Skatteministeriet

4. april 2016
J. nr. 15-1492216
Plannr. 115-002

Intern Revision

Rapport 2015

SKAT IT

It-revision af adgangsstyring

Modtager
Direktør Jesper Rønnow Simonsen, SKAT

Kopi
Direktør Karsten Juncher, SKAT IT
Departementet
Rigsrevisionen

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

Forord

Intern Revision (IR) har, jævnfør orienteringsbrev af 29. april 2015, revideret adgangsstyring. Den udførte revision er en del af den samlede revision for 2015.

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.

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.

København, den 4. april 2016

Kurt Wagner
Revisionschef

Aliriza Özden
Manager

1. Formål

Formålet med revisionen af adgangsstyring er at undersøge og vurdere, hvorvidt SKAT overholder ”A.9 Adgangsstyring” i ISO-standarden 27001, som omfatter:

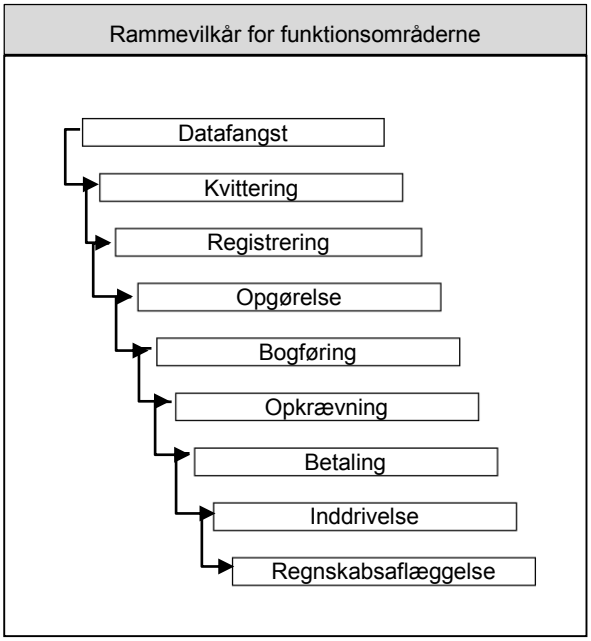
1. ”at begrænse adgangen til information og informationsbehandlingsfaciliteter”,
2. ”at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester”,
3. ”at gøre brugere ansvarlige for at sikre deres autentifikationsinformation”,
4. ”at forhindre uautoriseret adgang til systemer og applikationer”.

2. Omfang

Revisionen er udført i perioden maj til november 2015 med udgangspunkt i ISO 27001:2013 og har omfattet emne ”A.9 Adgangsstyring” med følgende hovedområder:

- A.9.1 Forretningsmæssige krav til adgangsstyring
- A.9.2 Administration af brugeradgange
- A.9.3 Brugernes ansvar
- A.9.4 Styring af system- og applikationsadgange

SIR anvender følgende model til operationel beskrivelse og kategorisering af aktiviteterne i SKAT:



I forbindelse med denne revision har vi revideret følgende funktionsområde:

- Rammevilkår for funktionsområderne

ISO 27001 standarden for informationssikkerhed har været obligatorisk for statslige myndigheder siden starten 2014 og skal være implementeret primo 2016. Departementet er bekendt med, at SKATs implementering af ISO 27001 først vil være gennemført ved udgangen af 2016 (j.nr. 15-1528730).

Revisionen er udført i henhold til gældende revisionsstandarder, herunder vejledninger fra Rigsrevisionen. Revisionen er gennemført ved interviews, og stikprøvevis gennemgang af foreliggende materiale.

Ved revisionen har vi interviewet medarbejdere fra Økonomi, IT, Kundeservice og HR.

Revisionen er udført af Aliriza Özden og Klaus Myssen.

3. Konklusion

Det er vores vurdering, at der **i større omfang er behov** for ændringer i de reviderede processer i relation til "A.9 Adgangsstyring".

Denne vurdering baserer vi på følgende forhold:

- Formålet med hovedområde "A.9.1 Forretningsmæssige krav til adgangsstyring" er at undersøge, om der er kontroller som sikrer, at adgangen til information og informationsbehandlingsfaciliteter er begrænset. Det er vores vurdering, at **formålet er opnået**.

- Formålet med hovedområde "A.9.2 Administration af brugeradgange" er at undersøge, om der er kontroller som sikrer adgange for autoriserede brugere og forhindrer uautoriseret adgang til systemer og tjenester. Det er vores vurdering, at **formålet ikke er opnået**. Dette er begrundet i, at:
    - den gældende proces og it-system for brugeradministration (BRAS) i nogle tilfælde er tilsidesat, hvor der er tildelt adgangsrettigheder direkte på mappeniveau.
    - eksisterende kontroller for styring af adgange generelt er mangelfulde i design og udførelse, da vi bl.a. har konstateret ubenyttede brugeradgange, adgangsrettigheder der ikke sammenholdes på tværs af væsentlige it-systemer og manglende systematisk overvågning af brugerhandlinger.

- Formålet med hovedområde "A.9.3 Brugernes ansvar" er, at undersøge om der er kontroller som sikrer, at brugere gøres ansvarlige for at sikre deres autentifikationsinformation. Det er vores vurdering, at **formålet er opnået**.

- Formålet med hovedområde "A.9.4 Styring af system- og applikationsadgang" er at undersøge, om der er kontroller som sikrer, at uautoriseret adgang til systemer og applikationer forhindres. Det er vores vurdering, at **formålet er opnået**.

Vi har prioriteret de observerede forhold således:

Revisionsemne	Prioritet 1 *Høj risiko*	Prioritet 2 *Middel risiko*	Prioritet 3/4 *Lille risiko*	I alt
A.9.1 Forretningsmæssige krav til adgangsstyring	**0**	**1**	**1**	**2**
A.9.2 Administration af brugeradgange	**1**	**5**	**0**	**6**
A.9.3 Brugernes ansvar	**0**	**0**	**1**	**1**
A.9.4 Styring af system- og applikationsadgange	**0**	**1**	**0**	**1**
I alt	**1**	**7**	**2**	**10**

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.

Bilag 1: Observationer, risici og anbefalinger

Nr.	Observationer	Risici	Anbefalinger
1	**Revisionsemne: A.9.1 Forretningsmæssige krav til adgangsstyring**		**Funktionsområde: Rammevilkår**
1.1 2015 **Prio. 3**	<u>Dokumentation for gennemgang af administratoradgange</u> Vi har konstateret, at gennemgangen af administratoradgange på netværket (Active Directory) ikke dokumenteres. Vi er informeret om, at de har været gennemgået og set, at brugerlisterne har været udtrukket, hvilket kan antyde, at de har været gennemgået.	Ingen forøget risiko.	Som følge af at der ikke er en forøget risiko, har vi ikke udarbejdet anbefalinger.
1.2 2015 **Prio. 2**	<u>Overvågning af brugerhandlinger</u> Brugerhandlinger på netværket og i it-systemer registreres (logning), men bliver ikke overvåget for at identificere eventuelle forsøg på uautoriserede brugerhandlinger. Loggen bliver udelukkende anvendt til fejlsøgning, hvis der fx er fejl i brugerrettigheder.	Manglende overvågning øger risikoen for, at forsøg på uautoriserede brugerhandlinger ikke opdages.	SKAT bør overvåge brugerhandlinger systematisk fx ved også at anvende alarmer på bestemte handlingsmønstre både på netværket og i it-systemerne.

Nr.	Observationer	Risici	Anbefalinger
	Handleplan fra Martin Wood, It-service og Teknologi: **Kontaktperson: Leif Schandorph** Der er allerede etableret alarmer/overvågning af brugernes handlinger i forhold eksterne tilgange til sites med forhøjet risiko. I forhold til interne adgange, er der etableret logning i forhold til anvendelse af sharepoint sites. Men ikke i forhold til f.eks. h-drev. Der er via Informationsikkerhed iværksat en plan for overgang til sharepoint ved personhenførbare data. Og etablering af special netværksshare med logning ved anvendelse af personfølsomme data, som af applikationsmæssige årsager ikke kan placeres på sharepoint. I forhold til brugere på SKAT netværk er det rimeligt at se dette i forhold til en risikovurdering af hvilke data, hvad mulighederne er for misbrug, og hvilke muligheder der er for at finde/overvåge sådanne hændelser teknisk og ressourcemæssigt. Efter iværksættelse af ovennævnte plan fra Informationssikkerhed, vil der være mulighed for at opsætte alarmer ved fejlforsøg på adgang til specifikke dataområder, og lave en periodisk rapport over sådanne hændelser. Informationssikkerheds plan har en estimeret slutdato 31-12-2016. Iværksættelse af Revisionens anbefalinger – tidsfrist: 31-03-2017.		

Nr.	Observationer	Risici	Anbefalinger
2	**Revisionsemne: A.9.2 Administration af brugeradgange**		**Funktionsområde: Rammevilkår**
2.1 2015 **Prio. 2**	Ubenyttede brugeradgange Vi har konstateret ubenyttede brugeradgange på netværket. 303 brugeradgange har ikke været anvendt i mere end 3 måneder (257 brugeradgange tilhører konsulenter). Ydermere har 174 brugeradgange ikke været anvendt i 6 måneder og 91 adgange siden 2014.	Der er forøget risiko for misbrug af brugeradgange, som ikke bliver slettet eller deaktiveret i tide.	En kontrol af ubenyttede brugeradgange bør sikre, at alle typer af adgange slettes eller deaktiveres i tide herunder også konsulent- og testadgange.
	Handleplan fra Martin Wood, It-service og Teknologi: **Kontaktperson: Leif Schandorph** Langt hovedparten af disse adgange vedrører driftspersonale adgange fra SKATs leverandører – disse adgange er policy-mæssigt nedlukket til kun at kunne udføre de driftsmæssige handlinger, som de pågældende driftsleverandører udfører for SKAT. 1) Infrastruktur har allerede nedlukket brugeradgange der ikke har været anvendt i længere periode. 2) Infrastruktur vil foretage henvendelse til SKATs leverandører for at få aftalt en procedure for oprettelse og vedligeholdelse af disse brugerkonti, da leverandørerne åbenbart ikke selv forstår at håndtere deres muligheder for selv at administrere disse. 3) Infrastruktur vil i 2. kvartal se på mulighederne for indførelse af en ny workflow-baseret bruger- og rettigheds-provisionering, med indbygget auditerings rapportering og mulighed for løbende opfølgning. Tidsfrist: 31-12-2016		

Nr.	Observationer	Risici	Anbefalinger
2.2 2015 **Prio. 2**	<u>Tildeling af brugeradgange</u> Systemet til brugeradministration (BRAS) benyttes bl.a. til tildeling af systemrettigheder. Autorisationer tildeles af medarbejdere, der varetager rollen som autorisationstildeler. Autorisationsansvarlige ledere adviseres først, når rettigheder er tildelt. Det er vores vurdering, at kombinationen af utilstrækkelig beskrivelse af rettigheder i BRAS, sammenholdt med de mange it-systemer og forskelligartede rettigheder kan medføre, at det i praksis ikke bliver muligt for funktionsledere og BRAS-ansvarlige at tage stilling til konsekvensen af tildelte rettigheder.	Kombinationen af utilstrækkelig beskrivelse af rettigheder i BRAS, sammenholdt med de mange it-systemer og forskelligartede rettigheder, kan medføre risiko for uautoriseret adgang til SKATs it-systemer, da det ved tildelingen ikke i alle tilfælde er muligt at vurdere, om brugeradgange er baseret på arbejdsbetingede behov.	Vi anbefaler, at SKAT etablerer en forebyggende kontrol, der bør sikre, at især udvidede/privilegerede rettigheder er omfattet af en ledelsesgodkendelse, før rettighederne aktiveres i systemerne. Det bør endvidere sikres, at rettighederne, både isoleret set og i kombination, ikke tilsidesætter funktionsadskillelse og/eller udgør en risiko for uautoriseret adgang til it-systemerne.
	Handleplan fra John K C Madsen, IT Center Haderslev: Der er udarbejdet en beskrivelse af, hvordan den eksisterende proces skal ændres for at leve op til revisionens anbefalinger. Implementeringen forventes ved udgangen af marts 2016.		
2.3 2015 **Prio. 2**	<u>Intern kontrol for tildeling af systemer og grupper</u> Det fremgår af Business Objects (BO) udtræk fra medio november 2015, at 20 afdelinger ikke har dokumenteret, at de har gennemført den obligatoriske halvårlige interne kontrol for tildeling af systemer og grupper (jf. beskrivelse af kontrol S44501000000) i 2015.	Der er forøget risiko for, at tildelte brugeradgange ikke fortsat er arbejdsbetinget.	SKAT bør sikre, at den interne kontrol for tildeling af systemer og grupper gennemføres og bliver tilstrækkelig dokumenteret af alle afdelinger minimum halvårligt som angivet i kontrolbeskrivelsen.

Nr.	Observationer	Risici	Anbefalinger
	Handleplan fra Kim Saastamoinen-Jakobsen (KC Michael K. Svendsen) – Økonomi, Controlling og Service: 1. SKATs generelle vejledning til det interne kvalitetssikringssystem udvikles og tilpasses ift. følgende: - Styringsmodellen - Dialog/opfølgning mellem Økonomi og forretning - Rolle/ansvar ift. gennemførelse, indberetning, opfølgning og dokumentation af SKATs interne kvalitetssikring Udvikling af vejledning: 20. juni 2016 Ikrafttrædelse af den nye vejledning: August 2016 2. Der udarbejdes en særskilt vejledning til controllerkontorene til brug for løbende opfølgning, afrapportering og risikovurdering af resultater fra SKATs interne kvalitetssikring: - Vejledningen vil give controllerne et ensartet fremadrettet fokus på, hvilke centrale elementer Økonomi skal medtage i den løbende opfølgning og afrapportering på SKATs interne kvalitetssikring på tværs af alle afdelinger Udarbejdelse af vejledning til controllerkontorerne: 20. juni 2016 Ikrafttrædelse af vejledning til controllerne: August 2016		
2.4 **2015** **Prio. 2**	<u>Udtræk og sammenligning af brugeradgange</u> Det er ikke muligt for SKAT løbende at verificere brugeradgange ved at sammenholde disse fra Den Centrale Sikkerhedsløsning (DCS) med BRAS og/eller Active Directory, da det udelukkende er serviceleverandøren CSC, der kan fremsøge disse mod betaling. Flere væsentlige it-systemer anvender DCS bl.a. NTSE, eIndkomst og DIAS.	Risikoen for uautoriseret adgang til SKATs it-systemer øges ved en manglende periodisk sammenholdelse af brugeradgange fra væsentlige it-systemer såsom DCS med BRAS og/eller Active Directory.	Vi anbefaler, at SKAT periodisk sammenholder brugeradgange fra alle væsentlige it-systemer med BRAS og/eller Active Directory. SKAT bør muliggøre udtræk af brugeradgange fra egne it-systemer gennem fx ny funktionalitet for it-systemer, der kræver involvering af serviceleverandører.
	Handleplan fra Johnni Mandrup Jensen - IT Drift, Platforme: En sammenholdelse af BRAS og DCS brugerrettigheder igangsættes, og vil være tilendebragt ultimo april måned 2016. Opgaven bliver udført af system- og platformejer Johan Wøldicke og Helle B Kofoed fra sikkerhedsgruppen.		

Nr.	Observationer	Risici	Anbefalinger
2.5 2015 **Prio. 1**	<u>Inddragelse af brugeradgange</u> Vi har konstateret, at adgangsrettigheder ikke er inddraget for medarbejdere, der er flyttet mellem afdelinger eller styrelser. Rettighederne er tildelt direkte på mappeniveau uden om BRAS og/eller Active Directory, og kan således ikke opfanges af eksisterende kontroller.	Risikoen for uautoriseret adgang til fortrolige informationer og ændring af disse er øget, når den gældende proces for adgangsstyring tilsidesættes.	Brugeradgange bør til enhver tid styres gennem den gældende proces, som er BRAS. SKAT bør forbedre processen for inddragelse af adgangsrettigheder for medarbejdere, der flytter. Endvidere bør SKAT etablere en kontrol, der periodisk sikrer, at tildelte brugeradgange på mappeniveau er i overensstemmelse med BRAS og/eller Active Directory.
	Handleplan fra Martin Wood, It-service og Teknologi: **Kontaktperson: Leif Schandorph** Infrastruktur har allerede iværksat change, således at alle rettigheder (gruppemedlemskaber) bliver nulstillet i AD ved flytning af medarbejder mellem koncernens styrelser. Det er den BRAS ansvarliges opgave, at fjerne rettigheder i BRAS – nulstillingen i AD sikrer alene adgangs sletningen teknisk i forhold til den AD baserede rettighedsstyring. Tilgange til data på mappeniveau hænger sammen med den under punkt 1.2 nævnte flytning af personfølsomme data. Det må efter implementering af punkt 1.2 proceduremæssigt sikres at tværgående adgange dokumenteres, da der stadig vil være behov for dette. Dette forventes som punkt 1.2, at kunne løses via indførelse af nyt workflow-baseret bruger- og rettigheds-provisionering. Tidsfrist: 31-03-2017.		

Nr.	Observationer	Risici	Anbefalinger
2.6 2015 **Prio. 2**	<u>Inddragelse af brugeradgange</u> Det er muligt for funktionsledere og BRAS-ansvarlige at tildele adgang til arbejdsmapper på netværket (H-drevet) for andre styrelser og departementet, uden godkendelse fra de enkelte styrelser eller departementet. Funktionaliteten eksisterer i BRAS, hvor det endvidere også er muligt at opsætte funktionsadskillelse mellem afdelinger.	Der er øget risiko for uautoriseret adgang til arbejdsmapper på netværket.	Det bør sikres, at funktionsledere og BRAS-ansvarlige ikke kan tildele adgangsrettigheder på tværs af styrelser og departementet uden forudgående godkendelse.
	Handleplan fra Martin Wood, It-service og Teknologi: **Kontaktperson: Leif Schandorph** Såfremt funktionsledere og BRAS-ansvarlige kan tildele adgange på tværs af styrelserne, må dette være en BRAS-baseret mulighed, da de ikke har muligheder for dette andre steder. Infrastruktur koordinerer med systemejer for BRAS, at denne mulighed lukkes i BRAS. Tidsfrist: 30-04-2016		

Nr.	Observationer	Risici	Anbefalinger
3	**Revisionsemne: A.9.3 Brugernes ansvar**		**Funktionsområde: Rammevilkår**
3.1 2015 **Prio. 3**	Krav til adgangskoder Det fremgår ikke af "Sikkerhedshåndbog for medarbejdere", at adgangskoder ikke må nedskrives på papir, samt at adgangskoder skal udskiftes ved mistanke om kompromittering.	Ingen forøget risiko.	Som følge af at der ikke er en forøget risiko, har vi ikke udarbejdet anbefalinger.

Nr.	Observationer	Risici	Anbefalinger
4	**Revisionsemne: A.9.4 Styring af system- og applikationsadgange**		**Funktionsområde: Rammevilkår**
4.1 2015 **Prio. 2**	Registrering af brugerhandlinger Vi har konstateret, at der på netværket sker registrering af mislykkede forsøg på logon (Audit logon events=Failure), men det registreres ikke, når logon er lykkedes.	Der er forøget risiko for, at SKAT ikke kan spore handlinger rettet mod misbrugte brugeradgange.	Registrering af brugerhandlinger bør omfatte både logon forsøg der lykkedes og mislykkedes (Audit logon events=Success, Failure) i det omfang, det kan lade sig gøre af driftsmæssige hensyn.
	Handleplan fra Martin Wood, It-service og Teknologi: **Kontaktperson: Leif Schandorph.** Allerede i forbindelse med udførelse af revisionen har Infrastruktur udført en change i policy for logon, således at også succesfulde logon registreres. Tidsfrist: Udført.		

Bilag 2: Anvendt skala

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

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

Prioritering af de enkelte observationer:

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

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

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

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