

19. april 2016  
J. nr. 15-3134981  
Plannr. 115-044

# Intern Revision

## Rapport 2015

**SKAT Kundeservice & Økonomi**

**Rapport om kontroller og  
funktionalitet i TastSelvBorger**

**Modtager**

Direktør Jesper Rønnow Simonsen, SKAT

**Kopi**

Direktør Karin Bergen, Kundeservice  
Direktør Karsten Juncher, Økonomi  
Departementet  
Rigsrevisionen

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

# Forord

---

Intern Revision (IR) har, jævnfør orienteringsbrev af 13. november 2015, revideret kontroller og funktionalitet i TastSelvBorger (TSB). 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 19. april 2016



**Kurt Wagner**  
Revisionschef



**Aliriza Özden**  
Manager

# 1. Formål

---

Formålet med revisionen af kontroller og funktionalitet i TastSelvBorger (TSB) er at undersøge og vurdere, hvorvidt den elektroniske platform til datafangst i form af TSB sikrer, at datafangsten sker korrekt, og at opfangede data videreføres fuldstændig og uforvansket til øvrige funktionsområder i processen.

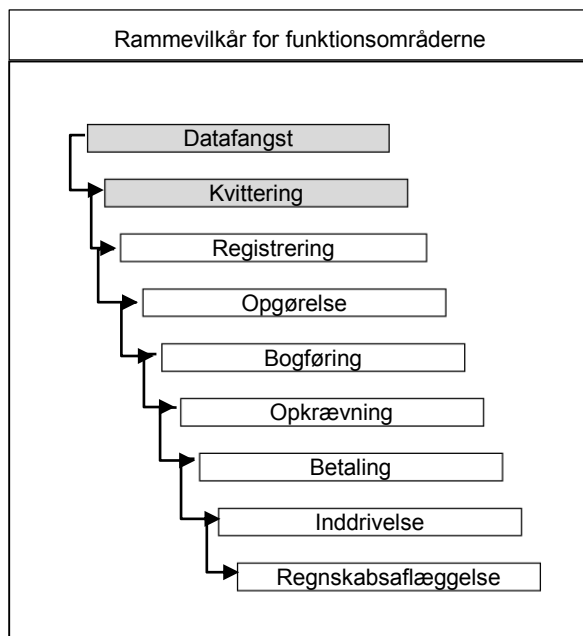
# 2. Omfang

---

Revisionen af kontroller og funktionalitet i TSB, som er udført i perioden november 2015 til februar 2016, har omhandlet følgende hovedområder:

- 1) Systemdokumentation og brugervejledninger
- 2) Adgange og adgangsrettigheder til systemet
- 3) Funktionsadskillelse
- 4) Transaktions- og kontrolspor
- 5) Logning og overvågning
- 6) Revision af nøglekontroller

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



I forbindelse med denne revision har vi revideret et område, som udgør en del af funktionsområderne "datafangst" og "kvittering".

Revisionen er udført af Aliriza Özden i henhold til gældende revisionsstandarder, herunder vejledninger fra Rigsrevisionen. Revisionen er gennemført ved

interviews, og stikprøvevis gennemgang af foreliggende materiale i samarbejde med medarbejdere fra Økonomi/IT, Kundeservice og Indsats.

### 3. Konklusion

---

Det er vores vurdering, at der i **større omfang er behov** for ændring af kontroller og funktionalitet i TastSelvBorger (TSB). Denne vurdering baserer vi på følgende forhold:

- På grund af manglende kontroller og funktionalitet i TSB er det ikke muligt at afvise de mest oplagte forsøg på misbrug af fradragsfelter i forskuds- eller årsopgørelser såsom indtastning af store tal med mange nuller. En del af misbruget opdages af Person og Datakontrol fra Indsats gennem stikprøvevis og manuel efterkontrol af borgeres gennemførte ændringer. Dette sker ved manuel opslag i flere forskellige systemer, hvorefter oplysningerne sammenholdes. Det er således ikke muligt at opdage misbrug på en nem måde og i så stort et omfang som muligt.
- En brugerprofil med kun læseadgang (forespørgselsadgang) eksisterer ikke i TSB. Adgange i TSB tildeles pr. skærmbillede og med skriveadgang (indberetningsadgang), selvom der udelukkende er behov for læseadgang.

Vi har prioriteret de observerede forhold således:

Revisionsemne	Prioritet 1 <i>Høj risiko</i>	Prioritet 2 <i>Middel risiko</i>	Prioritet 3/4 <i>Lille risiko</i>	I alt
1) Systemdokumentation og brugervejledninger	0	1	0	1
2) Adgange og adgangsrettigheder til systemet	0	2	0	2
3) Funktionsadskillelse	0	0	1	1
4) Transaktions- og kontrolspor	0	0	1	1
5) Logning og overvågning	0	0	1	1
6) Revision af nøglekontroller	1	1	0	2
<b>I alt</b>	<b>1</b>	<b>4</b>	<b>3</b>	<b>8</b>

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 vil medvirke til en reduktion af de vurderede risici.

## Bilag 1: Observationer, risici og anbefalinger

Nr.	Observationer	Risici	Anbefalinger
1	<b>Revisionsemne: Systemdokumentation og brugervejledninger</b>		<b>Funktionsområde: Datafangst/kvittering</b>
1.1 2015 Prio. 2	<p><b>Systembeskrivelse</b></p> <p>SKAT har ikke udarbejdet en selvstændig systembeskrivelse af TSB. TSB er derimod omfattet af en systembeskrivelse af online løsninger i SLUT-systemet udarbejdet af it-serviceleverandøren CSC.</p>	Der er øget risiko for, at SKAT ikke kan vurdere, om funktionaliteten og kontrollerne i TSB i tilstrækkelig omfang understøtter processen for dannelse af forskuds- eller års-opgørelser.	<p>Vi anbefaler, at SKAT udarbejder en systembeskrivelse af TSB, som blandt andet omfatter:</p> <ul style="list-style-type: none"> <li>• Kontroller og funktionalitet</li> <li>• Anvendte registre og/eller databaser</li> <li>• Dataflow fra TSB til andre systemer</li> </ul>
	<p><b>Handleplan fra Søren Kjær Jensen – Økonomi, IT Services, Person- og Ejendomssystemer:</b></p> <p>Det er korrekt, at vi ingen systembeskrivelse har af TastSelv Borger, men alle krav/ændringer hertil bliver beskrevet i kravspecifikationen til Årsopgørelsen. Inden 1. juni får vi i samarbejde med leverandøren afdækket, hvorledes der kan udarbejdes en systembeskrivelse. Herefter træffes beslutning i IT Services, hvorvidt anbefalingen skal følges samt eventuelt, hvornår anbefalingen er gennemført. Konkret er det allerede aftalt, at et overblik over Dataflow fra TastSelv Borger til andre systemer leveres inden udgangen af 2016.</p>		
Nr.	Observationer	Risici	Anbefalinger
2	<b>Revisionsemne: Adgange og adgangsrettigheder til systemet</b>		<b>Funktionsområde: Datafangst/kvittering</b>
2.1 2015 Prio. 2	<p><b>TastSelv-kode</b></p> <p>Det er muligt at logge på TSB med både NemID og TastSelv-kode. Sikkerheden ved anvendelse af NemID er højere end ved TastSelv-kode, da NemID kræver to-faktor autentificering. TastSelv-koden stiller udelukkende krav om et</p>	Den lavere sikkerhed i anvendelsen af TastSelv-kode øger risikoen for misbrug.	Anvendelsen af TastSelv-kode bør udelukkende begrænses til personer, der ikke kan tildeles NemID, fx personer under 15 år eller uden dansk cpr-nummer.

Nr.	Observationer	Risici	Anbefalinger
	<p>cpr-nummer og en selvvalgt kode, mens NemID også stiller krav om en ekstra kode fra et nøglekort eller nøgleviser.</p>		
<p><b>2.2</b> <b>2015</b> <b>Prio.</b> <b>2</b></p>	<p><b>Adgangsrettigheder</b> En brugerprofil med kun læseadgang (forespørgselsadgang) eksisterer ikke i TSB. Adgange i TSB tildeles pr. skærmbillede og med skriveadgang (indberetningsadgang), selvom der udelukkende er behov for læseadgang.</p>	<p>Risikoen for uautoriserede ændringer af forskuds- eller års-opgørelser via TSB er forøget af, at medarbejdere i SKAT, med behov for læserettigheder, også tildeles skriverettigheder.</p>	<p>SKAT bør implementere en brugerprofil med læse- eller forespørgsels-adgang i TSB, foretage en oprydning af rettighederne og kun tildele læse- og skrive-adgang til medarbejdere med arbejdsbetinget behov.</p>
	<p><b>Handleplan fra Søren Kjær Jensen – Økonomi, IT Services, Person- og Ejendomssystemer:</b> Vi er efterfølgende blevet opmærksom på, at der faktisk eksisterer en brugerprofil, der kun giver læse- eller forespørgsels-adgang til TastSelv Borger. Denne har dog en "mangel", da man i visse tilfælde ikke vil kunne se, hvad borgeren bliver præsenteret for, når de går i Ret Årsopgørelsen, og at man ved at bruge læse- og forespørgsels-adgangen heller ikke kan se borgerens tal/indberetninger i Beregn Aktier. Inden 1. juni 2016 afdækkes om "manglerne" ved den omtalte eksisterende brugerprofil kan rettes op. Herefter vil vi i samarbejde med Procesejer introducere ændrede beskrivelse af brugerprofiler, samt hvorledes denne brugerprofil skal tildeles.</p>		

Nr.	Observationer	Risici	Anbefalinger
3	Revisionsemne: Funktionsadskillelse		Funktionsområde: Datafangst/kvittering
Ingen bemærkninger til revisionsemnet.			

Nr.	Observationer	Risici	Anbefalinger
4	Revisionsemne: Transaktions- og kontrolspor		Funktionsområde: Datafangst/kvittering
Ingen bemærkninger til revisionsemnet.			

Nr.	Observationer	Risici	Anbefalinger
5	Revisionsemne: Overvågning og logning		Funktionsområde: Datafangst/kvittering
Ingen bemærkninger til revisionsemnet.			

Nr.	Observationer	Risici	Anbefalinger
6	Revisionsemne: Revision af nøglekontroller		Funktionsområde: Datafangst/kvittering
<b>6.1 2015 Prio. 1</b>	<p><b>Mangel på funktionalitet</b></p> <p>På grund af manglende kontroller og funktionalitet i TSB er det ikke muligt at afvise de mest oplagte forsøg på misbrug af fradragsfelter i forskuds- eller års-opgørelser</p>	<p>Uhensigtsmæssig design af eller manglende maskinelle kontroller og funktionalitet i TSB samt høj grad af manuel arbejde, øger risikoen for, at misbrug af fradragsfelter ikke opdages, eller at kun en mindre andel af misbruget opdages.</p>	<p>SKAT bør implementere maskinelle kontroller i TSB, der allerede i forbindelse med datafangsten kan afvise de mest oplagte forsøg på at misbruge fradragsfelter i forskuds- eller års-opgørelser.</p> <p>Endvidere bør en forbedring af funktionaliteten i eller omkring TSB gøre det nemmere for Indsats at sammenholde oplysninger på tværs af systemer for at opdage misbrug i så stort et omfang som muligt.</p>

Nr.	Observationer	Risici	Anbefalinger
	<p>såsom indtastning af store tal med mange nuller.</p> <p>En del af misbruget opdages af Person og Datakontrol fra Indsats gennem stikprøvevis og manuel efterkontrol af borgeres gennemførte ændringer. Dette sker ved manuel opslag i flere forskellige systemer, hvorefter oplysningerne sammenholdes. Det er således ikke muligt at opdage misbrug på en nem måde og i så stort et omfang som muligt.</p>		
	<p><b>Handleplan fra Jørgen Wissing Jensen – Kundeservice, Forretningsprocesser, Person:</b></p> <p>Kundeservice, Forretningsprocesser, Person har udarbejdet et forslag til udvidelse af Intelligent TastSelv (ITS) med kontroller og processer, der kan styrke TastSelv Borger. ITS-pakken indeholder bl.a. kontroller, der skal dæmme op for indberetningen af meget store og/eller runde beløb, samt bedre sammenholdelse af borgers rettelser med 3. partsindberetninger.</p> <p>ITS-pakken indgår som element i det samlede oplæg til Årsopgørelsesprojekt for indkomståret 2016, som Kundeservice vil forelægge direktionen til prioritering på det første kvartalsmøde efter sommerferien. Hvis direktionen prioriterer ITS-pakken på kvartalsmødet, og dermed sikrer finansiering til gennemførelsen, vil pakken blive implementeret således at de styrkede kontroller vil have virkning fra årsopgørelsen for 2016, når denne offentliggøres marts 2017. Relevante elementer fra ITS-pakken vil efterfølgende kunne udbredes til forskudsopgørelsen.</p> <p>Oplysninger fra Årsopgørelsessystemet er tilgængelige i BO, og i forbindelse med årsopgørelsen for 2016 har Kundeservice, Forretningsprocesser, Person bestilt en hyppigere aflevering af data fra årsopgørelsessystemet til BO. Kundeservice, Forretningsprocesser, Person vil inden sommerferien gå i dialog med Indsats i forhold til at afklare, om data- og analysebehovet på den baggrund kan imødekommes via BO.</p>		



Nr.	Observationer	Risici	Anbefalinger
<b>6.2</b> <b>2015</b>  <b>Prio.</b> <b>2</b>	<p><b>Helhedsorienteret risikovurdering</b></p> <p>Vi har fået oplyst fra SKAT, at de manuelle kontroller fra Person og Datakontrol (Indsats) ikke er et resultat af en helhedsorienteret risikovurdering af processen for dannelse og ændring af forskuds- eller års-opgørelser. Eksisterende manuelle kontroller er etableret på baggrund af en risikovurdering fra Indsats og uden en tværgående risikovurdering fra procesejere.</p>	<p>Der er øget risiko for, at der ikke arbejdes systematisk med de identificerede risici.</p>	<p>SKAT bør iværksætte tiltag med henblik på, at den samlede viden om risici i processen bliver inddraget ved den overordnede risikovurdering.</p>
<p><b>Handleplan fra Jørgen Wissing Jensen – Kundeservice, Udvikling, Person:</b></p> <p>Complianceanalysen, der gennemføres af Indsats, udgør SKATs overordnede ramme for vurderingen af, hvor skattegab er under pres, og analysens konklusioner kan medføre ændring af de digitale løsninger, som feltlåsnings er et eksempel på, eller i allokering af ressourcer til manuel kontrol, som etableringen af Person- og Datakontrol er et eksempel på. Kundeservice mener på den baggrund, at det overordnede udgangspunkt er en helhedsorienteret risikovurdering. Desuagtet finder Kundeservice, at det er ønskeligt med et mere struktureret samspil mellem arbejdet med den digitale forskuds- og årsopgørelse og de manuelle kontrolprocesser i Indsats. Derfor er Kundeservices projekt vedrørende Styrkede Forretningsprocesser netop ved – i samarbejde med procesejere i Kundeservice og Indsats – at kigge på de processer, der knytter sig til kontrollen af årsopgørelser for borgere, herunder de fejl- og stoplister, der genereres af årsopgørelsessystemet. I forlængelse af dette arbejde skal projektet foreslå en struktur for feedback mellem projekterne i Indsats og årsopgørelsen i Kundeservice.</p> <p>Herudover har Underdirektøren Johnny Schaadt Hansen netop igangsat et arbejde med at etablere en generisk risikomodel. Den generiske risikomodel skal implementeres i alle afdelingens proceskontorer, hvor de forskellige risici skal identificeres og beskrives med udgangspunkt i de procesetegninger, der er udarbejdet i regi af Styrkede Forretningsprocesser. Den generiske risikomodel skal være beskrevet ved årsskiftet 2016/2017.</p> <p>Endelig gennemføres der i regi af GPS kvartalsvise møder med deltagelse af procesejere og produktionsenhederne. Møderne gennemføres for hhv. årsopgørelse borger, årsopgørelse erhverv/udland og forskud, og risikovurderingen vil blive taget op som emne i en fast frekvens – eksempelvis halvårligt eller årligt – i dette regi.</p>			

## Bilag 2: Anvendt skala

Ved udarbejdelsen af konklusionen er følgende skala anvendt:	
<b>Intet behov for procesændringer</b>	Intern Revision har ikke observeret svagheder i de forretningsgange og processer, der understøtter det reviderede område.  Prioritet 1: Ingen observationer Prioritet 2: Ingen observationer
<b>Behov for procesændringer i mindre omfang</b>	Intern Revision har observeret enkelte svagheder i de forretningsgange og processer, der understøtter det reviderede område.  Prioritet 1: Ingen observationer Prioritet 2: Enkelte observationer
<b>Behov for procesændringer i større omfang</b>	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
<b>Behov for procesændringer i væsentligt omfang</b>	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 svagthed.

**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.