Granskning av behörighetsrutiner Treserva

Linköpings Kommun

Februari 2023

Martin Westholm

PwC

pwc

Revisionsrapport

Innehållsförteckning

pwc

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna genomfört en granskning av behörighetsrutiner kopplat till systemet Treserva, som används inom äldre-, handikapp- och individ- och familjeomsorgens myndighetsutövning och verksamheter inom Linköpings kommun. Syftet med granskningen har varit att utreda den interna kontrollen kring behörighetstilldelningen i Treserva samt hur lagar och interna riktlinjer följs i det avseendet, samt i vilken omfattning åtgärder bör vidtas för att uppnå en tillförlitlig behörighetsadministration.

Utifrån genomförd granskning är vår samlade bedömning att Treserva i all väsentligt uppfyller kraven på god intern kontroll inom de områden som granskats, men att det finns utvecklingsområden i enlighet med det som beskrivs i rapporten.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten eller det avslutande avsnittet "Samlad bedömning".

Frågeställningar	**Bedömning**
Följer behörighetsstrukturen gällande lagkrav?	Ja
Är behörighetsstrukturen ändamålsenlig utifrån de verksamheter de tjänar?	Ja
Finns behörighetsstrukturen dokumenterad?	Delvis
Fungerar rutinen för tilldelning/ändring av behörighet i Treserva och är den ändamålsenlig med tanke på risk för brister, dvs att obehöriga får tillgång till uppgifter i systemet?	Ja
Kontrolleras periodiskt att behörigheterna följer gällande rutiner?	Delvis
Behöver åtgärder vidtas för att åtgärda eventuella brister i behörighetsstrukturen samt rutinen för behörighetshantering?	Delvis

Rekommendationer

För rekommendationer gällande möjligheter att ytterligare stärka behörighetshanteringen i Treserva, se nedan samt det som nämns i respektive avsnitt gällande iakttagelser och rekommendationer.

1. *Följer behörighetsstrukturen gällande lagkrav?*

   - Vi rekommenderar att det tydliggörs i verksamhetsombudens riktlinjer för behörighetstilldelning att användarna ska få till sig denna information på ett strukturerat sätt. Det ligger ett stort ansvar på den enskilde användaren i detta och det måste vara tydligt vad lagen säger om detta och även eventuell påföljd vid överträdelse mot dessa riktlinjer.
   - Vi rekommenderar att funktionaliteten kring logghanteringen i Treserva ses över och att utdrag av loggar möjliggörs ute i verksamheten, hos utförarna. Loggförfarandet bör förenklas för att det ska vara praktiskt möjligt att följa kraven som finns på granskning av detta. Rutiner bör utarbetas som möjliggör utförande av loggkontroll en gång per år per användare som riktlinjerna stipulerar.

2. *Är behörighetsstrukturen ändamålsenlig utifrån de verksamheter de tjänar?*

   - Vi rekommenderar att det arbete som påbörjats kring mappningen av behörighetsuppsättningen slutförs. Det skulle ge en bättre bild av nuvarande uppsättning och hur väl den följer de faktiska behoven i verksamheten.
   - Vi rekommenderar att även Filter ses över i samband med dokumentationen av behörighetsstrukturen och att Filter som ej används tas bort eller inaktiveras i systemet för att förenkla arbetet med tilldelning av rätt behörigheter.

3. *Finns behörighetsstrukturen dokumenterad?*

   - Vi rekommenderar att arbetet med att kartlägga och dokumentera behörighetsuppsättningen i Treserva fortsätter och slutförs, att befintliga Profiler och Filter dokumenteras utanför systemet. Det bör finnas ett ägarskap för upprätthållande av en ändamålsenlig behörighetsstruktur i Treserva för att säkerställa detta över tid.
   - Vi rekommenderar även att riktlinjer utformas som tydliggör hur processen för ändring/tillägg av Profiler och Filter eller annan förändring av behörighetsstrukturen skall hanteras.

4. *Fungerar rutinen för tilldelning/ändring av behörighet i Treserva och är den ändamålsenlig?*

   - Vi rekommenderar att riktlinjerna kring behörighetstilldelningen för utförare förtydligas för att skapa en bättre förståelse för processen och det ansvar som ligger på verksamhetschefen på utförarsidan. Det bör tydligt framgå hur rutinen för behörighetstilldelning skall gå till samt även vilket ansvar som finns vad gäller avslut av behörighet.

- Vi rekommenderar även att införa en formaliserad rutin för avslut och byte av behörighet samt att införa periodiska genomgångar av tilldelade behörigheter i systemet.

5. *Kontrolleras periodiskt att behörigheterna följer gällande rutiner?*

- Vi rekommenderar att en förenkling av utförarnas loggkontroller utreds, som t ex möjliggör utdrag av loggar av verksamhetschefer på utförarsidan.
- Vi rekommenderar även att rutinbeskrivningen som beskriver hantering och granskning av loggar i Treserva tydliggörs för såväl utförarsidan som den interna organisationen hur detta regelmässigt och rutinmässigt skall skötas.

Inledning

Bakgrund

Verksamhetssystemet Treserva används inom äldre-, handikapp- och individ- och familjeomsorgens myndighetsutövning inom Linköpings kommun, samt inom utförandeverksamheten. Systemet behandlar känsliga data som personuppgifter och patientdata. Förutom Linköpings kommun använder även privata utförare systemet i sin verksamhetsutövning.

Brister i den interna kontrollen av behörighetsstrukturen i verksamhetssystemet innebär en risk att personuppgifter kan komma obehöriga tillhanda. Granskningen ska svara på om behörighetsstrukturen är ändamålsenlig och följer de legala kraven.

Revisorerna i Linköpings kommun ser i sin risk- och väsentlighetsbedömning att den interna kontrollen gällande behörigheter i Treserva är en viktig process att granska.

Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om behörighetsstrukturen i Treserva är ändamålsenlig och följer de legala kraven, med tillräcklig styrning och intern kontroll.

Följande revisionsfrågor har besvarats inom ramen av granskningen:

- Säkerställs att behörighetsuppsättningen i Treserva följer gällande lagkrav?
- Behöver åtgärder vidtas för att uppnå en behörighetsstruktur som följer ställda krav och är ändamålsenlig för verksamheten?

Frågeställningar

Den övergripande granskningen av behörighetsstrukturen i Treserva skall utreda följande frågeställningar:

- Följer behörighetsstrukturen gällande lagkrav?
- Är behörighetsstrukturen ändamålsenlig utifrån de verksamheter som omfattas?
- Finns behörighetsstrukturen dokumenterad?
- Hur fungerar rutinen för tilldelning/ändring av behörighet i Treserva och är rutinen ändamålsenlig med tanke på risk för brister, dvs att obehöriga får tillgång till uppgifter i systemet?
- Kontrolleras periodiskt att behörigheterna följer gällande rutiner?
- Behöver åtgärder vidtas för att åtgärda eventuella brister i behörighetstrukturen samt rutinen för behörighetshantering

Revisionskriterier

Nedan revisionskriterier utgör de bedömningsgrunder som har bildat underlag för revisionens analyser och bedömningar.

- Offentlighets- och sekretesslagen
- Patientdatalagen
- Lagen om behandling av uppgifter inom socialtjänsten
- Verksamheternas interna styrande dokument relevanta för granskningen

Avgränsning

Granskningen avser systemet Treserva för ovan nämnda verksamheter inom Linköpings kommun.

Metod

Granskningen har genomförts genom intervjuer med ansvariga tjänstemän och systemadministratörer inom berörda verksamheter inom Linköpings kommun, samt med systemleverantören. Granskning har även skett av aktuell lagstiftning inom området genom inläsning av lagtexter samt relevanta föreskrifter gällande dokumentation och informationshantering. Vi har även tagit del av de policys, rutiner och riktlinjer som finns inom Linköpings kommun i syfte att stämma av dessa mot förvaltningsrutinerna för Treserva. Vidare har relevant dokumentation kring behörighetsadministration samt behörighetsstruktur i Treserva inhämtats och granskats i syfte att verifiera det som framkommit under genomförda intervjuer.

De förhållanden som råder inom Linköpings kommun för drift och förvaltning av Treserva har sedan även jämförts med best practise gällande administration av behörigheter i syfte att ge ytterligare rekommendationer kring utvecklingsområden.

De intervjuade har sakgranskat och godkänt det faktamässiga innehållet i rapporten.

Granskningsresultat

Vad säger aktuell lagstiftning och föreskrifter?

I granskningen har ett antal lagar, föreskrifter och allmänna råd studerats för att se vilka krav lagstiftaren ställer samt vilka föreskrifter och allmänna råd Socialstyrelsen har utgivit utifrån gällande lagar.

Följande lagar reglerar området:

- Offentlighets och sekretesslag (2009:400)
- Personuppgiftslag (1998:204)
- Lag (2001:454) om behandling av personuppgifter inom socialtjänsten
- Lag (1993:387) om stöd och service till vissa funktionshindrade
- Socialtjänstlag (2001:453)
- Lag (1990:52) med särskilda bestämmelser om vård av unga
- Hälso- och sjukvårdslag (2017:30)
- Patientdatalag (2008:355)
- Patientsäkerhetslag (2010:659)

Följande föreskrifter är uppmärksammade rörande området:

- SOSFS 2014:5. Socialstyrelsens föreskrifter och allmänna råd om dokumentation i verksamhet som bedrivs med stöd av SoL, LVU, LVM och LSS
- SOSFS 2008:14. Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården

Iakttagelser

Enligt ***Personuppgiftslagen*** ska lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda personuppgifter utifrån den säkerhetsnivå som är lämplig utifrån tekniska möjligheter, kostnader, risker som behandling av personuppgifterna medför utifrån dess känslighet.

Inom hälso- och sjukvårdverksamhet sägs specifikt att behörighet ska begränsas till vad som är nödvändigt för att ge en god och säker vård och varje aktuell användare ska ges en individuell behörighet för åtkomst till patientuppgifter. Tilldelningen ska föregås av en behovs- och riskanalys. Det ska finnas rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheterna.

Vårdgivaren ska också ansvara för att det finns rutiner för att säkerställa att eventuell överföring (öppna system) av patientuppgifter görs på ett sådant sätt att ingen obehörig kan ta del av uppgifterna, och åtkomst till patientuppgifter föregås av stark autentisering."

Information om vilka vårdenheter som har uppgifter om en viss patient ska inte kunna göras tillgänglig utan att den behörige användaren gör ett aktivt val, dvs. gör ett ställningstagande till, om han eller hon har rätt att ta del av dessa uppgifter vilket ska följas av ytterligare ett val innan uppgifterna görs tillgängliga.

Är vårdgivaren ansluten till ett system för sammanhållen journalföring ska det framgår av systemet att det finns ospärrade patientuppgifter hos någon annan vårdgivare. Ett ansvar finns för att en behörig användares åtkomst till dessa ska föregås av att användaren gör ett aktivt val efter att ha hämtat in patientens samtycke till behandling av uppgifterna.

Det ska finnas en informationssäkerhetspolicy som ska säkerställa att patientuppgifter är åtkomliga och användbara för den som är behörig och att det i systemet ska vara möjligt att kunna härleda åtgärder till en identifierad användare. Den som inom kommunen är ansvarig för informationssäkerhetssystemet ska minst en gång om året till vårdgivaren rapportera om granskningar som gjorts enligt policyn, riskanalyser som har utförts avseende informationssäkerheten, och förbättringsåtgärder som har vidtagits.

Vidare ska det finnas rutiner som säkerställer att vid loggkontroller framgår vilka åtgärder som har vidtagits med patientuppgifterna, vilken vårdenhet och vid vilken tidpunkt åtgärderna har vidtagits, att användarens och patientens identitet framgår, att systematiska och återkommande stickprovskontroller av loggarna görs samt att de dokumenteras och sparas i minst tio år.

Verksamhetschefen ska ansvara för att utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med aktuella arbetsuppgifter, att befattningshavaren är informerad om de bestämmelser som gäller för hantering av patientuppgifter och att uppföljning av informationssystemens användning görs genom regelbunden kontroll av loggarna.

I föreskriften regleras också att en som arbetar för en vårdgivare eller som har slutit avtal med en vårdgivare ska ansvara för att personliga lösenord och hjälpmedel för autentisering inte kan bli tillgängliga för obehöriga, för att datorer eller andra informationsbärare inte lämnas utan att patientuppgifterna är skyddade från obehörig åtkomst och att hen endast får ta del av patientuppgifter om hen behöver uppgifterna för sitt arbete.

Vid handläggning av ärenden och genomförande av insatser enligt SoL, LVU, LVM och LSS ska handlingar som rör enskildas personliga förhållanden förvaras så att obehöriga inte får tillgång till dem. Handlingar ska sekretesskyddas från dem som inte har legitim anledning att ta del av handlingen i sin tjänsteutövning.

Informationssystem som används i verksamheten ska vara utformade så att integritetsskyddet tillgodoses, att en användares behörighet till uppgifter anpassas och begränsas till de behov som användaren har samt att åtkomsten till uppgifterna kan kontrolleras.

Det ska i efterhand gå att fastställa vilka personer som har tagit del av informationen genom så kallade loggkontroller. Dessa bör visa användarens identitet, datum och tid för åtkomst samt information om vilka uppgifter användaren har haft åtkomst till.

Nämnden bör utarbeta en rutin för regelbunden uppföljning av loggen och de anställda måste få information om loggning och uppföljning av loggen.

Efterlevnad av lagkrav och riktlinjer

Revisionsfråga 1: Följer behörighetsstrukturen gällande lagkrav?

Iakttagelser

Rutiner och riktlinjer på kommunal nivå har studerats och jämförts mot de ovan nämnda lagarna och regelverken..

Gällande social och omsorgsförvaltningen har följande rutiner och riktlinjer studerats:

- *Riktlinje för inhämtande av samtycke till sammanhållen journalföring*
- *Riktlinjer behörigheter i Treserva (arbetsmaterial)*
- *Behörighetstilldelning – chefer*
- *Behörighetstilldelning – hälso- och sjukvårdspersonal*
- *Behörighetstilldelning - verksamhetsombud*
- *Rutin för skyddade personuppgifter*
- *Rutin för loggkontroll - Treserva (arbetsmaterial)*

De rutiner som granskats avseende behörighetstilldelning i Treserva, samt riktlinjer för inhämtande av samtycke till sammanhållen journalföring bedöms i allt väsentligt följa gällande lagkrav. Det finns dock områden som bör åtgärdas och förtydligas för att säkerställa efterlevnad av lagar och riktlinjer generellt gällande Treserva.

Det gäller i huvudsak följande områden:

Åtkomst till information om brukare/klienter i Treserva; Åtkomst till brukare/klienter i Treserva styrs av ett filter som sätts på varje användare i systemet. Filtret innebär i de flesta fall att åtkomst medges till ett större antal klienter än de som användaren faktiskt arbetar med/är ansvarig för. Detta ställer stora krav på utfärdaren av behörigheten att informera om detta och exakt vad det innebär i eget ansvar, samt att användaren måste ta till sig och följa de riktlinjer som finns. Vår uppfattning efter genomförd granskning är att det på myndighet ges tillräcklig information kring detta samt att användaren signerar villkoren, men att det finns utrymme för att ytterligare tydliggöra det ansvar som ligger på enskild användare i systemet innan denne ges tillgång på utförarsidan.

Vi rekommenderar att det tydliggörs i verksamhetsombudens riktlinjer för behörighetstilldelning att användarna ska få till sig denna information på ett strukturerat sätt. Det ligger ett stort ansvar på den enskilde användaren i detta och det måste vara tydligt vad lagen säger om detta och även eventuell påföljd vid överträdelse mot dessa riktlinjer.

Rutin för utförande av loggkontroller; Rutinen för loggkontroller på myndighet och hos utförare bedöms ej hanteras enligt de krav som finns på att varje användare skall kontrolleras en gång per år. Det är i dagsläget en tidskrävande process, då utförare ej själva tar ut loggar från systemet utan måste begära ut det från IT-samordnarna på förvaltningen. Utdrag av loggar kräver även en sekretessprövning innan de lämnas ut, vilket ytterligare försvårar hanteringen.

Vi rekommenderar att funktionaliteten kring logghanteringen i Treserva ses över och att utdrag av loggar möjliggörs ute i verksamheten, hos utförarna. Loggförfarandet bör förenklas för att det ska vara praktiskt möjligt att följa kraven som finns på granskning av detta. Rutiner bör utarbetas som möjliggör utförande av loggkontroll en gång per år per användare som riktlinjerna stipulerar.

Personer som är förföljda och utsatta för hot eller våld kan få sina adress- och personuppgifter skyddade inom hela den offentliga förvaltningen enligt OSL. Sekretess gäller för uppgift som kan användas för att komma i kontakt med personen och kan också gälla för om den enskildes anhöriga, om det kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida allvarligt men om uppgiften röjs.

I Linköpings kommun läses uppgifter om sekretessmarkering in automatiskt i Treserva från Skattemyndigheten för att säkerställa att informationen alltid är uppdaterad i systemet, för att minska risken för fel i hanteringen. I verksamhetssystemet finns även möjlighet att manuellt lägga in en varning om att uppgifterna är sekretessmarkerade. Detta innebär att en varning aktualiseras i samband med åtkomst till akten.

Mottagning på myndighet har åtkomst till alla individer, även sekretessmarkerade, för att kunna se om de finns i systemet, medan utredning/uppföljning på myndighet behöver ansöka om specifika ärenden för att få tillgång till dem. Utförare får skicka in ansökan till IT-samordnare för att få access.

Inom äldreomsorgen används endast utförandewebben av omvårdnadspersonalen och där saknas idag möjligheten att se och hantera sekretesskyddade personer. De får uppdrag via post istället i det fall det behövs. ***Vi rekommenderar*** att möjligheten att se sekretesskyddade personer undersöks för att möjliggöra åtkomst till dessa i förekommande fall. I annat fall finns risken att dokumentationsplikten åsidosätts, om åtkomst till journaler ej är tillgänglig för omvårdnadspersonalen.

Bedömning

Följer behörighetsstrukturen gällande lagkrav och riktlinjer?

Ja, Behörighetsstrukturen följer i allt väsentligt gällande lagkrav.

Det finns dock brister som bör åtgärdas enligt det vi skriver ovan, vad gäller användarnas åtkomst till de individer som förekommer i Treserva, samt den brist som identifierats avseende utförande av loggkontroller.

Behörighetsstrukturens ändamålsenlighet

Revisionsfråga 2: Är behörighetsstrukturen ändamålsenlig utifrån de verksamheter som omfattas?

Iakttagelser

Den behörighetsstruktur som är uppsatt i Treserva idag har, som tidigare nämnts, satts upp vid implementationen av systemet och sedan löpande modifierats för att tillmötesgå kraven från verksamheten. Det innebär att behörigheterna löpande har blivit mer ändamålsenliga och anpassade till användarnas behov i arbetet.

Som vi skrivit ovan har dock dessa förändringar tidigare skett utan att dokumenteras och utan att man följt en fastslagen struktur eller formell process. Det har ökat risken för att behörigheten som är kopplad till Profiler och Filter löpande utvidgas, utan en fullständig analys av vad detta innebär i form av ökade möjligheter för användarna i systemet. Det kan innebära att vissa användare i dagsläget har en högre behörighet i systemet än vad deras ansvar är i verksamheten. Vid tiden för denna granskning har dock ett arbete påbörjats för att kartlägga och dokumentera behörighetsstrukturen i Treserva, vilket är positivt för möjligheten att bibehålla en bra struktur i systemet.

I detta arbete har vi inte haft möjlighet att granska ner på den detaljnivån det innebär att granska Profiler och Filter och mappa behörighetsuppsättningen mot rollbeskrivningar eller ansvarsfördelningen i verksamheten. ***Vi rekommenderar*** dock att det arbete som påbörjats kring mappningen av behörighetsuppsättningen slutförs, enligt det vi skriver i avsnittet nedan gällande dokumentation av behörighetsstruktur. Det ger en bättre bild av nuvarande uppsättning och hur väl den följer de faktiska behoven i verksamheten.

Vid tidigare utförd genomgång av Treserva (2015) noterade vi att det fanns ett stort antal Profiler uppsatta, ett betydligt större antal än de som faktiskt används, eller borde behövas, i verksamheten. Inom de olika verksamheterna som granskats (äldre-, individ- och familjeomsorg) används dock endast ett begränsat antal Profiler per verksamhet, vilket underlättar vid tilldelning av behörighet. Vi har i denna granskning noterat att en större rensning av Profiler har utförts under 2022 med syftet att gallra bort Profiler som ej används. Behörighetsstrukturen uppfattas som väl fungerande enligt de rutiner som finns inom de olika verksamheterna.

Vi rekommenderar att även Filter ses över i samband med dokumentationen av behörighetsstrukturen och att Filter som ej används tas bort eller inaktiveras i systemet för att förenkla arbetet med tilldelning av rätt behörigheter. Ett förslag är att göra en registerkörning i systemet för att se vilka Filter och Profiler som inte används och sedan bedöma om dessa skall tas bort.

Den generella behörighetsstrukturen i Treserva, som det fungerar idag, innebär att användaren vid en generell sökning i systemet även medges åtkomst till viss information gällande individer som inte ingår i de Filter användaren har behörighet till. Detta inträffar då en sökning på namn görs, då sökresultatet innehåller samtliga individer i systemet med det sökta namnet. Användaren kan då, medvetet eller omedvetet, klicka sig vidare på en individ man egentligen inte har systemmässig behörighet att komma åt och se uppgifter om dennes förekomst i Treserva. Åtkomst till journaler eller annan individspecifik information medges dock ej.

Vi rekommenderar att detta undersöks vidare tillsammans med systemleverantören och att en lösning utarbetas, då en användare får tillgång till mer information än denne har rätt till. Individer man ej har systemmässig behörighet till bör ej komma upp i det sökresultat som erhålls vid sökning. Alternativet är att sökning endast skall ske med hjälp av personnummer, vilket dock kan bli opraktiskt för användaren om den uppgiften ej är känd.

Ytterligare en faktor som idag gör att behörighetsstrukturen inte är helt ändamålsenlig är att de Filter som lagts in i systemet, dvs. de begränsningar som gäller tillgång till olika

enheter, oftast omfattar flera enheter. Det innebär att behörighet ofta tilldelas för flera enheter, även om användaren inom omsorgen endast arbetar på/har ansvar för brukare på en enhet. Det ger användaren systemmässig behörighet att se fler brukare än nödvändigt, även om riktlinjerna kring det egna ansvaret skall reglera detta.

Vi rekommenderar att dessa filter ses över för att utvärdera om det finns möjlighet att skapa ett 1-1 förhållande mellan Filter och enhet, eller på annat sätt göra en mer ändamålsenlig indelning av behörigheten till enheter/klienter i Treserva.

Bedömning
Är behörighetsstrukturen ändamålsenlig utifrån de verksamheter som omfattas?

Ja, behörighetsstrukturen är ändamålsenlig utifrån de verksamheter som omfattas.

Bedömningen motiveras av att den granskning vi gjort och att arbete redan inletts för att åtgärda de iakttagelser vi gjort i samband med granskningen. De iakttagelser vi gjort är kända av myndigheten och det finns vissa kompenserande kontroller, i form av t ex utbildningsinsatser och riktlinjer, som minskar risken som följer av dessa iakttagelser.

Dokumentation av behörighetsstruktur

Revisionsfråga 3: Finns behörighetsstrukturen dokumenterad?

Iakttagelser
Med behörighetsstruktur avses den uppsättning som gjorts i systemet som styr behörigheten för användare, till funktioner och brukare/klienter. Detta styrs i systemet av Profiler och Filter, vilket kopplas till användaren vid tilldelning av behörighet.

Dokumentation av behörighetsstrukturen är viktig för att möjliggöra en översikt av uppsättningen i systemet, för t ex IT-samordnare eller systemförvaltare/systemägare. Det gör det möjligt för personer utan access till Treserva att se över behörighetsstrukturen och dess ändamålsenlighet. Strukturen har satts upp vid implementationen av Treserva och har successivt byggts ut och omarbetats under åren, utan att detta löpande har dokumenterats. Detta minskar möjligheten att spåra de ändringar som gjorts och kan leda till att man till viss del tappar kontrollen över behörighetsstrukturen.

Dokumentation av behörighetsstrukturen i Treserva har dock påbörjats och är pågående vid tiden för vår granskning. Vi har tagit del av det arbetsmaterial som finns framtaget och bedömer att det utgör en bra start för arbetet med att dokumentera uppsättningen i Treserva.

Vi rekommenderar följande:

Dokumentation av behörighetsstruktur; Vi rekommenderar att arbetet med att kartlägga och dokumentera behörighetsuppsättningen i Treserva fortsätter och slutförs, att befintliga Profiler och Filter dokumenteras utanför systemet. Det bör finnas ett ägarskap för upprätthållande av en ändamålsenlig behörighetsstruktur i Treserva för att säkerställa detta över tid.

Dokumentationen av behörighetsstrukturen skall sedan hållas uppdaterad i takt med att strukturen i Treserva förändras, om t ex en Profil ändras eller läggs till. I dagsläget fördelas behörigheter av de centrala IT-samordnarna som varit med under en längre tid och känner till behörighetsstrukturen, men en extern dokumentation minskar det personberoende som finns idag och förenklar processen att lära upp nya IT-samordnare/behörighetsansvariga.

Spårbarhet avseende utförda förändringar; För att öka säkerheten i Treserva och minska risken för felaktig åtkomst bör samtliga ändringar som görs i behörighetsstrukturen sedan dokumenteras och föregås av ett formellt godkännande från behörighetsansvarig (systemägare eller annan utsedd person). Med förändringar i behörighetsstrukturen avses förändring/tillägg av Profiler eller Filter. Syftet med det är att få spårbarhet i de förändringar som görs och att förändringar ej ska göras utan att en viss analys av dess effekter gjorts. De ändringar som görs ska sedan loggas där det framgår vilken Profil/Filter som ändrats, vad ändringen avser samt vem som utfört ändringen. Vi har i vår granskning uppfattat att detta har påbörjats, att loggning av förändringar i behörighetsstrukturen görs löpande.

Utöver ovanstående bör ***riktlinjer utformas*** som tydliggör hur processen för ändring/tillägg av Profiler och Filter eller annan förändring av behörighetsstrukturen skall hanteras.

Bedömning

Finns behörighetsstrukturen dokumenterad?

Behörighetsstrukturen finns ***delvis dokumenterad***. Arbetet med det har påbörjats men behöver slutföras och sedan hållas uppdaterat då förändringar i strukturen sker.

Rutiner för hantering av behörigheter i Treserva

Revisionsfråga 4: Hur fungerar rutinen för tilldelning/ändring av behörighet i Treserva och är rutinen ändamålsenlig med tanke på risk för brister, dvs att obehöriga får tillgång till uppgifter i systemet?

Iakttagelser

För att över tid säkerställa en korrekt tilldelning av behörigheter, som är i linje med lagkrav och användarens ansvar i verksamheten, är det viktigt med en strukturerad och formaliserad process för godkännande och tilldelning av behörighet. Processen bör finnas dokumenterad och möjliggöra spårbarhet i de behörigheter som tilldelats.

Tjänstemän inom omsorgskontoret uppfattar att det finns väl beskrivna rutiner gällande tilldelning av behörighet i verksamhetssystemet. Dessa uppfattas som väl förankrade i verksamheten samt hos ansvariga chefer.

Övergripande fungerar processen så att ansvarig chef har att beskriva behov av behörighet och godkänna tilldelning av behörighet via en särskild digital beställningsrutin i ärendehanteringssystemet. Beslutet verkställs genom tilldelning av behörighet i Treserva av IT-samordnaren. Behörighet är alltid personlig och kopplas till personnummer. Behörigheter som tilldelas är i vissa fall tidsbegränsad, varefter behörigheten måste begäras om. Detta gäller personal inom utförarverksamheten (1 år)

samt vid tidsbegränsad anställning på myndighet (tidsbegränsning enligt anställningstid).

Vår genomgång visar på att det finns en beskriven och formaliserad process för tilldelning av behörighet på myndighetssidan, där ansvar finns beskrivet och formell digitaliserad rutin finns som används för godkännande och tilldelning av behörighet. Det saknas dock tydliga riktlinjer för utförare vad gäller tilldelning/ändring och avslut av behörighet då utföraren ansvarar för tilldelning av behörighet till den egna omvårdnadspersonalen.

Vi rekommenderar att riktlinjerna kring behörighetstilldelningen för utförare förtydligas för att skapa en bättre förståelse för processen och det ansvar som ligger på verksamhetschefen på utförarsidan. Det bör tydligt framgå hur rutinen för behörighetstilldelning skall gå till samt även vilket ansvar som finns vad gäller avslut av behörighet.

I anslutning till tilldelning av behörighet har vi i granskningen noterat att det för vissa användare läggs till behörighet till funktioner vid sidan av de Profiler som tilldelas användaren. Den typ av hantering skapar en större risk för att behörighetsuppsättningen blir mer svåröverskådlig i systemet och svårare att revidera/övervaka. Vi har dock förstått att risken för detta delvis hanteras genom att sätta tidsbegränsning på denna typ av tilläggsbehörighet, i de fall det finns en känd tidsbegränsning kopplat till det utökade ansvaret.

Utöver tilldelning av ny behörighet är formaliserade rutiner för ändring och avslut av behörighet viktigt för att upprätthålla en ändamålsenlig behörighetsuppsättning där användaren har behörighet som motsvarar det ansvar man har i verksamheten. Vi har i vår granskning noterat att det saknas en fullt fungerande rutin för avslut av behörigheter, vid såväl avslutad anställning som vid byte av ansvarsområde. Vi har dock noterat att det finns en informell årlig rutin där behörigheten användare som ej varit aktiva i Treserva under de senaste 6 månaderna avslutas.

Vid byte av ansvarsområde är det viktigt att gammal behörighet/profil avslutas och att enbart den profil som motsvarar nytt ansvar tilldelas, en rutin som inte alltid fungerar. Tidsbegränsning av behörighet uppväger till viss del risken med att felaktiga behörigheter ligger kvar i Treserva men fångar dock inte upp alla behörigheter i Treserva.

Med anledning av ovanstående ***rekommenderar vi*** följande;

- Inför formaliserad rutin för avslut och byte av behörighet. Detta kan göras genom ett samarbete med löneavdelning för verksamheter som myndigheten ansvarar för, samt genom att tydliggöra ansvaret för detta för utförare.

- Inför periodiska genomgångar av tilldelade behörigheter i systemet. Detta genom att lista på användare och deras behörighet skickas ut till ansvariga chefer med viss periodicitet, för genomgång och korrigering

- Tidsbegränsa behörigheten för ALLA användare i systemet, även befintliga användare som idag inte har en tidsbegränsad behörighet

- Använd alltid tidsbegränsning på tillfälliga behörigheter, då t ex en användare tillfälligt ges extra behörighet för att lösa vissa arbetsuppgifter under en begränsad period

Förutom behörighet finns en etisk kod och ett enskilt ansvar, ett ansvar som innebär att man inte tar del av journaler eller personuppgifter för individer man inte arbetar med. Som nyanställd får man information genom introduktionsutbildningen om vad som gäller angående sekretessgränser och det framgår även av den digitala behörighetsblanketten som signeras av myndighetspersonal samt av verksamhetschefer hos utförarna.

Bedömning

Hur fungerar rutinen för tilldelning/ändring av behörighet i Treserva och är rutinen ändamålsenlig med tanke på risk för brister, dvs att obehöriga får tillgång till uppgifter i systemet?

Ja, vår bedömning är att rutinen tilldelning och ändring av behörigheter i Treserva i allt väsentligt är ändamålsenlig. Det finns dock utrymme för förbättringar i hanteringen av bland annat avslut av behörigheter enligt våra rekommendationer ovan.

Periodisk kontroll av behörigheter

Revisionsfråga 5: Kontrolleras periodiskt att behörigheterna följer gällande rutiner?

Iakttagelser

Kontroll av att gällande rutiner för behörigheter i Treserva följs ska enligt lag genomförs en gång per år för varje användare i systemet. Detta ska då göras genom utdrag av logglistor från systemet där en användares alla aktiviteter framgår, bl a vilka individer användaren varit inne och tittat/skrivit på. Ansvaret för detta ligger på verksamhetscheferna, internt på myndighet alternativt på utförarsidan. På utförarsidan krävs att verksamhetschef begär ut logg från IT-samordnare på omsorgskontoret då de ej kan ta ut detta själva i Treserva.

Inom social- och omsorgsförvaltningen sker enligt uppgift interna loggkontroller enligt framtagna rutiner, dock ej i den utsträckningen så att alla användare kontrolleras en gång per år. Från utförarorganisationerna begärs i vissa fall stickprov för att göra loggkontroller. Detta uppfattas som ineffektivt och betungande då det ställer större krav på såväl verksamhetschefer som IT-samordnare på myndigheten.

Som vi noterat i avsnittet kring efterlevnad av lagkrav och riktlinjer ***rekommenderar vi*** att en förenkling av utförarnas loggkontroller utreds, som t ex möjliggör utdrag av loggar av verksamhetschefer på utförarsidan i syfte att möjliggöra loggkontroller en gång per år för alla användare. Alternativt bör riktlinjerna ses över, i det fall det inte är möjligt att uppfylla kraven.

Vi rekommenderar att rutinbeskrivningen som beskriver hantering och granskning av loggar i Treserva tydliggör för såväl utförarsidan som den interna organisationen hur detta regelmässigt och rutinmässigt skall skötas. Det krävs en enhetlig policy och en beskriven process för att loggkontroller ska kunna utföras på ett effektivt och kvalitativt sätt. I processen bör ingå en kontroll att policyn efterlevs, att ansvariga utför loggkontroll enligt gällande rutiner.

Det finns idag rutiner för hur en situation som innebär att en obehörig tagit del uppgifter användaren inte har rätt till, ska hanteras. Det finns en rutin för incidenthantering, vilket är viktigt för att hantera alla ärenden på ett likartat sätt. Det kan även vara en känslig fråga, vilket ytterligare ökar behovet för verksamhetschef eller annan ansvarig att ha en policy för hur dessa incidenter skall hanteras. Det är av stor vikt att det är tydligt hur en incident ska anmälas, hur den ska utredas och vilka eventuella följder en incident ska ha för den användare som obehörigen använt åtkomsten i Treserva. Detta har även ett värde för att förebygga obehörig insyn, om användarna känner till konsekvenserna av sitt handlande.

Bedömning

Kontrolleras periodiskt att behörigheterna följer gällande rutiner?

Vår samlade bedömning är att revisionsmålet ***delvis*** uppnås, vad gäller att behörigheterna kontrolleras för att säkerställa att de följer gällande rutiner. Det finns utvecklingsområden gällande frekvensen av loggkontrollerna samt utförande av periodisk uppföljning av behörigheter i Treserva.

Behöver åtgärder vidtas för att åtgärda eventuella brister i behörighetstrukturen samt rutinen för behörighetshantering?

Vår genomgång av hanteringen av behörigheter i Treserva visar på att det skett en förstärkning av behörighetsrutinerna under de senaste åren men att det finns fortsatt utvecklingspotential i hur behörigheter hanteras och hålls ändamålsenliga. I avsnitten ovan har vi infogat vår syn på de åtgärder som bör vidtas för att nå en strukturerad, säker och effektiv hantering av behörighetrelaterade rutiner kring Treserva och de processer systemet stödjer.

Samlad bedömning

Vår samlade bedömning är att revisionsmålet ***delvis*** uppnås. Vi ser att myndigheten i allt väsentligt uppfyller god intern kontroll gällande behörigheter i Treserva, men de rekommendationer vi avger i denna rapport bör beaktas för att nå upp till en god intern kontroll enligt best practise. Det finns utrymme för förbättring av rutiner i syfte att uppnå en bättre styrning av behörigheterna i Treserva.

Samlad bedömning

PwC har under januari - februari 2023 genomfört en granskning av behörighetsrutiner kopplat till systemet Treserva, som används inom äldre-, handikapp- och individ- och familjeomsorgens myndighetsutövning och utförandeverksamheten inom Linköpings kommun. Granskningen har genomförts genom intervjuer, genomgång av systemet Treserva samt granskning av dokumentation, lagar och riktlinjer.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning	
1. Följer behörighetsstrukturen gällande lagkrav?	**Ja** Behörighetsstrukturen följer i allt väsentligt gällande lagkrav baserat på vår granskning. Det finns dock vissa utvecklingsområden gällande åtkomst och loggkontroller.	
2. Är behörighetsstrukturen ändamålsenlig utifrån de verksamheter de tjänar?	**Ja** Behörighetsstrukturen är ändamålsenlig och uppfyller verksamhetens behov i allt väsentligt.	
3. Finns behörighetsstrukturen dokumenterad?	**Delvis** Behörighetsstrukturen finns delvis dokumenterad. Arbetet med det har påbörjats men behöver slutföras och sedan hållas uppdaterat då förändringar i strukturen sker.	
4. Fungerar rutinen för tilldelning/ändring av behörighet i Treserva och är den ändamålsenlig?	**Ja** Vår bedömning är att rutinen tilldelning och ändring av behörigheter i Treserva i allt väsentligt är ändamålsenlig. Det finns dock utrymme för förbättringar i hanteringen av bland annat avslut av behörigheter enligt våra observationer.	

5. Kontrolleras periodiskt att behörigheterna följer gällande rutiner?	**Delvis** Vår samlade bedömning är att revisionsmålet delvis uppnås, vad gäller att behörigheterna kontrolleras för att säkerställa att de följer gällande rutiner. Det finns utvecklingsområden gällande frekvensen av loggkontrollerna samt utförande av periodisk uppföljning av behörigheter i Treserva.	
6. Behöver åtgärder vidtas för att åtgärda eventuella brister i behörighetsstrukturen samt rutinen för behörighetshantering?	**Delvis** Vår samlade bedömning är att revisionsmålet ***delvis*** uppnås. Vi ser att myndigheten i allt väsentligt uppfyller god intern kontroll gällande behörigheter i Treserva, men de rekommendationer vi avger i denna rapport bör beaktas för att nå upp till en god intern kontroll enligt best practise.	

Datum 2023-03-01

Martin Westholm

Lena Salomon

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Linköpings kommun enligt de villkor och under de förutsättningar som framgår av projektplan från PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.