Skatteministeriet

15. april 2016
J. nr. 15-1747289
Plannr. 115-006

# Intern Revision

# Rapport 2015

## Betalings- og Inddrivelsessystemer

## It-revision af SAPIntern Basis

**Modtager**
Direktør Jesper Rønnow Simonsen

**Kopi**
Direktør Karsten Juncher
Departementet
Rigsrevisionen

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

# Forord

Intern Revision (IR) har, jævnfør orienteringsbrev af 3. juni 2015, revideret SAPIntern. Den udførte revision er en del af den samlede revision for 2015.

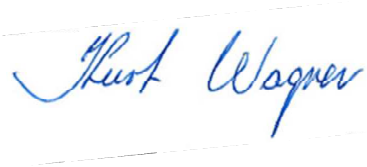
Rapporten indeholder en samlet konklusion omfattende det reviderede område. I konklusionsafsnittet redegør vi for de observationer, som konklusionen i det væsentligste er baseret på. Konklusionsafsnittet indeholder Intern Revisions bedømmelse af det reviderede område samt en beskrivelse af grundlaget 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 15. april 2016



Kurt Wagner
Revisionschef

Klaus Myssen
Senior Manager

# 1. Formål

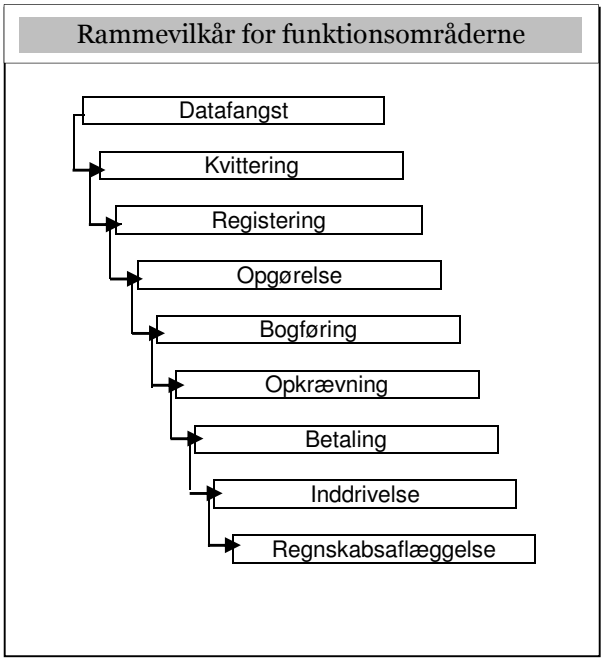
Formålet med revisionen har været at vurdere, hvorvidt interne it-kontroller kan medvirke til at opretholde informationernes integritet og sikkerhed af data, som SAPIntern behandler i relation til det interne regnskab.

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

# 2. Omfang

Revisionen er gennemført i juni 2015 og har omfattet en gennemgang af følgende områder af produktionsmiljøet for SAPIntern:

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




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 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 SAPIntern.

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

# 3. Konklusion

På baggrund af den udførte revision af de undersøgte områder, er det vores samlede vurdering, at der **i mindre omfang er behov** for ændringer i de reviderede processer.

Denne konklusion baserer vi på følgende forhold, som er vurderet væsentlige for forretningen:

- Parameteropsætningen i SAPIntern muliggør, at samme brugere kan logge på flere terminaler samtidig, hvilket er et brud på licensbetingelserne (se evt. bilag 1. anbefaling 2.1.2015).

- BrasFC bruges til rettighedsstyring i SKAT. Vi har konstateret uoverensstemmelser mellem de rettigheder, der er tilknyttet enkelte brugere i SAPIntern, med de rettigheder som fremgår af BrasFC (se evt. bilag 1. anbefaling 4.4.2015).

Vi har prioriterede de observerede forhold således:

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

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

Vi har modtaget handleplaner fra det reviderede direktørområde. Det er vores vurdering, at implementeringen af de udarbejdede handleplaner vil medvirke til en reduktion af de vurderede risici.

Vi har ved revisionen konstateret, at systemet ikke understøtter kravet i "Sikkerhedshåndbogen for medarbejdere" afsnit 11 om, at "Du må ikke genbruge passwords". SKAT har tilkendegivet, at de anser sikkerhedsrisikoen for værende minimal, og accepterer risikoen, ved at tillade hyppig anvendelse af tidligere anvendte password. "Økonomi og Tilsyn" i DEP er orienteret herom, hvilket ikke gav anledning til yderligere bemærkninger.

## Bilag 1: Observationer, risici og anbefalinger

| Nr. | Observationer | Risici | Anbefalinger |
|---|---|---|---|
| **1.** | **Opsætning og anvendelse af SAP** | | **Funktionsområde:**<br>**Rammevilkår for funktionsområderne** |
| | Revisionen af området har ikke givet anledning til bemærkninger. | | |
| | | | |
| **2.** | **Parametre og tabeller** | | **Funktionsområde:**<br>**Rammevilkår for funktionsområderne** |
| **2.1.**<br>**2015**<br><br>**Prio. 2** | <u>Flere logons på samme tid.</u><br>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.<br><br>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 | 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 SAPIntern fra flere terminaler samtidigt. |

| | | | |
|---|---|---|---|
| | overensstemmelse med SAP-licensbetingelserne. | | |
| | **SKAT Handleplan 2015 fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:<br>Betalingssystemer er enig. Ved servicevinduet i marts 2016 hvor serverne genstartes, bliver parameteren ændret, så det som standard ikke vil blive muligt at have flere logons på samme tid. | | |
| **2.2. 2015**<br><br>**Prio. 2** | <u>Muligheden for genbrug af password</u><br>Vi har undersøgt parameteren ”login/password_history_size” og har konstateret, at den er tildelt værdien ”1”, hvilket betyder, at det kun er forrige password, som ikke kan genbruges.<br><br>Kravet jf. ”Sikkerhedshåndbog for medarbejdere” afsnit 11 er, at ”Du må ikke genbruge passwords”. | Ved at tillade hyppig anvendelse af tidligere anvendte password øges risikoen for, at dialogbrugerne benytter tidligere anvendte password, hvilket øger risikoen for uautoriserede adgang. | Vi anbefaler, at værdien for parameteren ”login/password_history_size” ændres fra ”1” til ”24” i lighed med kravet fra AD således, at SAPIntern stiller krav om, at dialogbrugerne i SAPIntern ikke kan anvende de sidste 24 password. |
| | **SKAT Handleplan 2015 fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:<br>I forbindelse med implementering af passwordsynkronisering mellem Windows og SAP, var det nødvendigt at sætte parameteren for passwordsynkroniseringen i SAP til 1. Opsætningen i AD’et styrer muligheden for genbrug af password. Betalingssystemer anser sikkerhedsrisikoen for værende minimal, og accepterer risikoen, da det alene er de enkelte brugere hos leverandøren der ikke vil være omfattet af synkroniseringen. | | |
| **2.3. 2015**<br><br>**Prio. 2** | <u>Initial periode for skift af password</u><br>Vi har undersøgt parameteren: ”login/password_max_idle_Initial” og har konstateret, at den er tildelt værdien ”0”, hvilket betyder, at nyoprettede brugeres initialpassword ikke udløber. | Et stort antal brugere som aldrig har været logget på, samt en ubegrænset password initialperiode, øger risikoen for uautoriserede adgange. | Vi anbefaler, at initial password perioden fastsættes til 15 dage således, at nye brugere bliver spærret hvis de ikke logger på SAPIntern inden for tidsfristen. |

| | | | |
|---|---|---|---|
| | **SKAT Handleplan 2015 fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:<br>I forbindelse med implementering af passwordsynkronisering mellem Windows og SAP, var det nødvendigt at sætte parameteren for passwordsynkroniseringen i SAP til 1. Opsætningen i AD'et styrer initialperioden for skift af password. For de enkelte brugere hos leverandøren, der ikke vil være omfattet af synkroniseringen, gennemfører Betalingssystemer i forbindelse med housekeeping opgaverne kontrol af at der sker skift af password, hvorfor vi vælger ikke at gøre yderligere. | | |
| | | | |
| **3.** | **Password og login** | | **Funktionsområde:**<br>**Rammevilkår for funktionsområderne** |
| **3.1. 2015**<br><br>**Prio. 2**<br><br>**(tidligere 3.2. 2013)** | <u>Regelmæssigt skift af password</u><br>Vi har konstateret, at der sker password synkronisering mellem Active Directory og SAPIntern.<br>SIR har foretaget en gennemgang af samtlige dialogbrugere, og har konstateret, at der er 87 gyldige dialogbrugere, som ikke har skiftet password som forventet inden for 90 dage, jf. kravet fra informationssikkerhed.<br>En af disse er ATOS_EJP brugeren som har været logget på den 21.08.2013, og hvor password senest er skiftet den 27.11.2012.<br>SIR er blevet gjort opmærksom på, at SKAT er i proces med at følge op på alle brugere og specielt brugerID, der ikke anvendes.<br>**Status 2015:** | Manglende regelmæssigt password skift øger risikoen for uautoriseret adgang. | Vi anbefaler, at alle gyldige dialogbrugere skifter password i henhold til password reglerne. |

| | | | |
|---|---|---|---|
| | Vi har den 8. juni 2015 konstateret, at der er 34 gyldige og ikke låste dialogbrugere, som ikke har skiftet password på SAP Intern siden den 5. marts 2015. Dermed har de ikke som forventet skiftet password inden for 90 dage, jf. kravet fra informationssikkerhed. SKAT har efterfølgende oplyst, at der er udført kontrol i august, oktober og december 2015. Vi har den 14. december 2015 foretaget en ny gennemgang, og har ikke identificeret dialogbrugere som ikke har skiftet password som forventet.<br>**Vi anser punktet for lukket.** | | |
| | **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:**<br>Betalings- og Inddrivelsessystemer er enig i anbefalingen.<br>Synkroniseringen sker mellem Active Directory og SAP Intern.<br>Der er iværksat en oprydning i SAP Intern, som vil fjerne en del af de inaktive brugere, bl.a. dem, som mangler skift af password. Derudover er der iværksat en proces for at følge op på eksterne konsulenter, og fjerne inaktive brugere. Opgaven forventes afsluttet i første kvartal 2014. | | |
| | | | |
| **4.** | **Brugere** | | **Funktionsområde:**<br>**Rammevilkår for funktionsområderne** |
| **4.1.**<br>**2015**<br><br>**Prio. 2** | <u>Standardbrugere med standard password</u><br>Brugeren TMSADM (se ordforklaring) har standardpassword i klienterne 000 og 900. | Risikoen ved at anvende SAPs standard passwords er, at alle med adgang til internettet og SAPs dokumentation kan få kendskab til | Vi anbefaler, at SKAT ændrer alle SAP standard passwords til passwords, der opfylder SKATs regler. |

| | | | |
|---|---|---|---|
| **(tidligere 3.1. 2013)** | TMSADM er en kommunikationsbruger.<br><br>Vi har fået oplyst, at SKAT er i proces med at rette passwords for TMSADM.<br>**Status 2015:**<br>Vi har konstateret, at TMSADM brugeren nu er slettet i PROD (klient 900)<br>**Vi anser punktet for lukket.** | disse. Derudover er standard passwords de første, som en eventuel misbruger/indbrudstyv vil forsøge sig med. | |
| | **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:**<br>Betalings- og Inddrivelsessystemer er enig i anbefalingen.<br>Ændring af standardpasswordet er bestilt hos driftsleverandøren. Ændringen forventes gennemført i december 2013. | | |
| **4.2. 2015**<br><br>**Prio. 3**<br><br>**(tidligere 3.3. 2013)** | <u>Brugere, som aldrig har været logget på SAP Intern.</u><br>Vi har konstateret 60 dialogbrugere, som aldrig har været logget på SAPIntern. Det er både SKAT w-brugere og ATOS konsulentbrugere samt enkelte andre.<br>Vi har fået oplyst, at SKAT er i proces med at følge op på brugere, som ikke har været logget ind i en periode.<br>**Status 2015:**<br>Vi har den 4. juni konstateret, at der er oprettet 95 dialogbrugere i SAPIntern, som aldrig har været logget på SAPIntern. 6 af disse dialogbrugere er ikke låste og er oprettet i 2014 eller tidligere. SKAT oplyser, at der er gennemført kontrol i | Oprettede brugere, som ikke benytter sin adgang, øger risikoen for misbrug og uautoriseret adgang. | Vi anbefaler, at der foretages en revurdering af brugernes arbejdsbetinget behov for adgang. Hvis brugerne ikke har været logget på SAPIntern i 6 måneder eller mere, bør adgangen spærres. |

| | | | |
|---|---|---|---|
| | august, september, oktober og december 2015. Vi har den 14. december foretaget en ny gennemgang som viser, at der nu er 61 dialogbrugere i SAPIntern, som aldrig har været logget på. Disse brugere er oprettet i september 2015 eller senere.<br>**Vi anser punktet for lukket.** | | |
| | **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:**<br>Betalings- og Inddrivelsessystemer er enig i anbefalingen.<br>Brugere bliver oprettet i SAP HR selvom brugerne først logger på ved ansættelse. Nogle ender med aldrig at blive ansat, hvorefter deres brugere er inaktive og skal slettes.<br>Det er aftalt med procesejer, at Betalings- og Inddrivelsessystemer jævnligt foretager oprydning i brugere, som aldrig har været logget på. | | |
| **4.3. 2015**<br><br>**Prio. 3**<br><br>**(tidligere 3.4. 2013)** | <u>Manglende SAP autorisationer i BRAS</u><br>Medarbejdere, der er godkendt som bestillere, er beskrevet i Serviceboksen, men autorisationen fremgår ikke af BRAS, hvorfor den ikke er omfattet af den halvårlige kontrol.<br>Autorisationer i SAP9 bliver ligeledes ikke synliggjort i BRAS og bliver således heller ikke vurderet halvårligt. SIR har fået oplyst, at autorisationsteamet er i proces med at forbedre processen vedrørende synliggørelse af autorisationer i BRAS.<br>**Status 2013:** | Manglende synliggørelse af autorisationer vanskeliggør gennemførelse af den halvårlige kontrol af autorisationer. | SIR anbefaler, at processen, på såvel autorisationer til at bestille varer som autorisationer i SAP9, færdiggøres og bliver synlig ved eventuelt at lægge dem i BRAS eller sikre, at den interne kontrol bliver opdateret til også at omfatte bestillere. |

| | | | |
|---|---|---|---|
| | Vi har ikke modtaget dokumentation for at denne procedure er ændret, men har fået oplyst, at SKAT fortsat er i proces med at implementere SAP Intern i Bras.<br>**Status 2015:**<br>Vi har set, at de profiler som indeholder autorisationer til SAPIntern nu fremgår af BrasFC. Ligeledes er det set, at der er udarbejdet en vejledning som beskriver, hvilken type medarbejdere som må tildeles de enkelte profiler.<br>**Vi anser punktet for lukket.** | | |
| | **Bemærkninger fra SKAT, herunder handlinger til at håndtere risikoen:**<br><u>SKATs høringssvar i 2012:</u><br>Økonomi- og regnskab skal bemærke, at oprettelsen som godkendt bestiller foregår manuelt i indkøbskontoret og styres derfra og kan ikke indgå i BRAS.<br><u>SIRs Kommentar til høringssvar fra 2012:</u><br>SIR har efterprøvet høringssvaret hos it udviklerne af Bras, som har oplyst, at rettigheden godt kan etableres i Bras med den ønskede kontrol af funktionsadskillelse. SIR fastholder derfor anbefalingen.<br>**Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:**<br>Betalings- og Inddrivelsessystemer er enig i anbefalingen.<br>Der er fokus på at få SAP Intern lagt i BRAS, hvilket forventes gennemført i første kvartal 2014. | | |
| **4.4. 2015**<br><br>**Prio. 2** | <u>Brugere i BrasFC og i SAPIntern</u><br>Vi har foretaget en undersøgelse af dialogbrugerne "NNIT_ALHV", "NNIT_JORT", w00117, w00120 og w01749 for at se, om de tildelte rettigheder i SAPIntern er i | Manglende sammenhænge mellem tildelte rettigheder i subsystemerne med de rettigheder, der fremgår af BrasFC bevirker, at den kontrol som udføres via BrasFC - til sikkerhed | Vi anbefaler, at der foretages en afstemning mellem oprettede dialogbrugere og deres rettigheder i SAPIntern, med BrasFC til sikkerhed for, at der ikke er tildelt yderligere rettigheder end dem, som fremgår af BrasFC. |

| | | | |
|---|---|---|---|
| | overensstemmelse med rettighederne, der fremgår af BrasFC.<br><br>Vores gennemgang viser, at der er enkelte unøjagtigheder imellem det som fremgår af BrasFC, og det som faktisk er tildelt i SAPIntern, ligesom der er fundet dialogbrugere med tildelte rettigheder i SAPIntern, som ikke fremgår af BrasFC. | for, at brugerne er tildelt korrekte rettigheder - ikke er effektiv og dermed forøget risiko for uautoriseret adgang. | |
| | **SKAT Handleplan 2015 fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:<br>Betalingssystemer er enig og vil sikre at alle brugere bliver oprettet i BrasFC inden udgangen af juni måned 2016. | | |
| | | | |
| **5.** | **Profiler i SAP** | | **Funktionsområde:**<br>**Rammevilkår for funktionsområderne** |
| **5.1. 2015**<br><br>**Prio. 2** | <u>Profilen "Faktura godkendelse"</u><br>Vi har foretaget en gennemgang af profilen "ZFIA_FAKTURA_GODKEND_GUL", som anvendes af medarbejdere, som har til opgave at godkende modtagne købsfaktura i Workflowet (WF).<br><br>Vores gennemgang af profilen med tilhørende authorisationsobjekter viser, at der via authorisationsobjekterne ikke sker afgrænsning på firmakoder. Dermed kan | Manglende opdeling øger risikoen for, at en medarbejder godkender en købsfaktura, som medarbejderen ikke er berettiget til. | Vi anbefaler, at den nuværende profil gøres mere "smal" og specifik således, at den kun omfatter godkendelse af bestemte firmakoder. Ligeledes anbefaler vi, at der oprettes nye/yderligere profiler til anvendelse af andre firmakoder, således at det er muligt at opnå funktionsadskillelse på tværs af firmakoder. |

| | | | |
|---|---|---|---|
| | en medarbejder, som har denne profil godkende alle købsfakturaer, der modtages i dennes medarbejder WF - også købsfakturaer fra andre "firmakoder", end den hvori medarbejderen er ansat. | | |
| | **SKAT Handleplan 2015 fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:<br>Betalingssystemer er enig i, at der ikke er afgrænsning på firmakode i rollen ZFIA_FAKTURA_GODKEND_GUL. Denne afgrænsningen ligger implicit i faktura workflowet, og sikrer at fakturagodkender alene får faktura inden for eget området og firmakode til godkendelse. Vi finder dermed den nuværende proces tilstrækkelig. | | |
| | | | |
| **6.** | **Egenudviklede programmer** | | **Funktionsområde:**<br>**Rammevilkår for funktionsområderne** |
| **6.1. 2015**<br><br>**Prio. 3**<br><br>**(tidligere 2.1. 2013)** | <u>Systemdokumentation – beskrivelse af programmer</u><br>Vi har foretaget en gennemgang af tabellen "TSTC" med 206 programmer. Vi har i den forbindelse konstateret, at der er 11 programmer, hvor der ikke er en kort beskrivelse af formålet.<br>SAP "Best Practice" er, at der for hvert program findes en beskrivelse af, hvad programmet benyttes til inklusiv en kort beskrivelse i tabellen TSTC.<br>**Status 2015:** | Manglende beskrivelse af formålet med de enkelte programmer og deres funktioner, reducerer gennemsigtigheden af systemet og øger risikoen for at samme funktion gentages i nye programmer. | Vi anbefaler, at SAP "Best Practice" på området følges, og at der etableres beskrivelser til alle egenudviklede programmer. |

| | | | |
|---|---|---|---|
| | Vi har foretaget en gennemgang af egenudviklede programmer og konstatere at der til hvert program er medtaget transaktionstekst som beskriver/fortæller noget om programmet.<br>**Vi anser punktet for lukket.** | | |
| | **Bemærkninger fra SKAT 2013, herunder planlagte handlinger til at håndtere risikoen:**<br>Betalings- og Inddrivelsessystemer er enig i anbefalingen.<br>Tabellen vil blive gennemgået og formål vil blive opdateret. Det forventes af opdateringen bliver afsluttet i januar 2014. | | |
| **6.2. 2015**<br><br>**Prio.2**<br><br>**(tidligere 2.2. 2013)** | <u>Autoritetscheck i egne programmer</u><br>Vi har foretaget en gennemgang af 23 udvalgte egenudviklede programmer. Gennemgangen viser, at der ikke er indarbejdet autorisationscheck i de udvalgte programmer.<br>**Status 2015:**<br>Det har ikke været muligt at identificere programmer, som er sat i drift i 2014 eller derefter. Derfor er der foretaget en gennemgang af 20 udvalgte egenudviklede programmer ud fra listen over samtlige egenudviklede programmer. Gennemgangen viser, at der fortsat ikke er indarbejdet autorisationscheck i de undersøgte programmer.<br>**Vi anser fortsat punktet for åbent** | Manglende autorisationscheck øger risikoen for uautoriseret adgang til at afvikle egenudviklede programmer. | 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:**<br>Betalings- og Inddrivelsessystemer er enig i anbefalingen.<br>Der er ikke tidligere indsat autorisationscheck i egenudviklede programmer. Ved alt fremtidig nyudvikling, vil der blive indsat autorisationscheck.<br>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.<br>**SKAT Handleplan 2015 fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:<br>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. | | |
| **6.3. 2015**<br><br>**Prio. 2** | <u>Adgang til SA38</u><br>Via s_tcode: SA38 kan en dialogbruger afvikle alle programmer i SAPIntern.<br>Vi har konstateret, at 37 dialogbrugere har adgang til SA38. Herunder NNIT udviklingskonsulenterne:<br>• NNIT_CKJA<br>• NNIT_MTPZ<br>Vi har endvidere konstateret, at disse brugere har været logget på SAPIntern i juni måned 2015. Dermed har udviklingskonsulenter haft adgang til SAPIntern. | Risikoen ved at tillade brug af SA38 i produktion er, at der kan ske bevidst eller ubevidst afvikling af programmer i SAPIntern, som kan påvirke den løbende drift.<br><br>Endvidere er der er forøget risiko for uautoriseret afvikling, når udviklingskonsulenter har adgang til produktionsmiljøet. | Vi anbefaler, at SAP ”best Practice” på området følges, og at ingen brugere i produktion opnår adgang til SA38. En eventuel adgang bør gives via en nødbrugerrolle.<br><br>Endvidere anbefaler vi, at ingen udviklingskonsulenter opnår adgang til produktionsmiljøet med mindre der sker fuld logning af deres færden. |
| | **SKAT Handleplan 2015 fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:<br>Betalingssystemer har gennemgået adgangene til SA38. Systemejere og NNITs driftspersonale har et arbejdsbetinget behov for adgang. Udviklere hos NNIT har i forbindelse med fejlsøgning fået adgangen når behovet opstår, ved en særskilt rolle der | | |

| | | | |
|---|---|---|---|
| | omfatter SA38 og SE38. Betalingssystemer vil ændre rollen så udviklere ikke vil få adgang til SA38. Rolleændringen vil være tilendebragt inden 1. maj 2016. | | |
| | | | |
| **7.** | **Væsentlige transaktioner** | | **Funktionsområde:**<br>**Rammevilkår for funktionsområderne** |
| **7.1. 2015**<br><br>**Prio. 3** | <u>Systemændringer udenom STMS (se ordforklaring)</u><br>Vi har for perioden 1/1-2014 til 11/6-2015 foretaget en sammenholdelse mellem alle de SAPIntern programændringer, der fremgår af tabel E070 med de ændringer, som er kørt igennem STMS.<br>Gennemgangen viser, at der er 1 ændring (SAPKBBJ106) i tabel E070 som ikke fremgår af STMS.<br>Vi har via Remedy ITSM gennemgået ændringen, og har ikke identificeret begrundelser for, at ændringen skal ske uden om STMS. | Manglende anvendelse af etablerede processer og procedurer i forbindelse med transporter, øger risikoen for uautoriserede ændringer, hvilket kan medføre fejl i finansielle data. | Vi anbefaler, at alle transporter, hvis muligt idriftsættes via STMS. Hvis der udføres SAP transporter uden om STMS, bør der udarbejdes en begrundelse for afvigelsen, som dokumenteres i Remedy. |
| | **SKAT Handleplan 2015 fra Betalings- og Inddrivelsessystemer, Bente Kristensen**:<br>Der er en transport, som ikke er idriftsat via STMS. Ændring skyldes pålægning af supportpakker og kan systemmæssigt ikke idriftsættes via STMS. Pålægning af supportpakker sker i forbindelse med driftsafviklingen og der kan systemmæssigt ikke indsættes en henvisning til en konkret sag. | | |
| | | | |
| **8.** | **Batchkørsler** | | **Funktionsområde:** |

| | | | Rammevilkår for funktionsområderne |
|---|---|---|---|
| | Revisionen af området har ikke givet anledning til bemærkninger. | | |
| | **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.<br><br>Prioritet 1: Ingen observationer<br>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.<br><br>Prioritet 1: Ingen observationer<br>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.<br><br>Prioritet 1: Flere observationer<br>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.<br><br>Prioritet 1: Flest observationer<br>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. |
| **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. |
| **STMS** | SAP Transport Management System (STMS), der anvendes til styring af programændringer i SAP. |
| **Systemparametre** | Omfatter sikkerhedsindstillinger, der kan anvendes til at konfigurere systemet. |
| **TMSADM** | En standardbruger i SAP, som benyttes i forbindelse med konfigurationen/opsætningen af SAP. |
| **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. |