Riksrevisionen

Granskning av uppbördsprocessen moms med fokus på IT-risker

Skatteverket

30:e november 2011

Granskning utförd av:	Ernst & Young AB
Granskningsperiod:	oktober-november 2011

Mottagare:

Lars Nordstrand	Riksrevisionen
Jonas Björkdahl	Riksrevisionen

1 Sammanfattning

Riksrevisionen har uppdragit åt Ernst & Young AB att genomföra en granskning av den interna kontrollen i uppbördsprocessen för moms med avseende på applikationskontroller och behörighetskontroller. Granskningen innefattar en kartläggning av verksamhetsprocessen samt identifiering av nyckelkontroller i denna process. Granskningen omfattar även en kartläggning över hur kontrollstrukturen kring tilldelning av behörigheter är uppbyggd.

Granskningen har genomförts under oktober - november 2011. Informationsinsamling har skett genom intervjuer med nyckelmedarbetare inom Skatteverket, granskning av tillhandahållen dokumentation och systemexporter.

Vår bedömning

Skatteverket har en väl fungerande riskhanteringsprocess för att med hjälp av automatiska kontroller i applikationer identifiera momsdeklarationer av intresse. De kontroller som Skatteverket har skapat i uppbördsprocessen för moms syftar till att dels identifiera formella fel i momsdeklarationer men även för att förhindra bedrägeri. Vi har granskat båda typerna av kontroller och med hjälp av urval valt nyckelkontroller inom respektive område inom riskhanteringsprocessen. De kontroller som vi har granskat i systemen bedöms fungera effektivt.

Behörighetshanteringen hos Skatteverket sker enligt en till stora delar centraliserad process med visst inslag av lokal påverkan. Skatteverket gör skillnad på vem som kan ge behörighet till vilken roll och till vilka deklaranter varje enskild handläggare granskar, där den senare sker på lokal nivå.

Processerna för nytilldelning och uppföljning av behörigheter både inom verksamhet och IT har granskats och kontroller i processerna bedöms fungera effektivt.

Vi har observerat ett antal brister. De vi bedömer mest kritiskt är:

Utvecklare har tillgång till produktionsmiljön
Vi har noterat att två stycken utvecklare har tillgång och möjlighet att ändra data i produktionsdatabasen för MOMS AG.

Skatteverket har meddelat att de ändringar som utvecklare utför i produktionsdatabasen är tekniska rättelser av data exempelvis på grund av teknisk låsning i databasen eller misstag av någon handläggare. Ändringar kan även avse parametervärden/konstanter, nyckeltal och formella kontroller.

Alla ändringar loggas och sparas. Åtkomst till loggfilerna är begränsade och skilda från utvecklarna.

Användare med hög behörighet medges ofta obegränsad åtkomst till systemet. Risken för medvetna eller omedvetna oegentligheter som att förvanska eller radera kritisk information i MOMS AG ökar då den höga behörigheten tillåter att befintliga kontroller kan kringgås. Till exempel kan en enskild utvecklare på egen hand genomföra icke godkända förändringar eller ändra kritiska inställningar.

Avsaknad av dokumentation och enhetlighet vid kontrollförändringar
Vi har noterat att förändringar av händelsekontroller och urvalskontroller är bristfälligt dokumenterat och följer olika förändringsprocesser.

Bristande kontroll i hanteringen av kontrollförändringar innebär ökad risk för att icke godkända eller otillräckligt testade kontroller förs in i produktionsmiljön. Detta kan leda till fel i validering av deklarationsärenden.

2 Inledning

2.1 Uppdrag

Avsikten med vår granskning är att få en uppfattning om Skatteverkets interna kontroller vid hantering av momsdeklarationer med avseende på applikationskontroller. Granskningen innefattar en kartläggning av verksamhetsprocessen samt identifiering av nyckelkontroller i denna process samt en beskrivning över hur kontrollstrukturen kring tilldelning och hantering av behörigheter är uppbyggd.

2.2 Bakgrund

Skatteverket är förvaltningsmyndighet för beskattning, fastighetstaxering, folkbokföring och registrering av boupptеckningar. Skatteverket tar in cirka 1400 Miljarder SEK årligen i skatter. Vid handläggning av momsdeklarationer, stöds uppbördsprocessen av egenutvecklade system.

2.3 Genomförande

Arbetet är baserat på intervjuer med nyckelpersoner inom Skatteverket samt granskning av tillhandahållen dokumentation och systemexporter. Utöver detta har vi gjort observationer och följt transaktionsflöden på plats i systemen.

Arbetsgången har delats upp i 3 delar:

- ***Del 1 - Kartläggning av uppbördsprocessen för moms och identifiera applikationskontroller i flödet samt uppföljning av tidigare granskningar***

  Arbetet innebar en övergripande kartläggning av processen för riskhantering, hantering av momsdeklarationer, skapa en förståelse för processerna och samtidigt identifiera de kontroller som granskas enligt Del 2 respektive Del 3.

- ***Del 2 - Granskning av IT-kontroller i processerna med fokus på processen gällande tilldelning av behörigheter och walkthrough av processkontroller***

- ***Del 3 - Test av kontroller***

2.4 Avgränsning

Granskningen har enbart fokuserat på applikationer och kontroller som är en del av uppbördsprocessen för moms hos Skatteverket.

Granskning av programförändringsrutinen ingår ej i denna rapport. Rapportens omfattning är i sig inte tillräcklig för att identifiera samtliga brister som kan förekomma i verksamhetsprocesser eller IT-miljön. Granskningens omfattning syftar till att vi med rimlig säkerhet ska kunna identifiera de mest kritiska bristerna.

3 Uppbördsprocessen moms

3.1 Processbeskrivning

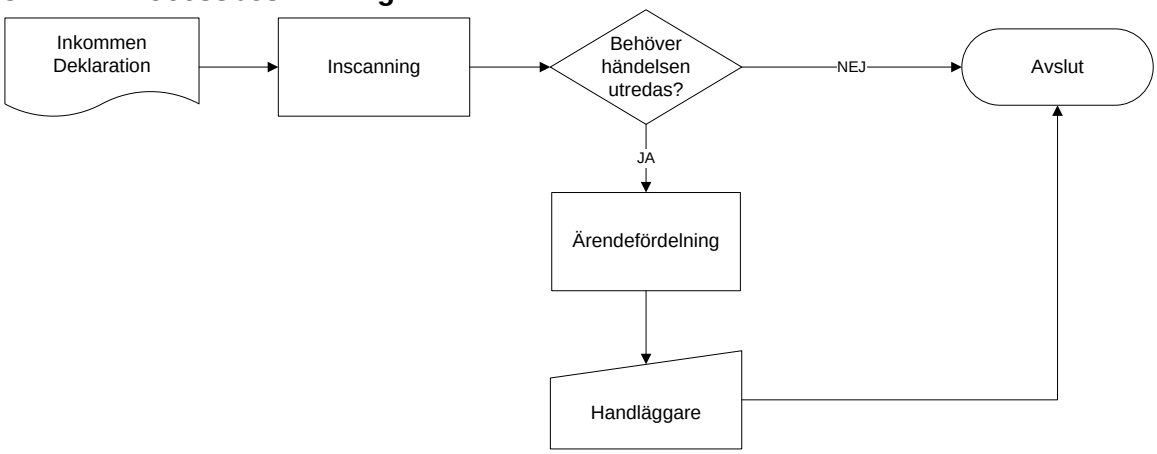

Bild 1. Förenklad bild av uppbördsprocessen för moms ritad av oss, se en detaljerad bild mottagen från Skatteverket i Bilaga 2.

Steg 1: Skatteverket mottar en momsdeklaration, genom en e-deklaration eller en pappersdeklaration. I de fall det är pappersdeklaration, scannas den in och konverteras till ett elektroniskt ärende.

Steg 2: Deklarationen valideras och utgången är:

- Ärendet har träffats av en eller flera kontroller och behöver utredas av en handläggare. Ärendet går vidare till **Steg 3.**
- Ärendet har inte träffats av någon spärr, ärendet går vidare till **Steg 5**.

Steg 3: Ärendet blir fördelat till en lämplig handläggare.

Steg 4: Handläggaren utreder ärendet och initierar lämplig åtgärd.

Steg 5: Åtgärd genomförs och ärendet avlutas.

3.2 Riskhantering

3.2.1 Bakgrund

Skatteverket måste granska alla inkommande deklarationer. Det är viktigt att upptäcka formella fel i deklarationen (oläsbara tecken, belopp som saknas, etc) samt att förhindra bedrägerier. Skatteverket har under lång tid designat och utvecklat applikationer vars uppgift är att granska deklarationer och selektera de

som anses felaktiga för särskild handläggning. Formella fel i en deklaration är enligt Skatteverket relativt enkla att upptäcka och skapa kontroller för i Skatteverkets IT-system. En svårare utmaning är att finna och förhindra avsiktliga och oavsiktliga fel. Skatteverket har därför utvecklat en typ av kontroller vars uppgift är att analysera en deklaration utifrån multipla villkor som baseras på faktisk data från aktuell momsdeklaration och på tidigare händelser och risker. Kontrollerna finns i det Skatteverket kallar ett spärrsystem.

3.2.2 Spärrsystem

För att lösa granskningsproblematiken har Skatteverket utvecklat ett spärrsystem. Spärrsystemet består av flera komponenter fördelade på flera applikationer: MOMS AG och PUMA/SAS, som kontrollerar momsdeklarationerna. Spärrsystemet innehåller i huvudsak två typer av kontroller, händelsekontroller och urvalskontroller. Huvudsyftet med spärrsystemet är att förhindra felaktiga utbetalningar genom att analysera momsdeklarationer och beakta historiska händelser samt risker. Eftersom risker och händelser förändras med tiden så blir spärrsystemets beslut dynamiskt och förändras i takt med att deklarationsbeteenden förändras.

3.3 Identifiering av applikationskontroller

Med applikationskontroller menas automatiska kontroller i ett IT-system som förebygger eller upptäcker avvikelser som kan leda till oönskade resultat. Detta kan exempelvis gälla fel i IT-systemets in-, ut- och masterdata orsakade av antingen omedvetna eller medvetna otillåtna aktiviteter och/eller felaktiga registreringar.

I samråd med Riksrevisionen har vi valt att fokusera på applikationskontroller som syftar till att upptäcka formella fel och indatafel från momsdeklarationen (händelsekontroller) samt kontroller som kontrollerar ifall momsdeklarationen från kund är regelrätt (urvalskontroller). Vi har identifierat att nyckelkontrollerna är beroende av tre applikationer, MOMS AG (händelsekontrollerna) och PUMA/SAS (urvalskontroller).

Applikationen MOMS AG utnyttjas även som ärendehanteringssystem där handläggarna hanterar momsdeklarationsärenden.

3.3.1 Händelsekontroller

Typen händelsekontroller består av flertal händelsegrupper där varje grupp består av kontroller som fångar upp en typ av händelse.

3.3.2 Urvalskontroller

Urvalskontrollerna är idag beroende av två applikationer, PUMA och SAS. Anledningen till att det är två applikationer är att det pågår en migrering av kontrollerna från PUMA-applikationen till SAS-applikationen. Skatteverket planerar att helt fasa ut PUMA och ersätta det med SAS. Vid tiden för vår granskning hade cirka 80 % av kontrollerna flyttats från PUMA till SAS. SAS-systemet bygger på en Oracle databas och har ett mer lättarbetat grafiskt gränssnitt som underlättar arbetet med kontrollerna.

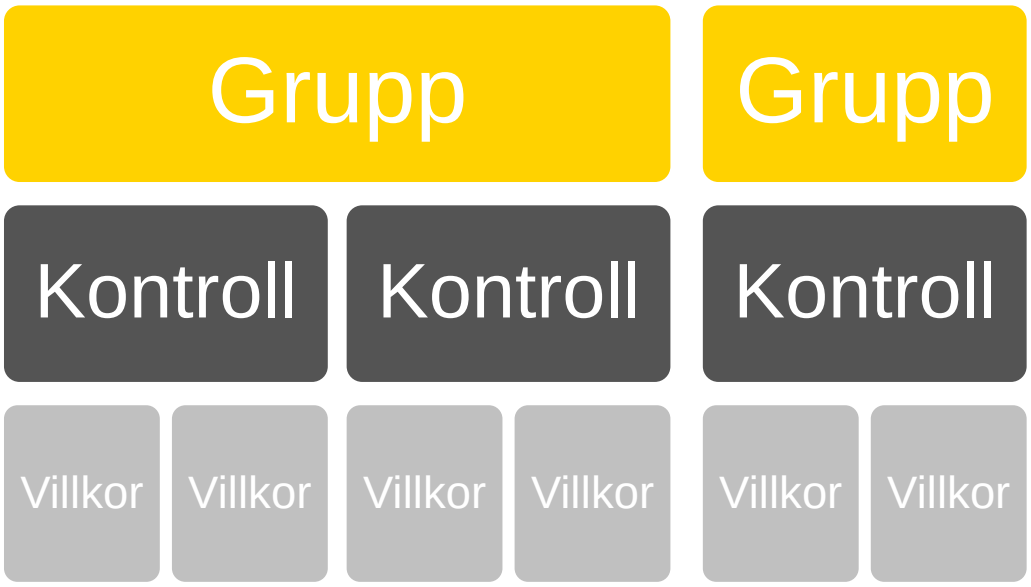

Bild 2. Strukturen för Urvalskontroller

Urvalskontrollerna är uppdelade i grupper, där varje grupp fångar upp en specifik händelse eller företeelse. Ofta är händelsen komplicerad och kräver att flera kontroller aktiveras samtidigt. Varje kontroll är i sin tur uppbyggd av ett antal villkor.

3.4 Kontrollförändringsprocess

Förändringar av kontroller i MOMS AG eller PUMA/SAS pågår kontinuerligt i förvaltningsform. Förvaltningsgruppen har behållit namnet på det projekt som ledde fram till kontrollurvalet, nämligen Urvalsprojektet.

En kontrollförändring initieras av verksamheten genom ett registrerat ärende i för ändamålet skapad förändringskö. Deltagarna från Urvalsprojektet går igenom och utvärderar registrerade förändringsärenden.

Kontrollförändringar som projektet anser vara små plockas från förändringskön och implementeras av urvalsgruppen. Större kontrollförändringar registreras av en berättigad beställare.

Kontrollförändringar utvecklas, testas och förs in i produktion av urvalsgruppen. Mindre förändringar produktionssätts utan ett formellt godkännande från verksamheten. För större kontrollförändringar tas beslut om produktionssättning under ett planeringsmöte mellan Urvalsprojektet och beställaren.

Processen för kontrollförändringar finns inte beskriven. Det saknas även specifikation på vad som är en mindre kontrollförändring eller en större kontrollförändring.

3.5 Ärendefördelning

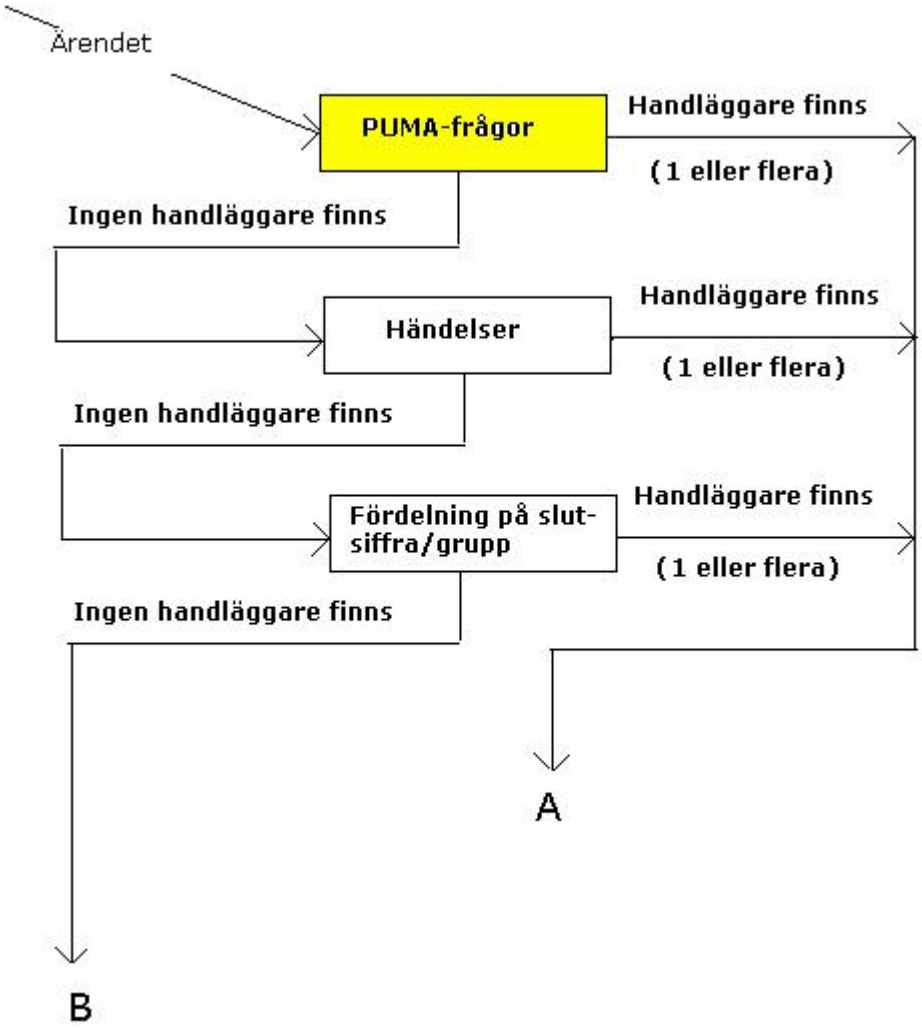

Bild 3. Ärendefördelningsflöde, bild mottagen från Skatteverket

För varje ”box” i bild 2 letar fördelningsprogrammet fram samtliga handläggare som innehar en roll där ärendet ingår eller innehar en grundfördelning som matchas av ärendet. Första ”boxen”, PUMA-frågor, är i detta fall synonym för kontrolltypen urvalskontroller.

Resultatet av fördelningsprogrammet är ”Handläggare finns” (**A**) eller ”Ingen handläggare finns” (**B**). Arbetsledaren på ett lokalkontor kontrollerar kontinuerligt inkommande ärenden för att fånga upp de ärenden som inte blir tilldelade till en handläggare.

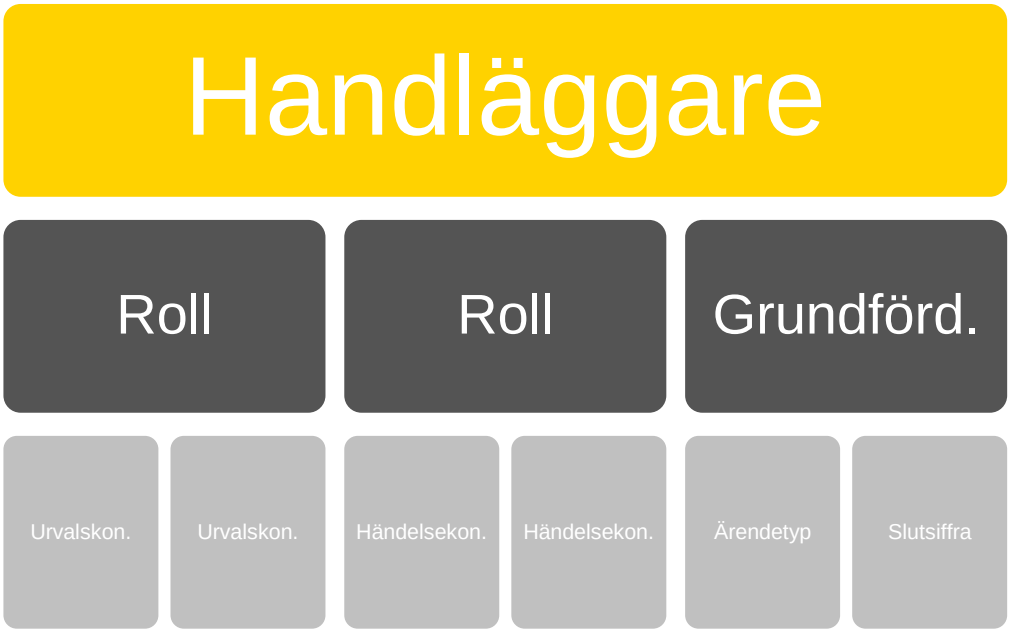

Bild 4. Fördelningsstrukturen för en handläggare

En handläggare kan kopplas till en eller flera roller. En roll är uppbyggd av en eller flera kontroller. Exempelvis så kan det finnas olika urvalsroller där varje roll innehåller olika urvalskontroller eller roller som är uppbyggd av händelsekontroller. På detta sätt kan handläggarens kompetens matchas med inkommande ärenden.

Handläggaren kan också vara kopplad till en grundfördelning som innehåller de ärendetyper som handläggaren är behörig till och en slutsiffra som talar om vilka företag som handläggaren ska hantera. Slutsiffran är en siffra mellan 0 – 9 som matchas med den 10:e siffran i ärendets organisationsnummer. En handläggare kan inneha en eller flera slutsiffror. Skatteverket informerade att de ska uppgradera grundfördelningen så att slutsiffran inte är statisk utan dynamisk. Uppgraderingen innebär att en handläggare inte kan förutse vilka företag som ska handläggas.

En handläggare kan vara uppsatt utan några kopplingar mot roller eller grundfördelning. Följden av detta är att handläggaren inte erhåller några ärenden.

Arbetsledaren på ett lokalkontor har behörigheten att bygga upp och fördela ut roller samt att bygga upp handläggarens grundfördelning.

3.6 Test av applikationskontroller

Av sekretesskäl och aktsamhet har vi, i samråd med Riksrevisionen, beslutat att lämna testunderlag och bevis hos Skatteverket i särskild akt. För spårbarhet kommer vi att referera till specifika dokument i akten.

Skatteverket har hjälpt oss ta fram testdata. För varje grupp, inom händelsekontroller och urvalskontroller, som vi valt att testa har vi från Skatteverket erhållit ett slumpmässigt ärendeurval. Vi var närvarande hos Skatteverket då de för varje grupp slumpmässigt tog fram 100 ärenden. Utifrån urvalet har vi slumpmässigt tagit fram (med hjälp av för ändamålet anpassad applikation) ett representativt antal stickprov som vi använt som testfall. För testning har vi i samråd med Riksrevisionen valt en testmetodik enligt principen att testa ett urval per händelse eftersom vi i dialog med Riksrevisionen antog att kontrollerna inom behörighetsprocesserna och programförändringsrutinerna skulle resultera i ett effektivt resultat. Att testa ett urval per händelse vid effektiva IT generella kontroller är del av gängse standard inom revision som beskrivs i detalj i International Standards on Auditing (ISA).

3.6.1 Händelsekontroller

Tillsammans med Riksrevisionen har vi identifierat fyra grupper av kontroller som vi valt att testa. För gruppen formella fel granskade vi samtliga kontroller medan vi för de tre övriga tre grupperna gjorde urval av nyckelkontroller i samråd med Riksrevisionen och Skatteverket.

Grupp
Formella fel
Händelser + Spärr på höga belopp
Spärr av låga belopp
Rena skattedeklarationskontroller

Inkommande ärenden är testade mot samtliga kontroller som ingår i kontrolltypen händelsekontroller.

Några av kontrollerna innehåller beloppsgränser som vi av sekretesskäl inte kan konkretisera i denna rapport men som återfinns i akten hos Skatteverket.

Formella fel

Testunderlaget hittas i akten hos Skatteverket med följande dokumentnamn: *Query_FOR_M_FORM_FEL_MOMS_AG_SL.*

Kod i systemet	Namn på kontroll	Kommentar av granskningsinsats	Bedömning av kontroll
51	Felsummering	Kontrollen aktiveras då deklarationen innehåller felsummeringar av olika fält. Vi kontrollerad summeringen i den automatiskt inlästa deklarationen och kunde konstatera att villkoret var uppfyllt.	Effektiv
52	Rättelseuppgift	Kontrollen aktiveras då två inlästa deklarationer, från samma företag, innehåller olika uppgifter mellan deklarationerna. Vi har granskat deklarationerna i ärendet och noterat att de fanns skillnader.	Effektiv.
53	Utg m v-lokal > utg m	Kontrollen aktiveras då ett specifikt fält överstiger ett annat fält i deklarationen. Vi granskade deklarationen och kunde konstatera att villkoret var uppfyllt.	Effektiv
54	Ing m v-lokal > ing m	Kontrollen aktiveras då ett specifikt fält överstiger ett annat fält i deklarationen. Vi granskade deklarationen och kunde konstatera att villkoret var uppfyllt.	Effektiv
56	Moms-att-betala saknas	Kontrollen aktiveras då det saknas belopp i fältet Moms-att-betala. Vi inspekterade den inlästa deklarationen och kunde verifiera att det inte fanns ett belopp i fältet.	Effektiv

Kod i systemet	Namn på kontroll	Kommentar av granskningsinsats	Bedömning av kontroll
60	Utgående moms finns	Kontrollen aktiveras då utgående moms har deklarerats samtidigt som det saknas uppgift om omsättning i deklarationen. Vi granskade aktuella deklarationen och noterade att kontroller aktiverats med rätt förutsättningar.	Effektiv
61	Felsummering	Kontrollen aktiveras då deklarationen innehåller felsummeringar av olika fält. Vi kontrollerad summeringen i den automatiskt inlästa deklarationen och kunde konstatera att villkoret var uppfyllt.	Effektiv
62	Omprövning	Kontrollen aktiveras då en deklarationskund begärt omprövning. Vi noterade att kunden begärt omprövning och en ny deklaration var inskickad från kund.	Effektiv
63	Moms-att-betala saknas	Kontrollen aktiveras då det redovisats momspliktig omsättning/ momspliktiga inköp men saknas belopp i fältet Moms-att-betala. Vi inspekterade den inlästa deklarationen och kunde verifiera att det inte fanns ett belopp i fältet.	Effektiv
65	Utg m v-lokal>utg m	Kontrollen aktiveras då ett specifikt fält överstiger ett annat fält i deklarationen. Vi granskade deklarationen och kunde konstatera att villkoret var uppfyllt.	Effektiv
66	Ing m v-lokal >ing m	Kontrollen aktiveras då ett specifikt fält överstiger ett annat fält i deklarationen. Vi granskade deklarationen och kunde konstatera att villkoret var uppfyllt.	Effektiv

Kod i systemet	Namn på kontroll	Kommentar av granskningsinsats	Bedömning av kontroll
67	Momspliktig försäljn. finns	Kontrollen aktiveras då det redovisas momspliktig omsättning, men saknas redovisad utgående moms. Vi inspekterade den inlästa deklarationen och kunde verifiera att det inte fanns ett belopp i fältet.	Effektiv
68	Utgående moms finns	Kontrollen aktiveras då utgående moms redovisats, men det saknas redovisad momspliktig omsättning i deklarationen. Vi granskade aktuella deklarationen och noterade att kontroller aktiverats med rätt förutsättningar.	Effektiv
69	Momspliktiga inköp finns.	Kontrollen aktiveras då det redovisats belopp i fälten för Momspliktiga inköp, men det saknas redovisad utgående moms. Vi inspekterade den inlästa deklarationen och kunde verifiera att det inte fanns ett belopp i fältet.	Effektiv

Händelser + Spärr på höga belopp

Testunderlaget hittas i akten hos Skatteverket med följande dokumentnamn: *Händelse_MOMS*

Kod i systemet	Namn på kontroll	Kommentar av granskningsinsats	Bedömning av kontroll
68	Ej maskinell skön	Kontroll aktiveras då systemet inte kan utföra en maskinell skön. Om det inte har lämnats någon skattedeklaration för redovisningsperiod där sådan ska lämnas, får skatt att betala uppskattas skönsmässigt. Skatteverkets system MOMS AG försöker i detta läge sköntaxera deklaranten. Detta innebär att systemet söker fram de tre senaste momsdeklarationerna bakåt i tiden och väljer den momsdeklaration som hade högst belopp som deklaranten skulle betala. Om det inte existerar tre deklarationer eller av någon annan anledning inte går att sköntaxera aktiveras kontrollen, Ej maskinell Skön.	Effektiv
109	Godkännande av utbetalningsspärr krävs	Kontrollen aktiveras då utbetalningen kräver manuellt godkännande av handläggare. Vi noterade att ärendet manuellt hanterats av en handläggare som utfört åtgärd.	Effektiv
122	Utbetalningsspärr, stort belopp	Kontrollen aktiveras då utbetalningen kräver manuellt godkännande av handläggare. Vi noterade att ärendet manuellt hanterats av en handläggare som utfört åtgärd. Liknande kontroll som kod:109. Skillnaden är att denna kontroll fokuserar på högre belopp.	Effektiv

Kod i systemet	Namn på kontroll	Kommentar av granskningsinsats	Bedömning av kontroll
153	Ej maskinell förseningsavgift	Kontroll aktiveras då en handläggare manuellt väljer att inte lägga en förseningsavgift. Vi notera i ärendet att åtgärd från kund blivit försenat men handläggare har manuellt valt att inte skicka en förseningsavgift.	Effektiv
245	Deklarationsformulär utan belopp	Kontrollen aktiveras då belopp saknas i deklarationen. Vi inspekterade den inlästa deklarationen och kunde verifiera att belopp saknades.	Effektiv
246	Upplysningar, moms	Kontrollen aktiveras då deklaranten skrivit fritext i deklarationens upplysningsfält. Vi kontrollerade pappersdeklarationen och noterade att kontrollen korrekt aktiverats.	Effektiv

Spärr av låga belopp

Testunderlaget hittas i akten hos Skatteverket med följande dokumentnamn: *Lagasparradebelopp.* Kontrollen innehar ingen kod i systemet, vilket kontrollerna ovan har, och därför återfinns inte den informationskolumnen i tabellen nedan.

Kommentar av granskningsinsats	Bedömning av kontroll
Ärenden innehållande inbetalningar från kund, med belopp som är inom Skatteverkets intervall för låga belopp, ska maskinellt gå ut till kund. Vi granskade aktuellt ärende och kunde konstatera att beloppet var inom intervallet.	Effektiv

Rena skattedeklarationskontroller

Testunderlaget hittas i akten hos Skatteverket med följande dokumentnamn: *RenaSKD.* Kontrollen innehar ingen kod i systemet och därför återfinns inte den informationskolumnen i tabellen nedan.

Kommentar av granskningsinsats	Bedömning av kontroll
Vi tittade på en ”ren” momsdeklaration som inte blivit träffat av några spärrar.	Effektiv

Slutsats av genomförd granskning

Baserat på vår genomförda testning av de identifierade applikationskontrollerna bedömer vi att alla testade kontroller fungerar effektivt.

3.6.2 Urvalskontroller

Tillsammans med Riksrevisionen har vi identifierat fyra grupper av urvalskontroller som vi valt att testa.

Grupp
Angrepp mot utbetalningssystemet
Gräns-överskridande-Handel (GöH)
Spärrpaket
Felaktigt tillgodo moms

Testunderlaget för urvalskontrollerna återfinns i en lista samlat i ett dokument. Dokumentet återfinns i akten hos Skatteverket. För spårbarhet refererar vi till testfallets radnummer i listan.

Angrepp mot utbetalningssystemet

Gruppen består av kontroller som syftar till att finna felaktigheter i momsdeklarationer där uppsåt misstänks från deklaranten.

Rad-nummer	Kontroll	Beskrivning	Bedömning av kontroll
70	Företagsform	Vi kontrollerade att de villkor som ingick i kontrollen var uppfyllda.	Effektiv
559	Restförd	Vi kontrollerade att de villkor som ingick i kontrollen var uppfyllda.	Effektiv

Gräns-överskridande-Handel (GöH)

Handel över landsgränser innebär ofta fler och mer komplicerade momsregler. Gruppen innehåller kontroller som har för avsikt att kontrollera momsdeklarationer mot de regler som rör handel över landsgränser. Fel som upptäcks är ofta oavsiktligt deklarerade eftersom reglerna blir mer komplexa för gränsöverskridande handel.

Rad-nummer	Kontroll	Beskrivning	Bedömning
117	Ny exp lev varor,	Vi kontrollerade att de villkor som ingick i kontrollen var uppfyllda.	Effektiv
251	Eg Var levä	Vi kontrollerade att de villkor som ingick i kontrollen var uppfyllda.	Effektiv

Spärrpaket

Kontroller inom grupper syftar till att förhindra felaktiga utbetalningar.

Rad-nummer	Kontroll	Beskrivning	Bedömning
312	Neg > sn 1R	Vi kontrollerade att de villkor som ingick i kontrollen var uppfyllda.	Effektiv

Felaktigt tillgodo moms

Rad-nummer	Kontroll	Beskrivning	Bedömning
493	Omv 41 ä	Vi kontrollerade att de villkor som ingick i kontrollen var uppfyllda.	Effektiv

Slutsats av genomförd granskning

Baserat på vår genomförda testning av de identifierade applikationskontrollerna bedömer vi att alla testade kontroller fungerar effektivt.

4 Generella IT-kontroller

Testning av generella IT-kontroller ligger till grund för bedömningen av nivån på den interna kontrollen för de IT-miljöer/system som omfattas av testningen. Kontrollområden som testas är processerna för behörighetshantering. En god intern kontroll inom IT-miljön ger en rimlig säkerhet för att applikationskontroller i IT-system är stabila och tillförlitliga över tid. System som var i scope för denna granskning var MOMS AG systemet, PUMA och SAS. Slutanvändare arbetar endast i MOMS AG systemet som sedan kallar på funktionalitet från PUMA och SAS.

Granskning av behörighetshantering har skett mot revisionskriterier inom god sed av intern kontroll vilka används av Ernst & Young vid granskning.

Revisionskriterierna är följande:

Säkerhetsinställningar gällande tillgång till data är relevant inställda.

Hög behörighet till nyckelkomponenter inom IT är begränsat till relevanta individer. Med nyckelkomponenter menas administratörsgränssnitt till applikation, databas, operativsystem och eventuella verktyg kopplade till känsliga IT-komponenter.

Nya, ändrade behörigheter till applikation, databas och operativsystem är godkända och skapade med rätt behörighetsnivå med avseende på respektive användares arbetsuppgifter

Uppföljning av behörigheter genomförs periodiskt med avseende på vem som ska ha vilken behörighet till applikation, databas och operativsystem

Behörighet till serverhallar är begränsat till lämpliga individer

Ändamålsenlig ansvarsfördelning är uppsatt gällande tilldelning, ändring och granskning av behörigheter där den följande funktioner inte får göras av samma person: beställning av behörighet, administration av behörighet, godkännande av behörighet och granskning av befintliga behörigheter.

4.1 Process för logisk åtkomst

4.1.1 Fysisk åtkomst till serverrum

Skatteverket har outsourcat drift av system tillhörande momshantering till Tieto. Servrarna är lokaliserade vid huvudkontoret i Solna samt i Älvsjö. Inpassering till serverrummen bestäms av en behörighetslista som förvaltas av Skatteverket. Ett besök måste bokas i förväg och vid ankomst kontrolleras tillträdet. Då personer utan egen behörighet behöver vistas i serverrummen måste de under hela vistelsen ledsagas.

Personalförändring som påverkar behörighetslistan ska anmälas genom en förändringsblankett vilken fylls i av den anställdas chef och skickas för godkännande till utsedd ansvarig på säkerhetsstaben. Ansvarig på staben uppdaterar listan och skickar ut den till berörda parter. Samma process gäller samtliga anställda på Skatteverket och Tieto.

Säkerheten för serverrummen diskuteras under regelbundna möten mellan säkerhetschefen från Skatteverket och representanter från Tieto.

Vi har tillsammans med Riksrevisionen gått igenom huvudavtalet mellan Skatteverket och Tieto (DNR = 132 630106-07/21). Avtalet hanterar tjänstenivåer, skadeståndskrav, separat säkerhetsavtal, övergripande krav på vilka personer som har behörighet, rätt att revidera klausul, säkerhetsskyddsinstruktioner samt destruktionsinstruktioner.

4.1.2 Behörighetshantering

Det finns tio behörighetsprofiler i applikationen MOMS AG. En profil bygger på arbetsuppgifter kopplade till en arbetsroll inom Skatteverket. Nya och ändrade behörigheter beställs av lokalkontorets avdelningschef genom att fylla i en ansökningsblankett. Ansökan skickas till lokalkontorets behörighetsadministratör som lägger upp önskad behörighet, arkiverar ansökan i en pärm samt skickar en kopia till Skatteverkets callcenter (central enhet inom Skatteverket som bland annat hanterar arkivering). Behörighetsadministratören är en centralt anställd person som inte arbetar med linjearbete gällande hantering av deklarationer.

Avdelningschefen genomför årligen en genomgång på att medarbetarnas behörigheter korresponderar med deras arbetsuppgifter. Genomgångarna dokumenteras och skickas till lokalkontorets behörighetsadministratör. Eventuell borttag av behörighet noteras i dokumentationen. Behörighetsadministratören utför de behörighetsförändringar som blivit noterade i genomgången och skickar därefter genomgången till callcentret som scannar och arkiverar den.

Behörigheter som läggs upp har en tidslängd på ett år och förnyas genom den periodiska genomgången.

Höga behörigheter till Skatteverkets databaser är begränsat till anställda på IT-avdelningen. Nya behörigheter måste beställas genom en ansökningsblankett som ska signeras av den anställda och närmsta chefen. Det krävs även ett godkännande från driftchefen. Signerad och godkänd ansökan skickas till IT-avdelningens behörighetsadministratör som lägger upp ett konto.

Utvecklare på IT-avdelningen har tittbehörighet till produktionsmiljön för MOMS AG. Av utvecklarna finns det två personer som har behörighet att modifiera produktionsdata. Loggning av utvecklarnas aktiviteter i produktionsmiljön genomförs och sparas undan på dedikerad serverplats som utvecklarna inte har tillgång till. Vi har tillsammans med Skatteverkat gått igenom listan med utvecklare som har tillgång till produktionsmiljön. Skatteverket kunde konfirmera att användarna var lämpliga. Listan återfinns i akten hos Skatteverket.

I granskningen har även grundläggande säkerhetsinställningar, främst kring lösenordsinställningar, granskats. Användare på Skatteverket loggar in genom att använda sitt tjänstekort kombinerat med ett lösenord. Skatteverket har Single-Sign-On (SSO) vilket innebär att en inloggning räcker för åtkomst till applikationer som användaren är behörig till. Vi har noterat att lösenordskomplexiteten följer riktlinjer för god praxis och inställningarna återfinns i akten hos Skatteverket.

4.1.3 Test av behörighetshanteringen

Vi har i akten hos Skatteverket en namnlista med namn som identifieras med ett unikt Id-nummer. Vi kommer i rapporten att referera till Id-numret.

Antalet användarkonton för MOMS AG är mycket stort (ca 10 000 konton) och användarna är utspridda över landet på olika lokalkontor.

Nyupplägg

Under 2011 har två nyanställda erhållit en högre behörighet i MOMS AG. Med hög behörighet menar vi möjlighet att förändra information i MOMS AG. Eftersom denna population var liten och processen för behörighet inte förändrats på en längre tid valde vi att utöka populationen med två personer som erhållit hög MOMS AG behörighet från tidigare år.

För varje person i populationen kontrollerade vi att behörighetsansökan existerar och var godkänd av behöriga individer.

Id-nummer	Kommentar	Bedömning
1	Ansökningsblankett hittad och signerad.	OK
2	Ansökningsblankett hittad och signerad.	OK
3	Ansökningsblankett hittad och signerad.	OK
4	Ansökningsblankett hittad och signerad.	OK

Borttag av behörighet

Vi har slumpmässigt valt ut en anställd från arkivet som enligt den periodiska genomgången bytt arbetsuppgift och därmed blivit av med behörigheter till MOMS AG. Vi har kontrollerat att behörigheterna blivit fråntagna från systemet enligt noteringarna i genomgången.

Id-nummer	Kommentar	Bedömning
31	Tillsammans med behörighetsadministratören kontrollerade vi i behörighetssystemet att personens behörigheter var borttagna.	OK

Periodisk genomgång

Varje år sker en genomgång av medarbetarnas behörigheter. Vi har ur Skatteverkets arkiv slumpmässigt valt ut 25 personer och kontrollerat att de ingick i översynen för 2010. Översynen för 2011 var under granskningstillfället inte klar och därför valde vi att granska översynen för 2010.

Ur våra tester framgick att personer med arbetsrollen servicehandläggare inte ingått i översynen. Skatteverket förklarade att det finns gemensamma servicekontor där handläggare kan handlägga ärenden från flera myndigheter. Servicehandläggare är en arbetsroll som finns på dessa kontor. Behörighetsprocessen för personer inom samarbetet är åtskilt från Skatteverkets behörighetsprocess och därför ingår inte servicehandläggarna i Skatteverkets översyn. Skatteverket förklarade att servicehandläggarna ingår i översynen för behörighetsprocessen som finns i det gemensamma samarbetet.

Efter genomförda tester har vi noterat att två personer (Id-nummer 15 och 28) inte ingått i översynen för 2010. Skatteverket bekräftade att medarbetarna fortfarande arbetar på Skatteverket och bör därför ha inkluderats i översynen. Vi

har genom medarbetarnas chefer verifierat att medarbetarnas behörighet är korrekt.

Id-nummer	Kommentar	Bedömning
6	Översyn fanns för 2010.	OK
7	Översyn fanns för 2010.	OK
8	Var anställd 2007-03 – 2007-09. Ingick därför inte i översynen då den utförs i oktober.	OK
9	Översyn fanns för 2010.	OK
10	Översyn fanns för 2010.	OK
11	Fått behörigheter 2008. Arbetsroll: Servicehandläggare och ingår därför inte i översynen.	Ej OK
12	Översyn fanns för 2010.	OK
13	Fått behörigheter, Arbetsroll: Servicehandläggare och ingår därför inte i översynen.	Ej OK
14	Fått behörigheter, Arbetsroll: Servicehandläggare och ingår därför inte i översynen. Dock har han i år fått högre behörigheter och bör ingå i översynen för 2011	Ej OK
15	Genomgång finns 2009, men ej 2010.	Ej OK
16	Översyn fanns för 2010.	OK

Id-nummer	Kommentar	Bedömning
17	Översyn fanns för 2010.	OK
18	Översyn fanns för 2010.	OK
19	Översyn fanns för 2010.	OK
20	Ingen översyn hittad. Ansökte om behörighet under en kort period och därefter spärrades hennes konto. Kontot var spärrat då översyn genomfördes och därför ingick hon inte.	OK
21	Översyn fanns för 2010.	OK
22	Översyn fanns för 2010.	OK
23	Översyn fanns för 2010.	OK
24	Översyn fanns för 2010.	OK
25	Översyn fanns för 2010.	OK
26	Översyn fanns för 2010.	OK
27	Översyn fanns för 2010.	OK
28	Tilldelad Behörighet 2010-07, ej med i översynen för 2010.	Ej OK
29	Översyn fanns för 2010.	OK
30	Översyn fanns för 2010.	OK

5 Uppföljning av tidigare iakttagelser

De brister som identifierades under ITGC-granskningen 2010 har inte återfunnits i denna granskning. Den tidigare granskning av internkontrollmiljön inom IT hos Skatteverket har inte avsett de applikationer som används inom uppbördsprocessen för moms.

6 Iakttagelser och rekommendationer

6.1 Statisk företagsfördelning då ärenden fördelas

Iakttagelse

Arbetsledare på ett lokalkontor konstruerar och kopplar grundfördelningen till lokalkontorets handläggare. I grundfördelningen finns en slutsiffra som talar om vilka företag som handläggaren ska hantera. Slutsiffran är en siffra mellan 0 – 9 som matchas med den 10de siffran i ärendets organisationsnummer. En handläggare kan inneha en eller flera slutsiffror. Slutsiffran är ofta oförändrad under längre perioder vilket innebär att en handläggare i förväg vet vilka företag som den ska handlägga.

Risk

Vanan att hantera ett företag kan leda till minskad granskningsinsatts då handläggaren ska utreda företagets ärenden. Vilket i sin tur ökar risken för felaktiga beslut. Det finns också risk för bedrägeri eftersom det sker begränsad rotation av vilken handläggare som granskar ärenden.

Rekommendation

Skatteverket är medveten om fördelningsproblemen och har meddelat att de planerar att implementera en ny version av ärendefördelningssystemet som innehar en dynamisk företagsfördelning. Vi rekommenderar Skatteverket att fortsätta arbetet med att uppgradera fördelningsprogrammet.

6.2 Avsaknad av kontroll som begränsar rollfördelningen för en arbetsledare

Iakttagelse

Ärendefördelningen på ett lokalkontor baseras bland annat på handläggarnas roller. Det är arbetsledaren för aktuellt lokalkontor som kopplar roller i bemärkelsen till vilka deklaranter som kan behandlas till en handläggare.

Vi har noterat att en arbetsledare kan koppla roller till handläggare som arbetar på lokalkontor som inte ingår i arbetsledarens ansvar.

Risk

Risken för felaktig tilldelning av roller ökar. Som i sin tur ökar risken för felaktiga beslut från handläggaren genom att handläggaren kan komma att hantera ärenden som den inte har kompetens för.

Rekommendation

Implementera en kontroll som begränsar möjligheten för en arbetsledare att koppla roller till handläggaren som inte arbetat på aktuellt lokalkontor. Alternativt utvärdera om det finns värde i att centralisera processen för rollfördelning.

6.3 Bristande process för regelbunden uppföljning och kvalitetssäkring av handläggarnas beslut

Iakttagelse

Vi har noterat att det hos Skatteverket saknas rutiner för att kvalitetssäkra handläggarnas arbete på individnivå. Skatteverket har små möjligheter att följa upp varför en handläggare väljer att avskriva ett ärende dels ur legal synpunkt men också systemtekniskt.

Risk

Risk finns att handläggare på slentrian godkänner momsdeklarationer vid tung arbetsbelastning och eller under annan typ av extern press utan att det finns möjlighet att i efterhand granska orsak.

Rekommendation

Utvärdera om det ur legalt perspektiv går att införa möjlighet att granska orsaker varför ett ärende avskrivs. Vid resultat att det är genomförbart behöver också systemstöd för uppföljning utvecklas.

6.4 Servicehandläggare ingår inte i Skatteverkets behörighetsöversyn

Iakttagelse

Servicehandläggare är en arbetsroll som en handläggare kan inneha då den arbetar på ett servicekontor som hanterar ärenden från flera myndigheter.

Vi noterade att de personer som hade arbetsroller servicehandläggare inte ingått i Skatteverkets behörighetsöversyn. Vi har blivit informerade av Skatteverket att servicehandläggarna ingår i en separat rutin som det gemensamma myndighetssamarbetet skapat och underhåller för uppföljning av behörigheter.

Risk

En otillräcklig behörighetsprocess för styrning av åtkomst till företagets system kan innebära ökad risk för obehörig åtkomst till program eller information.

Rekommendation

Vi rekommenderar Skatteverket att i den årliga översynen inkludera ett kontrollsteg som syftar till att säkerställa att servicehandläggare i MOMS AG innehar rätt åtkomst baserat på arbetsuppgiften.

6.5 Utvecklare har tillgång till produktionsmiljön

Iakttagelse

Vi har noterat att två stycken utvecklare har tillgång och möjlighet att ändra data i produktionsdatabasen för MOMS AG.

Skatteverket har meddelat att de ändringar som utvecklare utför i produktionsdatabasen är tekniska rättelser av data exempelvis på grund av teknisk låsning i databasen eller misstag av någon handläggare. Ändringar kan även avse parametervärden/konstanter, nyckeltal och formella kontroller. Alla ändringar loggas och sparas. Åtkomst till loggfilerna är begränsade och skilda från utvecklarna.

Risk

Användare med hög behörighet medges ofta obegränsad åtkomst till systemet. Risken för medvetna eller omedvetna oegentligheter som att förvanska eller radera kritisk information i MOMS AG ökar då den höga behörigheten tillåter att befintliga kontroller kan kringgås. Till exempel kan en enskild utvecklare på egen hand genomföra icke godkända förändringar eller ändra kritiska inställningar.

Rekommendation

Säkerställ att ansvar mellan kritiska moment såsom systemadministration, hantering av drift och utveckling samt implementering av programversioner i produktionsmiljö är åtskilda.

Vi rekommendera Skatteverket att regelbundet granska loggarna och säkerställa att utvecklarnas aktivitet varit befogad.

6.6 Avsaknad av dokumentation och enhetlighet vid kontrollförändringar

Iakttagelse

Vi har noterat att förändringar i villkoren för de formella kontrollerna, indatakontrollerna och urvalskontrollerna är bristfälligt dokumenterade och följer olika förändringsprocesser.

Risk

Bristande kontroll i hanteringen av kontrollförändringar kan innebära ökad risk för att icke godkända eller otillräckligt testade kontroller förs in i produktionsmiljön. Detta kan leda till fel i validering av deklarationsärenden.

Rekommendation

Vi rekommenderar Skatteverket att dokumentera kontrollförändringsrutinen och kommunicera den till samtliga berörda parter. Dokumentet bör minst omfatta följande punkter:

- Vem som är behörig att godkänna beställning av kontrollförändringar
- Vem som är behörig att beställa förändring av Urvalsprojektet
- Hur test av förändringar görs och av vem inklusive acceptanstestning
- Att separat utvecklings/test och produktionsmiljö etableras
- Hur migrering av förändringen till produktionsmiljön utförs och av vem
- Att systemdokumentation uppdateras enligt gjorda förändringar
- Hur brådskande förändringar (emergency changes) hanteras och dokumenteras
- Hur ändamålsenlig ansvarsfördelning inom processen upprätthålls. Utvecklingspersonal bör t.ex. inte migrera förändringar till produktionsmiljön.

Bilaga 1 – Intervjuade personer

Nedan är en lista på intervjuade personers ansvarsområde/avdelning:

Ansvarsområde/avdelning
Förvaltningsledare MOMS AG
Utvecklingsansvarig MOMS AG
Förvaltningsledare IT, för förvaltningsobjektet Moms, AG, Punktskatt
Deltagare i Urvalsprojektet
Arbetsledare
Behörighetsadministratör för IT och Huvudkontoret
Produktionsledare och funktionsansvarig för Fysisk Datamiljö
Säkerhetschef
Deltagare i Urvalsprojektet

Bilaga 2 – Detaljbild på uppbördsprocessen för moms