Upplands Väsby kommun

Genomgång enligt revisionsstandard (ISA 315)

Januari 2024

1. Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Upplands Väsby kommun granskat behörighetshanteringen, programförändringshanteringen samt IT-driftshanteringen inom tre av kommunens IT-system: ekonomisystemet Raindance, lönesystemet Heroma och försörjningsstödssystemet Combine. Syftet med granskningen var att bedöma om kommunstyrelsen har säkerställt en ändamålsenlig styrning, intern kontroll och uppföljning avseende hantering av programförändringar, behörighetshantering och driftsrutiner för system som är centrala för den finansiella rapporteringen.

Granskningens iakttagelser och bedömningar baseras på genomförda intervjuer med nyckelpersoner från respektive system samt mottagen dokumentation för samtliga granskade områden.

Den samlade bedömningen är att kommunstyrelsen inte i tillräcklig utsträckning har säkerställt en ändamålsenlig styrning, intern kontroll och uppföljning avseende hantering av behörigheter, programförändringar och IT-drift för de system som granskats. Kommunstyrelsen har inte säkerställt att relevanta styrdokument för vardera granskat område finns framtaget eller att tillhörande riktlinjer implementerats. Därtill har kommunstyrelsen inte säkerställt uppföljning och efterlevnad av kommunens riktlinjer. Avslutningsvis bedömer EY att kommunstyrelsen för två av de granskade systemen inte har säkerställt tydligt definierade roll- och ansvarsfördelningar för hantering av programförändringar och IT-driftsrutiner.

I granskningen har ett antal brister identifierats och rekommendationer lämnats. EY rekommenderar att kommunstyrelsen i Upplands Väsby kommun säkerställer att:

- Relevanta styrdokument och kontroller finns framtagna och att tillhörande riktlinjer implementeras.
- Processer för uppföljning av efterlevnaden av kommunens riktlinjer och rutiner implementeras och genomförs.
- Roll- och ansvarsfördelningar förtydligas och beslutas.

Innehållsförteckning

2. Inledning

2.1. Bakgrund

Från och med 2023 ska räkenskapsrevisionen i kommuner genomföras i enlighet med kommunal standard för revision, såsom den definieras i KISA (kommunal ISA). ISA betyder international standards on auditing och är den standard som auktoriserade revisorer följer vid revision av företag. KISA är en kommunal anpassning av denna. KISA ställer betydligt tydligare krav på vad som ska göras i den årliga revisionen av räkenskaperna. Bland annat gäller detta förståelsen för de IT-system som påverkar redovisningen och den interna kontrollen kring dessa system. Kraven innebär bland annat:

- Ett utökat fokus på att, oavsett revisionsstrategi, förstå IT-miljön, IT-styrningen och IT-infrastrukturen som stödjer de för den finansiella rapporteringen väsentliga IT-systemen.
- Krav att identifiera IT-system och relaterade IT-risker samt utvärdera de IT-generella kontrollerna.
- Specifika krav för bedömning av inneboende riskfaktorer relaterat till bl. a komplexitet, subjektivitet, förändring och osäkerhet.
- Krav på utökad revisionsdokumentation relaterat till ovanstående områden.

IT-system som är centrala för den finansiella rapporteringen innefattar vanligen ett stort antal användare. Det är av vikt att kommuner har fungerande rutiner avseende åtkomst- och behörighetshantering, programförändringar och driftshantering. System som är centrala för den finansiella rapporteringen kan exempelvis omfatta ekonomisystem, leverantörsfakturasystem och lönesystem, men även andra system som hanterar större summor pengar. Felaktig tilldelning av behörigheter kan exempelvis leda till att individer får felaktig lön eller att en leverantör får betalt trots att ingen tjänst har utförts. God intern kontroll bör föreligga avseende de IT-system som hanterar skattebetalarnas pengar, i syfte att minimera risken för felaktigheter. Det handlar om att säkerställa att rätt person har rätt behörighet och att det finns rutiner på plats som säkerställer att programförändringar inte äventyrar driften av något system.

I kommunen ansvarar kommunstyrelsen för IT-miljön och det finns enligt lagen om kommunal bokföring och redovisning krav på systemdokumentation och behandlingshistorik. Revisorerna har utifrån genomförd riskanalys beslutat att genomföra en fördjupad granskning av kommunstyrelsens rutiner för IT-infrastrukturen hänförlig till den finansiella rapporteringen.

2.2. Syfte och revisionsfrågor

Granskningen syftar till att ge revisorerna underlag för att bedöma om kommunstyrelsen har säkerställt en ändamålsenlig styrning, intern kontroll och uppföljning avseende hantering av programförändringar, behörighetshantering och driftsrutiner för system som är centrala för den finansiella rapporteringen.

Följande revisionsfrågor besvaras i granskningen:

- Har kommunstyrelsen säkerställt att det finns ändamålsenlig styrning för den finansiella IT-miljön?
- *Behörighetshantering*
  - Finns generella krav för säkerhetsinställningar och lösenordskrav och är de adekvata för verksamheten?
  - Finns rutiner för behörighetstilldelning och borttag av behörighet och finns rutiner för godkännande av dessa?
  - Finns rutiner för uppföljning av behörigheter i form av att anställda har relevanta behörigheter till system?
- *Programförändringar*
  - Finns tillräckliga rutiner implementerade i verksamheten för att genomföra programförändringar?
    - Finns tydliga roller och ansvar för hantering av programförändringar?
    - Finns rutiner för godkännanden och testning av ändringar och dokumenteras dessa?
- *IT-driftsrutiner*
  - Finns rutiner för hantering av säkerhetskopiering av system?
  - Finns rutiner för att testa att säkerhetskopior fungerar?
  - Finns rutiner för övervakning av schemalagda jobb samt rutiner för avhjälpning av eventuella fel?

2.3. Metod och avgränsning

Granskningen omfattar tre olika system med stor finansiell betydelse för Upplands Väsby kommun:

- Ekonomisystemet
- Lönesystemet
- Försörjningsstödssystemet

Granskningen sker huvudsakligen genom intervjuer med ansvariga tjänstemän inom berörd förvaltning, men även dokumentgranskning förekommer. Granskningen kommer även innefatta granskning av underliggande dokumentation genom att följa dokumentation av:

- Säkerhetsinställningar/lösenordskrav i relevant system
- En genomförd programförändring med avseende på beslut, testprotokoll mm
- En tilldelning av behörighet
- En borttagning av behörighet
- Periodisk genomgång av behörigheter
- En felaktig körning av schemalagda jobb

2.4. Revisionskriterier

I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Kommunallagen (2017:725)
- Lagen om kommunal bokföring och redovisning
- Eventuella av fullmäktige beslutade policyer och styrande dokument med bäring på området
- God praxis inom området

2.5. Definitioner

Se bilaga 3.

3. Granskningsresultat

I detta kapitel presenteras de övergripande resultaten från genomförd granskning med utgångspunkt från revisionsfrågorna. Iakttagelserna och bedömningarna i detta kapitel utgår från informationen som inhämtats under de genomförda intervjuerna samt under granskningen av mottagen dokumentation.

3.1. Ekonomisystemet

Ekonomisystemet Raindance är ett ekonomisystem som används av kommunen för bland annat bokföring och finansiell rapportering. I systemet finns även funktionalitet för reskontra och andra, för redovisning och uppföljning, centrala funktioner. Obehörig åtkomst, programfel eller liknande i ekonomisystemet skulle kunna leda till exempelvis fel i de finansiella rapporterna eller att skattepengar betalas ut till fel mottagare. CGI är leverantör av systemet som har cirka 450 aktiva användare.

3.1.1. Behörighetshantering

Iakttagelser

Enligt intervjuade nyckelpersoner loggar kommunens användare in i Raindance via Single Sign On (SSO) för att få åtkomst till systemet. Användare kan även logga in i Raindance från privat dator med identifiering via BankID. Ett fåtal användare hos leverantören har åtkomst till systemet genom användarnamn och lösenord. Vid tid för granskning har EY inte mottagit dokumentation som styrker kraven som finns på inloggningsfunktionen. Fyra systemförvaltare har behörighet att ändra i säkerhetsinställningarna och kan således ändra kraven på inloggningsfunktionen. Kommunen genomför inga genomgångar för att säkerställa att förändringar i säkerhetsinställningarna inte har genomförts.

Kommunen har en e-tjänst där användare kan ansöka om att få behörighet till systemet. Intervjuade nyckelpersoner uppger att förfrågan initieras via en e-blankett där användaren bland annat måste uppge vilken anställd förfrågan berör, från vilket datum behörigheten ska gälla, åtkomster som användaren ska ha samt vem som är närmsta chef. Godkännande av förfrågan sker av närmsta chef till den individ som berörs av behörighetsförfrågan, och medges i samband med att blanketten skickas av användaren. När en användare ansöker om hög behörighet behöver ansökan godkännas av både närmsta chef och kontorschef. Efter godkännande av närmsta chef (och kontorschef om nödvändigt) kan systemförvaltare tilldela korrekt behörighet utefter de svar som uppgetts i blanketten. Systemet har 7 behörighetsnivåer och cirka 400 användare har behörighetsnivå 1 eller 2, vilket motsvarar läs- och enklare skrivbehörighet. Det är endast de fyra nuvarande systemförvaltarna som har behörighet att tilldela, förändra eller ta bort behörigheter i systemet. Kommunen genomför inga genomgångar för att säkerställa att oönskade förändringar av behörighetsnivåerna inte har genomförts.

När en användare slutar hos kommunen avaktiveras användarens konto i AD vilket innebär att användaren automatiskt förlorar tillträde till systemet via SSO. Enligt intervjuade nyckelpersoner skickar ansvarig chef även e-post till systemförvaltare och ber att användarens konto i Raindance inaktiveras i samband med att användaren slutar. Därefter initieras en manuell process och systemförvaltarna inaktiverar kontot. Det händer ibland att e-postförfrågan uteblir och intervjuade nyckelpersoner uppger att systemförvaltare stämmer av användarna i Raindance mot listor med avslutad personal regelbundet som åtgärd för att säkerställa att personer som slutat tas bort från systemet. Vid tid för granskning finns ingen dokumenterad processbeskrivning för tillägg och borttag av behörigheter i Raindance. EY har inte heller mottagit dokumentation som styrker att användarna i Raindance regelbundet stäms av mot listor med avslutad personal.

Intervjuade nyckelpersoner uppger att systemförvaltare årligen genomför en periodisk genomgång av användare i systemet. Systemförvaltare tar då ut behörighetslistor ur systemet och skickar till controllers samt chefer som reviderar listan genom att sätta kryss vid de användare som ska tas bort från systemet. EY har inte mottagit formell dokumentation som beskriver denna process. Därtill uppger intervjuade nyckelpersoner att de listor som granskas inte täcker användare som har behörighet till systemet men som inte är anställda på kommunen, såsom konsultkonton.

Bedömning

EY bedömer att kommunen saknar en dokumenterad lösenordspolicy. Kommunen bedöms även sakna en process för att granska att obehöriga förändringar av säkerhetsinställningarna inte genomförts. Verksamheten har en informell process för behörighetshantering, men kommunen saknar en dokumenterad process avseende behörighetstilldelningen för samtliga anställda. Därtill saknas en dokumenterad process avseende behörighetsborttagning. Verksamheten har även en informell process för periodisk genomgång av användare, processen täcker dock inte alla användare och EY bedömer att kommunen saknar en formell dokumentation kring denna process.

3.1.2. Programförändringar

Iakttagelser

Programförändringar genomförs i systemet av både leverantören och av kommunen. Enligt intervjuade nyckelpersoner meddelar leverantören systemförvaltarna när det finns nya releaser. Systemförvaltarna beslutar därefter om releasen ska implementeras i kommunens system. Samtliga programförändringar sker i testmiljö innan de implementeras i kommunens produktionsmiljö av leverantören. Både leverantören och kommunen genomför testning när nya releaser ska installeras. Kommunen mottar då dokumentation från leverantören som beskriver vad det är som ska testas. Testmiljön uppdateras ungefär vartannat år enligt intervjuade nyckelpersoner. EY har inte mottagit processdokumentation som styrker ansvarsfördelningen mellan leverantören och kommunen samt hur programförändringar ska genomföras i Raindance.

Kommunen genomför själva vissa större programförändringar, till exempel integrationer. Större programförändringar initieras genom att beställare fyller i en blankett där den önskade förändringen beskrivs och ansvarig person uppges. Förändringen registreras sedan i en aktivitetslista kopplad till

förvaltningsplanen och godkännande för att genomföra förändringen utfärdas av styrgruppen. Enligt intervjuade nyckelpersoner sker även dessa programförändringar i testmiljö innan de implementeras i kommunens produktionsmiljö av leverantören. EY har inte mottagit en formell process som beskriver kommunens rutin för beslutsfattande samt testning av programförändringar i Raindance.

Bedömning

EY bedömer att kommunen saknar dokumenterade processer och rutiner för hur förändringar i systemet Raindance bör genomföras. Därtill bedöms kommunen sakna en dokumenterad process för ansvarsfördelning mellan leverantören och kommunen avseende programförändringar. För förändringar genomförda av kommunen finns det en informell process som saknar formell dokumentation. Kommunen saknar även en dokumenterad process för hur förändringar testas och godkänns innan de produktionssätts.

3.1.3. IT-driftsrutiner

Iakttagelser

Intervjuade nyckelpersoner uppger att kommunen hanterar driften av schemalagda jobb. Denna process uppges vara vedertagen men inte dokumenterad. Intervjuade nyckelpersoner uppger att en notis via e-post skulle skickas till ekonomienheten och systemförvaltare om ett schemalagt jobb skulle misslyckas. Systemförvaltare kan välja vem som ska få notifikationer. Därtill uppges att ansvaret för att åtgärda problemet ligger hos specialist för berörd modul i systemet. Vid kritiska problem som kommunen själva inte kan åtgärda kontaktar systemförvaltare leverantören. Ytterst ansvarig för drift av systemet är ekonomidirektören. EY har inte mottagit en formellt dokumenterad processbeskrivning för övervakning av schemalagda jobb samt hantering av eventuella misslyckade jobb.

Bedömning

EY bedömer att kommunen saknar dokumenterade processer och rutiner avseende felundersökningar av schemalagda jobb i systemet Raindance. Därtill bedöms kommunen sakna en dokumenterad ansvarsfördelning som specificerar ansvarsförhållandet inom kommunen vid kontroll av och åtgärder av schemalagda jobb som misslyckats.

3.2. Lönesystemet

Lönesystemet Heroma är ett HR- och lönesystem som används av kommunen främst för att betala ut löner till kommunens anställda, hantera kommunens anställningsregister samt personalschemaläggning. Obehörig åtkomst, programfel eller liknande i lönesystemet skulle kunna leda till exempelvis uteblivna eller felaktiga löneutbetalningar. CGI är leverantör av systemet som har

cirka 2800 användare.

3.2.1. Behörighetshantering

Iakttagelser

Enligt intervjuade nyckelpersoner loggar användare på löneenheten in i systemet med användarnamn och lösenord. Övriga användare loggar in med BankID. Det finns krav på lösenordskomplexitet, vilket EY har mottagit dokumentation för. Lösenordskomplexiteten kräver i dagsläget ett minimum på 10 tecken, varav minst en bokstav och en siffra. Det finns inga krav på gemener, versaler eller specialtecken. Leverantören sköter säkerhetsinställningarna och ansvarar för att lösenordspolicyn efterlevs. Leverantören har därmed möjlighet att ändra säkerhetsinställningarna. Kommunen genomför inga genomgångar för att säkerställa att förändringar i säkerhetsinställningarna inte har genomförts. Vid tid för granskning har EY inte mottagit formell dokumentation från kommunen som styrker att BankID respektive användarnamn och lösenord ska användas vid inloggning i Heroma.

Det finns ett antal roller i systemet med olika behörigheter beroende på vilken funktion som rollen avser, till exempel medarbetare eller chef. Kommunen väljer själva vilka behörigheter varje roll ska ha. Systemadministratörerna har möjlighet att ändra behörigheterna i rollerna eller skapa specialroller vid behov. Rollerna kontrolleras årsvis av kommunen enligt intervjuade nyckelpersoner. EY har inte mottagit någon dokumentation som bekräftar detta.

Intervjuade nyckelpersoner uppger att en tilldelning av användare i Heroma initieras genom att ett nytt anställningsavtal läggs upp i systemet och/eller att närmsta chef fyller i en e-blankett där lämplig roll efterfrågas. Samtliga medarbetare hos kommunen har, som följd av sitt anställningsavtal, godkänd medarbetarbehörighet till systemet i syfte att komma åt sin självservicefunktion. Denna roll kan läggas till i systemet av lönespecialister. För högre behörighet än rollen medarbetare, såsom chefs-, ekonomi- eller HR-roll behöver en förfrågan ske via en e-blankett som måste signeras av närmsta chef för godkännande. E-blanketten skickas därefter till systemadministratörer via löneenhetens ärendehanteringssystem. Systemadministratören granskar därefter e-blanketten och lägger till efterfrågad roll om ansökan ser korrekt ut. Denna process är dokumenterad. Det finns fyra systemadministratörer som har möjlighet att lägga till användare, ta bort användare samt ändra i roller i Heroma.

När en anställning avslutas i systemet inaktiveras användaren automatiskt. Närmsta chef fyller också i en e-blankett och begär borttag av användaren enligt samma process som för tillägg av roller i systemet. Eventuella roller kopplade till användaren tas sedan bort ur systemet av systemansvarig. Om en användare ska byta roll, till exempel byta till en chefsroll, beställs ändringen via e-blanketten likt tilldelning och borttag av roller samt signeras av närmsta chef. Systemförvaltare inaktiverar då den gamla rollen och tilldelar den nya.

Kommunen har relativt nyligen börjat genomföra årliga periodiska genomgångar av användare och dess roller i systemet. Vid den periodiska genomgången tar systemadministratör ut listor på samtliga användare i systemet och jämför mot HR-listor. Därefter tas olämpliga behörigheter bort. Intervjuade

nyckelpersoner uppger dock att det saknas dokumentation som beskriver processen för periodiska genomgångar.

Bedömning

Kommunen bedöms sakna en dokumenterad process som säkerställer att säkerhetsinstruktioner förblir aktuella i relation till vad som är beslutat. Därtill bedömer EY att lösenordskriterierna inte lever upp till vad EY anser god praxis. EY bedömer att kommunen har en dokumenterad process för tilldelning samt borttag av användare i systemet. Kommunen har en informell process som säkerställer att behörigheternas uppbyggnad förblir ändamålsenlig över tid, men saknar dokumentation på detta. Kommunen bedöms dessutom sakna en formell process för att säkerställa att de användare som har behörighet i systemet är lämpliga över tid.

3.2.2. Programförändringar

Iakttagelser

Intervjuade nyckelpersoner uppger att leverantören ansvarar samt tar beslut kring de programförändringar som genomförs i systemet. Vid tid för förändring erhåller kommunen en preliminär versionsbeskrivning innan versionsförändringen genomförs. Information avseende uppdateringar kommuniceras via e-post från leverantören samt via CGI:s (leverantörens) kundportal. Denna process finns dokumenterad.

Innan en förändring implementeras i kommunens produktionsmiljö ansvarar leverantören för testning av förändringen i en separat testmiljö, även denna process finns formellt dokumenterat. Leverantören har systemförvaltare med direktåtkomst till kommunens test- och produktionsmiljön. Vid större förändringar testar även kommunen programförändringen enligt instruktioner från leverantören och baserat på vad som anses relevant med hänsyn till innehållet i uppgraderingen. Intervjuade nyckelpersoner uppger att kommunens testmiljö uppdateras inför varje versionsförändring i systemet för att spegla produktionsmiljön. Denna process finns dokumenterad.

Bedömning

Kommunen bedöms ha en process för kontinuerlig kommunikation avseende programförändringar samt ansvarsfördelning avseende programförändringar. EY bedömer att kommunen har en dokumenterad process som beskriver leverantörens roll gällande programförändringar.

3.2.3. IT-driftsrutiner

Iakttagelser

Intervjuade nyckelpersoner uppger att leverantören ansvarar för drift, konfigurering samt uppföljning av schemalagda jobb och backuper. Leverantören ansvarar därmed för att åtgärda eventuella misslyckade schemalagda jobb. Denna process finns formellt dokumenterad.

Om ett jobb skulle misslyckas märker kommunen det i verksamheten och berörd chef eller lönespecialist tar då kontakt med systemansvarig. Det finns enligt intervjuade nyckelpersoner inte någon direktkommunikation med leverantören angående schemalagda jobb i dagsläget, men kommunen har en kundansvarig hos leverantören som kan kontaktas vid behov. Kommunen har nyligen börjat övervaka de schemalagda jobben genom att systemansvarig regelbundet går igenom körloggen. Denna process finns inte formellt dokumenterad.

Bedömning

Kommunen bedöms ha en dokumenterad process för kontinuerlig kommunikation samt ansvarsfördelning avseende rutiner för schemalagda jobb och backuper. Därtill bedöms kommunen sakna en dokumenterad process som säkerställer att leverantören uppfyller de krav som beslutats, främst gällande kommunikation vid hantering av misslyckade schemalagda jobb.

3.3. Försörjningsstödssystemet

Försörjningsstödssystemet Combine är ett verksamhetssystem som främst används för socialtjänstens myndighetsutövning. Systemet består av en myndighetsvy och en utförarvy. Obehörig åtkomst, programfel eller liknande i försörjningsstödssystemet skulle, i värsta fall, kunna leda till att felaktigt ekonomiskt bistånd betalas ut. Pulsen Omsorg AB är leverantör av systemet som har cirka 1000 användare.

EY noterar att kommunen har påbörjat ett arbete med att formellt dokumentera metod- och processbeskrivningar, bland annat avseende behörighetstilldelning och förändringshantering. Iakttagelser och bedömningar nedan är baserade på dokumentation som mottagits vid tid för granskning.

3.3.1. Behörighetshantering

Iakttagelser

Säkerhetsinställningarna i Combine kräver tvåfaktorautentisering via SITHS, BankID eller FrejaID för att kunna logga in i systemet. Kommunens IT-enhet har möjlighet att ändra säkerhetsinställningarna själva då det är kommunen som är ägare av inloggningen. EY har mottagit dokumentation som styrker att inloggning med tvåfaktorsautentisering ska användas av systemet. Däremot har EY inte mottagit dokumentation som styrker att kommunen har en formellt dokumenterad process som säkerställer att inställningarna förblir korrekta över tid.

För att lägga till en användare i systemet så använder närmsta chef en e-tjänst för att skapa en förfrågan där uppgifter om den anställde som förfrågan avser samt rollen som efterfrågas framkommer. Chefen signerar ansökan med BankID och förfrågan skickas då till systemadministratörer som kontrollerar att rätt chef är beställare. Om beställningen är signerad av rätt chef tilldelas användaren rollen. Om en icke lämplig person efterfrågar en roll i systemet så

nekas beställningen och beställaren meddelas. Intervjuade nyckelpersoner uppger att två personer från Servicedesk, två systemadministratörer samt utvecklingsledaren kan lägga till användare, ta bort användare eller ändra en användares roll i systemet.

Intervjuade nyckelpersoner uppger att processen för att ta bort användare eller förändra en användares roll i systemet är densamma som för tilldelning. Om en användare ska byta roll avslutas den gamla rollen av systemadministratör i samband med att den nya rollen tilldelas. Vid tid för granskning finns ingen dokumenterad processbeskrivning för tillägg och borttag av användare i Combine.

Intervjuade nyckelpersoner uppger att kommunen tidigare har genomfört en periodisk genomgång av användare manuellt, men att denna process har avskaffats. I dagsläget genomförs den periodiska genomgången med hjälp av en robot som en gång i veckan jämför användarlistor i Combine med HR-listor i Heroma. Roboten skickar därefter en rapport till utvecklingsledare för Combine som vid behov kontrollerar behörigheter som inte matchar i listorna. Intervjuade nyckelpersoner uppger dock att denna process inte är formellt dokumenterad.

Bedömning

EY bedömer att kommunen har dokumenterade krav på autentisering vid inloggning i systemet men att kommunen saknar en formellt dokumenterad process som beskriver hur kommunen säkerställer att inga förändringar av säkerhetsinställningarna har genomförts eller att andra metoder kan användas. Kommunen bedöms ha en informell process för behörighetstilldelning och behörighetsborttagning, men som saknar formell dokumentation. För periodiska genomgångar av användare i systemet bedöms kommunen ha en informell process, men saknar formell dokumentation av denna.

3.3.2. Programförändringar

Iakttagelser

Intervjuade nyckelpersoner uppger att leverantören i praktiken ansvarar för större förändringar och uppdateringar. Denna ansvarsfördelning är inte formellt dokumenterad. När en uppdatering planeras att levereras mottar kommunen leveransinformation i samband med en notifiering från leverantören. Leverantören bjuder även in till ”releasedagar” där kommande ändringar diskuteras och kommunen får möjlighet att ställa frågor. Kommunen har även månadsvisa möten med kundansvarig hos leverantören för att gå igenom eventuella supportärenden samt eventuellt diskutera kommande releaser.

Intervjuade nyckelpersoner uppger att kommunen inte kan välja vilka förändringar som ska implementeras i produktionsmiljön. Intervjuade nyckelpersoner uppger även att samtliga förändringar ska testas i testmiljö innan de implementeras i produktionsmiljön. En sådan process finns inte dokumenterad.

Bedömning

EY bedömer att kommunen saknar dokumenterade processer och rutiner för hur förändringar i systemet Combine bör genomföras. Försörjningsstödssystemet har däremot en informell process för att hantera kommande uppdateringar då det i praktiken finns ett informationsflöde inför kommande uppdateringar. Därtill bedöms kommunen sakna en dokumenterad process för ansvarsfördelning avseende förändringar samt en dokumenterad process för att säkerställa att förändringar initialt sker i testmiljö.

3.3.3. IT-driftsrutiner

Iakttagelser

Intervjuade nyckelpersoner uppger att leverantören är ansvarig för drift och övervakning av systemet, inklusive backuper. Systemet har automatiska schemalagda jobb, bland annat sker utbetalningar varje vardag samt hämtning av data dagligen. Schemaläggningen utförs av IT-enheten i samråd med ekonomienheten. Denna process är inte dokumenterad.

I praktiken övervakas utbetalningarna av kommunen och systemförvaltarna notifieras om eventuella felaktigheter genom de chefer som upptäcker problem i sin verksamhet. Även ekonomienheten hör av sig om den dagliga filen inte fungerar. Vid felaktigheter kontaktas leverantören av systemansvarig. En gång i månaden har kommunen och leverantören avstämningsmöten där bland annat driftstatistik och uppföljning kopplat till incidenthantering diskuteras. Vid tid för granskning har EY inte mottagit en av kommunen formellt beslutad och dokumenterad process eller rutin avseende felundersökningar av schemalagda jobb.

Bedömning

EY bedömer att kommunen saknar dokumenterade processer och rutiner avseende schemaläggning och felundersökningar av schemalagda jobb i systemet. Därtill bedöms kommunen sakna en dokumenterad ansvarsfördelning som specificerar ansvarsförhållandet inom kommunen samt mellan kommunen och leverantören gällande IT-driftsrutiner.

4. Rekommendationer

I detta avsnitt presenteras rekommendationerna baserat på genomförd granskning. Rekommendationerna presenteras övergripande för kommunstyrelsen. De övergripande rekommendationerna avser de främsta riskerna för samtliga system (ekonomisystemet, lönesystemet och försörjningsstödssystemet).

4.1. Våra rekommendationer

Övergripande rekommendationer

Säkerställande av styrdokument:
Upplands Väsby kommun saknar för samtliga granskade system flertalet styrande dokument som bedöms nödvändiga för ett tillfredsställande arbete avseende behörighetshantering samt hantering av programförändringar och driftsrutiner. Kommunstyrelsen rekommenderas således att säkerställa att relevanta styrdokument finns framtagna och att tillhörande riktlinjer, processer och metoder implementeras. Detta för att säkerställa ett systematiskt arbetssätt som medarbetare kan applicera för att säkerställa en säker användning av kommunens finansiellt viktiga system.

Säkerställande av uppföljning och efterlevnad:
Kommunen bedöms enligt flertalet områden avseende arbete kring behörighetshantering, programförändringar samt IT-drift sakna processer och metoder som säkerställer att efterlevnaden av beslutade riktlinjer och rutiner efterlevs i praktiken. Kommunen bedöms, för flera system, sakna formella processer för periodiska uppföljningar av användare samt kontroller som säkerställer att de granskade systemen hanteras som beslutat. Även om vissa system har informella periodiska genomgångar av användare rekommenderas dessa processer att ses över. Exempelvis noterar EY att den informella processen för periodiska genomgångar av användare inom ekonomisystemet inte inkluderar alla användare med åtkomst till systemet. Kommunstyrelsen rekommenderas således att säkerställa rutiner och processer som avser kontroll och uppföljning. Detta för att säkerställa en ändamålsenlig och tillfredsställande systemhantering samt relevans av rutiner och processer över tid.

Förtydligande av roll- och ansvarsfördelning:
Ekonomisystemet samt försörjningsstödssystemet bedöms sakna en tydlig roll- och ansvarsfördelning som specificerar ansvarsförhållandet mellan kommunen och leverantören vid kommande programförändringar samt avseende IT-drift och åtgärder av misslyckade schemalagda jobb. Exempelvis berättar intervjuade nyckelpersoner om leverantörens roll och ansvar, men EY har inte mottagit dokumentation som styrker att den roll- och ansvarsfördelningen är formellt beslutad. För att säkerställa en tillfredsställande och ändamålsenlig förändringshantering samt IT-driftshantering rekommenderas kommunstyrelsen att säkerställa att roll- och ansvarsfördelning mellan kommun och leverantör specificeras i ovan nämnda sammanhang.

Kommunstyrelsen rekommenderas att säkerställa att:

- Relevanta styrdokument och kontroller finns framtagna och att tillhörande riktlinjer implementeras.
- Processer för uppföljning av efterlevnaden av kommunens riktlinjer och rutiner implementeras och genomförs.
- Roll- och ansvarsfördelningar förtydligas.

5. Revisionsfrågor

Granskningen har utgått från revisionsfrågan: Har kommunstyrelsen säkerställt att det finns ändamålsenlig styrning för den finansiella IT-miljön? Revisionsfrågan har brutits ner och besvarats enligt tabell 2. Förklaring av färgkodningen som används i tabell 2 presenteras i tabell 1.

Tabell 1: Förklaring av färgkodning.

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvaras delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Tabell 2: Svar på revisionsfrågor.

Revisionsfråga	Svar	
Behörighetshantering: ▪ Finns generella krav för säkerhetsinställningar och lösenordskrav och är de adekvata för verksamheten? ▪ Finns rutiner för behörighetstilldelning och borttag av behörighet och finns rutiner för godkännande av dessa? ▪ Finns rutiner för uppföljning av behörigheter i form av att anställda har relevanta behörigheter till system?	Styrningen av kommunens arbete avseende behörighetshantering bedöms inte vara tillfredsställande. Svaret grundar sig i att kommunen inte har kunnat visa vilka säkerhetsinställningar som ska tillämpas i ekonomisystemet samt lönesystemet. EY noterar att lönesystemet har uppvisat lösenordsparametrar. Däremot bedömer EY att dessa inte lever upp till god praxis och därmed en lämplig nivå. Därtill saknas kontroller för att säkerställa att inställningarna förblir riktiga över tid inom samtliga system. Svaret grundar sig även i att kommunen bedöms ha vissa informella processer kopplat till behörighetshantering för två av systemen, och endast dokumenterade processer för lönesystemet. Vid tid för granskning saknar formell processbeskrivning och kravställning för ekonomisystemet samt	

	försörjningsstödssystemet. Därtill saknas processbeskrivningar för uppföljning av användare och dess behörigheter för samtliga system.	
Programförändringar: ▪ Finns tillräckliga rutiner implementerade i verksamheten för att genomföra programförändringar? ▪ Finns tydliga roller och ansvar för hantering av programförändringar? ▪ Finns rutiner för godkännanden och testning av ändringar och dokumenteras dessa?	Styrningen av kommunens arbete avseende programförändringar bedöms inte vara tillfredsställande. Svaret grundar sig i att kommunen bedöms ha vissa informella processer för förändringshantering men saknas formella processbeskrivningar för ekonomisystemet samt försörjningsstödssystemet. Bland annat saknas dokumenterade processer avseende ansvarsfördelning mellan kommun och leverantör, dokumenterade processer för beslutsfattande gällande programförändringar samt dokumenterad kravställning avseende testning av förändringen i testmiljö innan implementation.	
IT-driftsrutiner: ▪ Finns rutiner för hantering av säkerhetskopiering av system? ▪ Finns rutiner för att testa att säkerhetskopior fungerar? ▪ Finns rutiner för övervakning av schemalagda jobb samt rutiner för avhjälpning av eventuella fel?	Styrningen av kommunens arbete avseende IT-driftsrutiner bedöms inte vara tillfredsställande. Svaret grundar sig i att kommunen bedöms sakna formella processer för hur IT-driften ska skötas i två av systemen. Kommunen bedöms även sakna tydliga och dokumenterade processer och rutiner för IT-drift samt ansvarsfördelning mellan kommun och leverantör avseende övervakning och hantering av schemalagda jobb. Detta gäller för två system.	

6. Slutsatser

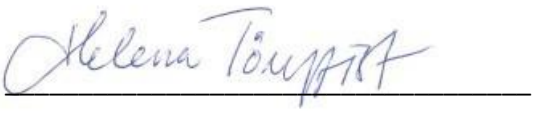
Granskningens syfte har varit att bedöma om kommunstyrelsen har säkerställt en ändamålsenlig styrning, intern kontroll och uppföljning avseende hantering av programförändringar, behörighetshantering och driftsrutiner för system som är centrala för den finansiella rapporteringen.

EY:s övergripande bedömning är att Upplands Väsby kommun inte har säkerställt att det finns ändamålsenlig styrning för den finansiella IT-miljön. Bedömningen grundar sig i att kommunstyrelsen inte har säkerställt att relevanta styrdokument för vardera granskat område finns framtaget eller att tillhörande riktlinjer implementerats. Därtill har kommunen inte säkerställt uppföljning och efterlevnad av kommunens riktlinjer. Avslutningsvis bedömer EY att kommunstyrelsen för två av de granskade systemen inte har säkerställt tydligt definierade roll- och ansvarsfördelningar för hantering av programförändringar och IT-driftsrutiner.

Med grund i ovan är EY:s främsta rekommendationer att kommunstyrelsen i Upplands Väsby kommun säkerställer att:

- Relevanta styrdokument och kontroller finns framtagna och att tillhörande riktlinjer implementeras.
- Processer för uppföljning av efterlevnaden av kommunens riktlinjer och rutiner implementeras och genomförs.
- Roll- och ansvarsfördelningar förtydligas.

Stockholm 2024-01-12



Helena Törnqvist,

Partner EY

Bilaga 1: Förteckning över intervjuade funktioner

6.1. Ekonomisystemet Raindance

- Ekonomichef
- Systemförvaltare

6.2. Lönesystemet Heroma

- Systemansvarig
- Systemadministratör
- Löneadministratör

6.3. Försörjningsstödssystemet Combine

- Chef för enheten individ och familj
- Enhetschef ekonomiskt bistånd
- Utvecklingsledare för systemet
- Verksamhetscontroller

Bilaga 2: Dokumentförteckning

Notera att samtliga dokument är namngivna som de är mottagna från kommunen.

Ekonomisystemet:

- Lägga upp ny användare.docx
- Lathund_Lägga in attesträtt i systemet.docx
- Ta bort användare.docx
- Se utdrag ur fil.JPG
- Tidplan årsbokslut 2022 ekonomienheten möte xls.msg
- Tidplan årsbokslut 2022 ekonomienheten möte.xls
- 230216-BEH-ZR56.pdf
- Gulmarkerat är behörighetsnivå för att kontera leverantörsfakturor.JPG
- metod för att säkerställa att behörighetsförfrågan var rimlig kolla att personen som skrivit under är chef.JPG
- metod för att säkerställa att behörighetsförfrågan var rimlig kolla om rimlig chef skrivit under anställd.JPG
- Underlag på behörighet i systemet som matchar blanketten.JPG
- Workplace Suite Scan.pdf
- Avslut användare rapport när namn lyser rött har person slutat på kommunen men finns med aktiv attesträtt i raindance.JPG
- Avslut av användare OSBE19.JPG
- Avslut av attest OSBE19.JPG
- Avslut på mail.JPG
- Borttagning av användare.JPG
- Ex Attestlista som skickas ut i slutet av året för avslut av attesträtter.xlsx
- Attestlistor förlängning 2023.msg
- Ex Attestlista som skickas ut i slutet av året för avslut av attesträtter.xlsx
- Underlag där det framgår hur listan togs ut vid period för genomgång.docx
- Ansvariga 2023.xlsx
- Attestlista 10.xlsx
- Attestlista 20.xlsx
- Attestlista 25.xlsx
- Attestlista 3 övergripande.xlsx
- Attestlista 302.xlsx
- Attestlista 304.xlsx
- Attestlista 305.xlsx
- Attestlista 34.xlsx
- Attestlista 50.xlsx
- Attestlista 6 övergripande.xlsx
- Attestlista 604.xlsx
- Attestlista 90.xlsx
- Attestlista 99.xlsx

- Attestlista kontorschefer.xlsx
- Attestlista regina.xlsx
- Balanskonton.xlsx
- Mall Attestlista 2023.xlsx
- Behörighetsposition per delsystem.xlsx
- Behörighetspositioner modul MSP.xlsx
- Behörighetspositioner per Användare.xlsx
- Förklaring behörigheter.xlsx
- Inloggning BankID 1.JPG
- Inloggning BankID 2.JPG
- Inloggning BankID 3.JPG
- Inloggning SSO.JPG
- Finns ingen total lista men man kan se per användare som i detta exempel.JPG
- Ex mail skapande av lösenord.JPG
- Tom.txt
- aktplan_uppgradering_test_2023v-ny-dbkopia_upplandv_.xlsx
- ManuellaAtgarder_2023v.pdf
- Nyheter_2023v.pdf
- testprotokoll Abonnemang.docx
- testprotokoll AR.doc
- testprotokoll BOP.docx
- testprotokoll Budget och Prognos.doc
- Testprotokoll E-handel.xlsx
- testprotokoll EK.docx
- testprotokoll IFP – ej aktuell för oss.doc
- testprotokoll Inköp – ej aktuell för oss.docx
- Testprotokoll KRP.docx
- testprotokoll LFP.doc
- Testprotokoll Raindance.xlsx
- testprotokoll TID.doc
- testprotokoll UDP och AXT-utskrift.docx
- Boka tid för uppgradering.msg
- Kommande programförändring servicepacks.JPG
- Kommande programförändring större version.JPG
- LÖST Problem efter uppgradering TEST som måste lösas innan PROD uppgradering.msg
- Problem efter uppgradering TEST som måste lösas innan PROD uppgradering.msg
- Uppgradering TEST klar.msg
- Dokumentation version riktiga miljön.JPG
- Dokumentation version Testmiljö.JPG
- Förvaltningsplan Ekonomi- och inköpsprocessen 2024.docx
- Boka tid för uppgradering.msg
- status lansering till produktiopnsmiljö.msg
- Ex beskrivning hur man gör ändringar i en typ av schemlagda jobb för portaljobb.docx
- Ex beskrivning hur man gör ändringar i en typ av schemlagda jobb.docx

- Bokföring stängd av robot rätt.msg
- Bokföring stängd av robot som gått fel.msg
- Ex rapport schemalagda jobb överföring till anläggningsregister.JPG
- Leveransrapport för Upplands Väsby kommun.msg
- Notification from AGETOR log system (project RD_Intern_AXT).msg
- Raindance filöverföring körd Fel finns.msg
- säkerhetskopia från PROD till TEST.JPG

Lönesystemet:

- 1.1 Behörighetsprocess för Heroma.docx
- 1.2 Processbeskrivning för periodisk genomgång av användare.docx
- 1.3 680211-9070 Fredrik Riström 231030-240430.pdf
- 1.3 Exempel på en upplagd behörighet.docx
- 1.4 Ex på avslut av behörighet.docx
- 1.5 Behörighetsrapport221123 rättad.xlsx
- 1.6 Roller i Heroma.xlsx
- 2.1 Inloggning med UserID och lösenord eller BankID.docx
- 2.2 Användare som loggar in med UserID och lösenord.docx
- 2.3 Lösenordspolicy.docx
- 3.1 Förändringshantering tillsammans med leverantör.docx
- 3.2 Processbeskrivning uppdatering av Testmiljön.docx
- 3.3 Avtal med CGI Sverige AB om HR- och lönesystem.pdf
- 4.1 CGI Årsplan 2024 inkl Pluto.xlsx

Försörjningsstödssystemet:

- Avbeställning behörigheter – Komplettering.docx
- Avbeställning behörigheter.docx
- Behöriga beställare utöver chefer.docx
- Beställning behörighet – Komplettering.docx
- Beställning behörighet.docx
- Combine 2023-09-05.docx
- Combine.aktiva.roller.docx
- Förvaltningsplan handläggning och dokumentation inom socialtjänsten 2023.pdf
- Mail kring systemförändringar.docx
- Objektspecialisters uppdrag.docx
- Release notes Combine Core 1.36.pdf
- Releasetester 1.35.pptx
- Revision.xlsx
- Stickprov releasehantering.docx
- Underlag Wiki.docx
- Upplands Väsby Avtal Standard-SLA 221001-260930.pdf

Bilaga 3: Definitioner

Active Directory (AD): Active Directory (AD) är en katalogtjänst som bland annat stöder autentiseringsprotokoll och inloggning.

Single Sign On (SSO): Single Sign On är en inloggningsmetod som innebär att en användare endast behöver logga in med samma inloggningsuppgifter en gång för att få tillgång till flera system.

SLA (Service Level Agreement): Servicenivåavtal mellan beställare och tjänsteleverantör där överenskomna krav som ställs på tjänsten definierats, tex drift, support och förvaltning av systemet.

Tvåfaktorsautentisering: Extra lager av säkerhet som kräver mer än ett lösenord för att autentiseras till den interna miljön