Granskning av behörigheter inom socialtjänstens IT-stöd

Revisionsrapport

Timrå kommun

KPMG AB

2017-09-12

Antal sidor 12

Antal bilagor 1

Timrå kommun
Granskning av behörigheter inom socialtjänstens IT-stöd

2017-09-12

Innehållsförteckning

1 Sammanfattning

Vi har av Timrå kommuns revisorer fått i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i socialtjänstens datoriserade verksamhetsstöd... Uppdraget ingår i revisionsplanen för år 2017.

Syftet med granskningen är att bedöma om socialnämnden har en ändamålsenlig styrning avseende behörigheter och med tillräcklig intern kontroll.

Vår sammanfattande bedömning är att det praktiska arbetet med behörigheter och loggkontroll sker på ett i huvudsak ändamålsenligt sätt, men att efterlevnad av styrdokument och föreskrifter är bristfällig samt att dokumentation behöver utvecklas inom flera områden.

Vi rekommenderar kommunstyrelsen:

— att nämndernas ansvar tydliggörs i berörda styrdokument (Informationssäkerhetspolicy samt VROB Förvaltning och drift av IT), se avsnitt 3.1.

— att fastställa obligatoriska utbildningar inom området samt följa upp att de genomförs för samtliga användare i kommunen, se avsnitt 3.2

Vi rekommenderar socialnämnden:

— att säkerställa att kraven i de kommunövergripande styrdokumenten uppfylls, se avsnitt 3.1.

— att tydliggöra dokumentationen av hur vårdgivaren uppfyller kraven gällande informationssäkerhet, se avsnitt 3.1.

— att se över behovet av kompetensstärkande åtgärder för att säkerställa ändamålsenlig ledning utifrån lagar, förordningar och styrdokument, se avsnitt 3.2.

— att tillse att en formaliserad och dokumenterad hantering av behörigheter tas fram som uppfyller såväl krav i styrdokument som socialstyrelsens föreskrifter, se avsnitt 3.3.

2 Inledning/bakgrund

Vi har av revisorerna i Timrå kommun fått i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i socialtjänstens datoriserade verksamhetsstöd.

Verksamheternas utveckling i en kommun har med åren blivit alltmer IT-beroende vilket innebär nya former av hot och risker. Behörighetsstyrning och åtkomstkontroll blir då i sammanhanget en viktig och central komponent i kommunens arbete med informationssäkerheten. Detta arbete innebär bland annat upprättande av rättigheter för användare så att dessa enbart får åtkomst till den information och de applikationer som de behöver i sitt dagliga arbete.

Timrå kommuns revisorer bedömer att det finns risk att brister i styrning och kontroll av behörigheter för att säkerställa en god informationssäkerhet. Revisorerna anser att det är väsentligt att otillåten tillkomst till information inte förekommer.

2.1 Syfte och revisionsfråga

Syftet med granskningen är att bedöma om socialnämnden har en ändamålsenlig styrning avseende behörigheter och med tillräcklig intern kontroll.

Vi har därför granskat

om det finns styrdokument som hanterar behörighetstilldelning

om kunskapen om och efterlevnaden av styrdokumenten är säkerställd

om ansvars- och arbetsfördelning inom organisationen är tydlig

om uppföljning och utvärdering av behörighetsstyrning och loggkontroll genomförs

2.2 Avgränsning

Granskningen är avgränsad att omfatta socialnämnden, samt i tillämpliga delar IT-enheten. Granskning omfattar inte val av autentiseringsmetoder.

2.3 Revisionskriterier

— Kommunallagen 6 kap 7 §

— HSLF-FS 2016:40

— Tillämpbara interna regelverk och policys

2.4 Ansvarig nämnd

Granskningen avser socialnämnden.

2.5 Projektorganisation/granskningsansvariga

Granskningen har utförts av Mikael Lindberg, kommunal revisor, under ledning av Lena Medin, kundansvarig och certifierad kommunal revisor.

Rapporten är saklighetsgranskad av Ingeborg Melin, förvaltningschef, Rose-Marie Dolk, IT-strateg, Ulrika Hedlund, MAS, samt Helen Peterzon, IT-samordnare.

2.6 Metod

Granskningen har genomförts genom:

— Dokumentstudier
— Intervjuer med berörda tjänstemän
— Registerkontroll verksamhetssystem

3 Resultat av granskningen

Granskningen har i huvudsak varit inriktad på socialförvaltningens verksamhetssystem Procapita. Se även bilaga 1 för en sammanställning över vilka IT-system som socialförvaltningen hanterar.

Utöver styrdokument inom kommunen finns föreskrifter från socialstyrelsen med särskild koppling till granskningen, Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården, samt Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete.

3.1 Styrande dokument

I det kommunövergripande styrdokumentet "Informationssäkerhetspolicy för Timrå kommun" (fastställd av kommunstyrelsen 2017-05-02) redovisas utgångspunkter (t ex lagar), mål, roller och ansvar samt generella krav. Enligt policyn har kommunstyrelsen det övergripande ansvaret för informationssäkerheten. Det operativa ansvaret är delegerat till kommunchefen. Vidare framgår att för prioriterade system (där Procapita är ett av tio prioriterade system) ska en GAP-analys med verksamhets- och riskanalys vara genomförd, och informationsklassning ska göras enligt systemet "KLASSA".

Policyn ska tillsammans med ett antal vägledande råd och bestämmelser (VROB) inom IT och informationssäkerhet styra kommunens informationssäkerhetsarbete. I styrdokumentet "Vägledande råd och bestämmelser – förvaltning och drift av IT inom Timrå kommun" (fastställd av kommunstyrelsen 2016-12-06) framgår mer detaljerad roll- och ansvarsfördelning samt krav och arbetsuppgifter. Av denna framgår att förvaltningschef är systemägare och ansvarig för IT-system som stödjer den egna verksamheten. Systemägaren är även informationsägare. Systemägaren utser systemförvaltare, som har ansvaret för den dagliga användningen av IT-systemet och ansvarar för systemförvaltning utifrån systemägarens direktiv. För större system ska två systemförvaltare utses. Vad gäller nämndernas ansvar uttrycks inget explicit om detta i styrdokumenten.

IT-forum (bestående av förvaltningschefer, systemförvaltare och centrala IT) har bl a till uppgift att besluta om strategi för IT-säkerhetsarbetet och kommunens säkerhetsinstruktioner efter underlag från IT-säkerhetssamordnaren. IT-säkerhetsamordnare utses av och är i dessa frågor direkt underställd kommunchefen samt har det operativa ansvaret för samordning av informationssäkerhetsarbetet. Denne ska bland annat stödja systemägarna i arbetet med risk- och sårbarhetsanalyser/GAP.

Gällande behörighetsadministration framgår att det är nödvändigt att administration av och regler för behörighetstilldelning är klart fastlagda och kända, samt ett antal riktlinjer för detta. Kraven för hur behörigheter ska hanteras ska finnas i GAP-analyserna, liksom även krav för loggning samt att systemägaren kan ställa krav på regelbunden analys av loggarna.

Ledningssystemet för systematiskt kvalitetsarbete ska innehålla de processer och rutiner som krävs för att vårdgivaren ska säkerställa kraven på informationssäkerhet. Vidare ansvarar vårdgivaren för att det finns en informationssäkerhetspolicy. Uppgifter från de intervjuade gör gällande att vårdgivaren inte formulerat en egen

informationssäkerhetspolicy utan att de kommungemensamma styrdokumenten enligt ovan tillämpas. Vidare framgår att kvalitetsledningssystemet inte uppfyller kraven gällande informationssäkerhet.

För närvarande finns ingen uppdaterad systemförvaltningsplan för Procapita. Vidare finns endast en systemförvaltare utsedd. Under hösten kommer en uppdaterad GAP- och riskanalys samt riskklassning av information att genomföras av kommunens prioriterade system, bl.a. Procapita.

Vår bedömning

Vi noterar att kommunstyrelsens men inte nämndernas ansvar anges i styrdokumenten.

Vi noterar att det finns flera kommunövergripande styrdokument inom området som bland annat ställer upp ett antal krav på aktiviteter med viss frekvens, men att detta inte efterlevs. Exempel på detta är att det endast finns en systemförvaltare gällande Procapita, vilket utgör en risk ur såväl säkerhets- som driftperspektiv. Andra exempel på brister är dokumenterade och uppdaterade systemägardirektiv, systemförvaltningsplaner, risk- och sårbarhetsanalyser (GAP) och informationsklassning.

Vi bedömer att det i dokumentationen saknas tydliggörande av hur vårdgivaren fullföljer krav gällande informationssäkerhet, dels gällande informationssäkerhetspolicy och dels avseende processer och rutiner gällande informationssäkerhet i kvalitetsledningssystemet.

Vi rekommenderar kommunstyrelsen att nämndernas ansvar tydliggörs i berörda styrdokument (Informationssäkerhetspolicy samt VROB Förvaltning och drift av IT).

Vi rekommenderar socialnämnden att säkerställa att kraven i de kommunövergripande styrdokumenten uppfylls.

Vi rekommenderar socialnämnden att tydliggöra dokumentationen av hur vårdgivaren uppfyller kraven gällande informationssäkerhet.

3.2 Kunskap om styrdokumenten

Av styrdokumentet "Vägledande råd och bestämmelser – förvaltning och drift av IT inom Timrå kommun" framgår att systemägaren ansvarar för

- Att de egna medarbetarna erhåller information och utbildning om innehållet i de riktlinjer (VROB) de är berörda av
- Att medarbetare, före tilldelning av behörighet, har tillräckliga kunskaper om de IT-system de behöver för de egna arbetsuppgifterna genom utbildning DISA (MSB informationssäkerhetsutbildning via webb) och VROB.

Vidare framgår av samma dokument att varje enskild medarbetare har ett ansvar att påtala det egna behovet av utbildning.

I samband med att personal anställs får denne underteckna en förbindelse att följa kommunens riktlinjer för informationssäkerhet, som sparas i personakten. I denna ingår att ta del av berörda VROB samt genomföra DISA vilket dock inte följs upp.

För närvarande pågår generell utbildning inom IT-säkerhetsområdet riktad till samtliga medarbetare inom kommunen, så kallad "Nano-utbildning". Den är upplagd i drygt 20 korta "lektioner", där man svarar på ett antal frågor efter att ha klickat på en länk i det automatiska mail som varje medarbetare erhåller för respektive lektion. Därigenom möjliggörs också uppföljning av bl.a. deltagandegrad. Vid intervjuer har framkommit att deltagandet hittills varit över förväntan, och en uppföljning kommer att göras inför eventuell fortsättning.

Vid intervjuer har framkommit att förståelse och kunskapsnivå gällande informationssäkerhet kan utvecklas i organisationen på alla nivåer, såväl nämnd som chefer och medarbetare. En bakgrund som nämns är den snabba utveckling som sker inom området som påverkar förutsättningarna, såväl tekniskt som regelverk.

Vår bedömning

Vi noterar att information och utbildning ska genomföras regelmässigt avseende nyanställda, och att "Nano-utbildningen" erbjuds samtliga medarbetare men att deltagande inte krävs.

Vi rekommenderar kommunstyrelsen att fastställa obligatoriska utbildningar inom området samt följa upp att de genomförs för samtliga användare i kommunen.

Vi rekommenderar socialnämnden att se över behovet av kompetensstärkande åtgärder för att säkerställa ändamålsenlig ledning utifrån lagar, förordningar och styrdokument.

3.3 Behörigheter

I dokumentet "Vägledande råd och bestämmelser – förvaltning och drift av IT inom Timrå kommun" framgår övergripande riktlinjer för behörighetsadministration.

- endast behörig användare anställd i kommunen, ges åtkomst till kommunens IT-system. Undantagsfall kan behörighet ges tillfälligt till leverantörer
- användares behörighet ska styras utifrån dennas arbetsuppgifter och efter beslut av chefen
- varje användare ska ha en personlig identitet bestående av login-id och lösenord. Lösenord ska bytas vid uppmaning efter 180 dagar.
- den som är tjänstledig eller av annan orsak har längre frånvaro skall ha sin identitet spärrad
- uppföljning och revidering av tilldelade behörigheter ska ske regelbundet av respektive systemförvaltare.

Krav för hur behörigheterna skall hanteras ska finnas i GAP-analyserna. Vid intervjuer framkommer att det inte finns beslutade och dokumenterade krav och rutiner gällande behörighetstilldelning inom socialförvaltningen.

Det praktiska tillvägagångssättet inom socialförvaltningen är att ansvarig chef beställer behörigheter på en blankett "Grundbeställning av behörigheter IT-system" till ansvarig behörighetsbeställare (BB). BB planerar upplägget utifrån vilken funktion den anställde innehar. Som en grund för behörigheter har BB upprättat en översikt som visar de olika funktioner som finns inom socialförvaltningen och vad de olika funktionerna har för åtkomst till olika delar av systemen. Analysgrund för tilldelning av behörigheter i form av behovs- och riskanalys finns inte dokumenterad, men bygger på praktiskt erfarenhet och är uppdelad på ca 50 funktioner.

BB beställer via mail, inloggning i domän, mailkonto samt hemkatalog, till servicedesk. Servicedesk lägger upp personen i AD samt meddelar uppgifterna till BB via mail. BB lägger upp den anställde i de system som socialförvaltningen hanterar och som beställts på blanketten Grundbeställning, och tilldelar roll och dataåtkomst till den anställde i det specifika systemet. BB beställer ev inloggning i andra system som ej socialförvaltningen är ansvarig för. BB fyller i inloggningsuppgifterna på blanketten Grundbeställning samt undertecknar och återsänder den tillsammans med dokumentet VROB Användare samt Förbindelse till den chef som beställt uppgifterna. Förbindelsen ska därefter undertecknas av den anställde och arkiveras i personalakten. Gällande omvårdnadspersonal sker ett liknande tillvägagångssätt, men där bl a dokument skickas hem till den anställde och ansvarig chef erhåller kopia på grundbeställning.

Avslut eller förändring av behörigheter ska ansvarig chef ansvara för att meddela till BB, t ex när personal slutar eller byter arbetsplats. BB (tillika IT-strateg) gör en kontroll kvartalsvis mot AD, och personer som inte finns med eller inte varit inloggade avslutas. Det finns sålunda ingen direkt koppling gentemot AD eller PA-system.

Någon ytterligare uppföljning eller utvärdering avseende behörighetsstyrning finns inte dokumenterad.

Vår bedömning

Vi noterar att det finns ett inarbetat tillvägagångssätt vid tilldelning av behörigheter och dataåtkomst, men det inte finns dokumenterat och att kunskapen i hög grad är personberoende vilket i sig är att betrakta som en säkerhetsrisk.

Vi rekommenderar socialnämnden att tillse att en formaliserad och dokumenterad hantering av behörigheter tas fram som uppfyller såväl krav i styrdokument som socialstyrelsens föreskrifter.

3.4 Loggkontroll

Socialförvaltningen har tagit fram en rutin för uppföljning av loggar gällande verksamhetssystem, gällande från 2017-01-01. Syftet med uppföljning av loggar är att säkerställa att socialförvaltningens pålitlighet gentemot medborgaren men även ge anställda en trygghet att genom loggen kunna styrka att åtkomst till informationen varit befogad. Ett särskilt informationsdokument har tagits fram för medarbetare som omfattas av rutinen för uppföljning av loggar. Rutinen beskriver tillvägagångssättet för loggkontroller och hur sådana kontroller ska dokumenteras.

Enligt rutinen så kombinerar tillvägagångsätten systematik och slumpmässighet i urval av loggar. Det innebär att två metoder för uppföljning används, dels månadsvisa

kontroller och dels stickprov. Grundprincipen är att överordnad chef genomför kontroller av direkt underställda. Som stöd har ett vägledande informationsmaterial tagits fram, samt utbildning genomförts med samtliga berörda granskare. Varje genomförd uppföljning ska dokumenteras i angiven protokollmall (en gemensam fil). Detta för att säkerställa att uppföljning görs regelbundet och att resultatet av uppföljningarna sparas. I protokollmallen redogörs för att uppföljning genomförts samt om avvikelser har förekommit eller inte. Varje avvikelse ska på något sätt undersökas och utredas. Exempelvis har IT-strategen fått i uppdrag att stödja chefer att göra närmare undersökningar som en följd av genomförda uppföljningar där avvikelse upptäckts.

IT-strategen har tidigare själv genomfört loggkontroller, som dokumenterats och samlats i pärm för respektive år.

Under flera år har den interna kontrollplanen omfattat kontrollmoment avseende loggar.

Vår bedömning

Vi noterar att en ny rutin för loggkontroll införts, och att loggkontroller även tidigare genomförts regelbundet och dokumenterats.

Vi bedömer att det finns ett systematiskt och dokumenterat arbete avseende loggkontroller.

KPMG, dag som ovan

Mikael Lindberg	Lena Medin
Kommunal revisor	Certifierad kommunal revisor

Bilaga: IT-system som hanteras inom socialförvaltningen

Namn	Typ av system	Användare av systemet	Inloggning
Procapita IFO	Verksamhets-system	handläggare, behandlare, arbetskonsulenter	single sign on
Procapita VOO	Verksamhets-system	biståndshandläggare, enhetschefer, omvårdnadspersonal, legitimerad personal	single sign on
Procapita BOU	Verksamhets-system	administratörer rektorer	single sign on
Mobipen	Kvittensverktyg hemtjänst	omvårdnadspersonal enhetschefer biståndshandläggare	lösenord
Lifecare Planering	planeringsverktyg hemtjänst	planerare enhetschefer	single sign on
HSA id	nationell katalog-struktur	alla system som kräver hsa-id samt siths-kort	
SITHS	Identitets-handling säker inloggning	biståndshandläggare, enhetschefer, legitimerad personal,omvårdnadspersonal, handläggare ifo	
Senior Alert	Bedömnings-verktyg fallrisker munhälsa mm	legitimerad personal	kräver siths
Palliativa Registret	stödsystem vård i livets slutskede	legitimerad personal	kräver siths
BPSD	demensregister	legitimerad personal samt undersköterskor	kräver siths
Lifecare Utförare Personlig Assistans	dokumentation och tidrapportering	personliga assistenter samt enhetschefer	kräver mobilt bankid
Prator	Vårdplanerings-verktyg	biståndshandläggare, legitimerad personal, enhetschefer	kräver siths
Pascal	Läkemedels-administration	legitimerad personal	kräver siths samt medarbetar-uppdrag i HSA

Nationell Patient-översikt	Informations-mängder från Landstingets hälso och sjukvårds-journal	legitimerad personal	kräver siths, medarbetar-uppdrag i hsa samt integration verksamhets-system