Skatteministeriet

20. marts 2015
J. nr. 14-4126779
Plannr. 114960

Intern Revision

Rapport 2014

Direktørområde it

NTSE – Generelle it-kontroller

Modtager
Departementschef Jens Brøchner, Skatteministeriet

Kopi
Direktør Jesper Rønnow Simonsen, SKAT
Direktør Jonatan Schloss, SKAT Kundeservice
Direktør Jan Topp Rasmussen, SKAT IT

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

Forord

Skatteministeriets Interne Revision (SIR) har, jævnfør orienteringsbrev af 1. september 2014, revideret de generelle it-kontroller (system-, data- og driftssikkerhed) i Ny TastSelv Erhverv (NTSE). Den udførte revision er en del af den samlede revision for 2014.

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

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

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

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

København, den 20. marts 2015

Kurt Wagner
Revisionschef

Jens Lundgaard
Revisor

1. Formål

Formålet med revisionen har været at efterprøve, om SKAT har sikret en korrekt og betryggende styring af generelle it-kontroller i NTSE.

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

2. Omfang

Revisionen er gennemført i perioden oktober til december 2014 og har omfattet en efterprøvning af:

1) adgangsstyring – om brugeradgange og rettigheder i NTSE styres på betryggende vis bl.a. oprettelse, ændring og nedlæggelse af adgange

2) driftsstyring – om driftsafvikling og rapportering af denne sker som aftalt mellem SKAT og leverandøren

3) ændringsstyring – om programændringer godkendes til udvikling, testes og godkendes i testmiljø, inden de verificeres i produktion.

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

Ved revisionen har vi interviewet medarbejdere fra følgende afdelinger i SKAT:

- Erhvervs- og Personafregningssystemer: Systemejere
- Platforme: Platformsejere
- Udvikling Erhverv: Procesejere
- Sikkerhed: Informationssikkerhed

3. Konklusion

Det er vores vurdering, at kontrolmiljøet for styring af generelle it-kontroller i NTSE kan karakteriseres som værende "**ikke helt tilfredsstillende**".

Følgende forhold er vurderet væsentlige for forretningen:

- Et større antal medarbejdere i SKAT kan indberette moms for virksomheder i NTSE, men indberetningen skal efter interne regler kun ske undtagelsesvis. Dette øger risikoen for uautoriserede ændringer herunder indberetning af fejlagtige beløb for virksomhederne.

- Det har ikke været muligt at indhente en samlet liste over alle gennemførte ændringer til NTSE og gennemgå disse, da styringen er decentralt forankret og involverer platformsejere, systemejere og flere forskellige procesejere. Den uensartede og decentrale styring medfører en øget risiko for, at SKATs ledelse ikke kan opnå et samlet overblik over planlagte som gennemførte ændringer med henblik på at kunne prioritere samt vurdere ressourcebehovet.

- Det fremgår ikke af dokumentationen, at samtlige relevante platform-, proces- og systemejere systematisk afprøver og godkender ændringer til NTSE, selvom ændringerne berører adskillige it-systemer og forretningsprocesser. Mangelfuld dokumentation for afprøvning medfører et reduceret overblik over testomfang og testresultat.

- Brugeraktiviteter i NTSE registreres i et system kaldet XpoLog, som SKAT ikke overvåger systematisk. Der er risiko for, at uautoriserede brugeraktiviteter i NTSE, fx fejlbehæftede ændringer til moms og lønsum eller uautoriserede adgange, ikke opdages.

Vi har prioriteret de observerede forhold således:

Revisionsemne	**Prioritet 1** *Kritisk for forretningen*	**Prioritet 2** *Væsentlig for forretningen*	**Prioritet 3** *Mindre betydning for forretningen*	**I alt**
1) Adgangsstyring	**0**	**2**	**0**	**2**
2) Driftsstyring	**0**	**0**	**1**	**1**
3) Ændringsstyring	**0**	**2**	**0**	**2**
I alt	**0**	**4**	**1**	**5**

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

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

Bilag 1: Observationer, risici og anbefalinger

Nr.	Observationer	Risici	Anbefalinger
1	**Adgangsstyring**		
1.1 fra 2014 **P2**	**Rettighedsstyring** SIR har konstateret, at 249 medarbejdere er tildelt rettigheden ”MomsPRG”, der giver mulighed for at se og indberette moms i NTSE uden kontrol og godkendelse fra en anden medarbejder. I følge SKATs interne regler, må SKATs medarbejdere kun undtagelsesvis indberette moms for virksomhederne, og hvis det sker, skal det logges af systemet og i Remedy.	Risikoen for uautoriserede ændringer i data via NTSE øges af, at et stort antal medarbejdere har mulighed for at indberette data. Der er risiko for, at SKATs medarbejdere kan indberette fejlagtige beløb for virksomhederne.	SIR anbefaler, at retten til at indberette for virksomhederne kun bør tildeles medarbejdere med arbejdsbetinget behov. Etablering af funktionsadskillelse bør overvejes for at sikre, at dataændringer fra en medarbejder først træder i kraft efter kontrol og godkendelse fra en anden medarbejder.
	Handleplan fra SKAT *Susanne Thorhauge, Selskaber og digitalisering*: SKAT er enig i observationen samt risikoen. Vi har udarbejdet en ny model for SKAT medarbejderes adgang til områder i NTSE. I den nye model, kan der skelnes mellem ”se”-adgang og ”rediger”-adgang. På den måde vil kun de medarbejdere som faktisk skal lave indberetninger for virksomheder, behøve at få adgang til dette. Modellen vil blive brugt på alle områder som fremover åbnes for SKAT medarbejdere. Det udestår at omlægge momsområdet, men dette forventes at blive implementeret i Q1 i forbindelse med DRI-moms (Digital Ret Indberetning). Samtidigt med denne implementering vil Udvikling Erhverv skrive ud i organisationen, hvorledes tildelingen af roller fremover skal varetages af funktionsledere via BRAS.		
1.2 fra 2014	**Registrering af brugeraktiviteter** Brugeraktiviteter i NTSE registreres i et system kaldet XpoLog, som SKAT ikke benytter til systematisk overvågning.	Der er risiko for, at uautoriserede brugeraktiviteter i NTSE, fx fejlhæftede ændringer til moms og lønsum eller uautoriserede adgange, ikke opdages.	SIR anbefaler, at SKAT etablerer en præventiv kontrol for periodisk overvågning af kritiske brugeraktiviteter for eksempel i form af alarmer, eller alternativt iværksætter en egentlig overvågning af loggen.

Nr.	Observationer	Risici	Anbefalinger
P2	**Handleplan fra SKAT** *Susanne Thorhauge, Selskaber og digitalisering*: SKAT er enig i observationen samt risikoen. Udvikling Erhverv mener, at det er SKAT IT's ansvar at overvåge brugen af NTSE. Det er således op til SKAT IT, hvordan man vil løse opgaven. Vi forventer et udspil fra SKAT IT (Søren Kjær Jensen) på dette. *Søren Kjær Jensen, Erhvervs- og Personafregningssystemer*: SKAT IT har nedsat en sikkerhedsgruppe, som skal arbejde fokuseret på blandt andet anvendelsen af Xpolog.		
2	**Driftsstyring**		
2.1 fra 2014 **P3**	**Revisorerklæring** SKAT har ikke modtaget en revisorerklæring for driften af TSE dækkende perioden fra idriftsættelsen i 2010 til 2014. Årsagen til de manglende revisorerklæringer er, at der ikke har været et krav om en årlig revisorerklæring i den gamle kontrakt, som var gældende frem til oktober 2014.	Når der ikke indhentes en revisionserklæring for NTSE, er der ingen kontrol af, om leverandøren lever op til de indgåede aftaler, og at sikkerheden omkring det væsentlige system ikke er tilstrækkelig.	Den netop indgåede driftskontrakt indeholder et krav om, at leverandøren skal levere en årlig revisorerklæring. SKAT bør periodisk følge op på eventuelle bemærkninger i erklæringerne.
	Handleplan fra SKAT *Søren Kjær Jensen, Erhvervs- og Personafregningssystemer*: SKAT er enig i observationen, og vil fremadrettet følge op på disse revisionserklæringer.		
3	**Ændringsstyring**		
3.1 fra 2014 **P2**	**Centraliseret proces**: Processen for styring af ændringer til NTSE er decentralt forankret, og der er ikke et samlet overblik over alle gennemførte ændringer. Den samlede population af alle gennemførte	En uensartet og decentral styring af ændringer til NTSE medfører en forøget risiko for, at SKATs ledelse ikke kan opnå et samlet overblik over planlagte som gennemførte ændringer med henblik på at kunne prioritere samt	SKAT bør centralisere og ensarte styringen af ændringer til NTSE for at minimere risikoen for omgåelse af formelle procedurer, der bl.a. stiller krav om tilstrækkelig: • godkendelse af ændringer til udvikling • dokumenteret afprøvning af ændringer i

Nr.	Observationer	Risici	Anbefalinger
	ændringer skal indhentes fra platformsejere, systemejere og flere forskellige procesejere. Det har ikke været muligt for Intern Revision at indhente en samlet liste over alle ændringer i NTSE.	vurdere ressourcebehovet.	testmiljø (se observation 4.2 herunder) • godkendelse af ændringer til idriftsættelse • funktionsadskillelse som sikrer, at udviklere ikke har adgang til produktionsmiljø • periodisk overvågning af processen for styring af ændringer og samlet ledelsesrapportering.
	Handleplan fra SKAT *Søren Kjær Jensen, Erhvervs- og Personafregningssystemer:* SKAT er enig i observationen og har allerede påbegyndt arbejdet med en forbedret styring af ændringer bl.a. via etablering af et CAB-board. Hertil kommer, at der er indgået en ny kontrakt med leverandøren og her vil change-processen fremadrettet også skulle fastlægges.		
3.2 fra 2014 **P2**	**Dokumentation for afprøvning**: Det fremgår ikke af dokumentationen, at samtlige relevante platform-, proces- og systemejere systematisk afprøver og godkender ændringer til NTSE, selvom ændringerne berører adskillige it-systemer og forretningsprocesser.	Mangelfuld dokumentation for afprøvning medfører et reduceret overblik over testomfang og testresultat.	Det bør sikres, at ændringer til NTSE bliver idriftsat med dokumentation for tilstrækkelig og systematisk afprøvning samt godkendelse fra alle relevante platform-, proces- og systemejere. Dokumentationen bør bl.a. indeholde oplysninger om testomfang, testresultat, godkendelse af drift, tidspunkt og navne på involverede enheder og/eller medarbejdere.
	Handleplan fra SKAT *Søren Kjær Jensen, Erhvervs- og Personafregningssystemer:* SKAT er enig i observationen og henviser til besvarelsen af punkt 3.1.		

Bilag 2: Anvendte skala

Ved vurderingen i konklusionen er følgende skala anvendt:	
Meget tilfredsstillende	Intern Revision har ikke konstateret svagheder i de forretningsgange og processer, der understøtter de reviderede område. Samtlige observationer kan henføres til prioritet 3. Prioritet 1: Ingen observationer Prioritet 2: Ingen observationer Prioritet 3: Samtlige observationer
Tilfredsstillende	Intern Revision har observeret enkelte svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationerne er omfattet af prioritet 3. Enkelte observationer med prioritet 2 kan dog forekomme. Samlet set udgør de implementerede forretningsgange et "tilfredsstillende" grundlag for administration af området. Prioritet 1: Ingen observationer Prioritet 2: Enkelte observationer Prioritet 3: Hovedparten af observationer
Ikke helt tilfredsstillende	Intern Revision har observeret flere svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationer er omfattet af prioritet 2 eller 3 med hovedvægten på prioritet 2. Enkelte observationer i prioritet 1 kan dog forekomme. Samlet set medfører svaghederne, at de implementerede forretningsgange udgør "et ikke helt tilfredsstillende" grundlag for administration af området. Der er som følge heraf en forøget risiko for • Væsentlig fejlinformation i regnskaber og ledelsesrapportering • Manglende overholdelse af gældende lovgivning • Manglende overholdelse af interne regler og retningslinjer • Manglende overholdelse af overordnede politikker • Manglende iagttagelse af "skyldige økonomiske hensyn" Prioritet 1: Enkelte observationer Prioritet 2: Hovedparten af observationer Prioritet 3: Et mindre antal observationer
Ikke tilfredsstillende	Intern Revision har observeret flere væsentlige svagheder i de forretningsgange og processer, der understøtter det reviderede område. Størstedelen af observationerne er omfattet af prioritet 1 eller 2 med hovedvægten på prioritet 1. Enkelte observationer i prioritet 3 kan forekomme. Samlet set medfører svaghederne, at de implementerede forretningsgange udgør et "ikke tilfredsstillende grundlag" for administration af området. Der er som følge heraf en væsentlig forøget risiko for: • Væsentlig fejlinformation i regnskaber og ledelsesrapportering • Manglende overholdelse af gældende lovgivning • Manglende overholdelse af interne regler og retningslinjer • Manglende overholdelse af overordnede politikker • Manglende iagttagelse af "skyldige økonomiske hensyn" • Manglende realisering af forretningsmålene for det reviderede område. Prioritet 1: Hovedparten af observationer Prioritet 2: Et mindre antal observationer Prioritet 3: Enkelte observationer

Prioritet skal ses i forhold til det reviderede område og er defineret således:

1. ***Kritisk for forretningen:*** Væsentlig svaghed i de etablerede forretningsgange/processer. Svagheden kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Der er en væsentlig forøget risiko for, at processens målopfyldelse ikke realiseres som følge af den konstaterede svaghed. Der bør straks iværksættes foranstaltninger med henblik på at udbedre de observerede svagheder.

2. ***Væsentlig for forretningen:*** Svaghed i de etablerede forretningsgange/processer. Svagheden kan omfatte manglende interne kontroller, uhensigtsmæssig design af interne kontroller, manglende regnskabsmæssige faciliteter. Der er forøget risiko for, at processens målopfyldelse ikke realiseres i fuldt omfang som følge af den konstaterede svaghed. Der bør iværksættes foranstaltninger med henblik på at udbedre de observerede svagheder.

3. ***Mindre betydning for forretningen:*** Ingen væsentlige svagheder i de etablerede forretningsgange/processer. Det er dog muligt at designe de enkelte processer på en mere hensigtsmæssig måde, således at eksekveringen forbedres.