Revisionsrapport 2018
Genomförd på uppdrag av revisorerna
September 2018

Lunds kommun

Granskning av behörighet till känsliga uppgifter samt interna kontroller

Building a better working world

Innehåll

1. Sammanfattning

De förtroendevalda revisorerna har gett EY i uppdrag att granska behörighet och åtkomst till IT-system med känsliga uppgifter samt interna kontroller. Syftet med granskningen är att bedöma om nämndernas och styrelsens arbete med behörigheter, åtkomster och loggkontroll i verksamhetssystemen hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Vår sammanfattande bedömning är att Lunds kommun, i de flesta fallen, har en tillräcklig intern kontroll avseende behörighetsfördelning och kontroller av systemloggar i de IT-system som ingått i granskningen. Det finns tydliga övergripande styrdokument som ligger till grund för systemdokumentation. Vidare finns rutiner för hantering av åtkomst och kontroll för systemen framtagna och dessa efterlevs. Därutöver sker uppföljning av systemen i form av s.k. loggkontroller i de flesta fallen. Inom ramen för granskningen har dock avvikelser noterats, framförallt i ett av systemen, Unikum. Granskningen har visat att barn- och skolnämnden och utbildningsnämnden behöver se över systemägarskapen i syfte att tydliggöra ansvarsfördelningen. Nedan följer våra svar på granskningens revisionsfrågor.

Vi har bland annat gjort följande iakttagelser:

- Vi bedömer att de styrdokument som finns inom området för informationssäkerhet och systemförvaltning är tydliga. Dokumenten behandlar relevanta delar avseende övergripande mål och åtaganden samt ansvarsfördelning. Vi ser det som positivt att styrdokumenten revideras löpande och utvecklas i syfte att skapa tydliga ramar för arbetet.
- Vi noterar vidare att det inom ramen för den interna kontrollen 2018 har genomförts en kommungemensam kontrollaktivitet avseende informationssäkerhet och dokumenthantering.
- I nästan alla system vi granskat finns en adekvat styrning av behörighetsfördelningen. I de flesta fallen krävs bekräftelse av överordnad chef att medarbetare behöver behörighet, och på vilket sätt. I alla systemen kan man också styra åtkomsten genom behörighetsfördelningen. I ett system (Unikum) sker behörighetsfördelningen delvis av administratörer ute i verksamheten med följden att väl många funktioner tilldelats behörighet i vissa verksamheter.
- I de flesta granskade system genomförs såväl en gallring av konton och behörigheter som löpande loggkontroller. Generellt sker uppföljning av konton och behörigheter framförallt i kärnverksamheten. Vad gäller s.k. loggkontroller finns det system där kontroller i form av systemloggar är svåra att genomföra (Unikum, Procapita BOU), vidare finns rutiner för loggkontroller som inte fungerar som planerat (Procapita VOO).

Utifrån granskningsresultatet rekommenderar vi samtliga nämnder att:

- Se över rutiner för gallring av behörigheter.

Utifrån granskningsresultatet rekommenderar vi utbildningsnämnden och barn- och skolnämnden att:

- Se över och säkerställa att ansvarsfördelningens avseende ägarskap och förvaltning av granskade IT-system är tydlig.
- Säkerställa att systematiska loggkontroller genomförs i samtliga system.
- Tillse att det finns ändamålsenliga rutiner för behörighetstilldelning och roller.

Utifrån granskningsresultatet rekommenderar vi vård- och omsorgsnämnden att:

- Stärka den interna kontrollen i samband med loggkontroller och gallring av behörigheter.

2. Inledning

2.1. Bakgrund

Behörigheter till kommunens verksamhetssystem som innehåller känslig persondata regleras av olika lagar bl.a. dataskyddsförordningen. Det ska finnas en rättslig grund för de uppgifter som kommunen registrerar om personer. Uppgifterna ska också skyddas så att ingen obehörig kan få del av dessa.

Flera verksamheter har med åren blivit alltmer beroende av IT-stöd, vilket innebär nya former av hot och risker. Behörighetsstyrning och interna kontroller är en viktig del i arbetet för att skydda uppgifterna och möta lagkrav. I detta ligger att upprätta och upprätthålla rättigheter för användare i de IT-system som brukas, så att användarna 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 kan information spridas till icke behöriga.

De förtroendevalda revisorerna har med utgångspunkt i ovanstående beslutat genomföra en granskning avseende hanteringen av behörigheter i relation till känslig persondata. Granskningen ska avse socialnämnd, barn- och skolnämnd, vård- och omsorgsnämnd, utbildningsnämnd och kommunstyrelsen.

2.2. Syfte och revisionsfrågor

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

I granskningen besvaras följande revisionsfrågor:

- Är de styrande dokumenten tillräckliga?
- Är ansvars- och arbetsfördelningen inom organisationen tillräckligt tydlig?
- Är uppföljning och utvärdering inom området ändamålsenlig?
- Sker en tillräcklig styrning av behörigheter till känsliga system?
- Säkerställer nämnderna att tillräcklig intern kontroll inom området har upprättats för att hindra otillåten åtkomst till och spridning av känslig information?
- Får ansvariga nämnder en adekvat rapportering avseende informationssäkerheten i verksamhetssystem som innehåller känsliga personuppgifter?

2.3. Genomförande och avgränsning

Granskningen omfattar fem verksamhetssystem. Urvalet är baserat på information från IT-avdelningen avseende vilka system som främst behandlar personuppgifter, inom de granskade nämnderna. Följande verksamhetssystem omfattas av granskningen:

- Procapita vård- och omsorg (VOO)
- Procapita individ- och familjeomsorg (IFO)
- Procapita barn- och ungdom (BOU)
- PMO (Elevhälsa)
- Unikum (Lärplattform grundskola och förskola)

Granskningen sker genom dokumentstudier och intervjuer med ansvariga tjänstemän samt presidierna i granskade nämnder. Verifiering av den interna kontrollen sker genom

loggkontroller i de granskade systemen och avstämning mot vilka funktioner som har skäl att ta del av informationen (t.ex. personens handläggare).

2.4. Revisionskriterier

I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Kommunallagen (2017:725), kap 6
- Lag (2001:454) om behandling av personuppgifter inom socialtjänst
- Skollagen (2010:800)
- Patientdatalagen (2008:355)
- Dataskyddsförordningen (GDPR)
- Offentlighet och sekretesslagen (2009:400)

3. Kommunövergripande styrdokument

3.1. Informationssäkerhetspolicy

Kommunstyrelsen beslutade i december 2015 om den nuvarande informationssäkerhetspolicyn för Lunds kommun. Informationssäkerhetspolicyn ska revideras vart tredje år och i skrivande stund pågår en revidering som ska vara klar till januari 2019.

Policyn anger att kommunens riktlinjer och rutiner för informationssäkerhet ska ha sin grund i de lagkrav som finns och inte stå i strid med demokratiska principer så som offentlighetsprincipen. Utöver detta ska kommunen följa föreskrifter från myndigheter inom informationssäkerhetsområdet så som MSB, SKL och Datainspektionen.

I policyn ges en definition av vad som avses med informationssäkerhet, förklarat genom ett antal krav som ska säkerställas; riktighet, konfidentialitet (sekretess), spårbarhet och tillgänglighet. Det framgår även att policyn gäller för samtliga verksamheter inom Lunds kommun, vilket även gäller externa verksamheter som anknyter till Lunds kommun. Policyn anger ett antal mål för kommunens informationssäkerhetsarbete:

- Personal har kunskap om gällande informationssäkerhetsregler.
- Informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för verksamheten.
- Lagar, förordningar och föreskrifter är kända och följs.
- Ingångna avtal är kända och följs.
- Krishanteringsförmågan upprätthålls.
- Alla investeringar både i form av information samt teknisk utrustning har skydd i tillräcklig grad.
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation.
- Hotbilden för varje enskilt informationssystem som är av vikt för verksamheten analyseras fortlöpande.
- Händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs.

Utöver dessa mål listas ett antal generella krav kring informationssäkerheten. Kraven består i att informationssystem ska vara identifierade och förtecknade samt att relevanta roller (framgår av systemförvaltningsmodellen) ska vara tillsatta. Informationssystem ska uppnå de mål som framgår av riktlinjer för informationssäkerhet (se avsnitt 2.2) och information som hanteras ska klassificeras utifrån den beskriva definitionen av informationssäkerhet som policyn uttrycker. Slutligen ska också alla anställda inom Lunds kommun, som använder informationstillgångar, vara skyldiga att känna till och efterleva riktlinjer, policys och regler.

Uppföljning anges vara en viktig del i informationssäkerhetsarbetet. Sådant som ska bevakas löpande är att beslutade åtgärder är genomförda, mål är uppfyllda, regler följs och att styrdokument regelbundet revideras.

Bilden nedan redovisar den övergripande ansvarsfördelningen avseende informationssäkerhetsarbetet, som framgår av informationssäkerhetspolicyn.

Bild: Övergripande roll- och ansvarsfördelning gällande informationssäkerhetsarbetet.

3.2. Riktlinjer för informationssäkerhet

De senast antagna riktlinjerna för informationssäkerhet fastställdes den 4 februari 2016 och är enlig uppgift även denna under revidering vid skrivande stund. Revideringen består i att utöka informationen samt att tydliggöra strukturen. Enligt uppgift kommer ett flertal områden att förtydligas, såsom användarkonton och behörigheter samt lösenordshantering.

Riktlinjerna ska beskriva rutiner och säkerhetslösningar som måste etableras för att uppnå de mål som framgår av informationssäkerhetspolicyn. Syftet är inte att riktlinjen ska beskriva hur dessa ska utformas på en detaljerad nivå, utan ska ange en minsta förväntad nivå för dessa.

Ett avsnitt benämns *åtkomst och behörigheter* och innefattar instruktioner för ansvar, kontroll och användande. Här framgår att det ska finnas dokumenterade rutiner för åtkomsthantering till olika system eller tjänster. Denna rutin ska innefatta processen från registrering av användare till borttagning av användare samt felhantering och uppföljning av behörigheter. Behörigheterna ska vidare vara begränsade till vad som krävs för att utföra de arbetsuppgifter som användaren har. Samtliga rutiner och processer rörande behörighetshantering ska dokumenteras i systemets förvaltningsplan.

I avsnittet *systemloggar* framgår att de vanligaste loggarna är

- Åtkomstlogg (exempelvis misslyckade eller lyckade inloggningar behörighetsförändringar)
- Driftavvikelselogg (logg över avvikelser och fel i systemet)
- Informationslogg (logg över förväntade systemhändelser)

Syftet med systemloggarna är att säkerställa spårbarhet av aktiviteter i systemet. Dokumentation om ett specifikts systems loggar ska framgå av förvaltningsplanen och innefatta minst:

- Vilka loggar som finns
- Vilket skydd för manuella förändringar som finns för loggen
- Vilka användare har access till loggen
- Gallrings- och arkiveringsrutin
- Rutin för analys av logg

I riktlinjen framgår även en roll- och ansvarsfördelning på verksamhetsnivå. Det anges att varje förvaltning är ansvarig för informationen och informationssäkerheten inom sitt eget

verksamhetsområde. Vid behov kan förvaltningen besluta om riktlinjer och instruktioner som kompletterar kommunens gemensamma riktlinjer för informationssäkerhet.

3.3. Lunds kommuns systemförvaltningsmodell

IT-avdelningen har formulerat en kommungemensam systemförvaltningsmodell som ska verka som stöd och skapa samsyn i systemförvaltningen. Modellen består av två delar, *systemförvaltningsprocesser*[1] och *systemförvaltningsorganisation*[2]. Vidare kan modellen tillämpas på två sätt, en variant som är anpassad för större verksamhetsövergripande system och en mindre variant som lämpar sig för system som används inom en förvaltning eller i liten omfattning.

Det som förvaltas kallas förvaltningsobjekt, och är ett begrepp som omfattar ett eller flera system som stödjer eller levererar en tjänst. Exempel på större förvaltningsobjekt är ekonomi och inköp som i regel består utav fler än ett IT-system men faller under samma objekt. Ett enskilt system kan endast ingå i ett förvaltningsobjekt. För varje förvaltningsobjekt ska följande finnas:

- Definition (vad som omfattas av förvaltningsobjekt)
- Förvaltningsorganisation
- Förvaltningsplan för varje system som ingår i förvaltningsobjektet
- Avtal mellan tjänsteägare, systemägare och leverantörsorganisation för varje system

Av modellen framgår vidare att ett antal förvaltningsprocesser bör innefatta samtliga objekt, som sedan kompletteras med systemspecifika processer. De gemensamma förvaltnings-processerna framgår även delvis *av riktlinjer för informationssäkerhet*. Bland annat ingår användarstöd, säkerhetshantering (systemloggar ingår) och behörighetshanering. En process benämns förvaltningsstyrning och innefattar exempelvis prioritering av aktiviteter, beslut om förvaltningsplan, fördela arbetsuppgifter och se till att systemförvaltningen är i linje med kommunens övriga styrdokument.

Förvaltningsplanen är det centrala styrdokumentet för ett systems operativa arbete och ett underlag för verksamhetens planering. Syftet med planen är att klargöra vilka uppgifter som ska utföras samt hur detta ska bemannas och styras. Förvaltningsplanen ska revideras årligen.

I tabellen nedan framgår de olika roller som finns i förvaltningsorganisationen. Antalet roller skiljer sig åt beroende på om det är ett stort förvaltningsobjekt eller om det är ett mindre.

Roll	*Beskrivning*
Objektägare	Ytterst ansvarig för förvaltningsobjektets långsiktiga mål och utveckling ur ett verksamhetsperspektiv.
IT-objektägare	Ytterst ansvarig för objektets långsiktiga mål och utveckling ur ett IT-perspektiv.
Objektförvaltare	Sammanhållande helhetsansvar för förvaltning av ett eller flera system. Ser till att planerade aktiviteter genomförs och upprätthålls.
IT-objektförvaltare	Ansvar för det IT-relaterade förvaltningsarbetet och säkerställer att målen i förvaltningsplanen nås, genom IT-avdelningens leveranser.
Systemägare	Ytterst ansvarig för ett system som ingår i förvaltningsobjektet.

[1] Aktiviteter som genomförs för att administrera och hantera ett system
[2] Beskriver vilka roller som ingår i arbetet

Systemförvaltare	Ansvarar för ett system eller en del av ett system.
Driftsansvarig	Huvudansvar för systemets IT-drift.
Systemspecialist	Användare med god kompetens inom det angivna arbetsområdet som systemet avser. Utgör ett stöd för systemförvaltaren och andra användare.

Tabell: Rollfördelning i förvaltningsorganisationer.

I en stor förvaltningsorganisation utgör objektägare och IT-objektägare en styrgrupp som tar beslut, säkerställer långsiktiga mål och strategier. De ska även se till att objektet hanteras enligt kommunens riktlinjer och styrdokument. Under styrgruppen, finns en förvaltningsgrupp bestående av objektförvaltare, IT-objektsförvaltare, systemägare, systemförvaltare och driftansvarig. Förvaltningsgruppen har i uppgift att planera, utföra och dokumentera aktiviteter som ingår i förvaltningsplanen. I förvaltningsgruppen är systemägare, driftsansvarig och systemförvaltare fördelade utifrån system, och det kan därför finnas flera som innehar dessa roller, inom samma objekt.

I utvecklings- och utbildningssyfte finns ett nätverk för systemförvaltare. Gruppen träffas gemensamt vid två tillfällen per år och behandlar ett antal punkter som systemförvaltarna har önskat att belysa. Exempel på ämnen som har behandlats är:

- GDPR och system
- E-arkiv
- Informationssäkerhetspolicy och riktlinjer
- Kontinuitetsplaner

Inför verksamhetsåret 2018 hölls även ett föredrag kring intern kontroll med anledning av en kommungemensam kontrollaktivitet avseende informationssäkerhet och dokumenthantering. Aktiviteten innebär att samtliga nämnder ska gå igenom de system som de ansvarar för och kontrollera att dokumentation finns på plats och är tillgängligt, i enlighet med ovan nämnda styrdokument. En del omfattar även att kontroll ska göras av att aktiviteter enligt förvaltningsplanen är genomförda.

3.3.1. Bedömning

Vi bedömer att de styrdokument som finns inom området för informationssäkerhet och systemförvaltning är tydliga. Dokumenten behandlar relevanta delar avseende övergripande mål och åtaganden samt ansvarsfördelning. Vi ser det som positivt att styrdokumenten revideras löpande och utvecklas i syfte att skapa tydliga ramar för arbetet. Vidare skapar dokumenten ett bra underlag för en ändamålsenlig organisation för informations-säkerhetsarbetet.

Vi noterar vidare att det inom ramen för den interna kontrollen 2018 har genomförts en kommungemensam kontrollaktivitet avseende informationssäkerhet och dokumenthantering. Vi bedömer att kontrollerna i sig reducerar riskerna i känsliga IT-system och förbättrar kontrollmiljön.

4. Verksamhetssystem

4.1. Procapita Vård och Omsorg

Systemet Procapita Vård och Omsorg utgör vård- och omsorgsförvaltningens modersystem, som styr behörigheter till ytterligare tre verksamhetssystem. I systemet finns 147 enheter upplagda och de omfattar samtlig utförarverksamhet inom förvaltningen så som hemvård, särskilt boende och LSS-verksamhet. I dagsläget finns 8107 brukare inlagda i systemet, dock är alla inte aktiva då legitimerad personal inte alltid avslutar brukares journaler korrekt, vilket leder till att de fortfarande står som aktiva i Procapita VOO.

I princip all information som lagras i Procapita bedöms vara känslig information. Detta innefattar allt från biståndshandläggarens bedömning till journalföring av medicinsk personal. Procapita VOO har två systemförvaltare som sitter på vård- och omsorgsförvaltningen.

I nedan tabell redovisas en sammanställning av Procapita VOOs användare från juni 2018. Antalet aktiva användare ökar något under sommarmånaderna då vikarier kommer in, dessa behörigheter tas sedan bort.

Antal användare	*Antal aktiva användare*	*Antal användare med fullständig behörighet*
10400	4000	2

Tabell: översikt över användare i Procapita VOO. Källa: Vård- och omsorgsförvaltningen

I systemet finns inget sätt att beräkna antalet användare som endast har läs- och eller skrivbehörighet då detta är olika i olika delar av systemet. De två användare som har fullständig behörighet är systemförvaltarna.

4.1.1. Utbildning och information

I samband med nyanställning skriver den anställde under en användarförsäkran för dator och internet. Av användarförsäkran framgår att medarbetare enligt lag endast får ta del av uppgifter som rör enskilda personer i det fall det behövs för att kunna utföra sitt arbete. Vidare informeras den anställde om att aktiviteten i Procapita VOO loggas och sparas, samt att kontroller av loggar genomförs löpande. Det finns inom förvaltningen dokumentationsregler som verksamhetens utvecklare ansvarar för.

Ansvarig nämnd, vård- och omsorgsnämnden, har fått information och utbildning avseende de förändringar som GDPR föranlett svensk lagstiftning under 2018. En hel del av dessa förändringar har en direkt påverkan på de system som handhar känsliga personuppgifter inom nämndens ansvarsområde. Någon mer specifik information om Procapita VOO har nämnden inte fått.

4.1.2. Behörigheter

Procapita VOO har en dokumenterad rutin för behörighetshantering som beskriver tillvägagångssätt för beställning, tilldelning och avslut. För att en användare ska få åtkomst till systemet krävs att ansvarig chef (enhetschef eller verksamhetschef) skickar en beställning till systemförvaltaren. Detta kan också delegeras till administratör eller motsvarande. Beställningen sker genom kommunens intranät. Av beställningen ska det framgå en beskrivning av vilken roll som användaren ska ha, beroende på yrkesroll och även inom vilken enhet denne ska arbeta.

Systemförvaltaren mottar beställningen i form av ett mail och tilldelar sedan behörighet utifrån en fastställd förteckning. Behörighetsförteckningen är indelad efter övergripande områden, exempelvis *Roller för legitimerad personal* som sedan delas in i undergrupper utifrån yrkesroll. När tilldelningen är klar skickas ett mail till beställaren med användarnamn och tillfälligt lösenord. Beställaren ansvarar sedan för att användaren får sina nya uppgifter. Vid första inloggningen måste användaren välja ett eget lösenord. Enhetschefer har behörighet till hela enheten. Inom hemvården finns det fall då en chef har behörighet till fler än sin egen hemvårdsenhet för att kunna täcka upp för varandra vid vakanser, semester och övrig frånvaro. Det finns också användare som jobbar på flera boenden, vilket kräver behörighet till samtliga arbetsplatser.

Systemförvaltarna har möjlighet att lägga in tidsbegränsade åtkomster för de anställda som endast ska arbeta under en definierad period. Vid avslut av behörighet är beställaren ansvarig för att meddela detta till systemförvaltaren, på samma sätt som när behörighet beställs. Även vid längre planerad frånvaro (sjukskrivning eller föräldraledighet) ska behörigheten avslutas. Systemförvaltaren spärrar kontot men tar inte bort användaren ur systemet, eftersom att det ska gå att söka upp information i efterhand.

Det finns en funktion i Procapita VOO som spärrar användare automatiskt om denne inte har varit aktiv de senaste 30 dagarna. För att låsa upp lösenordet kontaktar användaren IT och uppger sitt personnummer och användarnamn. Enligt uppgift finns det ett pågående arbete på IT-avdelningen som syftar till att tillämpa tvåfaktorsinloggning. I dagsläget finns detta endast för externa användare men inte för interna (anställda via Lunds kommun). För externa användare finns en specifik rutin gällande hur tillgång till systemet tilldelas, i dagsläget finns runt 100 externa konton i Procapita VOO.

Systemförvaltaren genomför en gallring av behörigheter två gånger per år, senaste gallringen genomfördes i april 2018. En lista med samtliga användare per enhet skickas till enhetschefen som ger besked gällande vilka konton som ska spärras. Vid intervju framkom att systemförvaltarna ofta har svårt att få svar från enhetschefer. Vid uteblivet svar spärrar systemförvaltaren de konton som inte använts de två senaste månaderna. Rutinen följs upp årligen enligt Procapita VOOs förvaltningsplan. Gallring av behörigheter omfattar således endast användare inom kärnverksamheten. Vid granskningen framkom att det finns ett antal konton som inte gallrats, där användarna finns utanför vård- och omsorgsförvaltningen men inom kommunen, såsom IT-avdelningen. Dock är omfattningen inte stor. Vid kontroll i samband med särskild granskning av dessa konton bedömdes 17 konton som inaktiva.

4.1.3. Loggkontroller

Förvaltningen har en dokumenterad rutin för kontroller av journalloggar, framtagen av kvalitetsutvecklaren. Kontrollen sker en gång varannan månad och omfattar en medarbetare per enhet. Medarbetaren slumpas fram och enhetschef har sedan i uppgift att genomföra en kontroll av aktiviteterna under tre sammanhängande dygn. Till stöd finns ett antal frågor som enhetschefen ska gå igenom för att kunna göra en bedömning av lämpligheten i aktiviteten. Om avvikelser uppkommer ska en riktad kontroll genomföras som även innefattar att medarbetaren får svara på ett antal frågor. Riktade kontroller kan även genomföras vid misstanke om oegentligheter.

När kontrollen är genomförd ska journalloggen, en undertecknat blankett med uppgifter om kontrollen samt eventuell avvikelsedokumentation skickas till registratorn för diarieföring. Vid intervju framkom att rutinen inte följs då det ofta drar ut på tiden och att kontrollen inte diarieförs i tillräcklig utsträckning. I förvaltningens kvalitets- och patientberättelse för 2017 framgår att en uppföljning av kontrollerna har genomförts och man konstaterar att varken rutinen eller

instruktionerna följs. I samband med denna granskning gjordes en kontroll av vilka enhetschefer som diarieförd journalloggen som genomfördes under november och december 2017. Resultatet visar att lite över hälften av loggarna, 58 % diarieförd.

4.1.4. Bedömning

Vi bedömer att det finns goda förutsättningar för kontroller och behörighetshantering inom vård- och omsorgsnämndens område. Systemet omfattar en stor mängd användare och brukare, vilket kräver en tydlig och medveten organisation. Vi bedömer dock att det kan vara en risk att man i gallringen av konton missar vissa konton då rutinen för gallring endast omfattar kärnverksamheten. Det kan därför finnas behov för att utöka gallringen.

Vi bedömer vidare att det är en brist att loggkontrollerna inte kan verifieras på grund av att enhetscheferna inte följer fastställd rutin och skickar in resultatet av kontrollerna för diarieföring på förvaltningen. Det samma gäller rutinen för gallring av behörigheter. Vi ser i detta avseende att nämnden bör stärka den interna kontrollen i syfte att säkerställa att kontroller genomförs.

4.2. Procapita IFO

I likhet med Procapita VOO betraktas i princip all information i Procapita IFO som känslig. Organisationen inom socialförvalförvaltningen är uppdelad på fyra verksamhetsområden som presenteras kortfattat i bilden nedan.

Bild: Organisationsskiss socialförvaltningen.

Inom varje verksamhetsområde finns övergripande enheter som kan delas in i olika boenden eller team. Enligt en organisationsskiss från mars 2018 finns 27 övergripande enheter inom förvaltningen. Vid tiden för granskningen finns 8348 brukare inlagda i Procapita IFO. Detta innefattar även exempelvis kontaktpersoner, det vill säga privatpersoner som agerar kontaktperson åt ensamkommande eller liknande, för dessa personer upprättas även en akt även om de inte är föremål för en insats.

Procapita IFO har tre systemförvaltare. Dessa tre har fullständig behörig till systemet, utöver detta finns supportfunktioner hos leverantören som också har fullständig behörighet.

Antal användare	*Antal aktiva användare*	*Antal användare med fullständig behörighet*	*Antal användare med läs- och skrivbehörighet*	*Antal användare med läsbehörighet*
627	564	6	564	57

Tabell: Översikt över användare i Procapita IFO. Källa: Socialförvaltningen

Inom förvaltningen arbetar ungefär 700 personer och det finns i skrivande stund 627 användare i systemet. Antal användare har beräknats utifrån de antal som varit inloggade de senaste sex månaderna och aktiva är dem som har ett fungerande lösenord. Några användare som har läs- och skrivbehörighet har inte behörighet att läsa journaler utan endast behörighet att se om en person förekommer i Procapita IFO. De har skrivbehörighet till ”Mina meddelande”, som är en funktion för säker epost i systemet.

4.2.1. Behörigheter

Vid tilldelning av behörighet eller ändring av en befintlig behörighet, skickar enhetschef, biträdande enhetschef, föreståndare eller samordnare en ifylld behörighetsblankett till systemförvaltarna via meddelandefunktionen i Procapita IFO. På blanketten anges titel, enhet, eventuell specialfunktion och personnummer. Baserat på detta avgör systemförvaltaren vilken roll som ska tilldelas, samt vilket dataurval som ska appliceras.

När behörigheten är klar skickas inloggningsuppgifter till beställaren och lösenord mailas direkt till användaren. Blanketten sparas även på en gemensam server. Chefen har även ansvar att meddela om en anställd avslutar sin tjänst och om en anställd byter arbetsplats, då måste den nya chefer begära behörigheten. De intervjuade uppger att det finns önskemål om att införa ett kommungemensamt system för ansökan om behörigheter, till samtliga system. Detta för att kunna ha ett säkert sätt att kommunicera känsliga uppgifter så som personnummer för samtliga system.

Lösenordet byts var 60e dag vilket innebär att kontot låses om man inte varit aktiv under den tiden. För att återställa ett lösenord får användaren ringa systemförvaltaren eller maila en gemensam mailbox. Det nya lösenordet meddelas per mail (endast lund.se-adress).

För närvarande finns 62 olika roller i Procapita IFO som kopplas till olika tjänster. Rollen styr vilka delar av systemet som användaren kan tillgå och vad man har möjlighet att göra. Dataurvalet styr vilka journaler som användaren kommer åt och vilken information man får tillgång till. Detta innebär att olika tjänster kan ha samma roll, men olika dataurval. Inom förvaltningen finns en rutin som beskriver hur cheferna ska gå tillväga för att begära behörigheter samt att det även finns förteckningar över roller och dataurval. I juli 2015 genomfördes en inventering av personalkategorier och behörigheter i Procapita. Ledningsgruppen tog då ett beslut, med anledning av inventeringen, hur behörigheten för olika personalkategorier skulle se ut. Listan uppdateras dock efterhand som nya behov uppstår i verksamheten. Vid intervju uppgavs att det behöver vara ett levande dokument som följer verksamhetsförändringar för att personalen ska kunna göra sitt jobb.

Fyra gånger per år genomförs en granskning av behörigheter. Systemansvarig skickar då en förteckning över aktuella behörigheter till respektive arbetsledare. Arbetsledaren ansvarar sedan för att gå igenom listan och återkomma med eventuella ändringar som ska genomföras. Vid varje tillfälle granskas samtliga användare som har behörighet till journaler i sekretessorganisationer[3]. Ett av verksamhetsområdena granskas per granskningstillfälle, vilket innebär att alla verksamhetsområden granskas en gång per år. Resultatet av granskningen sparas sedan i en excelfil. Rutinen för granskning av behörigheter infördes under oktober 2017.

Vid intervju framkom att det är en brist i systemet att man inte kan lägga in att en anställd får en ny tjänst i förväg. Detta måste ske samma dag, vilket innebär att systemförvaltarna får hålla personliga bevakningar för att gå in i systemet exakt den dag då personen börjar sin nya tjänst. Vid nyanställningar går det dock att lägga in personen i förväg.

4.2.2. Utbildning och information

Ansvarig chef eller arbetsledare ska se till att varje ny användare tar del av en användarförsäkran för Procapita. Av användarförsäkran framgår att man endast har rätt att ta del av uppgifter som rör enskilda personer, i det fall det krävs för att utföra sitt arbete. Det

[3] De som har tillgång till uppgifter om personer med skyddad identitet. Sekretessorganisationer är ett sätt att ytterligare begränsa vilka som får behörighet till journaler för personer som har skyddade personuppgifter. En del användare har alltid behörighet utifrån sina arbetsuppgifter och andra användare tilldelas behörighet när de handlägger ärenden där brukaren har skyddade personuppgifter.

framgår även att den som olovligen tar del av information kan dömas till böter eller fängelse. Användaren informeras också om att det finns en loggfunktion i systemet som kan spåra vad man har läst, sparat eller sökt på, samt att loggarna kontrolleras regelbundet. Undertecknad användarförsäkran ska sparas i personakten på respektive enhet. Det finns även en kortare instruktion för nya användare i Procapita som beskriver inloggning och kontaktuppgifter till systemansvariga, som skickas till användaren i samband med tilldelning av lösenord. På kommunens Portal för IT-stöd, finns även en sida med nyheter och information om Procapita. Utöver detta finns specifika rutiner för hantering av skyddade personuppgifter.

Systemansvariga håller även i instruktionsutbildningar, ca fyra utbildningstillfällen per användargrupp (myndighetsansvar med utredning/beslut samt utförare av insatser) och år. Introduktionen är inte obligatorisk eftersom nyanställda kan ha arbetat i systemet tidigare. Enligt uppgift varierar det hur många som deltar på utbildningarna. Det är enhetschefens ansvar att rätt personer kommer på utbildningarna.

Socialnämnden har fått information om dataskyddsförordningens (GDPR) effekter för såväl den kommunala verksamheten som nämndens ansvarsområde. Hela nämnden, men framförallt myndighetsutskottet, blir informerade om aktuella händelser. Någon mer genomgripande information om IT-säkerheten inom Procapita IFO har inte erhållits.

4.2.3. Loggkontroller

Socialförvaltningen har en upprättad rutin för kontroll av loggar, daterad 2018-02-20. Enligt rutinen genomförs loggkontroller en gång i månaden och avser:

- Fem slumpvis utvalda datum den senaste månaden
- Fem slumpvis utvalda användare den senaste månaden
- Fem slumpvis utvalda brukare (kontroll av vilka användare som varit inne i journalen)
- Slumpvis utvald användare som gjort sökningar i sökverktyg samt sammanställningsverktyg

Vid behov kan kontroll genomföras av en specifik brukare för att se vem som har varit inne i dennes journal. En sådan kontroll initieras av arbetsledare om denne bedömer att det finns ett behov. Kontroller genomförs även av utbetalningar för att säkerställa att utbetalningar inte skett till samma mottagare från olika journaler, om det skett dubbla utbetalningar i samma journal samt särskilda kontroller för höga belopp.

Systemansvariga genomför kontrollerna och dokumenterar en redovisning i september varje år. I den senaste redovisningen framgick att kontrollerna genomförts varje månad mellan september 2016 och augusti 2017 med undantag för april, på grund av hög arbetsbelastning. Under perioden har fem avvikelser uppkommit som alla berörde misstanke om otillåten läsning av journal. I tre av fallen kunde enhetschef klargöra att det funnits skäl för personalen att ta del av journalerna. Vid övriga två tillfällen har vidare utredning krävts. Dock återkopplas inte eventuella påföljder till systemansvariga vilket innebär att det saknas vidare information i redovisningen. Även vid redovisningen för föregående år framkom att det vid fem tillfällen noterats misstanke om otillåten läsning av journal.

4.2.4. Bedömning

Vi bedömer sammantaget att det inom socialnämnden finns ett ändamålsenligt arbete med behörigheter och loggkontroller. Vi bedömer dock att det kan finnas en risk att användare utanför kärnverksamheten missas i samband med gallring av behörigheter. Vi bedömer därför att nämnden kan se över rutinen i syfte att säkerställa att så inte sker.

4.3. Procapita BOU

Procapita BOU innehåller uppgifter om samtliga elever (grundskola, gymnasium, SFI, komvux och särvux), förskolebarn, vårdnadshavare, lärare och gode män/kontaktpersoner. Systemet styr även vissa andra skoladministrativa system, då Procapita BOU fungerar som elevregister. För att säkerställa att personuppgifter är korrekta samkörs Procapita med kommuninvånares register (KIR) en gång varannan månad. Vid tiden för granskningen fanns 25 200 elever och barn registrerade i systemet. Procapita BOU har tre systemförvaltare som ansvarar för olika skolformer. Utbildningsdirektören är systemansvarig, vilket innebär att systemet faller under utbildningsförvaltningens område.

I systemet finns bland annat information om:

- Adress
- Familjerelationer
- Personnummer
- Placering i särskola
- Modersmålsundervisning
- Elevens val och studieplaner (gymnasiet och vuxenutbildning)
- Betyg
- Inkomst (avser vårdnadshavare gällande förskoleavgift)

Nedan tabell redovisar en översikt över användare i Procapita BOU, i den modul som är avsedd för administrativ personal samt personal som arbetar på flera enheter (se avsnitt 3.3.1 för beskrivning av klient-modulen).

Antal användare	*Antal aktiva användare*	*Antal användare med fullständig behörighet*	*Antal användare med läs- och skrivbehörighet*	*Antal användare med läsbehörighet*
607	307	3	360	424

Tabell: Översikt över användare i Procapita BOU. Källa: Utbildningsförvaltningen

Antalet fysiska användare i klient-modulen är 607, av dessa kan vissa ha fler än en roll, vilket innebär att antalet som har läs- och skrivbehörighet eller endast läsbehörighet överstiger antalet användare i tabellen.

4.3.1. Behörigheter

Procapita BOU består utav två moduler, en webbaserad modul som används av lärare och vårdnadshavare och en klient-modul som används av administrativ personal samt personal som arbetar för flera enheter såsom studie- och yrkesvägledare och skolsköterskor. För respektive modul finns olika behörighetsregler. I webb-modulen kan lärare se klasslistor, administrera betyg och ämnesprov, för de klasser som de är kopplade till. Vårdnadshavare kan administrera sina kontaktuppgifter och inkomstuppgifter. I den andra modulen kan den administrativa personalen med läsbehörighet se registrerad information (se avsnitt 3.3) och de som är handläggare (skoladministratörer) kan även administrera informationen. Det är även skoladministratörerna som hanterar elever och lärares tillhörighet till skolenheter och klasser i Procapita. Lösenordet byts var 90e dag och för att återställa det måste användaren kontakta servicedesk (IT-avdelningen). I likhet med vad som nämnts för andra system inväntar även Procapita BOU en lösning för att skapa en säkrare inloggning till systemet.

För att få behörighet till klient-modulen ska ansvarig chef lägga ett ärende till servicedesk med information om roll, kontaktuppgifter och vilken enhet som användaren ska ta tillgång till. Systemförvaltaren lägger sedan upp behörigheten och meddelar beställaren. Om behörighet

tas bort ska även detta gå genom servicedesk. När personal ska få behörighet till webb-modulen sker detta genom att skoladministratören tar emot en förfrågan och lägger in användaren i systemet. Avseende vårdnadshavare sker tilldelningen också av skoladministratör eller motsvarande roll. Det saknas i dagsläget en rutin för borttagning av behörigheter till webb-modulen. Detta är på grund av att när en elev inte längre är registrerad, kan vårdnadshavare inte heller se någon information. På samma sätt kan inte personalen se någon information om de inte är kopplade till en klass eller grupp.

Varannan månad genomförs en kontroll av behörigheter där användare som inte varit inloggade de senaste 12 månaderna inaktiveras. Varje kvartal genomförs även en stickprovskontroll av att behörigheter är korrekta. I samband med att systemet övergår till en ny version kommer systemförvaltarna att gå igenom och göra en översyn av samtliga behörighetsroller.

4.3.2. Utbildning och information

Det finns en specifik informationssajt för Procapita BOU som är tillgängligt för alla användare. Via kommunens intranät finns informationstext som berör hantering av personuppgifter i systemet. Användaren informeras även om att aktivitet i systemet loggas och att det genomförs kontroller utav dessa. Systemförvaltarna har även gått ut med information till samtliga skoladministratörer och rektorer. I nästa steg ligger ansvaret på skolledaren att kommunicera ut informationen i organisationen. Likaså gäller att utbilda och informera nya användare efter att behörighet har tilldelats.

Utbildningsnämnden och barn- och skolnämnden har fått utbildning om dataskydds-förordningen och dess effekter för respektive nämnds verksamhet. Båda nämnderna är informerade om att ansvaret för Procapita BOU är delat mellan nämnderna men systemet handhas av utbildningsförvaltningen. Barn- och skolnämnden genomför vid tidpunkten för granskningen vissa justeringar av organisationen.

4.3.3. Loggkontroller

I samband med intervju framkom att det nyligen installerats ett verktyg som möjliggör stickprov av loggar. Tidigare fanns inte möjlighet att göra stickprov utan endast kontroller vid specifika incidenter eftersom systemförvaltarna inte hade möjlighet att få fram loggarna utan att kontakta leverantören. Möjligheten att se händelser ser lite olika ut beroende på vilken skolform det gäller. För grundskola och förskola kan man se alla händelser, men för gymnasiet och vuxenutbildningen kan man endast se vissa ändringar såsom byte av kurser eller ändrat betyg. Det går däremot att se samtliga som varit inne och läst adressuppgifter från KIR.

I samband med att det nya verktyget kom på plats infördes även en rutin för loggkontroller som dokumenterats i Procapita BOUs förvaltningsplan. Stickprov ska göras på tre slumpvis utvalda användare inom förskola/grundskola och kontroller görs av vad de läst, sparat och tagit bort. Loggkontrollen genomförs av aktiviteten de tre senaste månaderna. Kontrollen dokumenteras sedan avseende vilka konton som granskats och vid vilket tillfälle. Eventuella avvikelser hanteras enligt en incidentrapporteringsrutin. Det pågår ett arbete inom kommunen med att ta fram en gemensam incidentrapporteringsrutin, som en del av anpassningen till GDPR. Rutinen är enligt uppgift ännu inte på plats och till dess använder systemförvaltaren IT-avdelningens mall för incidentrapportering.

4.3.4. Bedömning

Vi bedömer att det är positivt att utbildningsnämnden har tagit steg för att möjliggöra loggkontroller i verksamhetssystemet. Samtidigt vill vi påpeka att detta är en funktion som borde ha funnits på plats tidigare. Dock är det endast möjligt att göra loggkontroller i delar av systemet, vilket vi bedömer är en brist. Vi bedömer därför att det kan finnas ett behov av att se över möjligheterna för att ytterligare förbättra möjligheterna att genomföra kontroller, i syfte att stärka den interna kontrollen gällande systemet.

Vidare bedömer vi att barn- och skolnämnden samt utbildningsnämnden bör se över ansvarsfördelningen för systemet. Systemet behandlar information som berör båda nämnders verksamhet, men systemet handhas utav utbildningsförvaltningen. Enligt riktlinjer för informationssäkerhet ansvarar respektive förvaltning för information och informationssäkerhet inom sitt verksamhetsområde. Nämnderna bör säkerställa att ansvarsfördelning och organisation är tydlig vid fråga om ansvarsutkrävande.

4.4. PMO

PMO är ett journalsystem som används av de medicinska professionerna inom elevhälsan för grundskola och gymnasium. De primära funktionerna som använder systemet är skolläkare, skolsköterskor och skolpsykolog. Systemet är uppdelat i olika moduler som tillhör respektive yrkesgrupp vilket innebär att man endast har tillgång till den information som är kopplat till yrkesrollen. Se nedan bild för illustration av systemets olika moduler. I PMO dokumenteras alla besök och samtal som förs med en elev, samt även samtal med vårdnadshavare. Journalen innehåller bland annat information om längd, vikt, vaccination och eventuella diagnoser.

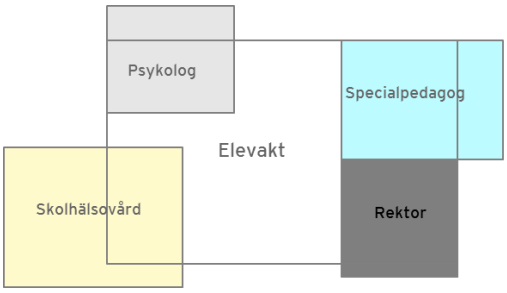

Bild: Moduler i PMO

Det pågår ett pilotprojekt där ett antal rektorer, specialpedagoger och kuratorer använder PMO för att dokumentera sådant som kan ingå i elevens akt. I elevakten görs anteckningar gällande den enskilde eleven i ärenden där elevhälsoteam är involverade och kan till exempel röra elevens speciella behov. Akten ska dock skiljas från elevens patientjournal som innehåller all hälso- och sjukvårdsdokumentation. Liksom för Procapita BOU är utbildningsdirektören systemägare, vilket medför att även PMO ligger under utbildningsförvaltningen.

PMO har två systemförvaltare, utöver detta finns en grupp skolsköterskor som har särskilt ansvar för systemet och fungerar som systemspecialister.

Antal användare	*Antal aktiva användare*	*Antal användare med fullständig behörighet*	*Antal användare med läs- och skrivbehörighet*
173	173	2	Samtliga

Tabell: Översikt över användare i PMO. Källa: Utbildningsförvaltningen

I PMO finns enligt uppgift 173 användare per juni 2018, de två användare med fullständig behörighet är systemförvaltarna. Samtliga användare har läs- och skrivbehörighet i systemet, dock är detta, som tidigare nämnt, begränsat till olika moduler.

4.4.1. Behörigheter

Behörigheter tilldelas genom att ansvarig chef kontaktar servicedesk med information om roll, enhet och kontaktuppgifter. Systemförvaltaren får därefter besked från Servicedesk att upprätta ett användarkonto i PMO, samt att denne bokar in ett utbildningsmöte med användaren. Beställaren (ansvarig chef) får sedan besked om användarens inloggnings-uppgifter. När en användare fått behörighet till systemet söker denne på personnummer för att få fram eleven. Om en användare söker på en elev som är registrerad på en annan enhet får användaren ett meddelande om att man saknar behörighet att gå in på eleven, för att komma vidare måste användaren skriva en förklaring till varför man väljer att gå vidare i systemet. Detta uppstår ofta när eleverna går över till gymnasiet, elevhälsopersonalen kan då ha anledning att gå in i på eleven då personalen haft kontakt med eleven tidigare.

När en behörighet ska avslutas eller inaktiveras meddelar ansvarig chef systemförvaltaren direkt, detta går således inte genom servicedesk. Om en användare behöver återställa sitt lösenord får denne kontakta systemförvaltare eller servicedesk (där det finns två personer med specialkompetens) som meddelar nytt tillfälligt lösenord via mail eller telefon. Det finns även utsedda skolsköterskor som kan återställa lösenord. Lösenordet ska bytas var 90:e dag. Det finns enligt uppgift planer på att övergå till en säkrare typ av inloggning, genom tjänsten Efos[4]. Tjänsten har tagits fram utav Försäkringskassan tillsammans med Inera men lanseringen har skjutits fram och är planerad till hösten 2018.

Enligt uppgift förväntas att rektor (ansvarig chef) meddelar systemförvaltare vid avslut av behörighet, dock sker detta mer ofta vid information om nyanställning. Vid intervju framkom att frånvaro och sjukskrivningar gör att detta kan fördröjas. I övrigt sker ingen gallring av behörigheter.

4.4.2. Utbildning och information

Vid nyanställning anordnas en utbildning i PMO som leds av systemförvaltaren. Utöver detta finns en metodbok för elevhälsans medicinska insats. Enheten för medicinskt ledningsansvar har även journalhanteringsrutin. Av rutinen framgår vilket ansvar som åligger personalen avseende sitt personliga lösenord samt att endast ta del av de patientuppgifter som krävs för att utföra sitt arbete. Vidare anges även att kontroll av loggarna i PMO genomförs. En gång om året genomförs ett gemensamt utbildningstillfälle för all medicinsk personal där gällande rutiner och policys gås igenom.

4.4.3. Loggkontroller

En gång i månaden genomförs slumpmässiga loggkontroller för samtliga yrkesgrupper. Antalet kontroller varierar mellan 5 och 10 stycken per tillfälle. Systemförvaltaren genomför kontrollerna och går igenom vilka vyer som personalen har varit inne i samt aktuella elever. Exempelvis kontrolleras om personalen har varit inne på en elev som går på en annan enhet och vad anledningen till detta är. Om en avvikelse framkommer kontaktas den samordnade sjuksköterskan, som har ett övergripande ansvar för personalgruppen. En händelseanalys genomförs även för att dokumentera händelseförlopp och klargöra vad som skett.

[4] E-identitet för offentlig sektor.

4.4.4. Bedömning

Det är utbildningsförvaltningen som hanterar systemet, men systemet hanterar också information där barn- och skolnämnden har ansvaret. I likhet med tidigare bedömning råder det därför oklarheter kring ansvarsfördelningen mellan utbildningsnämnden och barn- och skolnämnden avseende informationen som behandlas i PMO, detta förhållande bör redas ut.

Vi bedömer att utbildningsnämnden i stora delar har goda rutiner och strukturer för kontroller inom verksamhetssystemet. Det saknas dock en rutin för gallring av behörigheter i systemet. I granskningen framkom att avslut av behörigheter ska ske genom ansvarig chef, men att detta ofta fördröjs och istället uppmärksammas vid nyanställning. Vi bedömer därför att utbildningsnämnden bör tillse att gallring sker systematiskt, i syfte att säkerställa kontrollen av behörigheter till systemet.

4.5. Unikum

Systemet används av grundskolan och förskola framförallt för pedagogiska planeringar, bedömningar och vid utvecklingssamtal. Unikum fungerar som lärplattform vilket innebär att elever, personal och vårdnadshavare har tillgång till systemet. Unikum används även för att kommunicera med elever och vårdnadshavare och kontaktytorna är indelade i tre nivåer:

- Skolnivå: Bloggfunktion för hela skolenheten.
- Klassnivå: Veckobrev och inläggsfunktion där lärare kan delge information till enskilda klasser och elevernas vårdnadshavare.
- Individnivå: Kommunikation som är låst till den enskilde eleven, dess vårdnadshavare och lärare. Den som gör inlägg på individnivå kan själv avgöra vem som ska få läsa meddelandet.

Utöver detta finns en specifik modul för särskilt stöd, där man kan läsa information om en elev har åtgärdsprogram eller extra anpassningar. I Unikum är det endast den pedagogiska kartläggningen som är tillgänglig. Tillgången till modulen för särskilt stöd styrs av rektor som avgör vilka lärare och elevhälsopersonal som får ta del av informationen. Det är framförallt i den här modulen som det finns känsliga uppgifter. För att nå modulen för särskilt stöd måste användaren logga in med Bank-ID.

Systemägarskapet för Unikum ligger under utbildningsförvaltningen, trots att systemet endast används av verksamheter som tillhör barn- skolförvaltningen.

Antal användare	*Antal aktiva användare*	*Antal användare med fullständig behörighet*	*Antal användare med läs- och skrivbehörighet*
63000	63000	2	63000

Tabell: Översikt över användare i Unikum. Källa: Utbildningsförvaltningen

Alla användare har läs- och skrivrättigheter som är avhängigt den roll och koppling användaren har till enheter, klasser, grupper eller andra personer. Var man kan läsa respektive skriva bestäms utifrån den roll man har i Procapita BOU och i Unikum.

4.5.1. Behörigheter

Unikum är kopplat till elevregistret (Procapita BOU) som i sin tur styr elevers, personals (pedagoger främst) och vårdnadshavares kopplingar till varandra, till enskilda klasser och skolenheter. Det sker en automatisk synkronisering gentemot elevregistret varje natt för att säkerställa att uppgifterna är korrekta. Det finns åtta olika typer av behörighetsroller i Unikum.

Det finns kommunövergripande roller som tilldelas skolchef och systemförvaltare samt skolövergripande roller som tilldelas rektorer, skoladministratörer och pedagoger.

Pedagogerna kan få en roll som mentor vilket innebär ett övergripande ansvar för ett visst antal elever, eller rollen som lärare vilket knyts till specifika klasser eller grupper. De övriga skolövergripande rollerna delas in i två grupper: observatörer och administratörer. Skolobservatörsrollen är avsedd för rektorer/förskolechef samt viss elevhälsopersonal. I den rollen har användaren möjlighet att ta del av samtlig information om elever, personal och vårdnadshavare. Skolobservatören kan också registrera, ändra och ta bort användare i klasser eller grupper.

Skoladministratörsrollen är avsedd för skoladministratörer och ger behörighet till att skapa, ändra och ta bort klasser eller grupper. Administratören kan registrera, ändra och ta bort inställningar för samtliga användare inom skolenheten. I likhet med observatören kan även administratören göra ändringar i klasser och grupper. De har också möjlighet att ta del av samtlig information om elever, personal och vårdnadshavare.

Tilldelning av behörigheter till pedagoger, elever och vårdnadshavare sker som tidigare nämnts automatiskt i samband med att de registreras i Procapita. För personal och elever är inloggningen till Unikum kopplat till kommunens IT-plattform vilket innebär att man loggas in automatiskt när man loggar in på en kommundator. Vårdnadshavare får ett användarnamn och lösenord som gör det möjligt att nå plattformen externt via lund.se. Sedan mars 2018 ska alla vårdnadshavare logga in med Bank-ID, undantag får göras för dem som inte har möjlighet att skaffa Bank-ID.

För att få behörighet till de kommunövergripande rollerna måste systemägaren godkänna förfrågan, och systemförvaltaren tilldelar behörighet i systemet. Skoladministratörer på enhetsnivå tilldelas behörighet genom att ansvarig rektor kontaktar systemförvaltare som lägger in behörigheten. När det gäller observatörsrollen kontaktas istället enhets-administratören (i regel skoladministratör) som ansvarar för att lägga in användaren som observatör. När en sådan åtgärd genomförs ska det anmälas till servicedesk. Vid intervju framkom att rutinen kring behörighetstilldelningen inte har fungerat då administratörer har delat ut behörigheter till flertalet funktioner och personer. Detta har föranlett att systemförvaltaren har tagit bort samtliga administratörer inom förskolan, och det planeras att göra detsamma för grundskolan. Det framgick även att det inte är helt tydligt vilken roll som ska tilldelas rektorer med områdesansvar, då dessa inte har det operativa ansvaret för skolenheterna bedömer systemförvaltaren att man inte heller bör ha åtkomst till information om samtliga elever. Enligt uppgift finns önskemål om att kunna fler roller i systemet.

I samband med att läsåret tar slut fryses möjligheterna till behörighetstilldelning och öppnas upp igenom inför terminsstart. Då registreras nya klasser och kopplingar enligt elevregistret. Rektor får åter anmäla vilka som ska ha administratörs- och observatörsroller.

4.5.2. Utbildning och information

Enligt Unikums förvaltningsplan ansvarar systemförvaltare för att informera och utbilda administratörer och observatörer på skol- och kommunnivå. Dessa grupper träffas även genom ett nätverk, för diskussion och erfarenhetsutbyte. För alla anställda inom barn- och skolförvaltningen finns en FAQ som beskriver roller, instruktioner för lösenordbyte och andra funktioner. I FAQ:n har systemförvaltaren bland annat förtydligat att skoladministratörer inte får lägga till andra administratörer, även om det är möjligt att göra i systemet i dagsläget.

Enligt uppgift saknas dock tydliga riktlinjer kring vad en användare får göra i vissa roller. Som nämnts ovan är rollernas möjligheter till åtkomst i systemet inte alltid relevant för användarens yrkesroll, därav önskemålet om att ha möjlighet att ha fler behörighetsroller.

Barn- och skolnämnden är informerade om att nämnden ansvarar för systemet men utbildningsförvaltningen handhar systemet.

4.5.3. Loggkontroller

I systemet visas i vissa vyer vem som har varit inne och besökt en elevs sida, vem som skrivit inlägg och vem som har läst inläggen. Detta visas således för användarna direkt i systemet. Däremot har systemförvaltaren inte tillgång till systemloggar. I samband med granskningen framkom att Unikum inte har någon funktion på plats som kan generera loggar från systemet.

4.5.4. Bedömning

Vi bedömer att systemet i dagsläget saknar relevanta funktioner för att tillse en ändamålsenlig intern kontroll samt styrning av behörigheter. Granskningen visar att det finns ett behov av att stärka möjligheter och rutiner för behörighetstilldelning. Vidare finns det även skäl att se över vilka roller som ska finnas i systemet. Vi bedömer att det är en brist att saknas tillgång till systemloggar, vilket innebär att det inte är möjligt att genomföra systematiska loggkontroller.

Unikum innefattar information som endast omfattas av barn- och skolnämndens verksamheter, dock ligger systemägarskapet under utbildningsnämnden. Detta aktualiserar åter frågan om ansvarsfördelning mellan nämnderna.

5. Stickprovskontroll av loggar

För respektive system har minst 15 slumpmässiga urval genomförts baserat på elever för de system som avser skolan och baserat på brukare för de system som avser social och äldreomsorg. Systemförvaltarna har bistått med avidentifierade listor på elever och brukare som utgjort grunden för urvalet. Granskarna har sedan tillsammans med systemförvaltarna gått igenom befintliga loggar för att kontrollera vem som har varit inne och vad som har skett. Tidsperioden och antalet kontroller varierar mellan systemen då aktiviteten varierar beroende på vilken verksamhet som avses.

5.1. Loggkontroller Procapita VOO

14 av de 15 brukarna kontrollerades under en tidsperiod om 14 dagar. Ett utav stickproven avsåg en brukare med väldigt många insatser, då begräsandes tidsperioden till 3 dagar för att få ett hanterbart material. För varje brukare genereras en lista på vilken personal som varit inne, vid vilken tidpunkt och vilka delar av brukarens journal man tagit del av. Listorna skickades sedan till ansvariga enhetschefer för genomgång.

Eftersom en brukare kan ha insatser från olika enheter tillfrågades totalt 19 enhetschefer. Av dessa återkom 17 och bekräftade att det inte fanns några avvikelser. Två av enhetschefer återkom inte och vi saknar därför uppgifter om dessa delar av stickprovet.

5.2. Loggkontroller Procapita IFO

För detta system genomför de systemansvariga själva kontrollen, som beskrivet i avsnitt 3.2.3. Granskarna gick igenom stickprovet tillsammans med de systemansvarig som gjorde en bedömning avseende aktiviteten inne i systemet. Tidsperioden för kontrollerna avsåg mars månad 2018. I ett av fallen upptäcktes att systemförvaltaren hade missat att registrera brukaren som sekretesskyddad i en av dennes journaler, dock inte den journal som granskades.

I ytterligare ett fall misstänktes att obehörig personal varit inne på brukaren. Vid efterkontroll av enhetschef framkom dock att personalen hade ett särskilt bevakningsuppdrag som föranledde att denne var inne på en brukare som inte tillhörde personalens enhet. I övrigt förekom inga avvikelser i stickprovet.

5.3. Loggkontroller Procapita BOU

I detta stickprov gjordes ett större urval då fler av kontrollerna inte visade någon aktivitet alls. Av de 30 kontroller som genomfördes hittades inga loggar i 19 av fallen. Av denna anledning genomfördes även kontroller baserat på de som har läs-behörighet i systemet, utöver kontroller baserat på elever. För att kontrollera att personalen varit behörig att gå in på eleven i fråga verifierades yrkesroll och arbetsplats av systemförvaltaren. Vid två tillfällen uppkom misstanke om att personal varit inne på elever utan uppenbar anledning, vid efterkontroll framkom dock att det fanns anledning till detta. I sammantaget visade stickprovet inga avvikelser.

5.4. Loggkontroller PMO

Även för PMO genomfördes ett något större urval, om 20 elever samt att kontroller genomfördes utifrån elever och personal. Tidsperioden begränsades till 4 sammanhängande veckor. Granskarna gick igenom aktiviteten tillsammans med systemförvaltaren som gjorde en bedömning om aktiviteten var korrekt. I ett av fallen var en elev registrerad med olika

personnummer i Procapita BOU och i PMO. Efterkontrollen visade att eleven blivit uppskriven i ålder, vilket var noterat i PMO men inte i Procapita BOU eftersom beslutet ännu inte vunnit laga kraft. I övrigt visade stickprovet inga avvikelser.

5.5. Loggkontroller Unikum

Som framgår av avsnitt 3.5.3 finns i skrivande stund ingen funktion för att genomföra loggkontroller i systemet. Kontrollerna genomfördes istället per skola, utifrån ett slumpmässigt urval, där antalet observatörsroller och administratörsroller kontrollerades. Totalt genomfördes 15 kontroller. Systemförvaltaren gjorde under kontrollerna en bedömning om korrekt person hade rätt roll samt om antalet personer som de angivna rollerna var rimligt.

I 11 av 15 kontroller gjordes bedömningen att för många personer hade observatörs- eller administratörsroller. Samtliga avvikelser berörde grundskolan.

6. Sammanfattande bedömning

Vår sammanfattande bedömning är att Lunds kommun, i de flesta fallen, har en tillräcklig intern kontroll avseende behörighetsfördelning och kontroller av systemloggar i de IT-system som ingått i granskningen. Det finns tydliga övergripande styrdokument som ligger till grund för systemdokumentation. Vidare finns rutiner för hantering av åtkomst och kontroll för systemen framtagna och dessa efterlevs. Därutöver sker uppföljning av systemen i form av s.k. loggkontroller i de flesta fallen. Inom ramen för granskningen har dock avvikelser noterats, framförallt i ett av systemen, Unikum. Granskningen har visat att barn- och skolnämnden och utbildningsnämnden behöver se över systemägarskapen i syfte att tydliggöra ansvarsfördelningen. Nedan följer våra svar på granskningens revisionsfrågor.

Revisionsfrågor	Svar
Är de styrande dokumenten tillräckliga?	Ja. Vår bedömning är att de styrande dokumenten finns på plats och är tillräckliga i omfattning. Vidare har kommunen under 2018 valt området för en kommungemensam intern kontroll.
Är ansvars- och arbetsfördelningen inom organisationen tillräckligt tydlig?	Delvis. Enligt de styrande dokumenten ska en organisation med olika roller utses för alla viktigare system. Inom ramen för granskningen har vi dock kunnat konstatera att system som helt eller delvis avser barn- och skolnämnden hanteras av utbildningsförvaltningen vilket gör att ett ansvarsutkrävande försvåras.
Är uppföljning och utvärdering inom området ändamålsenlig?	Delvis. I de flesta granskade system genomförs såväl en gallring av konton och behörigheter som löpande loggkontroller. Kvaliteten i gallringen och kontrollerna skiljer sig dock åt. Generellt sker uppföljning av konton och behörigheter framförallt i kärnverksamheten, användare av annan karaktär riskerar man att missa i gallring. Vad gäller s.k. loggkontroller finns det system där kontroller i form av systemloggar är svåra att genomföra (Unikum, Procapita BOU), vidare finns rutiner för loggkontroller som inte fungerar som planerat (Procapita VOO).
Sker en tillräcklig styrning av behörigheter till känsliga system?	Ja. I nästan alla system vi granskat finns en adekvat styrning av behörighetsfördelningen. I de flesta fallen krävs bekräftelse av överordnad chef att medarbetare behöver behörighet, och på vilket sätt. I alla systemen kan man också styra åtkomsten genom behörighetsfördelningen. I ett system (Unikum) sker behörighetsfördelningen delvis av administratörer ute i verksamheten med följden att väl många funktioner tilldelats behörighet i vissa verksamheter.
Säkerställer nämnderna att tillräcklig intern kontroll inom området har upprättats för att hindra otillåten åtkomst till och spridning av känslig information?	Ja. Vår bedömning är att nämnderna i stort säkerställt en tillräcklig intern kontroll av de system som vi granskat avseende otillåten åtkomst till och spridning av känslig information.
Får ansvariga nämnder en adekvat rapportering avseende informations-säkerheten i verksamhetssystem som innehåller känsliga personuppgifter?	Delvis. Enligt vår bedömning har nämnderna erhållit en adekvat information om införandet av dataskydds-förordningen och dess effekter på kommunen. Information om de enskilda IT-systemen får nämnderna främst om avvikelser uppstår. T.ex. är såväl barn- och skolnämnden som utbildning-snämnden väl insatta i frågan om ansvarsfördelningen för de IT-system som gäller barn- och skolnämnden men hanteras av utbildningsförvaltningen.

Utifrån granskningsresultatet rekommenderar vi samtliga nämnder att:

- Se över rutiner för gallring av behörigheter.

Utifrån granskningsresultatet rekommenderar vi utbildningsnämnden och barn- och skolnämnden att:

- Se över och säkerställa att ansvarsfördelningens avseende ägarskap och förvaltning av granskade IT-system är tydlig.
- Säkerställa att systematiska loggkontroller genomförs i samtliga system.
- Tillse att det finns ändamålsenliga rutiner för behörighetstilldelning och roller.

Utifrån granskningsresultatet rekommenderar vi vård- och omsorgsnämnden att:

- Stärka den interna kontrollen i samband med loggkontroller och gallring av behörigheter.

Jakob Smith
EY

Emmy Lundblad
EY

Bilaga 1

Källförteckning

Intervjuade funktioner:

- Systemförvaltare för samtliga verksamhetssystem
- IT-strateg, IT-avdelningen
- Ordf. samt 2:e vice ordf. i ansvariga nämnder (avstämning via telefon)

Medverkat vid intervjuerna:

- Anna-Lena Håkansson, förtroendevald revisor

Dokument:

- Lunds kommuns Informationssäkerhetspolicy
- Lunds kommuns riktlinjer för informationssäkerhet
- Lunds kommuns systemförvaltningsmodell

Procapita VOO

- Förvaltningsplan
- Behörighetshantering
- Behörighetsförteckning
- Kvalitets- och patientberättelse 2017, Vård- och omsorgsnämnden
- Instruktion för externa användare
- Användarförsäkran för dator och internet, Vård- och omsorgsförvaltningen
- Rutin för loggkontroll

Procapita IFO

- Förvaltningsplan
- Rutin för behörighet
- Instruktion för registrering av användare
- Rutin för granskning av behörigheter
- Förteckning över roller
- Användarförsäkran
- Information och instruktion till nya användare
- Kontroll av loggar; anvisningar och för systemförvaltare
- Redovisning av loggkontroll 2016, 2017

Procapita BOU

- Förvaltningsplan
- Informationstext till användare

- Risk- och sårbarhetsanalys
- Incidentrapporteringsrutin

PMO

- Förvaltningsplan
- Journalhanteringsrutin

Unikum

- Förvaltningsplan
- Systemsäkerhetsanalys
- FAQ