enhed med henblik på at sikre, at Intern Revision og den reviderede enhed har en ensartet opfattelse af de observerede forhold. SKAT har efterfølgende udarbejdet handleplaner.

København, den 2. februar 2016



Kurt Wagner
Revisionschef

Klaus Myssen
Senior Manager

1. Formål

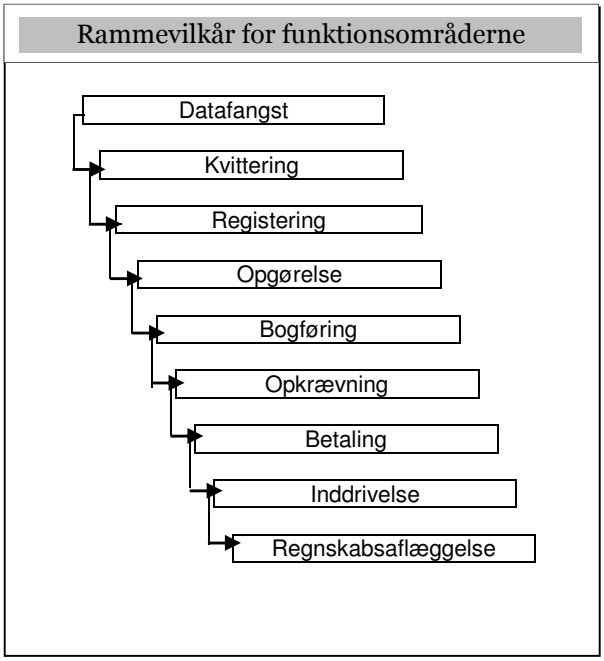
Formålet med revisionen er at vurdere, hvorvidt de interne it-kontroller kan medvirke til at opretholde informationernes integritet og sikkerheden af data, som SAP38 behandler i relation til indtægtsregnskabet.

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

2. Omfang

Revisionen er gennemført i perioden august til september 2015 og har omfattet en gennemgang af følgende områder af produktionsmiljøet for SAP38:

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



SIR anvender denne model til operationel beskrivelse og kategorisering af aktiviteterne i SKAT.

I forbindelse med denne revision har vi revideret følgende funktionsområde:

Rammevilkår for funktionsområderne

I de enkelte observationer har vi henvist til, hvilket funktionsområde, som observationen vedrører.

SAP-specifikke begreber er defineret i bilag 3.

Revisionen er udført af Klaus Myssen og 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 SAP38.

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

3. Konklusion

På baggrund af den udførte revision, er det vores vurdering, at der **i mindre omfang er behov**, for ændringer af de reviderede processer vedrørende de interne it-kontroller for SAP 38 i relation til opretholdelsen af informationers integritet og sikkerheden af data.

Denne vurdering baserer vi på følgende forhold:

- Vi har konstateret, at 56 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 har ikke et arbejdsbetinget behov for disse rettigheder.

- Vi har konstateret, at samme dialogbruger kan være logget på flere terminaler samtidig, hvilket ikke er i overensstemmelse med SAP-licensbetingelserne.

- Vi har konstateret, at der foretages password synkronisering mellem Active Directory og SAP38. Samtidig er det 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.

- Vi har identificeret at, der er 3.099 egenudviklede programmer hvoraf kun 478 af disse programmer er tilknyttet en transaktionskode. Den manglende transaktionskode bevirker, at der ikke kan etableres adgangsstyring til disse programmer.

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

Årets gennemgang har vist, at der fortsat er mange observationer fra tidligere år, som ikke er afklaret.

Vi har prioriteret de observerede forhold således:

Revisionsområde	Prioritet 1 *Høj risiko*	Prioritet 2 *Middel risiko*	Prioritet 3/4 *Lille risiko*	I alt 2015
1. Opsætning og anvendelse	0	1	0	1
2. Parametre og tabeller	0	3	0	3
3. Password og login	0	1	0	1
4. Brugere	0	0	1	1
5. Profiler i SAP	0	0	0	0
6. Egenudviklede programmer	0	2	0	2
7. Væsentlige transaktioner	0	2	1	3
8. Batchkørsler	0	0	0	0
9. Ændringsstyring	0	1	0	1
I alt	0	10	2	12

Prioriteterne skal ses i forhold til det reviderede område og er nærmere defineret i bilag 2.

Vi har modtaget handleplaner fra det revideret direktørområde. 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**		**Funktionsområde: Rammevilkår for funktionsområderne**
1.1. 2015 Prio. 2	<u>Opdatering af databasen (MSSQL)</u> Det er konstatere, at databasen afvikles på en SQL Server 2008 R2 med Service Packs 3 svarende til release 10.50.6000. Via Microsofts' hjemmeside er det set, at der den 9/2-2015 er frigivet en hotfix (et stykke kode, som retter fejl) samt en sikkerhedsopdatering den 14/7-2015, som fortsat mangler at blive implementeret i SAP38.	Manglende implementering af væsentlige opdateringer, herunder sikkerheds-opdateringer og support pakker medfører, at kendte sårbarheder og svagheder i ERP systemet ikke elimineres, med heraf forøget risiko for misbrug	Vi anbefaler, at der løbende foretages en vurdering af frigivne systemopdateringer, og at væsentlige opdateringer herunder sikkerhedsopdateringer implementeres.
	2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen: Betalingssystemer er enig. Patchning af SAP38 er bestilt og vil bliver gennemført inden udgangen af juni måned 2016.		
2	**Parametre og tabeller**		**Funktionsområde: Rammevilkår for funktionsområderne**
2.2. 2015 Prio. 2	<u>Ændring af klient afhængige tabeller</u> Vi har konstateret, at 56 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, øger risikoen for fejl og uautoriserede ændringer.	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
	brugere er placeret i Departementet og har ikke et arbejdsbetinget behov for disse rettigheder. Vi har konstateret lignende forhold i 2013 og 2014.		
	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. **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. **2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: Opgaven vil blive løst ved at tage analyseværktøjet APM-UM i brug. Installationen af værktøjet er forsinket pga. rettelser i netværket ikke gennemføres som forventet. Opgaven forventes gennemført ved udgangen af april måned 2016.		
2.3. 2015 Prio. 2	<u>Ændringer af klient uafhængige tabeller</u> Vi har konstateret, at 80 dialogbrugere har adgang til at ændre i klient uafhængige tabeller. En del af disse brugere er placeret i Departementet og har ikke et arbejdsbetinget behov for disse rettigheder. Vi har konstateret lignende forhold i 2013 og 2014.	Adgang til disse rettigheder for medarbejdere, som ikke har et arbejdsbetinget behov, øger risikoen for fejl og uautoriserede ændringer.	Vi anbefaler, at rettighederne til at kunne foretage ændringer af klient uafhængige tabeller 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.		

Observationer		Risici	Anbefalinger
	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. **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 et arbejdsbetinget behov, der har adgang til at ændre i klient uafhængige tabeller. **2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: Opgaven vil blive løst ved at tage analyseværktøjet APM-UM i brug. Installationen af værktøjet er forsinket pga. rettelser i netværket ikke gennemføres som forventet. Opgaven forventes gennemført ved udgangen af april måned 2016.		
2.4. 2015 Prio. 2	<u>Flere logons på samme tid.</u> Vi har undersøgt parameteren ”login/disable_multi_gui_login” og har konstateret, at den er tildelt værdien ”0”, hvilket muliggør, at samme dialogbruger kan være logget på flere terminaler samtidig. Vi har foretaget test af ovenstående opsætning og kan konstatere, at SAP fremkommer med en advarsel om, at flere logons i produktionsmiljøet med samme bruger-id ikke er i overensstemmelse med SAP-licensbetingelserne.	Muligheden for at samme dialogbruger kan være logget på flere terminaler samtidig bevirker, at brugeren kan ”låne” sit login til andre medarbejdere, hvilket øger risikoen for uautoriserede adgange. Ligesom en anvendelse af flere logins fra samme dialogbruger er i strid med licensrettighederne.	Vi anbefaler, at værdien for parameteren ”login/disable_multi_gui_login” ændres fra ”0” til ”1” således, at en dialogbruger ikke kan være logget på SAP 38 fra flere terminaler samtidigt.
	2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen: Betalingssystemer er enig. Inden udgangen af februar 2016 vil parameteren blive ændret, så det som standard ikke vil blive muligt at have flere logons på samme tid.		
3	**Password og login**		**Funktionsområde:**

Observationer		Risici	Anbefalinger
			Rammevilkår for funktionsområderne
3.1. 2015 Prio. 2	<u>Regelmæssigt skift af password</u> Vi har konstateret, at der foretages automatisk password synkronisering mellem Active Directory (AD) og SAP38. Vi forventer derfor, at password i SAP 38 skifter efter reglerne i AD. I relation til ovenstående, har vi ved vores gennemgang af samtlige dialogbrugere som har været logget på SAP38 i perioden 18/5 til 18/8 2015 konstateret, at 23 af disse brugere ikke har skiftet password som forventet inden for 90 dage. Vores gennemgang af brugerne viser, at der er tale om: - 15 NNIT-brugere - 1 fra SKAT - 1 SAP Teknik bruger - 6 Vikarer (w9xxxx) Vi har konstateret lignende forhold i 2013 og 2014.	Manglende regelmæssigt passwordskift øger risikoen for uautoriseret adgang.	Vi anbefaler, at alle gyldige dialogbrugere skifter password i henhold til password reglerne.
	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. de som mangler skift af password. Derudover vil inaktive eksterne konsulenter bliver fjernet. Oprydningen forventes afsluttet i første kvartal 2014. **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 **2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:		

Observationer		Risici	Anbefalinger
	Betalingssystemer har i 1. halvår af 2015 ikke gennemført housekeeping opgaven med at sikre at der sker regelmæssig skift af password. Opgaven er genoptaget i september 2015, da der blev ansat en medarbejder til disse opgaver og Betalingssystemer har fokus på at opgaven bliver gennemført fremadrettet.		
4	**Brugere**		**Funktionsområde: Rammevilkår for funktionsområderne**
4.2. 2015 Prio. 3	<u>Gennemgang af oprettede brugere, som ikke har været logget på.</u> Vi har foretaget en gennemgang af oprettede brugere pr. 24/8-2015 som viser, at der er 342 ulåste dialogbrugere, der ikke har været logget på SAP38 siden 24/2-2015, hvilket tyder på, at de ikke har et arbejdsbetinget behov for, at være oprettet. Vi har konstateret lignende forhold i 2013 og 2014.		Vi anbefaler, at der foretages en revurdering af oprettede brugere, som ikke regelmæssigt har været logget på SAP38.
	2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen: Betalingssystemer har i 1. halvår af 2015 ikke gennemført housekeeping opgaven med at gennemgå brugere, der ikke har været logget på. Opgaven er genoptaget i september 2015, da der blev ansat en medarbejder til disse opgaver og Betalingssystemer har fokus på at opgaven bliver gennemført fremadrettet.		
5	**Profiler i SAP**		**Funktionsområde: Rammevilkår for funktionsområderne**
	Området har ikke givet anledning til bemærkninger.		

Observationer		Risici	Anbefalinger
6.	**Egenudviklede programmer**		**Funktionsområde:** **Rammevilkår for funktionsområderne**
6.1. 2015 Prio.2	<u>Tilknyttet S_tcode til egenudviklede programmer.</u> Vi har via SE16 og tabel "TSTC" konstateret, • at der findes 3 egenudviklede programmer som starter med Y, og ingen af disse har tilknyttet en transaktionskode. • at der findes 3.096 egenudviklede programmer som starter med Z, og kun 478 af disse har tilknyttet en transaktionskode. Vi har konstateret lignende forhold i 2013 og 2014.	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.
	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. **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. **2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:		

Observationer		Risici	Anbefalinger
	Processen er beskrevet i samarbejdshåndbogen med leverandøren og der er taget stilling til at allerede udviklede programmer vil få tilknyttet en transaktionskode, efterhånden som der sker ændringer i programmerne. Samarbejdshåndbogen blev godkendt i december 2015.		
6.3. 2015 Prio.2	<u>Autorisationscheck i Z-programmer</u> Vi har foretaget en gennemgang af 20 tilfældigt udvalgte z-programmer som alle, enten er udviklet i 2015 eller blevet ændret i 2015. Vores gennemgang viser, at der fortsat ikke sker indarbejdelse af autorisationscheck i Z-programmer. Vi har konstateret lignende forhold i 2013 og 2014	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. **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. **2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: Processen er beskrevet i samarbejdshåndbogen med leverandøren. Betalingssystemer vil for de allerede udviklede programmer, få indbygget et autorisationscheck, efterhånden som der sker ændringer i z-programmerne. Samarbejdshåndbogen blev godkendt i december 2015.		

Observationer		Risici	Anbefalinger
7.	**Væsentlige transaktioner**		**Funktionsområde:** **Rammevilkår for funktionsområderne**
7.4. 2015 Prio.2	<u>Adgang til SCC4 – Klient ændringer</u> Vi har foretaget en gennemgang som viser, at der er 48 dialogbrugere som har adgang til at ændre klienter i produktion via transaktion SCC4. Det er følgende: • 22 NNIT-XBASIS brugere • 13 NNIT-XKON brugere • 8 NNIT-XPI brugere • 4 Systemejere fra SKAT • 1 SAP-Support bruger (gyldig til 18.09.2015) NNIT-XKON og NNIT-XPI brugere hos NNIT er udviklingsfolk som ikke burde have adgang til SCC4 i SAP 38 PROD. Vi har konstateret lignende forhold i 2013 og 2014	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. **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. 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. **2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:		

Observationer		Risici	Anbefalinger
	Adgangene er gennemgået og alle brugere har et arbejdsbetinget behov. Betalingssystemer vil følge op på adgangen ved at tage analyseværktøjet APM-UM i brug. Installationen af værktøjet er forsinket pga. rettelser i netværket ikke gennemføres som forventet. Opgaven forventes løst inden udgangen af april 2016.		
7.5. 2015 Prio.3	<u>Adgang til SM35, SM36 og SM37 – Baggrundsjob</u> Vi har foretaget en gennemgang som viser, at der er • 702 dialogbrugere, som via SM35 kan ”release” og ”delete” batch input. • 339 dialogbrugere, som via SM36 kan ”release” og ”delete” schedulerede baggrund job. • 338 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 anbefaler, at kun brugere med et arbejdsbetinget behov, får autorisationer til transaktionerne SM35, SM36 og SM37.
	2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen: Opgaven vil blive løst ved at tage analyseværktøjet APM-UM i brug. Installationen af værktøjet er forsinket pga. rettelser i netværket ikke gennemføres som forventet. Opgaven vil mindst tage 3 måneder, men pga. den store mængde af andre sikkerhedsopgaver/revisioner mv. som har en større vigtighed, er opgaven prioriteret senere på året. Opgaven forventes løst inden udgangen af december 2016.		
7.7. 2015 Prio. 2	<u>Vedligeholde nummer rækkefølger</u> Vores gennemgang viser, at der er 24 dialogbrugere, som har adgang til at vedligeholde nummer rækkefølger via transaktionen SNUM. Det er følgende dialogbrugere: • 1 NNIT-bruger • 1 SapSupport	Et stort antal brugere øger risikoen for uautoriserede ændringer.	Vi anbefaler, at der foretages en revurdering af brugerne, og at kun brugere med et arbejdsbetinget behov, får autorisation til at vedligeholde nummer rækkefølger via transaktionerne SNUM.

Observationer		Risici	Anbefalinger
	• 14 Procesejere i SKAT • 7 systemejere i SKAT • 1 SKAT medarbejder fra Inddrivelse Det er vores vurdering, at medarbejderen fra Inddrivelse ikke har et arbejdsbetinget behov for, at kunne vedligeholde nummer rækkefølger.		
	2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen: Betalingssystemer er enig i observationen. Adgangene er efterfølgende gennemgået og alle brugere har et arbejdsbetinget behov.		
8	**Batchkørsler**		**Funktionsområde:** **Rammevilkår for funktionsområderne**
	Området har ikke givet anledning til bemærkninger.		
9	**Ændringsstyring**		**Funktionsområde:** **Rammevilkår for funktionsområderne**
9.1. 2015 Prio.2	<u>Test og godkendelse af ændringer</u> SIR har via stikprøver foretaget en gennemgang af ændringerne for perioden 01.01.2015 til 06.10.2015 for SAP38. Gennemgangen viser, at der er ændringer, hvor det ikke tydeligt fremgår, at "kunden"/SKAT har godkendt konsekvensvurderingen eller det fremsatte løsningsforslag. Endvidere viser vores gennemgang, at	Manglende dokumentation for godkendelse af ændringsønsker samt implementering af disse, øger risikoen for, at der kan opstå tvivl om, hvorvidt en ændring er godkendt.	SIR anbefaler, at alle ændringer godkendes til udvikling og idriftsættelse med tydelig angivelse af, hvem som har godkendt ændringen og hvornår. Ydermere anbefaler vi, at det af dokumentationen tydeligt fremgår, hvilken transport som testes og godkendes.

Observationer		Risici	Anbefalinger
	der fortsat ikke i alle tilfælde udarbejdes tilfredsstillende dokumentation i Remedy i forbindelse med ændringer. Vi har konstateret lignende forhold i 2013 og 2014		
	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. **2014 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. **2015 Handleplan fra Betalings- og Inddrivelsessystemer, Bente Kristensen**: I forbindelse med overgang til nye leverandør primo 2015 har Betalingssystemer arbejdet på at sikre en ændringsproces, der sikrer at de nødvendige godkendelser sker. En detaljeret beskrivelse af ændringsprocessen er implementeret i november 2016. Betalingssystemer følger løbende op på at processen bliver overholdt.		
	SLUT		

Bilag 2: Anvendt skala

Ved udarbejdelsen af konklusionen er følgende skala anvendt:	
Intet behov for procesændringer	Intern Revision har ikke observeret svagheder i de forretningsgange og processer, der understøtter det reviderede område. Prioritet 1: Ingen observationer Prioritet 2: Ingen observationer
Behov for procesændringer i mindre omfang	Intern Revision har observeret enkelte svagheder i de forretningsgange og processer, der understøtter det reviderede område. Prioritet 1: Ingen observationer Prioritet 2: Enkelte observationer
Behov for procesændringer i større omfang	Intern Revision har observeret flere svagheder i de forretningsgange og processer, der understøtter det reviderede område. Observationerne er hovedsageligt omfattet af prioritet 1 og 2 med flest observationer i prioritet 2. Prioritet 1: Flere observationer Prioritet 2: Flest observationer
Behov for procesændringer i væsentligt omfang	Intern Revision har observeret flere svagheder i de forretningsgange og processer, der understøtter det reviderede område. Observationerne er hovedsageligt omfattet af prioritet 1 eller 2 med flest observationer i prioritet 1. Prioritet 1: Flest observationer Prioritet 2: Flere observationer

Det skal bemærkes, at ovenstående beskrivelse, med hensyn til antal observationer pr. prioritet, er vejledende i forhold til vores samlede vurdering af konklusionen.

Prioritering af de enkelte observationer:

Prioritet 1: Høj Risiko for manglende målopfyldelse:
Væsentlige svagheder i den etablerede forretningsgang/proces. Svaghederne kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Som følge heraf er der en væsentlig øget risiko for, at processens formål ikke realiseres. Manglende opfyldelse af processens formål vil have store konsekvenser for virksomheden. Der bør snarest muligt iværksættes foranstaltninger med henblik på at udbedre de observerede svagheder.

Prioritet 2: Middel risiko for manglende målopfyldelse:
Svagheder i den etablerede forretningsgang/proces. Svaghederne kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Som følge heraf er der en øget risiko for, at processens målopfyldelse ikke fuldtud realiseres. Manglende opfyldelse af processens formål vil have store konsekvenser for virksomheden. Der bør iværksættes foranstaltninger med henblik på at udbedre den observerede svaghed.

Prioritet 3: Lille risiko for manglende målopfyldelse:
Ingen svagheder i den etablerede forretningsgang/proces. Som følge heraf er der ikke en øget risiko for, at processens formål ikke realiseres. Den reviderede proces kan dog designes med henblik på at forbedre eksekveringen af processen. Processen vil dog være omfattet af den risiko, der, uanset styrken af de interne kontroller, altid vil være til stede.

Prioritet 4: Lille risiko for manglende målopfyldelse:
Ingen svagheder i den etablerede forretningsgang/proces. Som følge heraf er der ikke en øget risiko for, at processens formål ikke realiseres. Processen vil dog være omfattet af den risiko, der, uanset styrken af de interne kontroller, altid vil være til stede.

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.