Revisionsrapport 2015

Genomförd på uppdrag av revisorerna

Juni 2015

Granskning av IT-säkerheten inom Lunds kommun

Building a better working world

Innehållsförteckning

1 Sammanfattning

1.1 Bakgrund

På uppdrag av de förtroendevalda revisorerna i Lunds Kommun har EY genomfört en granskning inriktad mot kommunens IT-säkerhet. För att uppnå målen för kommunens verksamheter krävs att informationen i väsentliga verksamhetssystem är tillgänglig, riktig, skyddas från obehörig åtkomst samt är spårbar. Granskningen har inriktats mot verksamhetssystemen Procapita BOU, Procapita VOO samt Raindance.

Granskningens övergripande syfte har varit att granska om IT-säkerheten inom Lunds Kommun är ändamålsenlig beträffande dess väsentliga och mest kritiska verksamhetssystem.

1.2 Övergripande slutsatser

Granskningen som omfattat tre olika system på tre olika förvaltningar inom Lunds kommun har visat på stora skillnader i hantering. Den genomgående bristen är avsaknad av dokumenterade rutiner och processer för att hantera förvaltningen av systemen. Vi noterade att det i många fall inte finns någon dokumentation avseende exempelvis hantering av programförändringar och relaterad ansvarsfördelning. Under 2009-2010 genomfördes initiativ avseende IT – och informationssäkerhet med syfte att skapa en mer formaliserad hantering med dokumenterade rutiner och processer. I de fall där vi noterade dokumentation kring exempelvis säkerhetsklassning av verksamhetssystem och liknande så var den typen av underlag inte alltid allmänt kända på förvaltningarna. En bidragande orsak till att genomförda initiativ inte fått tillräckligt genomslag kan vara att de främst varit drivna av IT-avdelningen, inte i första hand av förvaltningarna själva.

1.3 Huvudsakliga iakttagelser på övergripande nivå

Fullständiga iakttagelser och rekommendationer finns i kapitel 5.

#	Iakttagelse	Prioritet
1.	Avsaknad av avbrottsplan för de mest kritiska systemen	Hög
2.	Svaga krav på lösenord i de olika applikationerna	Medel

1.4 Huvudsakliga iakttagelser Procapita BOU

Fullständiga iakttagelser och rekommendationer finns i kapitel 5.

#	Iakttagelse	Prioritet
1.	Avsaknad av systemförvaltningsmodell	Medel
2.	Avsaknad av regelverk för hantering av behörigheter	Hög
3.	Ansvaret för testning och driftsättning av programförändringar är otydligt	Medel
4.	Avsaknad av sårbarhetsanalys	Låg

1.5 Huvudsakliga iakttagelser Procapita VOO

Fullständiga iakttagelser och rekommendationer finns i kapitel 5.

#	Iakttagelse	Prioritet
1.	Avsaknad av systemförvaltningsmodell	Medel
2.	Ansvaret för driftsättning av programförändringar är otydligt	Medel
3.	Periodisk genomgång av användarbehörigheter sker ej med regelbundenhet	Medel

1.6 Huvudsakliga iakttagelser Raindance

Fullständiga iakttagelser och rekommendationer finns i kapitel 5.

#	Iakttagelse	Prioritet
1.	Avsaknad av systemförvaltningsmodell	Medel
2.	Avsaknad av regelverk för hantering av behörigheter	Hög
3.	Avsaknad av sårbarhetsanalys	Låg
4.	Ansvaret för programförändringar är otydligt	Medel

2 Bakgrund

2.1 Syfte

Idag bedrivs så gott som all verksamhet i en kommun med någon form av datoriserat stöd. Stödet har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet. För att uppnå målen för kommunens verksamheter krävs att informationen i väsentliga verksamhetssystem är tillgänglig, riktig, skyddas från obehörig åtkomst samt är spårbar.

På uppdrag av de förtroendevalda revisorerna i Lunds kommun har EY genomfört en granskning inriktad mot kommunens IT-säkerhet. Granskningen har inriktats mot verksamhetssystemen Procapita BOU, Raindance och Procapita VOO. Dessa system valdes ut av de förtroendevalda revisorerna baserat på en övergripande riskanalys genomförd av EY i samarbete med kommunen. Se punkt 3.1 för en detaljerad genomgång av riskanalysen.

Granskningens övergripande syfte har varit att granska om IT-säkerheten inom Lunds kommun är ändamålsenlig beträffande dess mest kritiska verksamhetssystem.

2.2 Metod

Granskningen har utförts mot utvalda kontroller från Myndigheten för samhällsskydd och beredskaps metodstöd för informationssäkerhet. Detta metodstöd utgår från den internationella standarden för informationssäkerhet ISO/IEC 27001/2. EY har valt ut ett antal relevanta kontroller, fördelat på följande huvudområden, för att besvara revisionsfrågorna:

1. Klassificering av verksamhetssystem
2. Systemförvaltningsmodell
3. Sårbarhetsanalyser
4. Styrning av åtkomst
5. Spårbarhet
6. Styrning av programändringar
7. Kontinuitets- och avbrottsplanering
8. IT-säkerheten hos utomstående part

Granskningen grundas på intervjuer samt stickprovstestning av identifierade kontroller enligt följande huvudmoment:

- Intervjuer med medarbetare inom Lunds kommun för övergripande kartläggning av väsentliga verksamhetssystem.
- Val av verksamhetssystem tillsammans med revisionen för besvarande av revisionsfrågorna.

- Intervjuer med medarbetare avseende utvalda verksamhetssystem för att förstå vilka kontroller som genomförs.
- Analys av intervjuer och stickprovstestning för att verifiera kontrollutförandet.
- Intern kvalitetssäkring och faktagranskning.

Följande roller inom Lunds kommun har intervjuats:

- IT-chef
- IT-strateg
- Förvaltningschef
- Systemförvaltare

Arbetet har genomförts av EY under mars till juni 2015.

2.3 Kvalitetssäkring

Samtliga intervjuade har fått möjlighet att lämna synpunkter på rapportutkastet för att säkerställa att revisionsrapporten bygger på korrekta fakta och uttalanden.

2.4 Avgränsningar

Iakttagelser och analyser baseras på information som har inhämtats vid intervjuer, förelagd dokumentation och stickprovstestning. Det kan finnas brister i kommunens hantering av IT-säkerhet som vi inte har identifierat. Arbetet har inte omfattat test av generella IT-kontroller och applikationskontroller, varför inte utförandet av kontrollerna har verifierats.

Denna rapport tar endast hänsyn till nuläget i Lunds kommun.

3 Iakttagelser

3.1 Övergripande riskanalys

Inom ramen för granskningen har en övergripande riskanalys av verksamhetssystemen genomförts tillsammans med medarbetare inom Lunds kommun. Analysen syftar till att belysa de system med störst verksamhetsrisk. Nedan visas de säkerhetsdimensioner och definitioner som använts.

Värde	Tillgänglighet	Riktighet	Sekretess
3	Effekten av avbrott > 0,5 dag är mycket allvarlig. Stora oönskade effekter för verksamheten och/eller medborgare.	Fel leder till mycket allvarliga konsekvenser. Stora oönskade effekter för verksamheten och/eller medborgare.	Obehörig åtkomst till information leder till allvarliga konsekvenser för verksamheten och/eller medborgare. Lagbrott.
2	Effekten av avbrott > 3 dagar medför stora problem för verksamheten och/eller medborgare.	Fel leder till begränsade oönskade effekter. Övertid, negativ publicitet.	Obehörig åtkomst till information leder till/ger negativa konsekvenser för verksamheten och/eller medborgare. Negativ publicitet.
1	Medför inga kännbara effekter.	Fel medför inga kännbara effekter.	Obehörig åtkomst medför inga kännbara effekter.

Nedan redovisas utfallet av riskanalysen. Av verksamhetssystemen har Procapita BOU, Procapita VOO samt Raindance bedömts vara förknippade med störst verksamhetsrisker, varför granskningen fokuserar på dessa verksamhetssystem.

Applikation	Asynia	e-companion	Fastighets-övervakning (Schneider)	Phoniro Lock	PMO	ProCapita BOU	Procapita VOO	Raindance	Tendsign	Unikum	W3D3
Förvaltning*	KK	KK	SF	VOO	UTB	UTB	VOO	KK	KK	UTB	KK
Tillgänglighet	2	2	2	1	1	3	3	2	2	1	2
Riktighet	2	3	2	2	1-2	3	3	3	2	2	2-3
Sekretess	3	3	1	1-2	3	3	3	3	3	2	1-2
Total	7	8	5	~5	~6	9	9	8	7	5	~6

*KK = Kommunkontoret; SF = Serviceförvaltningen; VOO = Vård - och omsorgsförvaltningen; UTB = Utbildningsförvaltningen

3.2 Grundläggande information om systemen

System	Procapita BOU	Procapita VOO	Raindance
Systemversion	9.4	9.4	2014 Service Pack 8
Huvudsakliga användningsområden	Verksamhetssystem för löpande dokumentation inom utbildningsförvaltningen samt skolförvaltning i Lund stad och Lund öster. Hantering av elevinformation (uppgifter om elevens identitet, resultat, ansökningar, klass, grupplaceringar, vårdnadshavare mm.) Känsliga uppgifter i form av elever/barn med skyddad identitet.	Dokumentationssystem inom vård och omsorg. Systemet används av handläggare och vårdpersonal. Innehåller patientjournaler.	Ekonomisystem som hanterar bokföring, fakturahantering, budget, prognos etc.
Systemleverantör	Tieto	Tieto	CGI
Driftleverantör	Lunds kommun	Lunds kommun	Lunds kommun
Datalagringsort	Lund	Lund	Lund
Antal användare	- (ej möjligt att få ut en lista över alla användare i samband med granskningen)	C:a 2500	2862
Informationsklassning enligt stadens egen systemsäkerhetsanalys	Hög	Hög	Hög
Anskaffningsdatum	1998	1999	1999
Databasversion	SQL Server 2008 R2 SP2	SQL Server 2008 R2 SP2	SQL Server 2008 R2 SP2
OS-version	Windows 2008 R2 SP1	Windows 2008 R2 SP1	Windows 2008 R2 SP1
Behörighetsväg	Klient (Navigator)	Alla ansluter via Citrix. Leverantörer loggar in via Citrix genom tvåfaktor-autenticiering.	Separat via Web alt. via Java. Även extern möjlighet för CGI via Citrix.
Anpassningsgrad	Mindre anpassningar	Få unika anpassningar.	Inga unika anpassningar, förändringar når alla användare samtidigt via uppdateringar eller service packs.

System	Procapita BOU	Procapita VOO	Raindance
Antalet ändringar/typer av ändringar per år	Versionsuppdatering 1 gång per år. Servicefönster varje månad för att anpassa sig utifrån myndighetskrav och lagförändringar.	Ny version årligen. Service Pack cirka fyra gånger per år.	Två gånger per år. Service Pack var tredje vecka.
Väsentliga integrationer	UNIKUM It's learning Book-IT	Raindance när det gäller avgiftssystemet.	Det sker både manuella och automatiska överföringar. Regelbundna jobb är automatiska. Främst integrationer kopplat till e-fakturering.
Transaktionsvolym/ ärenden/dag	Ingen uppgift	Något tusental per dag.	C:a 750 fakturor varje dag.
Väsentliga incidenter/problem	Mindre buggar (t.ex. ej möjligt att skicka in nationella prov).	Ett större avbrott under senaste året.	Långsamma överföringar mellan systemen, som påverkar automatiska transaktioner. Dessa problem har dock minskat i omfattning sedan en ny server togs i bruk.

3.3 Granskningsprotokoll

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
1 Klassificering av verksamhetssystem					
1.1	Finns det en ändamålsenlig modell för klassificering av verksamhetssystem?	Samtliga system som omfattas av granskningen: Det finns en klassificering framtagen per system som utgår från BITS klassificering (tillgänglighet, riktighet, sekretess). Respektive system som omfattades av denna granskning har klassificerats utifrån tillgänglighet, riktighet, sekretess.	Inga avvikelser identifierade		
1.2	Har verksamhetssystem klassificerats avseende hur kritiska de är?	Samtliga system som omfattas av granskningen: Ja, det har gjorts på individuell nivå per system, men det har inte genomförts någon klassificering utifrån hur kritiska system är i förhållande till varandra, dvs. vilka system som ska prioriteras vid eventuella incidenter/avbrott.	Vissa avvikelser identifierade		
2 Systemförvaltningsmodell					
2.1	Finns det en ändamålsenlig systemförvaltnings-modell?	Procapita BOU: Det finns ingen dokumenterad systemförvaltningsmodell, enbart informella rutiner för hur systemet ska förvaltas. Procapita VOO: Det finns ingen dokumenterad systemförvaltningsmodell, enbart informella rutiner för hur systemet ska förvaltas. Raindance: Det finns ingen dokumenterad och implementerad systemförvaltningsmodell. Förvaltningen av vissa av Lunds kommuns verksamhetssystem, däribland Raindance, diskuteras gemensamt i förvaltningsråd där respektive systemförvaltare deltar.	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade
2.2	Är befintlig systemförvaltnings-modell implementerad?	Procapita BOU: Nej, se 2.1 Procapita VOO: Nej, se 2.1 Raindance: Nej, se 2.1	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
3 Sårbarhetsanalyser					
3.1	Finns det en ändamålsenlig modell för genomförande av sårbarhetsanalyser?	Procapita BOU: Nej, det finns ingen modell för sårbarhetsanalyser inom utbildningsförvaltningen. Procapita VOO: En risk - och sårbarhetsanalys Vård och Omsorg är framtagen. Vi mottog detta dokument i samband med granskningen och verifierade att dokumentet uppdaterades under 2015 och att det bland annat innehåller en identifiering och värdering av risker och sårbarheter i verksamheten (däribland IT-driftstopp), kritiska beroenden etc. Inom Vård och omsorgsförvaltningen finns det även en MAS-rutin (Medicinskt ansvarig sjuksköterska) som exempelvis innehåller instruktioner om att det alltid ska finnas utskrivna journaler i pappersform. Raindance: Nej, det finns ingen modell för detta. Diskussioner är pågående kring att det finns ett behov av att ta fram detta.	Avvikelser identifierade	Inga avvikelser identifierade	Avvikelser identifierade
3.2	Har sårbarhetsanalyser upprättats och dokumenterats för verksamhetssystem?	Procapita BOU: Nej, se 3.1. Procapita VOO: Det finns en verksamhetsövergripande sårbarhetsanalys (se 3.1), men inget specifikt framtaget för Procapita VOO. Raindance: Nej, se 3.1.	Avvikelser identifierade	Vissa avvikelser identifierade	Avvikelser identifierade
4 *Styrning av åtkomst*					
4.1	Finns det ett regelverk för hur åtkomsträttigheter skall hanteras? Är regelverket beslutat, aktuellt och har en ägare?	Procapita BOU: Nej, det finns inget dokumenterat regelverk avseende åtkomsträttigheter för Procapita BOU. Användare kan både ringa eller maila någon av systemförvaltarna för att erhålla åtkomst. Procapita VOO: Ja, det finns en dokumenterad rutin för ”beställning av nytt/ändring/avslut Procapitakonto”. Rutinen finns tillgänglig på intranätet och anger vem som har rätt att beställa en behörighet, till vem beställningen ska läggas och övriga rutiner kopplat till behörighetshanteringen. Rutinen uppdateras vid behov av systemförvaltare. Det finns även en behörighetsmatris som visar roller och relaterade behörigheter. Behörighetsrutin och behörighetsmatris mottogs och verifierades i samband med granskningen. Raindance: Nej, det finns inget dokumenterat regelverk för behörighetshantering.	Avvikelser identifierade	Inga avvikelser noterade	Avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
4.2	Finns det en rutin för tilldelning av åtkomsträttigheter?	Procapita BOU: Rutinen är muntlig. Användare kan både ringa och maila för att erhålla behörighet. Spårbarheten är avhängig att användaren mailat och att personen som tagit emot mailet har sparat detta i sin personliga brevlåda. Procapita VOO: Ja, detta följer den rutin som beskrevs under punkt 4.1. För att verifiera att rutinen efterlevs valdes ett stickprov av en ny användare ut. Inga avvikelser noterades baserat på stickprovet. Raindance: Det saknas en dokumenterad rutin för tilldelning av åtkomsträttigheter. För att verifiera processen kring tilldelning av åtkomsträttigheter begärdes en systemgenererad lista över samtliga användare (totalt 2862 aktiva användare) ut i samband med granskningen. Vi fick se exempel på en beställning och kunde då verifiera att beställning var genomförd på korrekt vis.	Vissa avvikelser identifierade	Inga avvikelser noterade	Vissa avvikelser identifierade
4.3	Tilldelas användare åtkomsträttigheter endast efter beslut av utsedd behörig personal?	Procapita BOU: Normalt sett krävs godkännande av chefen. Det är endast systemförvaltare som ska lägga upp nya konton. Eftersom det ej finns någon spårbarhet kring upplägg och beställningar har vi inte kunnat verifiera hanteringen av detta. Procapita VOO: Ja, beställning godkänns enbart om det kommer från närmsta chef eller motsvarande. Det finns ingen lista över behöriga beställare, men listan följer attestlistan i ekonomisystemet, så i de fall behörighetsadministratören är osäker går det att dubbelkolla detta i ekonomisystemet. Utifrån det stickprov som valdes ut i samband med granskningen identifierades inga avvikelser, se 4.2. Raindance: En behörig person på ekonomiavdelningen lägger upp nya användare. Beställning ska komma från behörig ekonom på respektive förvaltning. Det finns ingen dokumenterad förteckning över behöriga beställare. Enligt uppgift vet behörighetsadministratörerna vem som har rätt att beställa behörigheter.	Vissa avvikelser identifierade	Inga avvikelser identifierade	Vissa avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
4.4	Tilldelas användare personliga användarkonton?	Procapita BOU: Respektive friskola och vuxenutbildning använder gruppkonton. Deras konton har begränsade rättigheter. I övrigt har användarna personliga konton. Vi har ej kunnat verifiera att så är fallet då det i samband med granskningen ej var möjligt att få ut en lista från systemet över samtliga användarkonton. Procapita VOO: Ja, enbart personliga användarkonton. Konsulter från Tieto har gruppkonton, men dessa konton måste låsas upp av IT-avdelningen innan de kan användas, och de kan då endast användas under en begränsad tid. Raindance: Ja, det finns enbart personliga användarkonton, och det gäller även CGI:s konsulter. Helpdesk har ett gemensamt sys-konto. Ovanstående verifierades efter genomgång av listan över samtliga användare som begärdes ut i samband med granskningen, se 4.2.	Vissa avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade
4.5	Tilldelas användaren behörighetsprofil som endast medger åtkomst som krävs för att lösa arbetsuppgifterna?	Procapita BOU: Ja, utifrån den roll personen har i organisationen får de en profil i systemet. Passar man inte in i en roll så får man lägsta behörighet och så utökas den utöver detta kopplat till vilka arbetsuppgifter som ska utföras. Vi har ej kunnat verifiera detta då det i samband med granskningen ej var möjligt att få ut en lista från systemet över samtliga användarkonton. Procapita VOO: Ja, detta regleras via behörighetsrutinen och verifierades genom stickprov, se 4.2. Raindance: Användare delas in efter vilken förvaltning de tillhör. Systemet har idag ingen funktionalitet för att applicera rollbaserade behörigheter, detta kommer komma i kommande releaser. Varje användare tilldelas dock enbart de behörigheter som krävs för att utföra sina arbetsuppgifter. Behörigheter graderas för respektive kommando/transaktion från 0-7 där 7 är högsta behörighet. I samband med granskningen erhöll vi en lista över samtliga användare innehållande vilken behörighetsgrad (0-7) de har för respektive transaktion. Antal användare för de mest kritiska transaktionerna (exempelvis inköp, fakturahantering) är begränsat till ett fåtal.	Vissa avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade
4.6	Sker återkoppling till användare (tilldelning av användarnamn och lösenord) enligt särskild rutin?	Procapita BOU: Det saknas en rutin, men enligt nuvarande förfarande mailas informationen ut till beställaren i det fall användaren är nyanställd. Annars skickas informationen ut direkt till användaren. Procapita VOO: Det sker via mail direkt till beställaren. Raindance: Det sker via mail direkt till användaren.	Inga avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
4.7	Finns ett begränsat antal systemadministratörer som tilldelar åtkomsträttigheter till nya användare, respektive ändrar åtkomsträttigheter för befintliga användare?	Procapita BOU: Det finns tre systemadministratörer utöver de på Tieto och den centrala IT-enheten. Detta har vi dock inte kunnat verifiera då det i samband med granskningen ej var möjligt att få fram någon dokumentation som stödjer detta. Procapita VOO: Ja, det finns enbart två utsedda systemadministratörer. Vi verifierade detta genom skärmdump från systemet över medlemmar i gruppen ”behörighetsansvarig”. Raindance: Det finns ett fåtal användare med administratörsbehörighet i systemet.	Vissa avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade
4.8	Finns det regler avseende lösenordskrav?	För samtliga system som omfattas av granskningen gäller att inloggning först måste ske via Active Directory (AD) och sedan separat inloggning till systemet. Vi mottog lösenordsinställningarna för AD i samband med granskningen. Komplexitetskrav är avaktiverade i inställningarna, men i övrigt är inställningarna inom ramen för vad som är acceptabelt ur ett säkerhetsperspektiv. Procapita BOU: Det är IT-avdelningen som ansvarar för regler och rutiner avseende lösenordskrav. Lösenordskrav kan ej ändras av Procapitas systemadministratörer utan enbart av IT. Systemadministratörerna kan dock begära åtkomst att ändra lösenordskrav, vilket görs via ett ärende till IT. Vi verifierade lösenordsinställningarna för Procapita BOU och de är inom ramen för vad som är acceptabelt ur ett säkerhetsperspektiv. Procapita VOO: Det finns inga generella riktlinjer centralt från Lunds kommun avseende lösenordskrav utan det ligger under respektive förvaltnings ansvar att ange lösenordskrav för de system de ansvarar för. Vi verifierade lösenordsinställningarna för Procapita VOO och de är inom ramen för vad som är acceptabelt ur ett säkerhetsperspektiv. Raindance: Det finns inga dokumenterade regler eller riktlinjer avseende lösenordskrav.	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Avvikelser identifierade
4.9	Följer implementerade lösenordskrav upprättade regler avseende lösenordskrav?	Procapita BOU: Se 4.8. Procapita VOO: Det finns implementerade lösenordskrav för Procapita VOO. Lösenordsinställningarna har verifierats genom stickprov (skärmdump från systemet) och de ligger inom ramen för rekommenderade nivåer. Raindance: Det finns inga dokumenterade lösenordskrav för Raindance. I samband med granskningen mottog vi en skärmdump från systemet över gällande lösenordsinställningarna, och vi noterade att det enbart finns krav på 3 tecken i lösenordet samt byte var 160:e dag, övriga krav (såsom komplexitetskrav i form av stora och små bokstäver, siffor etc.) är ej angivna och aktiverade.	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
4.10	Hanteras nya användares initiala lösenord på ett säkert sätt?	Procapita BOU: Användares initiala lösenord skickas ut från systemförvaltare till användare via okrypterad mail. Se 4.6. Lösenord och användarnamn är samma, det är dock tvingande byte vid första inloggning till ett lösenord som möter de uppställda lösenordskraven. Procapita VOO: Uppgifter går ut via mail, tillfälligt lösenord skrivs i klartext. Användaren måste byta till eget lösenord, annars ges ingen åtkomst till Procapita. Raindance: Sker via mail, se 4.6	Inga avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade
4.11	Leder felaktiga inloggningar till att användarens konto spärras?	Procapita BOU: Fem försök att logga in, sedan spärras kontot och måste aktiveras av sys admin eller IT innan det kan användas igen. Inställningarna verifierades genom skärmdump från systemet. Procapita VOO: Ja, efter fem inloggningsförsök. Inställningarna verifierades genom skärmdump från systemet. Raindance: Konton spärras först efter tio felaktiga inloggningsförsök. I tillägg är nuvarande lösenordsinställningar svaga (se 4.9).	Inga avvikelser identifierade	Inga avvikelser identifierade	Avvikelser identifierade
4.12	Öppnas låsta användarkonton först efter säker identifiering av användaren?	Procapita BOU: Är det en okänd person så mailas nya inloggningsuppgifter ut till personen med nytt (tillfälligt) lösenord. Om det är en för systemförvaltaren ”känd” person så får de nytt lösenord direkt i telefon. Det sker ej någon verifiering av att användaren också är den som ringt och begärt lösenord. Procapita VOO: Ja, genom verifiering av personnummer och användarnamn. Raindance: Kontakt ska tas med Servicedesk för att låsa upp konton, men detta kringgås ofta enligt uppgift från systemförvaltaren och direktkontakt tas ofta med systemförvaltare eller annan personal med höga behörigheter i systemet.	Avvikelser identifierade	Inga avvikelser identifierade	Avvikelser identifierade
4.13	Finns det en rutin för borttag av behörighet?	Procapita BOU: Det finns ingen dokumenterad rutin för detta utan det fångas upp av systemadministratörerna i de fall de får kännedom om att någon slutar. Vi har därför ej kunnat ta något stickprov. Procapita VOO: Ja, behörighetsrutinen innehåller ett avsnitt kring borttag av behörigheter, se 4.2. Raindance: Det finns ingen dokumenterad rutin för borttag av behörigheter. Vi har därför inte kunnat verifiera att rutin efterlevs.	Avvikelser identifierade	Inga avvikelser identifierade	Avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
4.14	Dras åtkomsträtten till information och verksamhetssystem in vid avslutande av anställning eller vid förflyttning?	Procapita BOU: Vid förflyttning ska den specifika rollen spärras och vid avslutande eller tjänstledighet avaktiveras användarkontot och därmed samtliga behörigheter för användaren. Detta under förutsättning att det kommer till systemförvaltarnas kännedom att personen har slutat. Enligt uppgift från systemförvaltaren missas detta dock ofta och baserat på detta har vi valt att ej ta några stickprov. Procapita VOO: Ja, enligt gällande rutin. Rutinen har verifierats via stickprov av indragen åtkomsträtt i samband med avslutad anställning. Inga avvikelser identifierades. Raindance: I de fall det framkommer att någon slutar tas behörigheten bort, men det händer enligt uppgift från systemförvaltaren att detta missas. Baserat på ovanstående information har stickprov ej tagits.	Avvikelser identifierade	Inga avvikelser identifierade	Avvikelser identifierade
4.15	Finns det en rutin för periodisk genomgång av åtkomsträttigheter?	Procapita BOU: Nej, det finns ingen rutin för periodisk genomgång av behörigheter. Procapita VOO: En implementerad rutin saknas, men periodisk genomgång av användare och deras behörigheter genomförs vanligtvis en gång per år, senast i oktober 2014. I samband med granskningen mottog vi underlag från den periodiska genomgången i form av mailunderlag till respektive enhetschef med bifogad användarlista samt begäran om granskning av listan och återkoppling till systemförvaltare. Raindance: Periodisk genomgång genomfördes en gång förra året avseende attesträttigheter. Genomgång av höga behörigheter genomförs ej.	Avvikelser identifierade	Vissa avvikelser identifierade	Avvikelser identifierade
4.16	Genomförs kvartalsvis kontroll av åtkomsträttigheter?	Procapita BOU: Nej, det sker inte. Se 4.15. Däremot så går systemförvaltarna igenom vilka som har möjlighet att se skyddad identitet med regelbundenhet. Denna genomgång dokumenteras ej varvid vi ej kunnat erhålla några stickprov. Procapita VOO: Nej, Se 4.15 Raindance: Nej, se 4.15.	Avvikelser identifierade	Vissa avvikelser identifierade	Avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
4.17	Godkänns kontrollen av åtkomsträttigheter av annan personal än den som administrerar åtkomsträttigheterna ?	Procapita BOU: Ja, det krävs att användarens enhetschef godkänner behörigheten. Då det inte krävs skriftlig beställning (se 4.2) så finns det inte alltid någon skriftlig dokumentation. Därför har vi ej tagit något stickprov kring detta. Procapita VOO: Ja, se 4.2. Raindance: Ja, godkännande sker av ekonomer/närmsta chef och läggs upp av systemadministratör. I det stickprov som testades (se även 4.2.) noterades inga avvikelser avseende ansvarsfördelning i samband med godkännande av åtkomsten.	Avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser noterade
4.18	Finns beslut om att ett verksamhetssystems information ska få bearbetas på distans med stationär eller mobil utrustning?	Procapita BOU: Nej, det finns inget dokumenterat. Procapita VOO: Nej, det finns inget dokumenterat. Raindance: Nej, det finns inget dokumenterat. Enligt systemförvaltaren finns beslut om möjlighet att arbeta på distans. Detta beslut är dock inte dokumenterat.	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade
4.19	Har verksamheten ställt tekniska säkerhetskrav och krav på praktisk hantering avseende användandet av mobil datorutrustning och distansarbete?	Procapita BOU: Verksamheten har inte ställt några specifika krav på mobil utrustning eller distansarbete. Procapita VOO: Med leverantörens nya modul ”Lifecare” krävs tvåstegsinloggning, som idag sker med Siths- kort. Raindance: Det krävs att användaren installerat Citrix. Det går även att attestera via en app.	Avvikelser identifierade	Inga avvikelser identifierade	Vissa avvikelser identifierade
4.20	Finns det segregering av arbetsuppgifter i hanteringen av åtkomsträttigheter?	Procapita BOU: Det har ej varit möjligt att verifiera segregering av arbetsuppgifter i samband med granskningen. Se 4.17. Procapita VOO: Ja, se 4.2 Raindance: Ja, se 4.17.	Avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
5 Spårbarhet					
5.1	Genomförs loggning av känsliga transaktioner i systemet?	Procapita BOU: Ja, alla transaktioner loggas som standard i Procapita. Procapita VOO: Ja, alla aktiviteter i systemet loggas. Det finns en implementerad rutin, ”Loggkontroll i Procapita – rutin för granskning av åtkomst till brukar- och patientuppgifter i intern regi”. Underlag för rutiner kring och hantering av loggar har mottagits och granskats. Raindance: Viss loggning genomförs för känsliga transaktioner, men det sker inte i någon större omfattning.	Inga avvikelser identifierade	Inga avvikelser identifierade	Vissa avvikelser identifierade
5.2	Genomförs granskning och uppföljning av loggar?	Procapita BOU: Nej, det sker inte. Procapita VOO: Ja, det sker enligt den rutin som beskrivs i 5.1. Vid granskningstillfället mottogs även ett exempel på begäran om stickprov på användare och loggade aktiviteter. Den här typen av kontroll sker varannan månad för att säkerställa att det inte sker någon obehörig åtkomst till brukar – och patientuppgifter. Chefen för den personal som ska granskas ansvarar för att kontrollera logg-rapporten. Raindance: Nej, se 5.1.	Avvikelser identifierade	Inga avvikelser identifierade	Avvikelser identifierade
6 Styrning av programändringar					
6.1	Finns det ett regelverk för hur programändringar skall hanteras? Är regelverket beslutat, aktuellt och har en ägare?	Procapita BOU: Det finns viss dokumentation och beskrivningar av rutiner i systemöverenskommelsen (SLA) mot IT-avdelningen, senast uppdaterad 2013. Där finns exempelvis angivet att systemägaren (förvaltningschefen) är den som ska godkänna förändringar från Tieto som initierats av systemförvaltarna. Det saknas dock beskrivning av hur testning av förändringar samt driftsättning ska hanteras. Procapita VOO: Det finns ingen intern dokumenterad rutin. Nya uppdateringar och service packs sker enligt standardavtal med Tieto. Ett schema över servicefönster (en gång per månad) finns på intranätet. Listan mottogs i samband med granskningen. Raindance: Nej, det finns inget dokumenterat regelverk för detta, men det finns ett erkänt arbetssätt/förfarande kring detta som innebär att CGI endast får godkänna beställningar som kommer från systemförvaltaren. Utvecklingsarbete hanteras även till viss del i serviceavtalet mot CGI.	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Vissa avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
6.2	Finns det en rutin för beslut om/beställning av uppdateringar/förändringar av verksamhetssystem?	Procapita BOU: Se 6.1. Det saknades dokumentation kring beställning och godkännande av genomförda förändringar i samband med granskningen, därför har kontrollutförandet inte kunnat verifieras. Procapita VOO: Nej, Se 6.1 Raindance: Nej, Se 6.1	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Vissa avvikelser identifierade
6.3	Sker beslut om/beställning av uppdateringar/förändringar av verksamhetssystem av endast utsedd behörig personal?	Procapita BOU: Se 6.2. Procapita VOO: Enligt en informell rutin är det förvaltningschefen som fattar beslut och har delegation på att skriva avtal. Det finns dock ingen dokumenterad rutin som beskriver detta förfarande. Raindance: Nej, Se 6.1	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Vissa avvikelser identifierade
6.4	Finns det en rutin för test av uppdateringar/förändringar av verksamhetssystem?	Procapita BOU: Nej. Förändringar produktionssätts av Lunds kommuns IT-avdelning efter leverans av den nya funktionen från Tieto. Vid stora förändringar (såsom versionsuppdateringar) ska den nya funktionen testas i testmiljö först. Mindre funktionsändringar (såsom fixar) produktionssätts direkt utan föregående testning. Procapita VOO: Det finns en separat testmiljö men denna används sällan då systemleverantören Tieto genomför egen testning innan nya releaser släpps. Raindance: För varje release/versionsuppdatering finns beskrivna rutiner hur test ska ske. Testning sker alltid först i testsystem innan det förs in i drift. Driftansvarig genomför ett test i form av uppstart av systemet, inloggning etc. för att säkerställa att detta fungerar. Vid större förändringar går även användare in och testar. Vi har mottagit testprotokoll från den senaste versionsuppdateringen som driftsattes i oktober 2014.	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Inga avvikelser identifierade
6.5	Genomförs tester av modifierade system innan uppdateringar/förändringar av verksamhetssystem?	Procapita BOU: Nej, se 6.4. Procapita VOO: Nej, se 6.4 Raindance: Ja, se 6.4.	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Inga avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
6.6	Godkänns testet av uppdateringar/förändringar av verksamhetssystem?	Procapita BOU: Nej, se 6.4. Procapita VOO: Nej, se 6.4 Raindance: Nej, inget dokumenterat godkännande, men testet dokumenteras, se 6.4	Avvikelser identifierade	Avvikelser identifierade	Vissa avvikelser identifierade
6.7	Sker system-/programutveckling samt tester av modifierade system åtskilt från driftmiljön?	Procapita BOU: Det finns en separat testmiljö som är åtskild från driftmiljön som dock inte alltid används. Procapita VOO: Det finns en separat testmiljö som är åtskild från driftmiljön som dock inte alltid används. Raindance: Det finns en separat testmiljö som är åtskild från driftmiljön som dock inte alltid används.	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Vissa avvikelser identifierade
6.8	Uppdateras testmiljön kontinuerligt?	Procapita BOU: Då testmiljön inte alltid används har vi valt att inte ta stickprov. Procapita VOO: Då testmiljön inte alltid används har vi valt att inte ta stickprov. Raindance: Ja, det sker i och med att förändringar testas först i testmiljön.	Vissa avvikelser identifierade	Vissa avvikelser identifierade	Inga avvikelser identifierade
6.9	Finns det en rutin för införande av uppdateringar/förändringar av verksamhetssystem?	Procapita BOU: Ja, det finns fastslagna servicefönster (månadsbasis). Tidsintervall för dessa finns dokumenterade i systemöverenskommelsen. Procapita VOO: Ja, det finns fastslagna servicefönster (månadsbasis). Datum för dessa finns dokumenterade på intranätet och kontaktpersoner som ansvarar för servicefönster är angivna. Raindance: Det finns ingen dokumenterad rutin, men förfarandet innebär att det alltid är driftansvarig som produktionssätter förändringar.	Inga avvikelser identifierade	Inga avvikelser identifierade	Vissa avvikelser identifierade
6.10	Sker godkännande av driftsättningar endast utsedd behörig personal?	Procapita BOU: Ja, Se 6.4. Procapita VOO: Ja, det sker av de kontaktpersoner som är angivna enligt anvisningar för servicefönster, se 6.9 Raindance: Ja, det sker av IT-driftsansvarig.	Inga avvikelser identifierade.	Inga avvikelser identifierade	Inga avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
6.11	Begränsas rätten att installera uppdateringar/förändringar till endast utsedd behörig personal?	Procapita BOU: Det är tre personer på IT-avdelningen som har rätt att installera uppdateringar. Procapita VOO: Driftsanvarig på IT-avdelningen ansvarar för driftsättning. Det finns även reservpersonal på IT-avdelningen som backup. Raindance: Det finns en utsedd IT-driftsansvarig på IT-avdelningen som ansvarar för driftssättning/installation av förändringar.	Inga avvikelser identifierade.	Inga avvikelser identifierade	Inga avvikelser identifierade
6.12	Finns det segregering av arbetsuppgifter i hantering av programändringar?	Procapita BOU: Ja, all utveckling sker av Tieto och Lunds kommuns IT-avdelning produktionssätter dessa förändringar. Procapita VOO: Ja, se 6.1 Raindance: Ja, se 6.1.	Inga avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade
7 Kontinuitets- och avbrottsplanering					
7.1	Har systemägare eller motsvarande beslutat om den längsta acceptabla tid som verksamhetssystemet bedöms kunna vara ur funktion innan verksamheten äventyras?	Procapita BOU: Det finns inget formellt eller dokumenterat beslut kring detta. Procapita VOO: Det finns inget formellt eller dokumenterat beslut kring detta. Raindance: Det finns inget formellt eller dokumenterat beslut kring detta.	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade
7.2	Regleras tillgänglighetskrav i avtal med IT-driftleverantören?	Procapita BOU: Det finns inget formellt eller dokumenterat beslut kring detta. Procapita VOO: Det finns inget formellt eller dokumenterat beslut kring detta. Raindance: Det finns inget formellt eller dokumenterat beslut kring detta.	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade
7.3	Genomförs uppföljning mot tillgänglighetskrav?	Procapita BOU: Nej, se 7.2. Procapita VOO: Nej, se 7.2. Raindance: Nej, se 7.2.	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
7.4	Regleras krav på avbrottsplan i avtal med IT-driftleverantören?	Procapita BOU: Nej, se 7.2. Procapita VOO: Nej, se 7.2. Raindance: Nej, se 7.2.	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade
7.5	Finns det en avbrottsplan med återstartsrutiner för IT-driften?	Procapita BOU: Nej, se 7.2. Procapita VOO: Nej, se 7.2. Raindance: Nej, se 7.2.	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade
7.6	Finns det en kontinuitetsplan med reservrutiner för verksamheten?	Procapita BOU: Nej, det finns inte. Procapita VOO: Ja, det finns en MAS-rutin, se 3.1 Raindance: Nej.	Avvikelser identifierade	Inga avvikelser identifierade	Avvikelser identifierade
7.7	Regleras säkerhetskopiering i avtal med IT-driftleverantören?	Procapita BOU: Ja, det regleras i SLA (Systemöverenskommelsen) med IT-avdelningen. Både Procapita BOU och SQL säkerhetskopieras. Procapita VOO: Ja, det regleras i systemöverenskommelsen mot IT-avdelningen. Raindance: Säkerhetskopiering regleras i systemöverenskommelsen med IT-avdelningen. Backup sker dock mer frekvent än vad som är angivet i systemöverenskommelsen.	Inga avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade
7.8	Genomförs säkerhetskopiering regelbundet?	Procapita BOU: Ja, se 7.7. Vi mottog även utdrag från säkerhetskopieringsverktyget för att verifiera senast genomförda säkerhetskopiering. Inga avvikelser noterades. Procapita VOO: Ja, se 7.7. Vi mottog även utdrag från säkerhetskopieringsverktyget för att verifiera senast genomförda säkerhetskopiering. Inga avvikelser noterades. Raindance: Ja, se 7.7. Vi mottog även utdrag från säkerhetskopieringsverktyget för att verifiera senast genomförda säkerhetskopiering. Inga avvikelser noterades.	Inga avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade

Granskningspunkt		Kommentar	Utvärdering Procapita BOU	Utvärdering Procapita VOO	Utvärdering Raindance
7.9	Genomförs regelbundna tester för att säkerställa att verksamhetssystem kan återstartas från säkerhetskopior?	Procapita BOU: Nej, det sker vid behov. Procapita VOO: Nej. Raindance: Ja, det genomförs minst årligen.	Avvikelser identifierade	Avvikelser identifierade	Inga avvikelser identifierade
8 IT-säkerheten hos utomstående part					
8.1	Har ansvaret för IT-säkerheten reglerats i avtal med IT-driftleverantören?	Procapita BOU: Det finns inget specifikt avtal kring detta. Se även 8.4 Procapita VOO: Det finns inget specifikt avtal kring detta. Se även 8.4 Raindance: Det finns inget specifikt avtal kring detta. Se även 8.4	Avvikelser identifierade	Avvikelser identifierade	Avvikelser identifierade
8.2	Reglerar avtalet med IT-driftleverantören överföring och lagring av data?	Samtliga system: IT-driften hanteras internt.	Ej tillämplig		
8.3	Hanteras överföringar/lagringar av verksamhetssystemens data endast inom Sverige?	Procapita BOU: All data lagras i Sverige. Procapita VOO: Ja, enbart inom Sverige. Raindance: Ja, enbart inom Sverige.	Inga avvikelser identifierade	Inga avvikelser identifierade	Inga avvikelser identifierade
8.4	Reglerar avtalet med IT-driftleverantören fysisk säkerhet för datorhallar?	Samtliga system: Det finns ingen dokumenterad rutin kring fysisk säkerhet. Lunds kommun hyr lokal/datorhall av Kraftringen. Fem personer på IT-avdelningen har åtkomst till datorhallen via tagg som förvaras i låst nyckelskåp där uttag av tagg registreras.	Inga avvikelser identifierade		
8.5	Genomförs periodiska genomgångar av personal med tillträde till datorhallar för att säkerställa att enbart behörig personal har tillträde?	Samtliga system: Nej, periodiska genomgångar genomförs inte.	Avvikelser identifierade		
8.6	Reglerar avtalet med IT-driftleverantören rätten att granska IT-driftleverantören?	Samtliga system: IT-driften hanteras internt.	Ej tillämplig		

4 Slutsatser

Sammanställning av slutsatser

EY har gjort en granskning av IT- och Informationssäkerheten i Lunds kommun utifrån utvalda granskningspunkter i BITS-ramverket. De mest verksamhetskritiska systemen identifierades i samarbete med Lunds kommuns IT-avdelning och respektive förvaltningschef. De tre system som ingår i granskningen har valts ut av de förtroendevalda revisorerna baserat på den övergripande riskanalysen, se 3.1.

Vår granskning av systemen Procapita BOU, Procapita VOO samt Raindance på respektive förvaltning inom Lunds kommun har visat på stora skillnader i hantering beroende på förvaltning. Den genomgående bristen är avsaknad av dokumenterade rutiner och processer för att hantera förvaltningen av systemen. Vi noterade att det i många fall inte finns någon dokumentation avseende exempelvis hantering av programförändringar och relaterad ansvarsfördelning. Vi noterade i samband med granskningen att det under 2009-2010 genomförts initiativ avseende IT – och informationssäkerhet med syfte att skapa en mer formaliserad hantering med dokumenterade rutiner och processer. I de fall där vi noterade dokumentation kring exempelvis säkerhetsklassning av verksamhetssystem och liknande så var den typen av underlag inte alltid allmänt kända på förvaltningarna. En bidragande orsak till att genomförda initiativ inte fått tillräckligt genomslag kan vara att de främst varit drivna av IT-avdelningen, inte i första hand av förvaltningarna själva.

Under 2015 kommer informationssäkerheten att ses över på de system som IT-avdelningen driftar och samtliga system kommer att revidera informationssäkerhetsklassningen och tillhörande instruktioner. I samband med detta kommer nya SLA (tjänstenivåavtal) att tecknas och ambitionen är bland annat att skapa en tydligare hantering för exempelvis kontinuitets - och avbrottsplanering.

Vi har under vår granskning noterat ett antal brister som kan tyda på ett generellt problem i Lunds kommuns hantering av sina verksamhetssystem. Vi skulle därför rekommendera att Lunds kommun undersöker om dessa brister är en del i ett större sammanhang där centrala styrdokument, i den mån de finns dokumenterade, inte når ut och efterlevs på förvaltningarna.

5 Rekommendationer

Nedan följer våra rekommendationer samt ett förslag på prioritering.

Rekommendationerna är prioriterade enligt följande:

Hög	Bristen bör åtgärdas snarast för att inte äventyra verksamheten.
Medel	Bristen bör åtgärdas på sikt för att undvika störningar och problem i verksamheten.
Låg	Bristen bör åtgärdas på lång sikt för att förbättra verksamheten.

5.1 Generella rekommendationer

#	Iakttagelse och rekommendation	Prioritet
1.	Iakttagelse: Avsaknad av avbrottsplan för de mest kritiska systemen Vi har noterat att Lunds kommun saknar en dokumenterad avbrottsplan för de verksamhetssystem som ingick i granskningen. Vi noterade även att Lunds kommun saknar en översikt och rangordning kring vilka system som är mest verksamhetskritiska. Rekommendation: Vi rekommenderar Lunds kommun att identifiera de mest kritiska systemen samt utforma en avbrottsplan för dessa. Rutinerna bör innehålla följande: • Proaktiva kontroller för att undvika avbrott • Reservrutiner vid avbrott för tänkta scenarios • Rutiner för återställning av system • Rutiner för återskapande av förlorad information • Rutiner för inmatning av data från reservrutiner • Periodisk testning av rutiner	Hög

#	Iakttagelse och rekommendation	Prioritet
2.	Iakttagelse: Svaga krav på lösenord i de olika applikationerna Vi noterade under vår granskning att kraven på användarnas lösenord avseende längd, komplexitet, frekvens på byte etc. skiljer sig åt mellan de olika applikationerna. För Raindance var lösenordsinställningarna inte inom ramen för rekommenderade nivåer, exempelvis ställs där endast krav på tre tecken i lösenordet samt inga komplexitetskrav. Rekommendation: Vi rekommenderar Lunds kommun att ställa centrala krav på lösenord samt implementera en single sign-on lösning som kopplar inloggningen till respektive applikation till Active Directory. Lösenordskraven bör minst omfatta följande: • Lösenordshistorik på minst 6 generationer • Byte av lösenord var 90:e dag • Minst 8 tecken • Lösenordskomplexitet i form av stora/små bokstäver, specialtecken och siffror • Låsning av konton efter 5 misslyckade inloggningsförsök	Medel

5.2 Procapita BOU

#	Iakttagelse och rekommendation	Prioritet
1.	Iakttagelse: Avsaknad av systemförvaltningsmodell Vi har noterat att det saknas en systemförvaltningsmodell för Procapita BOU som dikterar hur ansvaret för processerna kring systemet ska hanteras. Rekommendation: Vi rekommenderar Lunds kommun att implementera en systemförvaltningsmodell för sina system. Exempel på etablerade systemförvaltningsmodeller är exempelvis PM3 och ITIL.	Medel

#	Iakttagelse och rekommendation	Prioritet
2.	Iakttagelse: Avsaknad av regelverk för hantering av behörigheter Vi har noterat att det saknas dokumenterade rutiner för hantering av behörigheter avseende Procapita BOU. Rekommendation: Vi rekommenderar Lunds kommun att dokumentera ett övergripande regelverk för styrning av behörigheter i Procapita BOU. Rutinerna bör minst omfatta följande kontroller och aktiviteter: • Det bör framgå vem som har rätt att besluta om nya/ändrade behörigheter • Det bör framgå vem som har behörighet att lägga upp nya/ändrade behörigheter i systemet • Det bör framgå vem som får beställa borttag av behörigheter och på vilket sätt detta skall göras • Regelverket bör säkerställa segregering av arbetsuppgifter på så sätt att personen som beslutar om nya/ändrade behörigheter inte lägger upp behörigheten i systemet Regelverket bör innefatta krav på periodisk genomgång av användare, vilket innebär att en utsedd person säkerställer att samtliga behörigheter i Procapita BOU är korrekta i enlighet med användares arbetsroll. Genomgången innefattar även att rapportera och exekvera borttag av obehöriga behörigheter. Frekvensen på dessa genomgångar bör vara kvartalsvis.	Hög

#	Iakttagelse och rekommendation	Prioritet
3.	Iakttagelse: Ansvaret för testning och driftsättning av programförändringar är otydligt Rutiner för beställning av programförändringar finns delvis beskrivet i systemöverenskommelsen mot IT. Det saknas dock dokumenterade rutiner för testning och driftsättning av programförändringar. Systemutveckling driftsätts ofta direkt i produktionssystemet vilket får till följd att buggar och andra funktionsfel förekommer. Det finns en testmiljö men den används inte för att testa samtliga förändringar. Rekommendation: Vi rekommenderar Lunds kommun att införa ett dokumenterat regelverk för styrning av programförändringar i Procapita BOU, vilket bör inkludera såväl versionsuppdateringar som övriga programförändringar. Rutinerna i regelverket bör minst omfatta följande kontroller och aktiviteter: • Det bör framgå vem som får beställa programförändringar samt hur detta skall göras och dokumenteras • Det bör finnas krav på acceptanstesting vid såväl versionsuppdatering som övriga programförändringar samt hur det ska genomföras, dokumenteras och vem som är ansvarig för att utföra det. Acceptanstestning bör göras i testmiljön innan förändringen implementeras i produktionsmiljön • Det bör framgå vem som får godkänna driftsättning av programförändringar och hur detta skall göras och dokumenteras.	Medel
4.	Iakttagelse: Avsaknad av sårbarhetsanalys Vi har noterat att det inte har genomförts någon sårbarhetsanalys av Procapita BOU. Vidare saknas en beslutad modell för hur sårbarhetsanalyser ska genomföras. Rekommendation: Vi rekommenderar Lunds kommun att ta fram en modell för hur sårbarhetsanalyser ska genomföras. Vidare rekommenderar vi att sårbarhetsanalyser regelbundet genomförs enligt denna modell.	Låg

5.3 Procapita VOO

#	Iakttagelse och rekommendation	Prioritet
1.	Iakttagelse: Avsaknad av systemförvaltningsmodell Vi har noterat att det saknas en systemförvaltningsmodell för Procapita VOO som dikterar hur ansvaret för processerna kring systemet ska hanteras. Rekommendation: Vi rekommenderar Lunds kommun att implementera en systemförvaltningsmodell för sina system. Exempel på etablerade systemförvaltningsmodeller är exempelvis PM3 och ITIL.	Medel
2.	Iakttagelse: Ansvaret för driftsättning av programförändringar är otydligt Vi noterade att det saknas en intern dokumenterad rutin för driftsättning av förändringar. Rekommendation: Då Tieto har en stor del av ansvaret bör den interna rutinen fokusera på roller och ansvar kopplat till beställning av funktionalitet utöver standard samt underhåll och servicefönster. Rutinen bör även ställa krav på att alla förändringar oavsett storlek genomgår acceptanstest och användartest innan de driftsätts i produktionsmiljön.	Medel
3.	Iakttagelse: Periodisk genomgång av användarbehörigheter sker ej med regelbundenhet Vi noterade att periodisk genomgång ej genomförs med regelbundet intervall. Rekommendation: Vi rekommenderar Lunds kommun att med regelbundenhet genomföra genomgångar av användarkonton i Procapita VOO. Resultatet av dessa granskningar bör dokumenteras och arkiveras. Frekvensen på dessa genomgångar bör vara kvartalsvis.	Medel

5.4 Raindance

#	Iakttagelse och rekommendation	Prioritet
4.	Iakttagelse: Avsaknad av systemförvaltningsmodell Vi har noterat att det saknas en systemförvaltningsmodell för Raindance som dikterar hur ansvaret för processerna kring systemet ska hanteras. Rekommendation: Vi rekommenderar Lunds kommun att implementera en systemförvaltningsmodell för sina system. Exempel på etablerade systemförvaltningsmodeller är exempelvis PM3 och ITIL.	Medel
5.	Iakttagelse: Avsaknad av regelverk för hantering av behörigheter Vi har noterat att det saknas övergripande regelverk och dokumenterade rutiner för hantering av behörigheter avseende Raindance. Rekommendation: Vi rekommenderar Lunds kommun att dokumentera ett övergripande regelverk för styrning av behörigheter i Raindance. Rutinerna bör minst omfatta följande kontroller och aktiviteter: • Det bör framgå vem som har rätt att besluta om nya/ändrade behörigheter • Det bör framgå vem som har behörighet att lägga upp nya/ändrade behörigheter i systemet • Det bör framgå vem som får beställa borttag av behörigheter och på vilket sätt detta skall göras • Regelverket bör säkerställa segregering av arbetsuppgifter på så sätt att personen som beslutar om nya/ändrade behörigheter inte lägger upp behörigheten i systemet Regelverket bör innefatta krav på periodisk genomgång av användare, vilket innebär att en utsedd person säkerställer att samtliga behörigheter i Raindance är korrekta i enlighet med användares arbetsroll. Genomgången innefattar även att rapportera och exekvera borttag av obehöriga behörigheter. Frekvensen på dessa genomgångar bör vara kvartalsvis.	Hög

#	Iakttagelse och rekommendation	Prioritet
6.	Iakttagelse: Avsaknad av sårbarhetsanalys Vi har noterat att det inte har genomförts någon sårbarhetsanalys av Raindance. Vidare saknas en beslutad modell för hur sårbarhetsanalyser ska genomföras. Rekommendation: Vi rekommenderar Lunds kommun att ta fram en modell för hur sårbarhetsanalyser ska genomföras. Vidare rekommenderar vi att sårbarhetsanalyser regelbundet genomförs enligt denna modell.	Låg
7.	Iakttagelse: Ansvaret för programförändringar är otydligt Vi noterade att det saknas en intern rutin för att hantera programförändringar. Rekommendation: Vi rekommenderar Lunds kommun att upprätta en intern rutin avseende förändringshantering. Då CGI har en stor del av ansvaret behöver rutinen fokusera på roller och ansvar kopplat till beställning av funktionalitet utöver standard samt underhåll och servicefönster. Vi rekommenderar även att rutinen innehåller krav på att förändringar även testas av slutanvändare för att säkerställa att funktionalitet inte påverkas negativt.	Medel

6 Bilagor

6.1 Procapita BOU

- Ansvarsfördelning IKT-Team
- Lösenordsinställningar
- Systemansvarig per område
- Systemleverantörsavtal
- Systemöverenskommelse (SLA)

6.2 Procapita VOO

- Behörighetsmatris
- Behörighetsrollen
- Behörighetsrutin
- Exempel på behörighetsbeställning
- Exempel på process för avslutat användarkonto
- HSL Loggkontroll per enhet
- Loggkontroll rutinbeskrivning
- Loggkontroll handläggare
- Loggschema per enhet
- Lösenordsinställningar
- Periodisk genomgång av användare
- Schema för servicefönster
- Risk- och sårbarhetsanalys
- Systemöverenskommelse (SLA)

6.3 Raindance

- Administratörsbehörigheter
- Exempel på behörighetsbeställning
- Lista över användare och grupptillhörighet
- Lista över samtliga användare
- Loggning av transaktioner
- Lösenordsinställningar
- Periodisk genomgång av attesträttigheter

- Systemintegrationer
- Systemleverantörsavtal inkl. bilagor
- Systemöverenskommelse (SLA)
- Testprotokoll