www.pwc.se

Revisionsrapport

Behörigheter och loggkontroll

Gällivare kommun

PerÅke Brunström, Certifierad kommunal revisor

Christer Marklund, revisionskonsult

April 2016

pwc

Innehåll

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Gällivare har PwC kommunal sektor genomfört en granskning av om socialnämndens och kommunstyrelsens arbete med behörigheter, åtkomster och loggkontroll i verksamhetssystemet hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Vår **sammanfattande revisionella bedömning** är att arbetet med behörigheter, åtkomster och loggkontroll i begränsad utsträckning sker på ett ändamålsenligt sätt, samt att den interna kontrollen är bristande.

Bedömningarna av kontrollmålen som ligger till grund för svaret på revisionsfrågan framgår av kapitel 3.

Rekommendationer:

- Kommunstyrelsen och socialnämnden ser över vilka styrande dokument inom området behörighetsstyrning och loggkontroll som är i behov av uppdatering.
- Kommunstyrelsen och socialnämnden säkerställer att upprättade styrdokument tillämpas på avsett sätt.
- Socialnämnden säkerställer att ansvars- och arbetsfördelningen inom området behörighetsstyrning och loggkontroll är känd och tillämpas inom hela organisationen.
- Socialnämnden säkerställer att nämndens verksamhet lever upp till krav på informationssäkerhet enligt patientdatalagen och socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården, SOSFS 2008:14.
- Socialnämndens verksamhet beaktar resultat av genomförd registeranalys i framtida arbete med behörighetsstyrning och loggkontroll i verksamhetssystemet.

2016-04-04

Hans Forsström	***PerÅke Brunström***
Uppdragsledare	*Projektledare*

1. Inledning

1.1. Bakgrund

Kommunens revisorer har med hänsyn till risk och väsentlighet bedömt det angeläget att göra en granskning inom området behörigheter och loggkontroll i socialnämndens verksamhetssystem. Revisionsobjekt är socialnämnd och kommunstyrelse.

Socialnämndens verksamheter har med åren blivit alltmer beroende av IT-stöd, vilket innebär nya former av hot och risker. Behörighetsstyrning och loggkontroll är en viktig del i arbetet med informationssäkerhet[1]. I detta ligger att upprätta och upprätthålla rättigheter för användare, så att dessa enbart får och har åtkomst till den information som behövs i det dagliga arbetet. En bristfällig styrning och kontroll inom området kan riskera att verksamheten inte bedrivs på ett ändamålsenligt sätt samt att känslig information sprids till icke behöriga.

1.2. Syfte och Revisionsfråga/-or

Syftet med granskningen är att bedöma om nämndens och styrelsens arbete med behörigheter, åtkomster och loggkontroll i verksamhetssystemet hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Följande revisionsfrågor besvaras i föreliggande granskning:

- Är styrningen i form av styrande dokument tillräcklig?
- Är ansvars- och arbetsfördelningen inom organisationen tillräckligt tydlig?
- Sker en tillräcklig uppföljning och utvärdering inom området?
- Är styrning och kontroll inom området tillräcklig för att skydda otillåten åtkomst till och spridning av känslig information?
- Vilken rapportering erhåller ansvarig nämnd/-er avseende informationssäkerheten i socialnämndens verksamhetssystem?

1.3. Revisionskriterier

- Kommunallag 6 kap. 1 § samt 6 kap. 7 §.
- Kommuninterna styrande- och redovisande dokument.

1.4. Avgränsning och Metod

I tid avgränsas granskningen huvudsakligen till år 2015. Granskningen omfattar verksamhetssystemet VIVA som används inom socialtjänstens område. Metoder som använts i granskningen är analys av adekvat dokumentation, intervjuer med systemförvaltare, behörighetsadministratör samt avdelningschef kvalitetssäkring och bemanning. Data har inhämtats från IT-stöd som därefter bearbetats genom en registeranalys[2]. Resultatet från registeranalysen framgår av separat bilaga. Berörda tjänstemän har haft möjlighet att sakgranska rapporten.

[1] Sekretess, riktighet, tillförlitlighet
[2] Transaktioner från flera IT-system bearbetas och analysera utifrån angivna förutsättningar.

2. Iakttagelser och bedömningar

2.1. Styrande dokument

Kommungemensamma styrdokument för informationssäkerhetsarbetet *ska* vara **informationssäkerhetstrategi, handlingsprogram för informationssäkerhet, informationssäkerhetsinstruktion för beredskap och drift samt för användare**. Strategin redovisar kommunfullmäktiges organisation och roller för informationssäkerhetsarbetet samt krav på riktlinjer för områden av särskild betydelse.

Socialförvaltningen utövar styrning inom området genom dokumenten **Riktlinje - förvaltning av verksamhetssystem, rutin för IT-användande** och **verksamhetsplan för IT.**

I syfte att styrka följsamhet till styrande dokument har även en registeranalys genomförts, se kapitel 2.5.

2.1.1. Iakttagelser

Styrning på politisk nivå

Handlingsprogram för informationssäkerhet redovisar det ansvar som ingår i olika roller, riktlinjer som gäller för områden av särskild betydelse, regler för systemutveckling, systemunderhåll och incidenthantering. Dokumentens målgrupp är förvaltningsledning, systemägare och beskriver intern organisation för informationssäkerhetsarbete, förvaltningarnas ansvar, hur informationssäkerhetsarbete ska bedrivas samt aktuella krav. Programmet ska kompletteras av informationssäkerhetinstruktion för användare och för beredskap och drift. Målgrupp för dokumenten är samtliga medarbetare samt IT-driftansvariga. Vi noterar att informationssäkerhetsinstruktion för beredskap och drift *inte* är framtagen.

- Socialnämnden har inte säkerställt att det i nämndens ledningssystem för kvalitet finns en dokumenterad informationssäkerhetspolicy. Av intervjuer framkommer att det inte är tydligt om kommungemensamma styrdokument även utgör nämndens informationssäkerhetspolicy. De kommungemensamma styrdokumenten är inte en del av nämndens ledningssystem för kvalitet.
- Hur kommunstyrelsen och socialnämnden arbetat för att implementera ovan nämnda styrdokument har inte kunnat styrkas.

Styrning på förvaltningsnivå - socialförvaltningen

- Införandet av verksamhetssystemet VIVA påbörjades under 2012. Systemet är per 2015 inte leveransgodkänt, då införandet pågår.
- Riktlinje - förvaltning av verksamhetssystem är beslutad av förvaltningen 2015. Syftet med riktlinjen är att säkerställa god vård- och omsorg och integritet för brukarna. Av riktlinjen framgår systemägarens ansvar, systemförvaltarens ansvar, förvaltningsgruppens uppdrag, samt vilket uppdrag verksamhetens personal har.

- Rutin för IT-användande är beslutad av förvaltningen 2008. Rutinen innehåller allmänna regler, ansvar- och arbetsfördelning mellan chef och administratör samt tillvägagångssätt – arbetssätt. Av intervjuer framgår att dokumentet utgör huvudsakligt styrdokument för behörighetsstyrning, fastän informationen i dokumentet inte är fullt ut aktuell 2015.

För 2015 finns en verksamhetsplan för IT. Verksamhetsplanen består av två delar, systemförvaltning och support/behörigheter.

Av verksamhetsplan för systemförvaltning går följande uppdrag att utläsa:

- Att ta fram rutiner/riktlinjer för logghantering till verksamhetssystemet är prioriterat
- Förvaltningens ledningsgrupp har beslutat att all behörighetsadministration ska utföras av avdelningen kvalitetssäkring och bemanning
- Behörighetsadministration ska effektiviseras och kvalitetssäkras. En processbeskrivning som inkluderar hantering av alla personal, ordinarie, vikarie, via bemanningsföretag ska genomföras. Av intervjuer framgår att ovan nämnd rutin för IT-användande inte omfattar dessa grupper.
- Systemsäkerhetsplan[3] ska skrivas för verksamhetssystemet.

Av verksamhetsplan för support/behörighet går följande uppdrag att utläsa:

- Dokumentera antal behörighetsbeställningar och administrera behörigheter.

Om behörighetskontroll i styrande dokument

För att styra användarens åtkomst och säkerställa att endast behöriga användare förekommer i kommunens informationssystem ska beställning och borttagande av åtkomst till informationssystem ske på elektronisk blankett. Systemägare eller systemförvaltare fyller i och skickar blanketten till kommunens IT-enhet. Blanketten ska sparas hos både beställaren och IT-enheten. Samma blankett ska användas när konsulter eller andra utför arbete i informationssystem.

- Medarbetare ska informeras och utbildas i informationssäkerhetens betydelse för verksamheten, samt innehållet i informationssäkerhetsstrategin och informationssäkerhetsinstruktion för användare, i samband med anställning.
- Medarbetare ska informeras om att de behörigheter som tilldelas beror på arbetsuppgifter och avgörs av närmaste chef.

En behörighetsstruktur finns upplagd i verksamhetssystemet VIVA. Medarbetare med samma roll ska ha samma behörigheter. Medarbetare kan ha utvidgade behörigheter p.g.a. krav på viss specialistfunktion. Medarbetare får en behörighetsprofil kopplad till roll samt arbetsplats/-er. Behörighetsstrukturen har arbetas fram inom förvaltningen i samarbete med systemleverantören. Av intervjuer framkommer att det finns behov av att tydliggöra nuvarande behörighetsstruktur inom förvaltningen.

[3] Systemsäkerhetsanalys innebär att kartlägga kraven på sekretess, riktighet och tillgänglighet samt avstämma kraven mot befintlig IT-säkerhetsnivå på prioriterade IT-system. Systemsäkerhetsanalys är en förutsättning för att kunna fastställa basnivån för informationssäkerhet i en organisation.

Om loggkontroll i styrande dokument

I informationssäkerhetsinstruktion för användare informeras om att den enskilde användaren lämnar spår efter sig vid inloggning och arbete i IT-system. Loggningsfunktioner som finns i systemen ska användas för spåra obehörig åtkomst. Detta för att skydda informationen och för att undvika att oskyldiga misstänks om oegentligheter inträffar. I vilken utsträckning medarbetare informerats om att loggning kan ske, kan inte styrkas.

Något systematiskt arbete med loggkontroll i verksamhetssystemet VIVA har inte genomförts under 2015. Det finns inget styrdokument för loggkontroll som tillämpats inom socialnämndens verksamheter under 2015. Loggkontroller skulle kunna genomföras på förekommen anledning. Ingen loggkontroll har genomförts på förekommen anledning under 2015. Av intervjuer framkommer att det inte är tydlig inom organisationen att första linjens chefer förväntas initiera loggkontroller.

Sammanhålla akter

Verksamhetens brukare har sammanhållna personakter i verksamhetssystemet. Det innebär att alla insatser dokumenteras i samma akt. Det innebär alltså att mottagare av vård- och omsorgsuppdraget, chefer och legitimerad HSL-personal, tilldelas höga behörigheter. Höga behörigheter sätts för att säkerställa att framförallt legitimerad personal alltid har tillgång till den information som kan behövas för att utföra uppdraget. Av intervjuer framkommer att det förs en intern diskussion på förvaltningen om för och nackdelar med sammanhålla akter, utifrån perspektiven behörighetsstyrning och loggkontroll.

2.1.2. Bedömning

Styrning i form av styrande dokument är i begränsad utsträckning tillräcklig. Bedömningen baseras på att socialnämnden inte säkerställt att behörighetsstyrning, och framförallt loggkontroll, regleras av styrande dokument i tillräcklig utsträckning. Bedömningen baseras även på att socialnämnden inte säkerställt att det finns en dokumenterad informationssäkerhetspolicy. Det kan inte styrkas att beslutade styrdokument tillämpas i tillräcklig utsträckning. Vi noterar att vissa styrdokument är i behov av uppdatering. Vi noterar också att ett antal utvecklingsområden är identifierade i verksamhetsplan för IT.

2.2. Ansvars- och arbetsfördelning

Övergripande ansvarsfördelning för kommunens informationssäkerhetsarbete framgår av aktivitetsplan för säkerhetsarbete i **handlingsprogram för informationssäkerhet.** Ansvars- och arbetsfördelning på socialförvaltningen finns beskrivet i **riktlinje förvaltning av verksamhetssystem, rutin IT-användande på socialförvaltningen, samt rutin för användarstödjare verksamhetssystem.** Ansvars- och arbetsfördelning inom avdelning kvalitetssäkring och bemanning uppfattas tydlig avseende behörighetsstyrning.

Förvaltningen av verksamhetssystemet sköts av systemägare och en förvaltningsgrupp[4]. Gruppen leds av systemförvaltare och består av representanter från hela förvaltningen, t.ex. myndighetsutövning, medicinskt ansvarig sjuksköterska och användarstödjare.

2.2.1. Iakttagelser

Ansvarsfördelning på politisk nivå

Kommunstyrelsen är ytterst ansvarig för att kommunen har en god säkerhet och för att lagar, förordningar och de olika policydokumenten efterlevs. Kommunstyrelsen är övergripande ansvarig för kommunens IT-system. Operativt ansvar för varje enskilt IT-system uppfyller verksamhetens krav följer linjeorganisationen.

- Kommunstyrelsen fattar de avgörande besluten hur informationssäkerhetsarbetet ska bedrivas och har det övergripande ansvaret för informationssäkerheten.
- Socialnämnden är ansvarig för informationssäkerheten inom sin verksamhet, och att det bedrivs enligt fastställda mål i kommunen.
- Av verksamhetsplan 2015-2017 framgår att socialnämnden ansvarar för socialregistret[5].
- Socialnämnden är systemägare till socialtjänstens verksamhetssystem. Systemägare fattar beslut om införande, drift, förvaltning och avveckling av systemet samt utser systemförvaltare.

Ansvarsfördelning på förvaltningsnivå - förvaltningsgemensam ansvarsfördelning

Centrala IT-gruppen[6] ska på uppdrag av kommunledningen, hantera och utreda generella frågor avseende anskaffning, drift, förvaltning och avveckling av informations-hanteringsresurser inklusive frågor om informationssäkerhet.

- På uppdrag av kommunstyrelsen ska informationssäkerhetschefen arbeta med övergripande planering, samordning och uppföljning av internt arbete med informationssäkerhet på förvaltningsnivå. Informationssäkerhetschefen har en roll som intern revisor för att säkerställa att de av kommunfullmäktige fastställda målsättningarna i informationssäkerhetsfrågor efterlevs. Något resultat av internrevisionen kan inte styrkas.
- Kommunens personalenhet ansvarar för att nya medarbetare ges grundläggande informationssäkerhetshetsutbildning före tilldelning av behörigheter. Av intervjuer framkommer att rutinen inte tillämpas.

[4] Uppdrag: Initiera behov av ny eller ändrad funktionalitet. Hantera inkomna önskemål och/eller krav på ny eller ändrad funktionalitet från verksamheterna. Granska att inkomna önskemål och/eller krav är i enlighet med gällande lagstiftning och socialtjänstens riktlinjer samt att dessa ger ett ökat mervärde för brukarna. Meddela leverantören behov av ny funktionalitet i systemet. Skapa beslutsunderlag till systemägare för funktionalitet som kräver separat beställning till leverantören och/eller övriga kostnader.

[5] Kommunen har ett socialregister, där uppgifter som ligger till grund för beslut registreras i en personakt. Allt som dokumenteras i socialregistret betraktas som "känsliga uppgifter" och är starkt sekretessbelagt.

[6] Består av ansvariga för kommunens olika verksamheter, IT-chefen samt informationssäkerhetschefen.

- Systemägare[7] ansvarar för att användarhandledning för aktuellt system finns, samt att medarbetare har tillräckliga kunskaper om säkerhetsreglerna för de informationssystem de behöver för utförandet av egna arbetsuppgifter.
- För informationssystemens loggar ska systemägaren besluta hur ofta de ska analyseras, vem som ansvarar för analyser av dem, hur länge de ska sparas och hur de ska förvaras. Som framgår av kapitel 2.1 har detta inte gjort för socialnämndens verksamhetssystem.
- Detaljerad information samt anvisningar för användning och övervakning av loggfiler ska tas fram av kommunens IT-enhet.
- Chefer på alla nivåer ska ha kunskap om hur säkerhetsarbetet ska bedrivas och personalen ska ha nödvändig utbildning.
- Alla medarbetare förväntas ha ett säkerhetsmedvetande. Som enskild användare i kommunens informationssystem har medarbetare en del i ansvaret för säkerheten i informationshanteringen.

Ansvarsfördelning socialförvaltningen

Socialförvaltningens ledningsgrupp ansvarar för att politiska säkerhetsmål och riktlinjer förankras och efterlevs i verksamheten.

- I förvaltningen företräds systemägare av avdelningschef kvalitetssäkring och bemanning.

Avdelningen kvalitetssäkring och bemanning ansvarar bl.a. för att:

- nyanställd personal vid introduktion undertecknar och godkänner ”Förbindelse för IT-användare på Gällivare socialförvaltning
- dokumentera alla medarbetares användarnamn
- blanketter och dokument är korrekta och uppdaterade
- utbilda och/eller tillhandahålla information till användarstödjare då nya eller ändrade funktioner tillförs i systemet, samt hålla årliga nätverksträffar.

Systemförvaltare ansvarar för den dagliga driften av verksamhetssystemet i samverkan med kommunens IT-enhet och systemadministratörer. Systemförvaltare ansvarar för uppdraget, i verksamhetsplan för IT, att ta fram rutiner/riktlinjer för logghantering till verksamhetssystemet VIVA.

Support- och behörighetsadministratör ansvarar för att lägga upp/avsluta behörigheter i samtliga programvaror inom förvaltningen enligt rutin/riktlinjer, samt tillhandahålla användarmanualer på uppdrag av systemförvaltare/systemägare.

Användarstödjare verksamhetssystem ska ge den egna professionen, t.ex. undersköterskor, kunskap om hur verksamhetssystemet ska användas. Uppdraget som användarstödjare innebär bl.a. att:

[7] Systemägaren företräds på förvaltningsnivå av förvaltningschef eller avdelningschef.

- Handleda kollegor i hur de ska dokumentera, handleda kollegor i användandet av verksamhetssystemet, introducera/lära upp ny personal, utbilda kollegor i nya funktioner/förändringar i verksamhetssystemet, samla in synpunkter och önskemål från verksamheterna.

Linjechefer ansvarar för att skicka ifylld och underskriven blankett ”IT-användare socialförvaltningen”[8] till avdelningen kvalitetssäkring och bemanning. Chef ansvarar för att vid avslut, inaktivering eller förändring skicka in en ny blankett till avdelningen. När anställning upphör ska användare avslutas[9], vid frånvaro längre än tre månader ska användare inaktiveras. Av intervjuer framkommer att rutinen inte tillämpas fullt ut och att chefer behöver mer stöd i att beställa aktivering, förändring eller avslutning av behörigheter.

Det finns idag ingen koppling mellan att en medarbetare avslutas i kommunens AD[10], PA-system och avslut i verksamhetssystemet. Personer som inte längre är anställda, som inte har tillgång till kommunens IT-miljö, kan ändå vara registrerade som aktiva användare i verksamhetssystemet VIVA. Det innebär att kostnaden för användaren kvarstår.

Arbetsfördelning socialförvaltningen

Av rutin IT-användande framgår bl.a.:

- vilken verksamhet inom förvaltningen som ska göra alla upplägg och avslut av användare i verksamhetssystemet, vilken blankett som ska användare för upplägg och avslut av användare
- att linjechef beslutar om tilldelning av användare och att avdelningen kvalitetssäkring och bemanning arbetar på beställning av chefer i verksamheten.

Av granskningen framkommer avdelningen kvalitetssäkring och bemanning tillämpar kvalitetsledningssystemets rutin för avvikelsehantering vid avvikelser i arbetet med behörighetsstyrning.

2.2.2. Bedömning

Ansvars- och arbetsfördelning inom organisationen är inte tillräckligt tydlig. Bedömningen baseras på att ansvars-och arbetsfördelning inom behörighetsstyrning och loggkontroll i rimlig grad regleras av styrande dokument, framförallt inom avdelningen kvalitetssäkring och bemanning. Av intervjuer framkommer dock att den ansvars- och arbetsfördelning som är beslutad inte tillämpas fullt ut. Av granskningen framkommer också att den ansvars- och arbetsfördelning som tillämpas i praktiken inte fullt ut framgår av styrande dokument.

[8] Ska innehålla information om upprättad, namn, personnummer, yrkesroll, anställd i verksamhet, behörighet till vilka verksamheter, användarnamn, vem som är ansvarig chef.
[9] behörigheter i informationssystem tas bort
[10] Active directory

2.3. Uppföljning- och utvärdering

2.3.1. Iakttagelser

- Någon uppföljning eller utvärdering av behörighetsstyrning och loggkontroll har inte redovisats till socialnämnden under 2015.
- Av avdelningen kvalitetssäkring och bemannings delårsrapport 2015 framgår att avdelningen tagit fram en tidsplan för övertagande av behörighetsadministration för samtliga programvaror, verksamhetssystem, och kvalitetsregister.

Förvaltningsintern uppföljning av uppdrag i verksamhetsplan för IT visar att i *perioder* har:

- Rutin för upplägg av nyanställda brustit. Inga behörigheter i användarnas system har kunnat läggas upp. Nyanställda har inte haft tillgång till de system som behövs för att utföra sitt uppdrag. Patientsäkerheten och tryggheten för brukare inom socialförvaltningen brister.
- Tillgång till nätverket har varit föremål för stora driftstörningar. Personal har inte kunnat logga in i verksamhetssystem.
- Systemsäkerhetplan för VIVA är påbörjad.
- Mall för dokumentation av behörighetsbeställningar är framtagen i syfte att kvalitetssäkra behörighetsstyrningen.

Hur egenkontroll genomförs för att säkerställa att verksamheten lever upp till de krav på informationssäkerhet som ställs i patientdatalagen och Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården har inte kunnat strykas.

Avvikelser i arbetsprocessen, t.ex. att rutin för IT-användande inte följs, rapporteras till förvaltningens ledningstupp.

2.3.2. Bedömning

Uppföljning och utvärdering inom området är i begränsad utsträckning tillräcklig. Bedömningen baseras på att ingen uppföljning eller utvärdering har redovisats till socialnämnden under 2015. Bedömningen baseras också att det inte följts upp eller utvärderats om socialnämndens verksamhet lever upp till krav på informationssäkerhet i patientdatalagen och SOSFS 2008:14. Vi noterar att uppdrag i verksamhetsplan för IT följs upp samt att avvikelser från rutin för IT-användande rapporteras inom förvaltningen.

2.4. Styrning och kontroll

Beslutade styrdokument tillämpas inte i tillräcklig utsträckning. Beslutad ansvars- och arbetsfördelning tillämpas inte i tillräcklig utsträckning. Uppföljning och utvärdering inom området är i begränsad utsträckning tillräcklig.

2.4.1. Iakttagelser

- Under 2015 har det inte framgått av något kvalitetsledningssystem hur arbetet med behörighetsstyrning och loggkontroll ska bedrivas.

- Inga loggkontroller har genomförts under 2015.
- Något kontrollmoment i socialnämndens internkontrollplan 2015 som rör området behörigheter och loggkontroll finns inte.

2.4.2. *Bedömning*

Styrning och kontroll inom området är otillräcklig. Bedömningen baseras på att det inte framgår av socialnämndens kvalitetsledningssystem hur arbetet med behörighetsstyrning och loggkontroll ska bedrivas, något kontrollmoment i nämndens internkontrollplan finns inte, nämnden har inte begärt eller fått någon uppföljning eller utvärdering inom området under 2015. Det kan inte styrkas att styrning och kontroll inom området är tillräcklig för att skydda otillåten åtkomst till och spridning av känslig information, då någon loggkontroll inte genomförts av verksamhetssystemets händelselogg under 2015.

2.5. *Resultat från registeranalys*

Som tidigare noterats tillämpas inte styrande dokument avseende behörigheter och loggkontroll på avsett vis. För att bedöma eventuella konsekvenser av dessa brister har en registeranalys genomförts. Målsättningen har varit att jämföra uppgifter ur kommunens personal-/anställningsregister med uppgifter ur verksamhetssystemet Vivas användar-register och händelselogg. Uppgifter från händelseloggen är avgränsat till perioden vecka 1-10 2015. För att göra registerkontroller krävs ”nycklar” mellan posterna i filerna. Exempel på ”nycklar” som används vid dessa kontroller är personnummer eller användaridentitet som är unika för fysiska personer. Vi har i denna revision tvingats använda namn-fält i de olika registren vilket medför en viss osäkerhet i vårt granskningsresultat.

2.5.1. *Iakttagelser*

Kontrollmål	**Resultat**
Finns användare i verksamhetssystemets händelselogg som inte finns i anställningsregistren?	277 personer som skapat poster i händelseloggen kan inte matchas mot PA-systemets anställningsregister. Vi noterar att 11 personer i PA-systemets anställningsregister saknar användar-id. Användar-id finns i verksamhetssystemet, det utgörs av samma id som i PA-systemet i de fall användaren är en fysisk person. I verksamhetssystemet finns dock id:n som inte kan kopplas till en person.
Finns personer med brukbar användaridentitet i verksamhetssystemet som inte har använts enligt händelseloggen	Det finns 1 483 personer i Vivas användarregister. 869 av dessa har inte använts under den granskade perioden.
Finns testidentiteter i händelseloggen?	Nej. I händelseloggen finns 614 unika namn som synes vara verkliga namn och inte testidentiteter.

Finns andra identiteter än testidentiteter i händelseloggen som inte kan kopplas till en användare? Vilka identiteter genererar huvuddelen av alla avtryck i händelseloggen?	Ja, t.ex. finns två olika ordförande för socialnämnden, tre olika identiteter för vice ordförande i socialnämnden. Sex funktioner, olika ärendefördelare, finns även upplagda som identiteter. Dessa identiteter kan inte matchas mot PA-systemets anställningsregister. 433 325 händelser är utförda av 614 unika namn. I genomsnitt orsakar varje användare 705 poster i händelseloggen. Mest poster av en användare är 13 928 och det finns 2 namn som orsakar fler än 10 tusen poster. Dessa användare är systemförvaltare och biståndshandläggare. Tio användare orsakar 5 eller färre poster.
Finns användare som enbart läst, ej tillfört information (söka, titta, utskrift)?	Informationen finns inte tillgänglig.

2.5.2. Kommentar

Registeranalysen har genomförts för att styrka att styrande dokument avseende behörighetsstyrning och loggkontroll tillämpas på avsett vis. Vår förhoppning är att resultatet från registeranalysen, tillsammans med iakttagelser i kapitel 2.1-2.4, kan användas som underlag för socialförvaltningen i det fortsatta arbetet med behörighetsstyrning och loggkontroll. Nedan ges exempel på resultat som kan motivera en fördjupad undersökning:

- 869 av 1 483 användaridentiteter i verksamhetssystemet har inte använts.
- Ett antal andra identiteter som inte kan kopplas till en användare har identifieras.
- För att åstadkomma en effektiv kontroll av loggar och behörigheter bör förvaltningen säkerställa att den i framtiden kan ta fram och jämföra uppgifter ur kommunens personalregister, med uppgifter ur verksamhetssystemet Vivas användarregister och händelselogg.
- Vi noterar att den unika nyckeln mellan PA-systemet, verksamhetssystemets användarregister och händelseloggen skulle kunna vara användar-id. För att kunna göra egna registeranalyser i framtiden är det av vikt att kommunen alltid registrerar användar-id i PA-systemet och verksamhetssystemet, samt rensar bort användar-id som inte kan kopplas till en användare.

3. Bedömningar

3.1. Bedömningar mot kontrollmål

Kontrollmål	Kommentar
Styrande dokument	Styrning i form av styrande dokument är i begränsad utsträckning tillräcklig. Bedömningen baseras på socialnämnden inte säkerställt att behörighetsstyrning, och framförallt loggkontroll, regleras av styrande dokument i tillräcklig utsträckning. Bedömningen baseras även på att socialnämnden inte säkerställt att det finns en dokumenterad informationssäkerhetspolicy. Det kan inte styrkas att beslutade styrdokument tillämpas i tillräcklig utsträckning. Vi noterar att vissa styrdokument är i behov av uppdatering. Vi noterar också att ett antal utvecklingsområden är identifierade i verksamhetsplan för IT.
Ansvars- och arbetsfördelning.	Ansvars- och arbetsfördelning inom organisationen är i begränsad utsträckning tydlig. Bedömningen baseras på att ansvars- och arbetsfördelning inom behörighets-styrning och loggkontroll inte i tillräcklig utsträckning regleras av styrande dokument. Av intervjuer framkommer att den ansvars- och arbetsfördelning som är beslutad inte tillämpas fullt ut. Av granskningen framkommer också att den ansvars- och arbetsfördelning som tillämpas i praktiken inte fullt ut framgår av styrande dokument.
Uppföljning och utvärdering	Uppföljning och utvärdering inom området är i begränsad utsträckning tillräcklig. Bedömningen baseras på att ingen uppföljning eller utvärdering har redovisats till socialnämnden under 2015. Bedömningen baseras också att det inte följts upp eller utvärderats om socialnämndens verksamhet lever upp till krav på informationssäkerhet i patientdatalagen och SOSFS 2008:14. Vi noterar att uppdrag i verksamhetsplan för IT följs upp samt att avvikelser från rutin för IT-användande rapporteras inom förvaltningen.

Styrning och kontroll	Styrning och kontroll inom området är otillräcklig. Bedömningen baseras på att det inte framgår av socialnämndens kvalitetsledningssystem hur arbetet med behörighetsstyrning och loggkontroll ska bedrivas, något kontrollmoment i nämndens internkontrollplan finns inte, nämnden har inte begärt eller fått någon uppföljning eller utvärdering inom området under 2015. Det kan inte styrkas att styrning och kontroll inom området är tillräcklig för att skydda otillåten åtkomst till och spridning av känslig information, då någon loggkontroll inte genomförts av verksamhetssystemets händelselogg under 2015.