Södertälje kommun

Granskning av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur

maj 2023

1. Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Södertälje kommun granskat behörighetshanteringen, programförändringshanteringen samt IT-driftshanteringen inom tre av kommunens IT-system: ekonomisystemet ERP, lönesystemet Personec P 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 som bedömts relevant 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 kommunen inte säkerställt uppföljning och efterlevnad av kommunens riktlinjer. Avslutningsvis bedömer EY att kommunstyrelsen för ett av de granskade systemen inte har säkerställt tydligt definierade roll- och ansvarsfördelningar för arbete avseende programförändringar och driftsrutiner.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. EY rekommenderar att kommunstyrelsen i Södertälje 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

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 då stora mängder pengar flödar genom berörda system.

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 sker huvudsakligen genom intervjuer med ansvariga tjänstemän vid kommunförvaltningen, men även genom dokumentgranskning, inom följande områden:

- 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.
- Felundersökningar för 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 ERP är kommunens huvudsakliga affärssystem där bokföring och finansiell rapportering sker. 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.

3.1.1. Behörighetshantering

3.1.1.1 Iakttagelser

Enligt intervjuade nyckelpersoner kräver säkerhetsinställningarna för systemet ERP i dagsläget tvåfaktorautentisering, vilket innebär att en användare måste logga in via Active Directory (AD) samt via ett identifikationsverktyg för att ges åtkomst till systemet. Vid tid för granskning har EY inte mottagit dokumentation som styrker att tvåfaktorautentisering används av systemet. Leverantören har behörighet att göra ändringar i säkerhetsinställningarna och kan således ändra kraven på inloggningsfunktionen. Kommunen genomför inga genomgångar för att säkerställa att sådana eller andra förändringar i säkerhetsinställningarna inte har genomförts.

Kommunen har en e-tjänst där användare kan efterförfråga behörigheter till systemet. En sådan förfrågan kan göras åt en själv eller en annan person. För att komma åt e-tjänsten krävs en inloggning via personnummer och BankID. Behörighetsförfrågan initieras via en blankett där användaren bland annat måste uppge vem förfrågan berör, från vilket datum behörigheten ska gälla, åtkomster som användaren ska ha samt vem som är närmsta chef. Godkännande av behörigheten sker av närmsta chef till den individ som berörs av behörighetsförfrågan, och medges i samband med att blanketten skickas av användaren. Efter godkännande av närmsta chef kan systemförvaltarna tilldela korrekt behörighet utefter de svar som uppgetts i blanketten. Systemet har få behörigheter och alla användare får en bas-behörighet. Det är endast de två nuvarande systemförvaltarna som har behörighet att tilldela, förändra eller ta bort behörigheter.

När en användare slutar hos kommunen avaktiveras användarens konto i AD vilket innebär att användaren automatiskt förlorar tillträde till systemet. I samband med förändringen i AD skickas en notis till systemförvaltarna om att personens konto kan inaktiveras. Därefter initieras en manuell process och systemförvaltarna inaktiverar kontot.

Kommunen genomför inga periodiska genomgångar av behörigheter. Intervjuade nyckelpersoner uppger att anledningen till avsaknaden av periodiska genomgångar beror på att systemet introducerades i början av 2021 och att det därmed inte funnits tillräckligt med tid för att ta fram en sådan process.

Systemet tillåter kombinerade roller, vilket innebär det finns många olika behörigheter som kombineras och paketeras till så kallade roller. Uppbyggnaden av roller godkänns av systemförvaltningen tillsammans med leverantören. Intervjuade nyckelpersoner uppger att förändringar av roller sällan sker. Kommunen genomför inga periodiska genomgångar av sammansättningen av dessa kombinerade roller.

3.1.1.2 Bedömning

Kommunen bedöms sakna en dokumenterad process som säkerställer att säkerhetsinstruktioner förblir aktuella i relation till vad som är beslutat. Därtill bedöms kommunen ha en formell process för behörighetstilldelning. Kommunen bedöms sakna en dokumenterad process för att säkerställa att endast behöriga har åtkomst till systemet över tid, samt en process som säkerställer att samtliga konton som ska inaktiveras har inaktiverats. Därtill bedöms kommunen sakna en process som säkerställer att rollernas uppbyggnad förblir ändamålsenlig över tid.

3.1.2. Programförändringar

3.1.2.1 Iakttagelser

Leverantören Unit4 ansvarar för att programförändringar genomförs i systemet. Vid tid för uppdatering notifieras kommunen om uppdateringen och månatliga förvaltningsmöten hålls med leverantören för att diskutera uppdateringar. Intervjuade nyckelpersoner uppger att kommunen inte kan stoppa kommande uppdateringar, utan leverantören genomför dessa oavsett kommunens återkoppling. Samtliga uppdateringar sker i testmiljö innan de implementeras i kommunens produktionsmiljö. EY har inte mottagit en formell process som beskriver denna rutin.

Intervjuade nyckelpersoner uppger att kommunen inte genomför uppföljningar av leverantören samt att inga tredjepartsrapporter efterfrågas.

3.1.2.2 Bedömning

Kommunen bedöms ha en process för kontinuerlig kommunikation avseende förändringar samt ansvarsfördelning avseende förändringar. EY bedömer att kommunen saknar en process som beskriver att samtliga uppdateringar inledningsvis ska ske i testmiljö. Därtill bedöms kommunen sakna en process som säkerställer att leverantören uppfyller de krav som beslutats.

3.1.3. IT-driftsrutiner

3.1.3.1 Iakttagelser

Intervjuade nyckelpersoner uppger att kommunen själv sätter upp schemalagda jobb. Om sådana jobb skulle misslyckas notifieras både systemförvaltarna från kommunen och leverantören Unit4. Därtill uppges att ansvaret för att åtgärda problemet tilldelas antingen kommunen eller leverantören beroende på allvarlighetsgraden, vid kritiska problem ansvarar leverantören för åtgärdande medan systemförvaltarna från kommunen ansvarar för åtgärdande av mindre kritiska problem.

Intervjuade nyckelpersoner uppger att endast systemförvaltarna har behörighet att aktivera och inaktivera schemalagda jobb. I praktiken bedöms behovet av en sådan handling utefter verksamhetens behov, automatikens möjligheter samt ekonomiavdelningens godkännande. Förändringar sker först i testmiljö. Denna process uppges vara vedertagen men inte dokumenterad.

3.1.3.2 Bedömning

EY bedömer att kommunen har en dokumenterad process avseende uppsättning av schemalagda jobb samt ansvarsfördelning vid felundersökning och åtgärd. Därtill bedöms systemet sakna en dokumenterad process som beskriver att inaktivering och aktivering av schemalagda jobb först ska genomföras i testmiljö.

3.2. Lönesystemet

Lönesystemet Personec P används främst för att betala ut löner till kommunens anställda, men även till att lämna uppgifter till Skatteverket, SCB, Försäkringskassan och andra myndigheter. Systemet möjliggör även för anställda att tidsrapportera. Tjänsten är upphandlad av Visma och systemet har cirka 400 användare med högre behörighet än bas-behörighet.

3.2.1. Behörighetshantering

3.2.1.1 Iakttagelser

Enligt intervjuade nyckelpersoner ställer säkerhetsinställningarna i Personec P krav på tvåfaktorautentisering. Vid tid för granskning har EY inte mottagit dokumentation som styrker att tvåfaktorautentisering används av systemet. Kommunen har möjlighet att ändra säkerhetsinställningarna, men genomför inga granskningar för att säkerställa att inga oönskade förändringar av säkerhetsinställningarna genomförts.

Intervjuade nyckelpersoner uppger att systemet saknar en formell process för behörighetstilldelning och behörighetsförändring. I praktiken har samtliga anställda på kommunen behörighet till lönesystemet i syfte att komma åt sin självservicefunktion. Behörighet tilldelas vid anställning genom att lönekonsulterna verifierar signerat anställningsavtal. Ett Active Directory-konto skapas sedan av IT-enheten. I samband med att den nyanställdes Active Directory-konto skapas så tilldelas även behörighet till lönesystemet. Den nyanställdes chef tillhandahåller inloggningsuppgifterna och kan sedan kommunicera dessa till den nya användaren. Användaren kan sedan logga in i lönesystemet. En medarbetares konto avslutas per automatik när anställningen, och därmed kopplingen till Active Directory, avslutas.

Intervjuade nyckelpersoner uppger att anställningsavtalet ligger till grund för vilken behörighet som ska tilldelas om högre behörighet efterfrågas. I vissa fall kan informationsägaren även kontrollera rättigheten för behörighet. Högre behörigheter tilldelas utefter vad tjänsten kräver och appliceras för anställda vars arbetsuppgifter inkluderar hantering av lön samt de anställda som är systemförvaltare. Chefer har en medelbehörighet för att kunna godkänna anställdas frånvaro och eventuella avvikelser. Högre behörigheter såsom chefs-, ekonomi- eller HR-behörigheter kan endast tilldelas av systemförvaltarna. Anställda inom löneenheten har läsbehörighet och kan lägga till timvikarier i systemet. Om chefsroller ska ändras meddelas löneenheten som sedan meddelar systemförvaltarna om den förändrade behörigheten. Denna process är inte formellt dokumenterad.

Kommunen genomför inga periodiska genomgångar för att säkerställa att systemets användare har korrekt och aktuell behörighet. Intervjuade nyckelpersoner uppger att det sker ett arbete för att införa periodiska genomgångar i samband med en ny uppdatering av systemet. Denna uppdatering planeras vid tid för granskning att sättas i bruk inom snar framtid. I dagsläget sker mindre genomgångar i samband med att chefer byts ut, då felaktiga behörigheter kan upptäckas i samband med granskningen av chefens organisation.

3.2.1.2 Bedömning

EY bedömer att kommunen saknar en process för att granska att förändringar av säkerhetsinställningarna inte genomförts. Även om systemet bedöms ha en behörighetshantering som aktiveras i praktiken saknar kommunen en dokumenterad process avseende behörighetstilldelningen för samtliga anställda i samband med anställning. Därtill saknas en dokumenterad process avseende behörighetsborttagning i samband med att användares AD konto inaktiveras. Dessutom bedöms kommunen sakna en dokumenterad process avseende behörighetstilldelning för högre behörigheter. Vid tid för granskning bedöms kommunen sakna en tillfredsställande process för att säkerställa att de användare som har behörighet i systemet är korrekta samt att den behörighet som är tilldelad är korrekt.

3.2.2. Programförändringar

3.2.2.1 Iakttagelser

Intervjuade nyckelpersoner uppger att leverantören Visma ansvarar för merparten av de programförändringar som genomförs i systemet. Större versionsförändringar sker av Visma några gånger per år medan tabellförändringar sker på en månadsbasis. Även dessa genomförs av Visma. Avtalet mellan kommunen och Visma specificerar att de måste uppdatera systemet i enlighet med kollektivavtalet Allmänna bestämmelser (AB). Kommunen måste genomföra en beställning för att anpassa funktioner men kan delvis bygga om gränssnitt utan stöd från Visma. Kommunen behöver i de flesta fall genomföra de uppdateringar som Visma initierar. Intervjuade nyckelpersoner uppger att det kan förekomma typer av uppdateringar som de kan välja att ignorera, men att sådana är ovanliga och inte har förekommit under tiden som systemet brukats. Kommunen har inte en dokumenterad process för hur uppdateringar bör utvärderas för att besluta om de ska genomföras eller ej.

Kommunen erhåller en preliminär versionsbeskrivning en månad innan större versionsförändringar. Information avseende tabelluppdateringar kommuniceras via en kundportal samt e-post från Visma som påminner om att ny information finns tillgänglig.

Visma testar alla förändringar innan de implementeras i kommunens produktionsmiljö. Intervjuade nyckelpersoner uppger att kommunen har separata test- och utbildningsmiljöer och att dessa används. De tester som genomförs avser åtkomsttester. Vid tid för granskning har kommunen inga dokumenterade tester av genomförda förändringar. Visma har systemförvaltare med direktåtkomst till produktionsmiljön samt har två kopior av

systemet. Kommunen genomför inga granskningar avseende utvecklarnas behörighet i systemet.

3.2.2.2 Bedömning

Lönesystemet bedöms sakna en dokumenterad process för hur kommande uppdatering bör utvärderas för att besluta dess genomförande. EY bedömer att systemet har en framtagen mall avsedd för att dokumentera genomförda tester av förändringar, men att denna inte används i praktiken då kommunen inte har dokumenterat genomförda förändringar. Därmed bedömer EY att kommunen saknar en process för att dokumentera genomförda förändringar. EY bedömer att lönesystemet har en process för att hantera kommande uppdateringar då det i praktiken finns ett informationsflöde inför kommande uppdateringar. Däremot saknas en behörighetsgranskning avseende leverantörernas behörigheter i produktionsmiljön.

3.2.3. IT-driftsrutiner

3.2.3.1 Iakttagelser

Intervjuade nyckelpersoner uppger att leverantören Visma ansvarar för konfigureringen av schemalagda jobb. Om schemalagda jobb inte skulle genomföras får Visma en notifiering, och därefter tas processen över manuellt. Systemförvaltarna övervakar vissa körningar men inte som en konstant process. De notifieras av den individ som upptäcker att en körning inte genomförs och åtgärdar därefter problemet. Om större fel uppstår kommunicerar Visma felet till kommunen, vid mindre fel hanterar Visma situationen utan att involvera kommunen.

Intervjuade nyckelpersoner uppger att Visma har interna möten för att diskutera eventuella avvikelser samt möten med kommunen varannan månad för att informera om avvikelser som skett.

3.2.3.2 Bedömning

Lönesystemet bedöms ha en process som aktiveras av leverantören avseende felundersökning av schemalagda jobb. Därtill bedöms lönesystemet ha en process för kontinuerlig kommunikation med leverantören avseende schemalagda jobb.

3.3. Försörjningsstödssystemet

Försörjningsstödssystemet Combine är ett verksamhetssystem som främst används för socialtjänstens myndighetsutövning. Systemet består av en myndighetsvy och en utförarvy. Combine är upphandlat av leverantören Pulsen AB. Systemet har mellan 600 och 700 användare.

3.3.1. Behörighetshantering

3.3.1.1 Iakttagelser

Säkerhetsinställningarna i Combine kräver i dagsläget tvåfaktorautentisering. Kommunen har inte möjlighet att ändra inställningarna själva utan måste kontakta leverantören om sådant önskas. Intervjuade nyckelpersoner uppger att både leverantören och kommunens IT-enhet måste genomföra en kombinerad förändring av säkerhetsinställningarna för att en förändring ska möjliggöras. Kommunen genomför inga genomgångar för att säkerställa att inställningarna är fortsatt lämpliga och inte förändrats.

Kommunen använder ett ärendehanteringssystem (DF Respons) för att behandla systemets behörighetsansökningar. För att logga in på ärendehanteringssystemet krävs en tvåfaktorautentisering. En behörighetsansökan initieras när chefen till den anställde som önskas behörighet genomför en beställning i ärendehanteringssystemet. Godkännande av behörigheten sker av chefen i samband med beställningen. Därefter granskar systemförvaltarna beställningen i syfte att säkerställa att den behörighet som efterfrågar är rimlig i jämförelse med tjänsten. Om behörigheten anses orimlig eller om ansökan är bristfälligt utförd kontaktar systemförvaltarna chefen som lagt beställningen. Om beställningen är korrekt utförd och rimlig tilldelas behörigheten. Det är endast systemförvaltarna som har behörighet att tilldela, inaktivera eller förändra behörigheter.

Intervjuade nyckelpersoner uppger att behörigheter till systemet inte tas bort utan inaktiveras om åtkomst inte längre ska vara möjlig för en individ. Processen för att inaktivera en användares behörigheter eller förändra en användares behörigheter är densamma som för tilldelning av behörighet. Om en behörighet ska bytas inaktiveras den gamla behörigheten i samband med att den nya behörigheten tilldelas.

Systemförvaltarna genomför en periodisk genomgång av användare på halvårsbasis. Genomgången initieras av att systemförvaltarna skickar listor av användare och behörigheter till cheferna för godkännande. Intervjuade nyckelpersoner uppger att de inte har en process för att säkerställa att samtliga chefer genomför granskningen, systemförvaltarna förlitar sig på att cheferna genomför granskningarna samt kontaktar systemförvaltarna om behörigheter behöver förändras.

3.3.1.2 Bedömning

EY bedömer att kommunen saknar en dokumenterad process som säkerställer att säkerhetsinställningarna förblir aktuella i relation till vad som är beslutat. Kommunen bedöms ha processer avseende behörighetstilldelning samt behörighetsförändring, men bedöms sakna en tillfredsställande behörighetsgranskning för att säkerställa att de användare med behörigheter i systemet fortsatt bör ha de behörigheter som tilldelats.

3.3.2. Programförändringar

3.3.2.1 Iakttagelser

Intervjuade nyckelpersoner uppger att leverantören Pulsen AB i praktiken ansvarar för större förändringar och uppdateringar medan kommunen kan genomföra mindre anpassningar i systemet. Sådan ansvarsfördelning är inte formellt dokumenterad. När en uppdatering planeras att levereras mottar kommunen leveransinformation i samband med en notifiering från leverantören. Intervjuade nyckelpersoner uppger att kommunen kan välja när förändringen ska publiceras för användarna, och att kommunen kan välja vilka förändringar som ska implementeras. Leverantören kan däremot ställa krav på att vissa förändringar ska genomföras. Kommunen saknar en dokumenterad beslutsprocess avseende om förändringar ska genomföras eller ej, men det uppges finnas en process som i praktiken är vedertagen. Intervjuade nyckelpersoner uppger även att samtliga förändringar testas i testmiljö innan de implementeras i produktionsmiljön. En sådan process finns inte dokumenterad.

3.3.2.2 Bedömning

EY bedömer att kommunen saknar dokumenterade processer och rutiner för hur förändringar i systemet Combine bör genomföras. 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

3.3.3.1 Iakttagelser

Intervjuade nyckelpersoner uppger att systemet har automatiska och manuella schemalagda jobb, bland annat sker utbetalningar varje vardag samt hämtning av data dagligen. I praktiken övervakas utbetalningarna av kommunen och systemförvaltarna

notifieras om felaktigheter genom de chefer som upptäcker problem i sin verksamhet. Om felaktigheten beror på ett systemfel och inte ett verksamhetsfel kontaktas leverantören Pulsen AB. Vid tid för granskning har EY inte mottagit en formellt beslutad och dokumenterad process eller rutin avseende felundersökningar av schemalagda jobb. Därtill har EY inte tagit emot en ansvarsfördelning avseende felundersökningar och åtgärdande av schemalagda jobb.

3.3.3.2 Bedömning

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

4. Rekommendationer

4.1. Våra 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*).

Övergripande rekommendationer

Säkerställande av styrdokument
Södertälje kommun saknar för samtliga granskade system flertalet styrande dokument som bedöms nödvändiga för en säker behörighetshantering samt inom ett tillfredsställande arbete avseende 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 och programförändringar sakna processer och metoder som säkerställer att efterlevnaden av beslutade riktlinjer och rutiner efterlevs i praktiken. Kommunen bedöms därmed för flera system sakna periodiska uppföljningar och kontroller som säkerställer att de granskade systemen hanteras som beslutat. 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
Försörjningsstödssystemet bedöms sakna en tydlig roll- och ansvarsfördelning som specificerar ansvarsförhållandet mellan kommunen och leverantören vid både kontroll och åtgärder av misslyckade schemalagda jobb samt vid kommande förändringar. 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 och beslutas.

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 nedan.

Tabell 12: Förklaring av färgkod

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

Tabell 13: 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 tillämpas i två system. Därtill saknas kontroller för att säkerställa att inställningarna förblir riktiga över tid inom samtliga system. Svaret grundar sig även i att vissa styrande dokument, riktlinjer eller processer kopplat till behörighetshantering saknas inom flera granskade system för att säkerställa ett tillfredsställande arbete. Därtill saknas tillfredsställande rutiner för uppföljning av behörigheter för samtliga system.	
Programförändring ▸ Finns tillräckliga rutiner implementerade i verksamheten för att genomföra programförändringar?	Styrningen av kommunens arbete avseende programförändringar bedöms inte vara tillfredsställande. Svaret grundar sig i att för flera system saknas dokumenterade rutiner för beslutsfattande avseende förändringar samt att det för flertalet system saknas	

▸ Finns tydliga roller och ansvar för hantering av programförändringar? ▸ Finns rutiner för godkännanden och testning av ändringar och dokumenteras dessa?	dokumenterade kravställningar avseende användning av testmiljöer. Därtill saknas en tydlig roll- och ansvarsfördelning för försörjningsstödssystemet.	
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 delvis vara tillfredsställande. Svaret grundar sig i att kommunen bedöms ha vissa rutiner och riktlinjer för flera av systemen. Däremot saknas viss kravställning och vissa processbeskrivningar för ekonomisystemet respektive försörjningsstödssystemet. Därtill saknas en tydlig roll- och ansvarsfördelning inom försörjningsstödssystemet.	

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 Södertälje 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 ett av de granskade systemen inte har säkerställt tydligt definierade roll- och ansvarsfördelningar för arbete avseende programförändringar och driftsrutiner.

Med grund i ovan är EY:s främsta rekommendationer att kommunstyrelsen i Södertälje 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.

Stockholm 2023-05-30

Helena Törnqvist
Partner, EY

Bilaga 1: Förteckning över intervjuade funktioner

6.1. Ekonomisystemet Agresso

- Ekonomi och finansdirektör
- Förvaltningsledare
- Redovisningschef och systemansvarig
- Systemförvaltare

6.2. Lönesystemet Personec P

- IT arkitekt
- Systemförvaltare (lön)
- Systemförvaltare (HR)
- Lönechef och systemansvarig

6.3. Försörjningsstödssystemet Combine

- Systemförvaltare

Bilaga 2: Dokumentförteckning

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

Ekonomisystemet:

- Ansökan om behörighet i ekonomisystemet - 33987 (1)
- Appendix-(Bilaga)-C-Unit4-Globala-villkor-för-nivåindelad-support-v1.1-Mars-2018-(SW)
- Bilaga 1_Samverkansmodell
- Biträdesavtal Unit4 ERP
- Information på Kanalen_vårt intranät
- Ny användare i ERP
- Resurs kompl rollen INKREKV efter godkänt test
- Södertälje kommun_Förvaltning_och_utvecklingsavtal_juni_2021
- Unit4 Global Cloud - Hotfix Installation - Nordic Data Center
- Upplagd användare i ekonomisystemet

Lönesystemet:

- (Kopia innehåller avvikelse) Förvaltningsmöte Södertälje kommun_Agenda_22-10-04 (003)
- Användarhandbok NeptuneWeb 22.2
- Lägga till och avsluta användare
- Orsaksgruppstabellen i Personec P 22.10
- Personec
- Personec lönestystem 3 mars 2021 - Handlingsplan - 2023-04-13
- Personuppgiftsbiträdesavtal Södertälje kommun Lönesystem TI 2014-1038 Visma AB
- Saas-anspassad System Management Versionsinformation Personec P 22.10
- Södertälje2302
- Tabinfo2302
- Testprotokoll Södertälje
- Uppdateringsförslag Feb 2023
- Varning och felsignaler på lön Personec P Version 22.10
- Versionsinformation Foundation 22.2

Försörjningsstödssystemet:

- 230509 Komplettering till EY
- Exempel användarlista
- Exempel meddelande om utskickad användarlista
- Formulär för behörighetsansökan Combine via ärendehanteringssystemet
- Generellt SLA Combine

- Granskning Södertälje kommun - Dokumentation Försörjningsstödssystemet kompl. 230421
- Leveransdokumentation Ekonomiskt bistånd nödprövning
- MALL Testunderlag myndighet Release 1.35
- MALL Testunderlag utförare Release 1.35
- Process vid programförändringar
- Rutin Behörighetsadministration
- Rutin för felundersökning av schemalagda jobb

Bilaga 3: Definitioner

Informationssäkerhet: Säkerhetsfrågor som berör information, oberoende av system och plattformar.

IT-säkerhet: Säkerhet som huvudsakligen relaterar till IT-infrastruktur, systemfrågor och konfigurering.

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

Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller ofta uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.

Tvåfaktorsautentisering (2FA): Extra lager av säkerhet som kräver mer än ett lösenord för att autentiseras till den interna miljön.