Skatteministeriet

6. marts 2015
J. nr. 14-0049152
Plannr. 14230

Intern Revision

Rapport 2014

Direktørområdet it

Generelle it-controller i relation til adgangsstyring

Modtager:
Departementschef Jens Brøchner

Kopi:
Direktør Jesper Rønnow Simonsen
Direktør Jan Topp
Direktør Karsten Juncher

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

Forord

Intern Revision (IR) har som en del af den samlede revision for 2014 fulgt op på revisionsrapporten fra 2013 vedrørende "Revision af IT-adgangsstyring og IT-rettigheder".

Rapporten indeholder en samlet konklusion omfattende det reviderede område. I konklusionsafsnittet redegør vi for de væsentligste observationer, som konklusionen er baseret på.

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.

Sidst i rapporten er medtaget en beskrivelse af de prioriteter, der er anvendt ved klassifikationen af de enkelte observationer. Bilaget indeholder herudover en beskrivelse af koblingen mellem observationernes prioriteringer og den samlede overordnede konklusion.

Rapporten har været fremsendt i udkast til den reviderede enhed med henblik på at tilsikre, at IR og den reviderede enhed har en ensartet opfattelse af de faktiske forhold. SKAT har efterfølgende udarbejdet handleplaner, som er indarbejdet i denne rapport.

København, den 6. marts 2015

Kurt Wagner
Revisionschef

Jens Lundgaard
Revisor

1. Formål

Intern revision har i perioden januar til maj 2014 foretaget opfølgning på anbefalinger på tidligere fremsendte rapport vedrørende "SKATs styring af adgangsstyring".

Formålet med revisionen har været at vurdere, hvorvidt SKAT har implementeret tidligere givne anbefalinger samt om der er etableret tilfredsstillende procedurer, forretningsgange og kontroller i og omkring SKATs adgangsstyring. Manglende procedurer og kontroller på området, øger risikoen for væsentlige fejl eller mangler i de rettigheder, der tildeles brugere af SKATs systemer.

2. Omfang

Ved revisionen, har der været fokus på, følgende områder:

- Opfølgning på 34 anbefalinger, som er givet i forbindelse med tidligere fremsendt rapport "Revision af IT-adgangsstyring og IT-rettigheder" (j.nr. 13-0039263). Opfølgningen indbefatter anbefalinger på disse områder:
    - Ledelse, organisation og drift
    - Ledelsesmæssige kontroller og opfølgning
    - Styring af rettigheder via SKATs "Bruger Rettigheds Administrations System" (BRAS)
    - Styring af Administrator rettigheder via Infrastruktur
    - Styring af rettigheder via SKATs "Sikkerhed System" (SISY) og "Autorisationssystem" (AU)

- Gennemgang af designet i relation til den logiske adgangsstyring og processen i relation til adgangs- og rettighedsstyring.

Revisionen er udført i henhold til gældende revisionsstandarder, herunder vejledninger fra Rigsrevisionen. Revisionen er gennemført ved interviews, ved indsamling og stikprøvevis gennemgang af foreliggende materiale samt ved fysisk observation. I forbindelse med revisionen er der foretaget interviews af personer fra afdelingen "IT-drift". Der er i denne revision ikke foretaget test af kontroller.

3. Konklusion

På baggrund af vores opfølgning og den udførte revision er det vores samlede konklusion, at processen i og omkring SKATs håndtering af adgangsstyring fortsat er på et **ikke helt tilfredsstillende niveau**.

Konklusionen er baseret på følgende forhold.

En fornyet gennemgang af designet i relation til den logiske adgangsstyring og processen i relation til adgangs- og rettighedsstyring viser, at der fortsat er enkelte svagheder og mangler, hvorfor der er udarbejdet anbefalinger til styrkelse af væsentlige områder.

Vores opfølgning viser, at SKAT har efterlevet 16 af vores anbefalinger, hvorfor disse er lukket. Der er 2 anbefalinger, hvor SKAT har valgt at leve med risikoen, og der er fortsat 16 anbefalinger som er uafklaret.

I rapporten er der medtaget følgende åbne anbefalinger med Prioritet 1:

- Der foretages ikke revurdering af brugere og deres rettigheder, som ikke fremgår af BRAS. Alle oprettede brugere og deres rettigheder til alle væsentlige systemer bør revurderes regelmæssigt. (Anbefaling 2.3 i bilag 1)

Der er to observationer, hvor SKAT har tilkendegivet, at de er bekendt med og har valgt at leve med risikoen. Det er følgende observationer:

- Systemudvikleren på BRAS har adgang til BRAS i produktion. Dermed er der manglende funktionsadskillelse mellem udvikling og produktion, hvilket er i strid med it-sikkerhedspolitikkens afsnit 10.1 om funktionsadskillelse. Den manglende logiske adskillelse mellem udvikling og produktionsmiljøet øger risikoen for uautoriserede ændringer, hvilket kan påvirke integriteten af data. (Anbefaling 2.8 i bilag 1, som Prioritet 1)

- CSC udfører selv brugeradministration af CSC brugere i SKATs RACF system. Den manglende interne styring af eksterne brugere til RACF øger risikoen for uautoriseret adgang. (Anbefaling 5.5 i bilag 1, som Prioritet 2)

De åbenstående anbefalinger kan opsummeres således:

	Prioritet 1 *Kritisk for forretningen*	**Prioritet 2** *Væsentlig for forretningen*	**Prioritet 3** *Mindre betydning for forretningen*	**I alt**
1 Ledelse, organisation og drift	**0**	**1**	**0**	**1**
2 Ledelsesmæssige kontroller og opfølgning	**1**	**3**	**0**	**4**
3 Styring af rettigheder via BRAS	**0**	**3**	**0**	**3**
4 Styring af Admin rettigheder via Infrastruktur	**0**	**5**	**1**	**6**
5 Styring af rettigheder via SISY og AU	**0**	**1**	**1**	**2**
Anbefalinger, hvor SKATs ledelse har valgt at leve med risikoen	**1**	**1**	**0**	**2**
I alt 2014	**2**	**14**	**2**	**18**
I alt 2013	**4**	**23**	**7**	**34**

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

Vi har modtaget handleplaner fra de reviderede direktørområder som er indarbejdet i bilag 1. Det er vores vurdering, at implementeringen af de udarbejdede handleplaner vil medvirke til en reduktion af de vurderede risici.

Bilag 1: Observationer, risici og anbefalinger

Opfølgning på observationer fra revisionen i 2013

Nr.	Observationer	Risici	Anbefalinger
1.	**Ledelse, organisation og drift**		
1.1. **Prioritet 2**	<u>Procesoversigt til brug for autorisationsteamet</u> I henhold til it-sikkerhedspolitikkens it-regler skal procesejer skabe oveblik over, hvilke dele slutproduktet består af, og hvordan de bliver til. Dette gøres oftest via procesoversigter. SIR har fået oplyst, at der ikke findes egentlige procesoversigter som viser, hvor data kommer fra, hvordan de behandles, og hvor de flyder hen i forbindelse med autorisationsteamets arbejde. **Status 2014:** Autorisationsteamet oplyser, at de her en samlet procesoversigt/arbejdsbeskrivelse for opgaven. Vi har udarbejdet forslag til skematisk procesoversigt som er overdraget til it-drift til deres videre bearbejdning. **Vi anser punktet for lukket.**	Manglende formelle og godkendte procesoversigter bevirker, at kendskabet til processerne kun eksisterer hos de medarbejdere, som arbejder med området. Dermed øges risikoen for, at viden forsvinder i de tilfælde, hvor medarbejderne forlader organisationen.	SIR anbefaler, at der udarbejdes procesoversigter til illustration af informationsflowet i forbindelse med administrationsstyringen. Endvidere anbefaler vi, at oversigterne løbende ajourføres, således at de afspejler de faktiske forretningsgange.
	SKATs kommentar i 2013: Egentlige procesoversigter vil blive udarbejdet og løbende ajourført således, at disse oversigter hele tiden afspejler de faktiske forretningsgange		
1.2. **Prioritet 2**	<u>Autorisationsteamets behandling af autorisationssager</u> SIR har fået oplyst, at kravet til autorisationsteamet er, at de skal behandle initierede auto-	Manglende rettidig ajourføring af brugerrettigheder øger risikoen for uautoriseret adgang.	SIR anbefaler, at ordrelinjer afklares løbende og i henhold til aftalte SLA eller alftalte krav jf. serviceboksen.

Nr.	Observationer	Risici	Anbefalinger
	risationsændringer inden for 5 dage. Ved revision har SIR foretaget en gennemgang af åbne og igangværende ordrelinjer fra: • BRAS • Serviceboksen • Fælles Mail-kasse Ved gennemgangen er der konstateret et mindre antal ordrelinjer, som ikke er behandlet inden for forventet tid. **Status 2014:** SIR har fået oplyst, at SLA'en fra 2009 fortsat er gældende, og at det overordnede mål er, at 80% af alle bestillinger er løst indenfor 5 dage. SIR har modtaget dokumentation som viser, at der i 2014 er oprettet 3.748 autorisationssager i ITSM, og af disse er der 177 sager som ikke er behandlet inden for 5 dage. Dermed er 95,3% af disse sager løst indenfor 5 dage. Endvidere er der modtaget en BRAS opgørelse for perioden 1/1-30/9-2014 som viser, at 94% af 28.078 BRAS hændelserne er behandlet indenfor 5 dage. Det er SIR's vurdering, at dette er tilfredsstillende. **Vi anser punktet for lukket.**		
	SKATs kommentar i 2013: IT er enig med Revisionen i, at indkomne ordrelinjer bør afklares løbende og således, at den aftalte SLA overholdes. IT arbejder løbende på at sikre overholdelse af SLA. **SKATs kommentar i 2014:** Handleplan mangler fra autorisationsteamet		

Nr.	Observationer	Risici	Anbefalinger
1.4. **Prioritet 2**	<u>Hvem må initiere en ændring</u> SIR har fået oplyst, at der ikke findes fortegnelser i SKAT som viser, hvem der må fremsætte ændringsforslag fra eksterne offentlige myndigheder dog med undtagelse af Domstolsstyrelsen og kommunerne. Endvidere har SIR fået oplyst, at autorisationsteamet med tiden har opbygget et kendskab til, hvem der må fremsende ændringsønsker. **Status 2014:** SIR har fået oplyst, at der fortsat ikke er udarbejdet lister for "Politiet" og "Ministerierne", som viser, hvilke eksterne personer som må initiere ændringsønsker for eksterne offentlige myndigheder i forbindelse med autorisationer. **Vi anser fortsat punktet for åbent.**	Manglende formelt kendskab til hvem der må initiere ændringsønsker for eksterne brugere, øger risikoen for, at det ikke opdages, hvis et ændringsforslag fremsættes af en person, som ikke er autoriseret til at må initiere en ændring.	SIR anbefaler, at der udarbejdes lister indeholdende navne over de eksterne personer, som må initiere ændringsønsker, og at der følges op på ændringsforslag, hvis de fremsættes af personer, som ikke fremgår af listen.
	SKATs kommentar i 2013: Det er i systemet indlagt, hvilke specifikke – it-adgange den enkelte myndighed må tildeles. Tildelingen er defineret i indgået kontrakt og systemmæssigt understøttet. Den enkelte myndighed eller repræsentanter herfra kan således IKKE bestille adgange, som går udover det kontraktuelle og systemmæssige. IT vil vurdere om der udover ovenstående skal foretages en systemmæssig ændring eller igangsættes en manuel proces. **SKATs kommentar i 2014:** IT Center Haderslev / John K C Madsen. Der udfærdiges arbejdsbeskrivelse og en liste over hvem der må initiere ændringsønsker. Endvidere etableres en opfølgningsproces, der sikre at listen er up to date.		
1.5. **Prioritet 2**	<u>Ejerskab for BRAS</u> SIR har via Intranettet og siden "Systemoverblik" konstateret, at der ikke er udpeget nogen systemejer, platformsejer eller procesejer for BRAS. "Systemoverblik" eller "SKAT-overblik", som	Manglende formel angivelse af ejerformer øger risikoen for manglende ansvarsplacering, ligesom der kan opstå tvivl om, hvem der skal godkende eventuelle ændringer til systemet.	SIR anbefaler, at der formelt udpeges en systemejer, en platformsejer og en procesejer i relation til BRAS, og at "systemoverblik" listen på intranettet opdateres med disse informationer.

Nr.	Observationer	Risici	Anbefalinger
	siden også kaldes, er første skridt mod opbygningen af en central indgang til informationer om SKATs it-systemer. **Status 2014:** Vi har konstateret, at systemoverblik er opdateret med både proces- og systemejer og rollerne er besat på følgende måde: Procesejer: Ursula Schøn – w05656 Systemejer: Poul E. Petersen – W01941 **Vi anser punktet for lukket**		
	SKATs kommentar i 2013: Informationssikkerhed og IT er enige i, at der bør udpeges en proces-, platform- og systemejer. Informationssikkerhed og IT-Centrene deltager gerne i denne proces.		
1.6. **Prioritet 2**	<u>Autorisationsteamet – udførte ordrelinjer</u> SIR har fået oplyst, at de ordrelinjer, som behandles i BRAS(IT), ikke forbliver synlige efter, de er blevet behandlet. Der findes dog en funktion i BRAS(IT), som bevirker, at autorisationsteamet kan fremkalde samtlige ordrelinjer, hvis man har et aktivt medarbejdernummer. Medarbejdere som ikke længere er i SKAT, og som dermed ikke har noget aktivt medarbejdernummer, kan dermed ikke søges frem af databasen, hvilket besværliggør en ledelsesmæssig opfølgning. **Status 2014:** Vi har udtræk fra "Brasudtraek" som viser at det er muligt at fremfinde og søge på alle tidligere udførte ordrelinjer. **Vi anser punktet for lukket**	Manglende mulighed for fremkaldelse af ordrelinjer vedrørende tidligere medarbejdere bevirker, at det ikke ledelsesmæssigt er muligt, at følge op på, om brugerne slettes rettidigt.	SIR anbefaler, at SKAT overvejer en ny funktion i BRAS(IT), som gør det muligt at fremfinde og søge på alle tidligere udførte ordrelinjer.

Nr.	Observationer	Risici	Anbefalinger
	SKATs kommentar i 2013: IT er enige i, at der bør etableres en ny funion i BRAS, der viser ordrelinjer for samtlige medarbejdernumre uanset status.		
2.	**Ledelsesmæssige kontroller og opfølgning**		
2.1. **Prioritet 2**	Vejledning til brug for lederne vedrørende BRAS kontrollen (LISY-knt.nr. S44501000000 – Lbn 05) SIR har foretaget en gennemgang af vejledningen, hvoraf det fremgår, at lederne skal foretage en gennemgang af brugerne og deres rettigheder i BRAS, således som de er registreret i BRAS for at kontrollere, om medarbejderne har de rigtige rettigheder, og at det kan gøres ved "sammenhold arbejdsbeskrivelse og/eller arbejdsopgaver for personer med de faktiske tildelte autorisationer". Man kan ikke af vejledningen se, hvordan lederne skal dokumentere, at kontrollen er udført. SIR har foretaget en opfølgning på lederne udførsel af kontrollen og har konstateret, at dokumentationen for det udførte arbejde er meget forskelligt og ofte ikke eksisterende. **Status 2014:** Vejledningen til lederne i relation til udførelse af BrasFC kontrollen er ikke ændret. **Vi anser fortsat punktet for åbent**	Manglende dokumentation for udførelse af kontrollen bevirker, at der ikke kan følges op på det udførte arbejde. Endvidere er der risiko for, at der er medarbejdere, konsulenter og leverandører som har tildelt rettigheder til persondata, men som ikke fremgår af BRAS, og som derfor ikke bliver kontrolleret jævnligt.	SIR anbefaler, at vejledningen ajourføres i relation til kontrollens gennemførelse således, at den afspejler SKATs nuværende organisation. Endvidere anbefaler SIR, at vejledningen udbygges med forslag til, hvordan lederne kan dokumentere deres udførsel af kontrollen, eventuelt med forslag til brug af "langtekster".
	SKATs kommentar i 2013: Enig – Informationssikkerhed vil understøtte processen. **SKATs kommentar i 2014:** Sikkerhedskontoret / Bo Daugaard. Der vil sammen med Økonomi og virksomhedsstyring blive afholdt en workshop medio februar 2015, hvor der vil blive foretaget en risikovurde-		

Nr.	Observationer	Risici	Anbefalinger
	ring af bl.a. Sikkerheds ydelser (ydelse 189 'Sikkerhed i SKAT'). Målet er at sikre, at den gennemførte interne kvalitetssikring giver det rigtige billede af, hvor korrekte de producerede ydelser er. Det betyder, at der vil ske en revurdering af kontrolpunktet vedr. brugerrettigheder i overensstemmelse med SIR's anbefaling. Der er desuden etableret en arbejdsgruppe bestående af Sikkerhed, It-service og Teknologi og repræsentanter fra forretningen, som skal munde ud i en direktionsforelæggelse. Forelæggelse til direktionen forventes behandlet på møde i løbet af 1. kvartal 2015.		
2.3. **Prioritet 1**	<u>Revurdering af rettigheder udenfor BRAS</u> SIR har fået oplyst, at der ledelsesmæssigt kun foretages en struktureret revurdering af de brugere og rettigheder, som fremgår af BRAS. SIR har ikke set dokumentation som viser, at der også sker revurdering af brugere og rettigheder, som ikke fremgår af BRAS. **Status 2014:** IT Centrene og Sikkerhed er i gang med at udarbejde en direktionsforelæggelse med forskellige løsningsmuligheder. Denne forelæggelse vil blive forelagt direktionen i januar 2015. Sikkerhed faciliterer processen. **Vi anser fortsat punktet for åbent,**	Manglende revurdering af oprettede brugere og deres rettigheder øger risikoen for, at det ikke opdages, hvis en bruger har adgang til områder, der ikke er behov for. Dermed er der forøget risiko for uautoriseret adgang.	SIR anbefaler, at der udarbejdes processer som sikrer, at alle brugere og deres rettigheder til alle væsentlige systemer bliver revurderet i henhold til it-sikkerhedspolitikkens it-regler.
	SKATs kommentar i 2013: Informationssikkerhed og IT er enige i, at der bør udarbejdes processer, der sikrer en revurdering af rettigheder udenfor BRAS. **SKATs kommentar i 2014:** Sikkerhedskontoret / Bo Daugaard. Der er etableret en arbejdsgruppe bestående af Sikkerhed, It-service og Teknologi og repræsentanter fra forretningen, som skal munde ud i en direktionsforelæggelse. Forelæggelse til direktionen forventes behandlet på møde i løbet af 1. kvartal 2015.		
2.4. **Prioritet 2**	<u>Sammenholdelse mellem BRAS og subsystemer</u> SIR har fået oplyst, at der kun sker sammenholdelse mellem BRAS og 3 subsystemer. Denne sammenholdelse foretages for at sikre,	Manglende sammenholdelse bevirker, at det ikke opdages, hvis der er forskel mellem de rettigheder, som fremgår af BRAS, og de faktiske rettigheder som brugerne har i underliggende systemer.	SIR anbefaler, at Informationssikkerhed fremsætter et eksplicit krav via it-sikkerhedspolitikken om, at der skal foretages en regelmæssig (fx. ½ årlig) sammenholdelse mellem BRAS og tilhørende

Nr.	Observationer	Risici	Anbefalinger
	at de rettigheder, som fremgår af BRAS, også er de rettigheder, som faktisk er oprettet i subsystemerne. **Status 2014:** SIR har kendskab til, at der nu foretages sammenholdelse mellem rettigheder i BRAS og tildelte rettigheder i 16 subsystemer med bestemte intervaller. Det er samtidig oplyst, at der vil blive lavet programmer til de enkelte systemer, som gør det muligt for systemejerne, at fortage en egen løbende kontrol af om der er overensstemmelse mellem registreringerne i BRAS og de faktiske forhold. Det er endvidere oplyst, at det vil fremgå i den nye sikkerhedshåndbog, som er under udarbejdelse, at rettighederne skal kontrolleres periodisk og mindst 2 gange årligt. **Vi anser fortsat punktet for åbent.**		subsystemer til verifikation af, om der er overensstemmelse i tildelte rettigheder. For at undgå selvkontrol bør kontrollen ikke udføres af autorisationsteamet, men af de ansvarlige for de enkelte systemer, dvs. systemejerne.
	SKATs kommentar i 2013: Informationssikkerhed vil sikre, at der udarbejdes en proces for sammenholdelse mellem BRAS og subsystemer, så der bliver overensstemmelse mellem tildelte rettigheder. **SKATs kommentar i 2014:** Sikkerhedskontoret / Bo Daugaard. I SKATs sikkerhedshåndbog for risikoejere, afsnit 9. Adgangsstyring fremgår det som et krav, at • adgangsrettigheder kontrolleres periodisk, mindst to gang årligt • procesejer kontrollere periodisk, mindst to gang årligt for afvigelser og iøjnefaldende tildelinger af adgangsrettigheder Der er etableret en arbejdsgruppe bestående af Sikkerhed, It-service og Teknologi og repræsentanter fra forretningen, som skal munde ud i en direktionsforelæggelse. IT-centrene vil desuden, i arbejdsgruppens regi, gennemføre et pilotprojekt for to it-systemer, for at undersøge hvorledes en samkørsel mellem BRAS og udtræk fra fagsystemerne bedst kan gennemføres i praksis. Forelæggelse til direktionen forventes behandlet på møde i løbet af 1. kvartal 2015.		
2.5.	Risikoanalyse for BRAS	Manglende ajourføring af risikoanalysen øger risikoen	SIR anbefaler, at risikoanalysen ajourfø-

Nr.	Observationer	Risici	Anbefalinger
Prioritet 2	Via applikationen ”RISK” som anvendes til udarbejdelse af risikoanalyser for applikationer i SKAT, er det konstateret, at den sidst udarbejdede risikoanalyse for BRAS er foretaget den 20 marts 2007. Jf. SKATs it-sikkerhedspolitiks it-regler afsnit 4 skal der årligt ske udarbejdelse af risikoanalyser. Processen "BRAS" vurderes som værende "ikke kritisk for SKAT". Dog vurderes afhængigheden af nøglepersoner til at være "Mellem", ligesom det fremgår, at informationsressourcen er "kompleks" og "stigende i anvendelsen". **Status 2014:** Vi har via RISK konstateret, at den seneste risikoanalyse som er udarbejdet er dateret den 29/4-2014 og godkendt den 6/5-2014. Risikoanalysen viser, at fortroligheden, Integriteten og tilgængeligheden i relation til BRAS er tilfredsstillende. **Vi anser punktet for lukket**	for, at der ikke er opnået kendskab til eventuelle ændringer i væsentlige risici.	res, og at der tages stilling til eventuelle udvalgte områder med øget risiko.
	SKATs kommentar i 2013: Enig – der foretages en ny risikovurdering af BRAS, således at der tages stilling til, om risiko billedet har ændret sig. Dette følges op med en ajourføring af risikoanalysen		
2.6. **Prioritet 2**	<u>Backup af BRAS data</u> SIR har fået oplyst, at der primo marts 2013 var behov for en ”restore” af BRAS databasen, og at den nyeste backup, som virkede, var fra august 2012. Det blev endvidere oplyst, at der reelt ikke er	Manglende kendskab til backup forhold, øger risikoen for at der ikke tages backup som forventet af systemejeren og i overensstemmelse med risikovurderingen for systemet.	SIR anbefaler, at systemejeren med udgangspunkt i it-risikoanalysen for BRAS, stiller krav til forhold omkring backup. Herunder at der for eksempel tages daglig backup af database ændringer, og at backup gemmes i minimum 5 år.

Nr.	Observationer	Risici	Anbefalinger
	kendskab til, hvor hyppigt og i hvor mange generationer der tages backup af BRAS data, herunder om der sker test af backuppen. **Status 2014:** SIR har fået oplyst, at It-service og Teknologi er kontaktet, og de har tilkendegivet, at DBProd01 igen er med i backup-proceduren. Endvidere er det oplyst, at der efterfølgende har været et tilfælde, hvor der var behov for restore af data til et SKAT-program (Dipsy), hvilket ikke gav anledning til problemer. **Vi anser punktet for lukket**		
	SKATs kommentar i 2013: Enig – IT vil sikre at der stilles krav ift. backup af BRAS data		
2.7. **Prioritet 2**	<u>Dokumentation for systemændringer af BRAS</u> SIR har fået oplyst, at der i forbindelse med ændringer til applikationen BRAS ikke altid udarbejdes dokumentation for ændringerne herunder egentlige kravspecifikationer og dokumentation for udførte test. **Status 2014:** Vi har modtaget udtræk som viser en versionsstyringsproces. Vi kan ikke af dokumentet se, specifikationerne for ændringerne, ligesom det ikke fremgår, hvorvidt en ændring er blive testet og godkendt inden produktionen er ændret. Vi har efterfølgende fået oplyst, at der fremadrettet vil blive oprettet Remedy-sager på systemændringer i BRAS produktion og sagsnummeret i Remedy vil blive noteret i pro-	Manglende dokumentation for systemændringer øger risikoen for, at man ikke kan følge, hvilke ændringer systemet har været udsat for, og hvordan det har påvirket funktionaliteten.	SIR anbefaler, at SKATs regler på området for systemudvikling følges, og at der udarbejdes dokumentation til understøttelse af ændringen.

Nr.	Observationer	Risici	Anbefalinger
	grammet "Versionsstyring". **Vi anser fortsat punktet for åbent.**		
	SKATs kommentar i 2013: Enig - der iværksættes en procedure, der sikrer, at systemændringer dokumenteres **SKATs kommentar i 2014:** IT Center Haderslev / John K C Madsen. Versionsstyring er nu etableret.		
2.8. **Prioritet 1**	<u>Funktionsadskillelse mellem udvikling og produktion</u> SIR har konstateret, at systemudvikleren på BRAS har adgang til BRAS i produktion. Dermed er der manglende funktionsadskillelse mellem udvikling og produktion, hvilket er manglende efterlevelse af it-sikkerhedspolitikkens afsnit 10.1 om funktionsadskillelse. **Status 2014:** SIR har fået oplyst, at grundet den nuværende ressource situationen i Skat, accepterer IT ledelsen den risiko, der hersker, ved manglende funktionsadskillelse mellem udvikling og produktion i BRAS. **SKAT er bekendt med og har valgt at leve med risikoen.**	Manglende logisk adskillelse mellem udvikling og produktionsmiljøet øger risikoen for uautoriserede ændringer, hvilket kan påvirke integriteten af data.	SIR anbefaler, at der etableres en effektiv funktionsadskillelse mellem personerne, som har med udvikling af BRAS og personer, som anvender BRAS i produktion. Hvis det ikke er muligt at etablere en effektiv funktionsadskillelse, anbefales det, at der etableres kompenserende kontrolforanstaltninger, for eksempel overvågning eller logning, til fastholdelse af, hvad udvikleren har udført i produktionsmiljøet.
	SKATs kommentar i 2013: Funktionsadskillelse mellem udvikling og produktion etableres snarest **SKATs kommentar i 2014:** IT Center Haderslev / John K C Madsen. Ressource situationen er uændret så følgende bemærkning gælder - SKAT er bekendt med risikoen og har valgt, at leve med den.		

Nr.	Observationer	Risici	Anbefalinger
3.	**Styring af rettigheder via BRAS**		
3.1. **Prioritet 2**	<u>Automatisk sletning af rettigheder via BRAS</u> IT-centret foretager kun sletning af en brugers rettigheder, når de modtager en besked herom fra en chef eller via besked fra SAP-HR om, at en medarbejder er fratrådt. SIR har fået oplyst, at når en bruger stopper, noteres dette i SAP-HR, og på sidste arbejdsdag slettes brugeren i AD. Brugeren vil herefter ikke fremgå af personalefortegnelsen i SKAT. I BRAS er der en kontrol, som sikrer, at hvis en medarbejder ikke fremgår af personalefortegnelsen i 14 dage, så initieres der automatisk en sletning af brugerens rettigheder. Via denne kontrol bliver brugerne først slettet 14 dage efter fratrædelsen, hvilket ikke er i overensstemmelse med it-sikkerhedspolitikkens regler afsnit 11.2.2 om, at rettigheder skal slettes umiddelbart efter, at brugerne ikke længere har behovet. **Status 2014** Vi har set dokumentation for, at fratrådte brugere noteret i SAP, automatisk får fjernet sine rettigheder i BRAS 6 dage senere. **Vi anser punktet for lukket**	Manglende rettidig sletning af fratrådte medarbejdere øger risikoen for autoriseret adgang.	SIR anbefaler, at fratrådte medarbejdere får slettet deres rettigheder, når de ikke længere har behovet for adgang.
	SKATs kommentar i 2013: Enig - proceduren ændres, således at autorisationer slettes 2 – 3 dage efter medarbejderens fratrædelse.		
3.2.	<u>Udbredelsen af BRAS</u> Formålet med BRAS er, at applikationen skal	Ved at benytte BRAS opnås ensartethed og dokumentation for brugeradministrati-	SIR anbefaler, at udbredelsen og anvendelsen af BRAS fortsættes således, at brugeradministrationen

Nr.	Observationer	Risici	Anbefalinger
Prioritet 3	fungere som en erstatning for den manuelle blanketproces, som normalt anvendes ved brugeradministration. Det er dog ikke alle systemer, hvor brugeradministrationen sker via BRAS. **Status 2014:** SIR har fået oplyst, at SKAT løbende er i gang med at få nye systemer i BRAS. På nuværende tidspunkt er følgende systemer enten implementeret eller på vej til implementering i BRAS; EFI, Konfigurationsstyringsdatabase, SAP 38, SAP Intern og SAP PS **Vi anser punktet for lukket**	on.	i størst mulig omfang benytter de samme processer.
	SKATs kommentar i 2013: Enig - i forbindelse med alle projekter vedrørende udviklingen af nye systemer tages kontakt til projektet/systemejer med henblik på at få klarlagt brugerroller og få disse medtaget i BRAS.		
3.3. **Prioritet 2**	<u>BRAS integration til subsystemer</u> En gennemgang viser, at der i BRAS sker brugeradministration for ca. 111 applikationer. 38 af 111 applikationer har elektronisk dataudveksling med BRAS således, at rettighedsændringer overføres elektronisk fra BRAS til den pågældende applikation. For de resterende applikationer (ca. 73) overfører BRAS(FC) brugerændringerne til BRAS(IT), hvorfra autorisationsteamet manuelt foretager brugerændringen i den relevante applikation. **Status 2014:** Vi har modtaget en ajourført liste som viser, at der nu er 120 applikationer hvor brugeradministrationen sker via BRAS. 50 af 120 applikati-	Manglende elektronisk overførsel øger risikoen for fejl i brugeradministrationen.	SIR anbefaler, at den elektroniske integration mellem BRAS og tilhørende applikationer øges i størst muligt omfang, for at sikre integriteten, fuldstændigheden og rettigheden i overførte data både i relation til allerede eksisterende applikationer men også til ny udviklede applikationer.

Nr.	Observationer	Risici	Anbefalinger
	onerne har nu elektronisk dataudveksling med BRAS således, at rettighedsændringer overføres elektronisk fra BRAS til den pågældende applikation. Der er således fortsat 70 applikation, hvor integrationen fra BRAS til applikationen er manuel. Vi fastholder anbefalingen, og vil henlede opmærksomheden på, at det bl.a. undersøges om dataudvekslingen med applikationerne i relation til "TS-Tele familien" og SAP kan gøres automatiske. **Vi anser fortsat punktet for åbent.**		
	SKATs kommentar i 2013: Enig – som tiltag kan nævnes, at der i 2012 blev indledt et Lean projekt med henblik på at analysere, i hvilke systemer den store volumen var i brugerantal. I den forbindelse blev projektet præsenteret for systemet "Omada", der ifølge konsulenterne kunne lave den elektroniske dataudveksling. Der blev etableret et pilotprojekt på SAP Intern til indhøstning af erfaringer. **SKATs kommentar i 2014:** IT Center Haderslev / John K C Madsen. Vi er selvfølgelig enig i konklusionen, men punktet bør ses i relation til det arbejde sikkerhedskontoret har skudt i gang omkring "Styrkelse af brugerrettighedsstyring", så der sættes ikke noget i gang for nuværende, men det afventer direktionsbeslutningen.		
3.4. **Prioritet 2**	<u>Systembeskrivelse for BRAS</u> SIR har set, at der er udarbejdet en "Tabeloversigt" som viser anvendte tabeller i BRAS. Samtidig er det oplyst, at der ikke er udarbejdet egentlige systembeskrivelser. **Status 2014:** Det er oplyst, at der endnu ikke er udarbejdet en systembeskrivelse. SKAT har igangsat en proces som skal undersøge om det er muligt, at migrere BRAS til en nyere platform. I den forbindelse vil der blive udarbejdet en systembeskrivelse.	Manglende systembeskrivelser øger risikoen for, at der ikke er kendskab til, hvordan systemer fungerer. Endvidere er der risiko for, at det kun er udvikleren som har systemkendskabet.	SIR anbefaler, at der udarbejdes en anvendelig og opdateret systembeskrivelse for BRAS. Beskrivelsen bør indeholde beskrivelse af formål, systemsammenhænge, funktioner, kontroller, ind- og uddata forhold, logs. mm. Endvidere anbefaler SIR, at systembeskrivelsen udarbejdes på en sådan måde, at den er med til at reducere afhængigheden af nøglepersoner.

Nr.	Observationer	Risici	Anbefalinger
	Vi anser fortsat punktet for åbent		
	SKATs kommentar i 2013: Der udarbejdes en anvendelig og opdateret systembeskrivelse for BRAS, der samtidig har en form, der reducerer afhængigheden af nøglepersoner. **SKATs kommentar i 2014:** IT Center Haderslev / John K C Madsen. Grundet ressource situationen udarbejdes ikke systembeskrivelse. Skat er bevist omkring nøglepersonsproblematikken. Punktet afventer en politisk stillingstagen til fremtidig platform – Bras eller standard platform.		
3.5. **Prioritet 3**	<u>Vejledning for anvendelsen af BRAS</u> SIR har set, at der er udarbejdet en "Vejledning for afdelingsledere og kontorchefer" vedrørende BRAS. Vejledningen er fra 2010 og giver læseren en god forståelse af BRAS. Samtidig er det oplyst, at der pt. arbejdes på en ajourføring af vejledningen. **Status 2014:** SIR har modtaget kopi af seneste brugervejledning og kan se, at der nu er påført et versionsnummer svarende til den kørende version af BRAS. **Vi anser punktet for lukket**	Manglende regelmæssig ajourføring af vejledninger til anvendte systemer, øger risikoen for, at brugerne ikke opnår kendskab til ny funktionalitet, og at der sker forkert brug af systemet.	SIR anbefaler, at brugervejledningen ajourføres i takt med de systemmæssige ændringer, som udføres, således at vejledninger med mere passer til systemet i drift.
	SKATs kommentar i 2013: Der iværksættes en ny procedure der sikre, at brugervejledningen ajourføres i takt med systemmæssige ændringer.		
3.6. **Prioritet 2**	<u>Integritetskontrol i BRAS</u> Via dataudtræk fra BRAS, er det konstateret, at der pr. 12 marts 2013 findes 1.477 autorisationslinjer, hvor datafeltet "Afdid" = NULL. (Dvs. disse autorisationslinjer vises ikke i nogen afdeling). Samtidig er det oplyst, at brugerens chef får en pop-up, med besked om, at	Manglende korrekt tilhørsforhold i BRAS bevirker, at der ikke vil ske revurdering af de pågældende autorisationslinjer.	SIR anbefaler en programmeret kontrol i BRAS, som bevirker, at cheferne ikke kan initiere nye ordrelinjer i BRAS, så længe chefen har medarbejdere hvor tilhørsforholdet ikke er rettet til.

Nr.	Observationer	Risici	Anbefalinger
	der skal ske ændring af brugerens tilhørsforhold (Afdid), men til dette angiver mange blot "OK", og udfører ikke yderligere. En gennemgang af de 1.477 records viser, at mange er oprettet for langt tid siden, hvorfor cheferne burde have rettet tilhørsforholdet. **Status 2014:** SIR har set dokumentation som viser, at den anbefalede kontrol er testet i BRAS testmiljø således, at der ikke længere kan dannes ordrer, når der findes rettigheder der skal overtages. Samtidig er det oplyst, at den nye funktionalitet er flyttet til BRAS produktion den 3. april 2014 som en del af version 2.0.0.3583. **Vi anser punktet for lukket**		
	SKATs kommentar i 2013: Der etableres en kontrolfunktion i BRAS, der hindrer afgivelse af ordre, så længe medarbejderens tilhørsforhold ikke er korrekt.		
3.7. **Prioritet 2**	<u>Overførsel af rettigheder fra BRAS til subsystemer</u> SIR har kendskab til, at der foretages sammenholdelse mellem rettigheder i BRAS og tildelte rettigheder i 3 subsystemer. SIR har foretaget en enkelt stikprøve mellem BRAS og SISY systemet for en enkelt medarbejder og konstateret uoverensstemmelser mellem de rettigheder, som fremgår af BRAS og de rettigheder, som fremgår af SISY. (SISY systemet er ikke en del af ovennævnte 3 subsystemer.) **Status 2014:** SIR har fået oplyst, at der fortsat ikke er sket	Manglende overensstemmelse mellem oplistede rettigheder i BRAS med faktiske tildelte rettigheder i subsystemer øger risikoen for, at det ikke opdages, hvis en medarbejder har flere rettigheder end et arbejdsbetinget behov, og samtidig øger det risikoen for uautoriseret adgang.	SIR anbefaler, at der foretages sammenholdelse af noterede rettigheder i BRAS med anvendte rettigheder i SISY og andre subsystemer, og at eventuelle afvigelser afklares.

Nr.	Observationer	Risici	Anbefalinger
	sammenligning mellem SISY og BRAS. **Vi anser fortsat punktet for åbent**		
	SKATs kommentar i 2013: For SISY og andre subsystemer kan systemejerne rette henvendelse til IT-centrene og aftale en proces for afstemning med BRAS. Udtræk fra systemerne til sammenholdelse med BRAS skal generes af systemejerne i samarbejde med leverandørerne. **SKATs kommentar i 2014:** Erhvervs- og Personafregningssystemer, Søren Kjær Jensen. I forbindelse med udpegning af systemejer for SISY etableres en forretningsgang som skal sikre en løbende sammenholdelse mellem BRAS og SISY		
4.	**Styring af Administrator rettigheder via Infrastruktur**		
4.1. **Prioritet 2**	<u>Procedurer for administration af administratorer</u> SIR har foretaget en gennemgang af proceduren "Administration af administratorer", og har konstateret uoverensstemmelser mellem dokumentet og de faktiske handlinger. **Status 2014:** SIR har indhentet nyeste version af proceduren "Administration af administratorer" som er gennemgået. I proceduren fremgår, at "….ingen personer, får tildelt Enterprise Administrator rettigheder…..Skal der bruges Enterprise Administratorrettigheder i forbindelse med opgave skal der ske henvendelse til de AD ansvarlige……Henvendelsen skal indeholde grunden til den opgave hvor det er nødvendigt……". Vi er enige i formålet med brugen af Enterprise adm. rettighederne. Vi har foretaget en gennemgang af oprettede Enterprise admin i AD og har identificerede 3 navngivne bruge-	Manglende efterlevelse af udarbejdede procedurer øger risikoen for, at det ikke er alle ønskede handlinger, som udføres.	SIR anbefaler, at dokumentet "Administration af administratorer i SKATs Windows miljø" ajourføres i overensstemmelse med de handlinger, som faktisk udføres i forbindelse med administration af omtalte rettigheder.

Nr.	Observationer	Risici	Anbefalinger
	re. Jf. brugerlisten i excel, har en bruger været oprettet siden 2003 og en siden 2013. Dette tyder på, at proceduren fortsat ikke følges i alle tilfælde. **Vi anser fortsat punktet for åbent**		
	SKATs kommentar i 2013: IT er enige i observationen. IT har udvidet de enkelte regneark med oplysninger, der dokumenterer de kontroller/ændringer, der udføres. IT har gennemført ændringen. **SKATs kommentar i 2014:** Infrastruktur/Leif Schandorph: Administration af administratorer er implementeret i BRAS ultimo 2014, og følger reglerne for administrative rettigheder. Der sker kvartalsvis opfølgning på de tildelte rettigheder.		
4.2. **Prioritet 3**	<u>Admin administration via BRAS</u> Infrastruktur oplyser, at administrationen af brugere med administrator rettigheder indtil videre sker via et excelark styret i infrastruktur, men at det er hensigten, at bestillingen af udvidede rettigheder skal styres via BRAS. **Status 2014:** Det er oplyst, at IT Infrastruktur er i proces med at få administrator rettigheder registreret i BRAS. Vi lukker anbefalingen, når vi har modtaget dokumentation for integrationen i BRAS. **Vi anser fortsat punktet for åbent**	Manglende styring af it-rettigheder via BRAS øger risikoen for, at der ikke opnås et samlet overblik over brugernes rettigheder, ligesom der er risiko for, at man glemmer at slette alle rettigheder når en bruger fratræder.	SIR anbefaler, at infrastruktur tager initiativ til, at processen i relation til administration af administratorer flyttes til BRAS.
	SKATs kommentar i 2013: IT er enige i observationen. IT har taget initiativer til styring af bestilling af udvidede rettigheder fremgår af BRAS – IT finder det dog ikke hensigtsmæssigt, at rettigheden tildeles via BRAS, da området er for følsomt til større udbredelse. **SKATs kommentar i 2014:** Infrastruktur/Leif Schandorph: Administration af administratorer er implementeret i BRAS ultimo 2014, og følger reglerne for administrative rettigheder.		

Nr.	Observationer	Risici	Anbefalinger
4.3. **Prioritet 2**	<u>Kuvertbruger til administrator kontoen</u> SIR har fået oplyst, at den indbyggede administrator konto er disablet, og at der kun er et mindre antal brugere som har kendskab til dette password. SIR har endvidere fået oplyst, at der ikke gøres brug af kuvertbruger til opbevaring af password til en administrator konto. **Status 2014:** Vi har konstateret, at der hos IT opbevares to ubrudte kuverter i pengeskab. En kuvert med Domain Admin brugerid og password, og en kuvert med Entrise Admin brugerid og password. **Vi anser punktet for lukket**	Manglende anvendelse af kuvertbruger til en administrator konto kan bevirke, at der ikke kan opnås adgang via domainet i tilfælde af, at øvrige administratorer ikke kan få adgang.	SIR anbefaler, at der oprettes administrator konto, som tildeles et sikkert password, og at passwordet placeres i en forseglet kuvert, samt at kuverten bliver opbevaret et sikkert sted, som også vil være tilgængeligt for en beredskabsorganisation.
	SKATs kommentar i 2013: IT er enige i observationen. IT vil følge revisionens anbefaling om en kuvertbruger		
4.4. **Prioritet 2**	<u>Enterprise administratorer</u> I proceduren "Administration af administratorer" fremgår det, at 3 personer er medlem af gruppen "Enterprise admin". SIR har via opslag i Active Directory konstateret, at 9 personer var tilknyttet gruppen og dermed havde udvidede rettigheder. Ved revisionen blev antallet af medlemmer reduceret til 3. Man kan ikke af det excelark som Infrastruktur anvender til styring af rettigheder se, hvilke medarbejdere der skulle have disse rettigheder. **Status 2014:** Vi har foretaget en gennemgang af oprettede Enterprise administratorer i AD og sammenholdt til brugerlisten i excelarket, hvori IT noterer begrundelser og dato for oprettelserne.	Enterprise administrator rettigheder er de højeste rettigheder i et Active Directory domæne, hvormed brugerne kan oprette/nedlægge domæner og dermed påvirke alle øvrige brugeres adgange.	SIR anbefaler, at anvendte excelark til styring af administrator rettigheder udvides til også at omfatte notation af personer med enterprise rettigheder. Endvidere anbefales, at excelarket ajourføres i overensstemmelse med de ændringer, som udføres i domainet.

Nr.	Observationer	Risici	Anbefalinger
	Vi har konstateret en bruger som jf. excelarket skulle være oprettet, men som ikke fremgår af AD. **Vi anser fortsat punktet for åbent.**		
	SKATs kommentar i 2013: IT er enige i observationen. IT har udvidet regnearket til også at indeholde oplysninger vedrørende Enterprise Admin rettigheder og indført dato til dokumentation for ajourføringen. **SKATs kommentar i 2014:** Infrastruktur/Leif Schandorph: Administration af Enterprise administratorer er implementeret i BRAS ultimo 2014, og følger reglerne for administrative rettigheder.		
4.5. **Prioritet 1**	<u>Domain administratorer</u> SIR har indhentet udskrift fra domainet, som viser hvilke brugerkonti, som er placeret i gruppen "Domain Admin". Udskriften fra domainet er sammenholdt til excelark, hvori infrastruktur styrere deres brugere. • Ved en sammenholdelse har SIR konstateret 2 brugere som var noteret som inaktive i excelarket, men som fortsat var tilknyttet gruppen Domain admins. Dette tyder på manglende fjernelse af rettigheder fra domain admin gruppen. • Ved en gennemgang har SIR endvidere konstateret 3 konsulenter fra Venzo som jf. excel skulle have "domain ad-min" rettigheder, men ingen af disse personer var placeret i gruppen "domain admin". • SIR har endvidere konstateret 6 bruger account i domain admins gruppen, som ikke fremgår af excelarket fra infrastruktur. **Status 2014:** Vi har indhentet udskrift fra Domain Admin gruppen og sammenholdt til excelark, hvori infrastruktur styrer deres brugere. Ved vores sammenholdelse har vi ikke identificerede uover-	Manglende styring af domain admin brugere øger risikoen for uautoriseret adgang.	SIR anbefaler, infrastruktur foretager en gennemgang i domain admin gruppen og sammenholder til godkendte oprettelser. Herunder at udarbejdede excelark løbende ajourføres således, at det afspejler de faktiske forhold i domainet.

Nr.	Observationer	Risici	Anbefalinger
	ensstemmelser, hvorfor vi lukker anbefalingen. **Vi anser punktet for lukket**		
	SKATs kommentar i 2013: IT er enige i observationen Fejlen skyldes mht. konsulenter, stavefejl i Excel ark i forhold til account navn, og en konsulent der skulle have været hos os, men aldrig kom, og derfor var oprettet i Excel ark, men ikke i Domænet. Det har ikke for alle Domain Admins været kutyme at fjerne disablede Domain Admin accounts fra rettighedsgrupper – det vil blive indskærpet, så Domain Admins gruppen ikke indeholder lukkede accounts.		
4.6. **Prioritet 2**	<u>Revurdering af administrator brugere</u> Jf. dokumentet "Administration af administratorer i SKATs Windows miljø" side 4, fremgår det, at der en gang månedligt skal ske gennemgang af medlemmer af gruppen "Domain Admins". SIR har fået oplyst, at denne kontrol udføres som beskrevet en gang månedligt, men at der ikke udarbejdes dokumentation for gennemgangen, og at den ofte laves i forbindelse med, at der opstår en ændring af en anden bruger. **Status 2014:** Vi har indhentet det excelark som Infrastruktur anvender til styring af deres brugere. I arket kan man se, at der regelmæssigt siden maj 2013 er fortaget ajourføring af Enterprise admins, Domæne admins og brugere med begrænset admin. Rettigheder. Vores gennemgang har ikke givet anledning til bemærkninger, hvorfor vi lukker anbefalingen. **Vi anser punktet for lukket**	Manglende formel revurdering af oprettede brugere og deres rettigheder øger risikoen for, at uoverensstemmelser i brugerrettigheder og adgange ikke opdages, hvilket som afledt effekt øger risikoen for uautoriseret adgang.	SIR anbefaler, at SKAT it-sikkerhedspolitikkens it-regler på området følges, herunder at der udføres egentlige revurderinger af brugerne og deres udvidede rettigheder, og at revurderingen dokumenteres.
	SKATs kommentar i 2013: IT er enige i observationen. IT foretager løbende vurdering af Domain Admin rettigheder, og mindst en gang om måneden dokumenteres vurderingen med dato markering i regneark. For øvrige udvidede rettigheder overvejes det, hvordan revurdering kan foretages.		

Nr.	Observationer	Risici	Anbefalinger
	De enkelte regneark er udvidet med oplysninger, der dokumenterer de kontroller/ændringer, der udføres.		
4.7. **Prioritet 2**	<u>"Password settings" for SKATs domaine</u> SIR har modtaget udskrifter fra domænet, som viser, at brugerne er underlagt følgende password krav, når de logger på netværket: * Password skift hver 90 dage * Husker de sidste 24 passwords. * Minimum password alder er 5 dage * Minimum 8 tegn * Kompleksitet er aktiv/enabled * Brugerne har 10 logon forsøg, hvorefter man spærres i 24 timer, hvorefter man har 10 nye forsøg. Fra SKAT it-sikkerhedspolitiks it-regler afsnit 11.3 er følgende krav opsat til netværks logon: * Minimum 8 tegn * Være en blanding af store og små bogstaver (ikke æ, ø eller å) * Minimum indeholde et stort bogstav * Minimum indeholde et tal og/eller et specialtegn Fra SKAT it-sikkerhedspolitiks it-regler afsnit 11.5 skal adgangskontrolsystemet låse brugerkonti efter fem forgæves adgangsforsøg. **Status 2014:** Vi har indhentet ny udskrift fra domænet vedr. "password policy" og kan konstatere, at brugerne fortsat har 10 logon forsøg, hvilket er manglende efterlevelse af gældende it-	Ved et stort antal logon forsøg øges risikoen for uautoriseret adgang.	SIR anbefaler, at SKATs it-sikkerhedspolitik på området følges, og at brugerne maksimalt har 5 logon forsøg, inden kontoen spærres.

Nr.	Observationer	Risici	Anbefalinger
	sikkerhedspolitik. **Vi anser fortsat punktet for åbent.**		
	SKATs kommentar i 2013: IT er enige i observationen. IT har imidlertid fejl i nogle applikationer, der betyder, at hvis antallet af password forsøg sættes til 5, så vil vi få rigtig mange password låsninger. It arbejder for at få disse problemer løst, så vi igen kan nedsætte antallet af logon forsøg til 5, som informations sikkerheds politikken foreskriver. Tidshorisont for løsning kendes ikke på nuværende tidspunkt. **SKATs kommentar i 2014:** Infrastruktur/Leif Schandorph: Skat har løst en del af problemerne på de applikationer, der gav anledning til at setting måtte sættes op, der er imidlertid kommet andre løsninger til mobil mail mv. SKAT har derfor endnu ikke implementeret setting i produktionsmiljøet – der planlægges en styret change af setting senere i 2015 udenfor spidsbe-lastnings periode. Forventet implementeret 31-07-2015.		
4.8. **Prioritet 2**	<u>"Audit-policy settings" for SKATs domaine</u> Opsætning af logning, når medarbejderne logger på SKATs netværk. SIR har modtaget kopi af "audit policies" fra Domain Controlleren og kan se, at der kun i begrænset omfang sker logning af væsentlige hændelser. Gennemgangen viser, at logningen er sat til følgende: *Audit account logon events: Success, Failure *Audit account management: Success, Failure *Audit logon events: Failure *Audit policy change: Success, Failure *Audit privilege use: Failure *Audit system events: Success, Failure Fra SKATs It-sikkerhedspolitikkens it-regler afsnit 10.10 fremgår det blandt andet, at der skal ske logning, så man kan se, hvilke bruge-	Manglende registrering af sikkerhedsmæssige hændelser samt opfølgning herpå medfører risiko for, at eventuelle forsøg på angreb ikke opdages i tide.	SIR anbefaler, at der foretages gennemgang af logningskriterierne, og at der logges på følgende handlinger for efterlevelse af gældende it-sikkerhedspolitik. *Audit account logon events: Success, Failure *Audit account management: Success, Failure *Audit logon events: Success, Failure *Audit policy change: Success, Failure *Audit privilege use: Success, Failure *Audit system events: Success, Failure

Nr.	Observationer	Risici	Anbefalinger
	re, som har tilgået systemet, dvs. success for logon event, og success for privilege use og uautoriserede adgangsforsøg. **Status 2014:** Vi har set dokumentation som viser at følgende logningen er sat: *Audit acc. logon events: Failure *Audit acc. management: Success, Failure *Audit logon events: Failure *Audit policy change: Success, Failure *Audit privilege use: Success, Failure *Audit system events: Success, Failure **Vi anser fortsat punktet for åbent.**		
	SKATs kommentar i 2013: IT er enige i observationen. IT vil følge Revisionens anbefalinger og koordinere disse med informations sikkerhed, så der kan ske opdatering af politikkerne. Aktiviteten er igangsat. **SKATs kommentar i 2014:** Infrastruktur/Leif Schandorph: Settings er ændret i henhold til sikkerhedspolitik.		
4.9. **Prioritet 2**	<u>Manglende formel godkendelse af oprettelser</u> I dokumentet "Administration af administratorer i SKATs Windows miljø" fremgår det på side 4, at "Det er kun kontorchefen fra Infrastruktur, som kan godkende oprettelser". SIR har fået oplyst, at der faktisk ikke udføres nogen egentlig godkendelse ved oprettelse af brugere med udvidede rettigheder. Brugerne er godkendt implicit i kraft af deres organisatoriske placering i Infrastruktur gruppen.	Manglende godkendelse og automatisk tildeling øger risikoen for oprettelse af brugerkonti uden arbejdsbetinget behov.	SIR anbefaler, at kontorchefen for infrastruktur udfører en formel godkendelse af oprettede brugere med administrator rettigheder.

Nr.	Observationer	Risici	Anbefalinger
	Status 2014: Det er oplyst, at området på nuværende tidspunkt er uændret, men Infrastruktur er i proces med at overføre styringen til BRAS, hvor initieringen og godkendelse af brugererne vil ske af nærmeste chef. **Vi anser fortsat punktet for åbent.**		
	SKATs kommentar i 2013: IT er enige i observationen. IT påtænker at indføre en formel procedure. **SKATs kommentar i 2014:** Infrastruktur/Leif Schandorph: Oprettelsen af brugere med særlige administrative privilegier, er implementeret i BRAS ultimo 2014. Tildelingen af rettighederne sker derfor fremover via BRAS også for de centrale IT administrations rettigheder i infrastruktur.		
4.10. **Prioritet 1**	<u>Rettidig spærring af brugere med udvidede rettigheder</u> SIR har indhentet kopi af det regneark, som infrastruktur bruger til styring af brugere med udvidede rettigheder. Man kan af listen se, hvornår de enkelte medarbejdere har fået tildelt administrator rettigheder og hvornår de er blevet inaktive. SIR har sammenholdt regnearket med listen over fratrådte medarbejdere fra SAP-HR. Ved gennemgangen har SIR konstateret 5 brugere som jf. SAP-HR er stoppet, men deres account er først gjort inaktiv måneden efter. **Status 2014:** Vi har indhentet liste fra SAP-HR over seneste fratrådte medarbejdere i SKAT. Listen er sammenholdt til Infrastrukturs regneark over ADM brugere. Ved vores sammenholdelse er	Manglende inaktivering øger risikoen for uautoriseret adgang og er ligeledes manglende efterlevelse af it-sikkerhedspolitikken.	SIR anbefaler, at SKATs it-sikkerhedspolitik efterleves og at brugerne gøres inaktive, når de ikke længere har et arbejdsbetinget behov.

Nr.	Observationer	Risici	Anbefalinger
	der ikke konstateret brugere som burde have været slettet i Infrastrukturs regneark, grundet evt. fratrædelse. **Vi anser punktet for lukket**		
	SKATs kommentar i 2013: IT er enige i observationen. IT har hidtil i forbindelse med månedlig gennemgang konstateret, at en fratrædelse har fundet sted. Det skal dog tilføjes, at accounts er blevet lukket øjeblikkelig ved diskretionære afskedigelser. IT har allerede inden revisionen arbejdet med en løsning på problematikken, og løsningen forventes implementeret hurtigst muligt.		
5.	**Styring af rettigheder via SISY og AU**		
5.1. **Prioritet 3**	<u>Udpeget systemejer</u> Via Intranettet og siden "Systemoverblik" er det konstateret, at en medarbejder fra Intern Revision er udpeget som systemejer til SISY. Ingen er udpeget som platformsejer, og det er ligeledes medarbejderen fra Intern Revision, som skal kontaktes i relation til procesejerskabet. Medarbejderen har været i SIR siden 1/1 2009 og bør ikke være tildelt ejerskabet til nogle systemer. **Status 2014:** Vi har konstateret, at medarbejderen fra SIR ikke længere fremstår som systemejer til SISY på siden ”Systemoverblik”. Vi har dog også konstateret, at system- og procesejerskabet for SISY ikke er placeret hos specifikke medarbejdere men er placeret i bestemte kontorer. **Vi anser fortsat punktet for åbent.**	Manglende eller forkert angivelse af ejerform øger risikoen for manglende ansvarsplacering, ligesom der kan opstå tvivl om, hvem der skal godkende eventuelle ændringer til systemet.	SIR anbefaler, at der formelt i relation til SISY udpeges en system-, platforms- og procesejer, som påtager sig disse ejerskaber. Ligeledes anbefaler SIR at "systemoverblik" listen på intranettet opdateres med disse informationer. SIR anbefaler, at ejerskabet og ansvar placeres hos navngivende personer.
	SKATs kommentar i 2013: IT er enig i Revisionens anbefalinger.		

Nr.	Observationer	Risici	Anbefalinger
	SKATs kommentar i 2014: Erhvervs- og Personafregningssystemer, Søren Kjær Jensen. Der vil være udpeget systemejer, platformsejer senest ultimo april 2015. Procesejerskab ligger i Kundeservice som vil få forelagt SIR's anbefaling.		
5.2. **Prioritet 2**	Risikoanalyse for SISY Via applikationen "RISK" er det konstateret, at den sidst udarbejdede risikoanalyse for SISY er foretaget den 22. april 2008. Jf. SKATs it-sikkerhedspolitikkens it-regler afsnit 4 skal der årligt ske udarbejdelse af risikoanalyser. Processen "SISY" vurderes som værende "Kritisk for SKAT", og afhængigheden af nøglepersoner vurderes til at være "Stor", ligesom det fremgår, at informationsressourcen har et "stort aktivitsomfang" og er "stigende i anvendelsen". **Status 2014:** Vi har ikke modtaget dokumentation for udarbejdelse af ny risikoanalyse for SISY. **Vi anser fortsat punktet for åbent.**	Manglende ajourføring af risikoanalysen øger risikoen for, at der ikke er opnået kendskab til eventuelle ændringer i væsentlige risici.	SIR anbefaler, at risikoanalysen ajourføres, og at der tages stilling til eventuelle udvalgte områder med øget risiko.
	SKATs kommentar i 2013: IT er enige og vil få udarbejdet en risikoanalyse. (ultimo september 2013) **SKATs kommentar i 2014:** Erhvervs- og Personafregningssystemer, Søren Kjær Jensen. Der vil blive udarbejdet en risikoanalyse senest ultimo april 2015.		
5.3. **Prioritet 2**	Udpeget platformsejer eller procesejer for AU Via Intranettet og siden "Systemoverblik" er det konstateret, at der er udpeget systemejere fra it-drift. Ingen er udpeget som platformsejer	Manglende angivelse af ejerformer øger risikoen for manglende ansvarsplacering, ligesom der kan opstå tvivl om, hvem som skal godkende eventuelle ændringer til systemet.	SIR anbefaler, at der formelt i relation til AU udpeges en platforms- og procesejer, og at "systemoverblik" listen på intranettet opdateres med disse informationer.

Nr.	Observationer	Risici	Anbefalinger
	eller procesejer. **Status 2014:** Vi har via "Systemoverblik" konstateret, at der nu er udpegede egentlige personer til at være systemejere, modellører og It-arkitekt. **Vi anser punktet for lukket**		
	SKATs kommentar i 2013: Der er udpeget en platformsejer for AU, og vi vil tilsikre, at systemoverblikket opdateres. Procesejerskabet skal afklares med Kundeservice.		
5.4. **Prioritet 2**	<u>Risikoanalyse for AU</u> SIR har fået oplyst, at det er en ledelsesmæssig beslutning at fravælge udarbejdelse af en risikoanalyse for AU. Jf. SKATs it-sikkerhedspolitiks it-regler afsnit 4, skal der årligt ske udarbejdelse af risikoanalyser. Det er SIRs vurdering, at "AU" systemet udgør en "høj" risiko, med krævende oppetider og tilgængelighed, hvorfor det er vigtigt, at der udarbejdes risikoanalyser til afdækning af området. **Status 2014:** SIR har konstateret, at SKAT den 8/5-2014 har udarbejdet en risikoanalyse for AU, hvor konklusionen samlet set er "tilfredsstillende" i relation til fortrolighed, integritet og tilgængelighed. Vores gennemgang af risikoanalysen har ikke givet anledning til nye bemærkninger, hvorfor vi lukker anbefalingen. **Vi anser punktet for lukket.**	Manglende udarbejdelse af risikoanalyse for et specifikt system øger risikoen for, at der ikke er kendskab til, hvor lang tid organisationen kan "tåle", at det pågældende system ikke er tilgængeligt.	SIR anbefaler, at der via RISK bliver udarbejdet en risikoanalyse for systemet.
	SKATs kommentar i 2013: IT er enige og vil få udarbejdet en risikoanalyse. (ultimo september 2013)		

Nr.	Observationer	Risici	Anbefalinger
5.5. **Priori-tet 2**	CSC rettigheder i RACF SIR har fået oplyst, at autorisationsteamet også står for brugeradministrationen af RACF brugere. SIR har endvidere fået oplyst, at CSC også selv udfører brugeradministration af CSC brugere i SKATs RACF. **Status 2014:** Informationssikkerhed har oplyst, at der ikke er et krav om, at SKAT skal have oplysninger om leverandørers brugere og deres adgange, og da SKAT tidligere har tilkendegivet, at de mener den nuværende styring og opfølgning er betryggende, har de samtidig tilkendegivet at de ikke ønsker at følge anbefalingen, men i stedet valgt at leve med risikoen. **SKAT er bekendt med og har valgt at leve med risikoen.**	Manglende intern styring af eksterne brugere til RACF øger risikoen for uautoriseret adgang.	SIR anbefaler, at brugeradministrationen for eksterne brugere til RACF styres via SKAT' processer i lighed med interne brugere, således at SKAT har styr på, hvilke brugere som oprettes, og hvilke rettigheder som tildeles.
	SKATs kommentar i 2013: Aftalen med CSC har altid været sådan, at CSC selv har administreret deres adgange til SKATs systemer. Til SKATs verifikation fremsender CSC månedligt benyttelsesstatistikker til SKAT, som dokumenterer, hvilke medarbejdere der har benyttet sig af adgangen. SKAT gennemgår stikprøvevis disse benyttelsesstatistikker og følger op. Ligeledes foretager CSC ½-årlige gennemgange af oprettede CSC brugere til SKATs systemer for at se, om de fortsat har et arbejdsbetinget behov for adgang. Vi mener, at den nuværende styring og opfølgning er betryggende.		
	SLUT		

Bilag 2: Anvendt skala

Ved vurderingen i konklusionen er følgende skala anvendt:	
Meget tilfredsstillende	Intern Revision har ikke konstateret svagheder i de forretningsgange og processer, der understøtter det 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 observationerne 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.

Observationer, som vi har lukket i denne revision, er markeret med "Grå".