Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Styrelsen
Internrevisionen

Dnr SLU ua 2013.1.1.2-4732
Exp. den 2014-02-___

BESLUT
2014-02-19

Rektor

Granskning av informationssäkerhet i personaladministrativa system

Beslut

Styrelsen beslutar:

att fastställa internrevisionens rapport Granskning av informationssäkerhet i personaladministrativa system

att fastställa rektors åtgärdsplan med anledning av rapporten

Ärendet

I september – oktober 2013 har internrevisionen genomfört en granskning av informationssäkerheten i SLU:s personaladministrativa system. Granskningen har genomförts av Roger Karlsson KPMG AB.

Granskningens visar att förbättringar behövs avseende det strategiska och taktiska perspektivet när det gäller arbetet med informationssäkerhet, systemförvaltning och styrning/uppföljning av system- och driftleverantörer.

Åtgärdsplanen har utarbetats av universitetsdirektör Martin Melkerson.

Beslut i detta ärende har fattats av styrelsen efter föredragning av internrevisionschef Inga Astorsdotter.

Rolf Eriksson Brennerfelt

Inga Astorsdotter

Kopia för kännedom

Prorektor
Dekanerna
Universitetsdirektören
Avdelningschefer (motsv.) inom universitetsadministrationen

A B C D

Sveriges lantbruksuniversitet

Rapport

Granskning av informationssäkerhet i personaladministrativa system

Arbetet utfört under september-oktober 2013

Internal Audit, Risk & Compliance Services
KPMG AB
2013-11-07

Innehåll

Sammanfattning

Vår bedömning är att *förbättringar behövs* avseende det strategiska och taktiska perspektivet när det gäller arbetet med informationssäkerhet, systemförvaltning och styrning/uppföljning av system- och driftleverantörer till Primula, Vår bedömning är vidare att berörd personal löser de operativa uppgifterna efter bästa förmåga och förutsättningar.

Vår granskning visar att det finns förbättringsmöjligheter när det gäller att systematisk, aktivt och sammanhållet arbeta med:

- Tillgänglighetsaspekter inklusive katastrofplanering
- Åtkomst till system och data
- Systemförvaltning och leverantörsstyrning

Av kapitel två nedan framgår detaljerade iakttagelser, riskbedömning samt våra förslag på åtgärder.

1.Inledning

1.1 Bakgrund

Internrevisionen har, i enlighet med revisionsplanen för 2013, genomfört en granskning av informationssäkerheten i det personaladministrativa systemet Primula. KPMG har bistått SLU:s internrevision med att utföra granskningen.

1.2 Syfte

Syftet med granskningen har varit att kartlägga och bedöma informationssäkerheten för att utvärdera

1. **Tillgänglighe**t: Det finns kontroller som säkerställer att informationen är tillgänglig när och där den behövs i organisationen.
2. **Åtkomst**: Det finns kontroller som säkerställer att informationen är riktigt, fullständig, spårbar och skyddad mot obehörig åtkomst.
3. **Regelefterlevnad:** Det finns kontroller som säkerställer att legala och interna krav efterlevs.
4. **Systemförvaltning:** Det finns en effektiv och ändamålsenlig organisation kring förvaltning och drift av systemet.

1.3 Avgränsning

- Manuella rutiner kring personaladministration ingår inte i denna granskning.
- Vår granskning är en ögonblicksbild och är därför ingen garanti för att samtliga svagheter omfattas av vår rapportering.
- Verifiering av kontroller har skett via stickprov enligt överenskommelse med uppdragsgivaren.
- Införande eller kostnadsbedömning av eventuella förbättringsåtgärder har inte ingått i uppdraget.

1.4 Genomförande och rapportering

Granskningen baseras på analyser av erhållen och under granskningen inhämtad dokumentation kompletterat med intervjuer med relevanta personer från verksamheten samt platsbesök hos system- och driftleverantören Evry.

Granskningsinsatsen har genomförts enligt god internrevisionssed under september-oktober 2013. Granskningen har indelats i fem faser:

1.5 Rapportdisposition

Vår rapport, som är av avvikelsekaraktär, redovisar gjorda iakttagelser, risk och förslag till åtgärder och har grupperats i analogi med områdena under punkt 1.2 ovan i syfte att ge ledningen en överblick samt visa på riskområden där den interna kontrollen behöver förstärkas.

Rapporten har faktagranskats i utkastformat av berörda avdelningar vid SLU.

2. Rapport från internrevisionen

2.1 Tillgänglighet

Iakttagelse I

Tillgänglighet till ett IT-system kan exempelvis vara möjligheten att nå och kommunicera med en resurs, exempelvis en server, ett program eller information, men även tillgänglighet över tiden för användare av resursen. Beroende på hur kritiskt systemet och dess information är så kan olika krav på tillgängligheten ställas av berörda användare.

Primula består av ett antal olika komponenter; en databas där informationen lagras, applikationsserver, klientarbetsplats och Webb-gränssnitt.

Vår granskning visar att det inte skett någon strukturerad riskanalys för att definiera vilka krav som ställs på tillgänglighet på de olika komponenterna och som bör ligga till grund för kravställning på berörda system- och driftleverantörers lösningar.

Vår granskning visar även att det i det befintliga avtalet med driftleverantören Evry saknas krav på vilken tillgänglighet som Evry ska tillhandahålla.

Risk
Brister i kravställning på tillgänglighet kan innebära risk för att användare inte kan komma åt system och data för att fullgöra sina arbetsuppgifter. Risk finns att löneutbetalningar inte kan ske enligt tidplan.

Rekommendation
Vi rekommenderar att SLU genomför en riskanalys i syfte att definiera vilka tillgänglighetskrav som bör gälla för Primula och att dessa krav formuleras i avtalen med berörda leverantörer.

Iakttagelse II

Det är av avgörande betydelse att planera och regelbundet genomföra tester och öva situationer där olika katastrofscenarios simuleras. Syftet med detta är att säkerställa att det finns en avbrottsplanering som fungerar och att såväl alternativa driftmiljöer som alternativa manuella rutiner är tillräckligt dimensionerade och utvecklade. Vidare är syftet även att öva de olika aktiviteter som behöver genomföras vid en övergång till ett katastrofläge såväl som återgång till normaldrift efter ett katastrofläge.

Vår granskning visar att det i nuläget inte finns någon fastställd och kommunicerad reservplan hos SLU, dvs. en plan för hur universitet på ett effektivt sätt ska kunna hantera ett avbrott som innebär att information inte finns tillgänglig under längre period samt att sedan kunna återgå till normal drift efter det att katastrofläget har återgått till normalläge.

Vi noterar även att det i avtalen med driftleverantören inte finns några krav på avbrottsplaner, tester, prioriteringar och andra åtaganden för att tillhandahålla tjänster i händelse av allvarliga avbrott. Det har vid granskningen framkommit att om Evrys lokaler i Uppsala skulle drabbas av en allvarlig incident som innebär att det inte kan fungera som driftställe så finns det inget alternativt driftställe förberett där driften av Primula skulle kunna återupptas.

Risk
Svagheter i avbrotts/katastrofplaner innebär risk för bristande tillgänglighet då alternativ driftmiljö och alternativa arbetssätt inte finns förberedda. Risk finns även att tiden för återgång till normal drift ökar.

Rekommendation
Vi rekommenderar att SLU genomför en riskanalys i syfte att upprätta en sammanhållen avbrottsplan för Primula och tillhörande administrativa rutiner inklusive rutiner för löpande underhåll och test av planen. Vi ser det som väsentligt att planen inte bara avser IT-driften utan även övriga berörda verksamheter och där verksamheternas behov av tillgänglighet till systemet får styra omfattning och inriktning på valda lösningar.

Vi rekommenderar även att avtalen med berörda systemleverantörer, baserat på ovantstående riskanalys, kompletteras med avbrottsplanering så att tillgängligheten kan säkerställas över tid.

2.2 Åtkomst

Iakttagelse
För att säkerställa att endast rätt personer har tillgång till rätt information under rätt förutsättningar behövs en organisation, ansvar och rutiner för behörighetsadministration och behörighetskontrollsystem. Struktur och principer för styrning av åtkomst är väsentliga för att säkerhetsnivån när det gäller tillgång till system och information ska kunna hålla på lämplig nivå.

Det finns i Primula-systemet en stor flexibilitet för respektive användarorganisation att tillämpa det inbyggda behörighetssystemet och strukturen för användare, behörighetsmallar, behörighetsområden, lösenordspolicy etc.

Vår granskning visar att SLU inte fastställt och dokumenterat några principer och regler för hur behörighetssystemet i Primula ska tillämpas. Exempel på detta är om komplexitet på användarnas lösenord för att logga in i systemets klientdel ska följa universitetets AD-regler, hur och av vem som kraftfulla systemadministratörers rättigheter ska användas samt om användning av ”gruppkonton” på Personalavdelningen, dvs. ett användarkonto med gemensamt lösenord som flera personer har tillgång till, ska vara tillåtet. Enligt ”good practice” inom säkerhetsområdet ska gruppkonton undvikas så långt det är möjligt då det i efterhand är omöjligt att entydigt fastställa vem som använt kontot.

Vi konstaterar även att det inte finns några etablerade rutiner för att löpande följa upp system- och driftleverantörernas behörigheter till Primula.

Risk
Informell organisation och rutiner för hantering av behörigheter och behörighetskontrollsystem kan innebära risk för obehörig åtkomst till information. Risk finns även att det i efterhand inte klart och entydigt går att fastställa vilken i personalen som utfört en viss transaktion.

Rekommendation
Vi rekommenderar att universitetet stärker den interna kontrollen genom att formalisera och dokumentera principer och regler för administration och tillämpning av behörigheter i Primula.

Vi rekommenderar även att universitetet analyserar på vilket sätt som kontrollen av användningen av kraftfulla behörigheter kan förstärkas och därefter införa tillförlitliga och ändamålsenliga kontroller. Vi ser det också som väsentligt att SLU ökar insynen hos Evry om vilken personal som har kraftfulla systembehörigheter.

Vi har under granskningens gång fått information om att universitetet genomfört en säkerhetsrevision som avsåg driftmiljön av ett annat administrativt system. I den mån resultat från sådana säkerhetsanalyser kan vara användbara för andra enheter inom universitetet än den närmast berörda, bör Informationssäkerhetsansvarig svara för att sådan information delas.

2.3 Legala och interna krav – Arkivering

Iakttagelse
Av SLU:s arkivplan framgår att följande information ska arkiveras i Primula:

- Lönespecifikation/ Lönesammanställning
- Löneartskatalog
- Avstämning av betydelse för kontroll av transaktionsinformation
- När- och frånvarouppgifter
- Handling rörande namnändring
- Personalekonomisk sammanställning

Vår granskning visar att det inte finns någon aktuell beskrivning av hur kraven i arkivplanen realiseras och hur informationen i Primula ska sparas.

Risk
Risk finns att legala krav på arkivering inte uppfylls.

Rekommendation
Vi rekommenderar att Personalavdelningen, med utgångspunkt i SLU:s Arkivplan, dokumenterar och inför rutiner som säkerställer att arkivplanen efterlevs.

2.4 Systemförvaltning

Iakttagelse I
Systemförvaltning syftar till att löpande följa verksamhetens behov, dess förväntningar och krav och på bästa möjliga sätt stödja detta genom att underhålla befintliga systemfunktioner och tjänster på ett strukturerat, effektivt och ändamålsenligt sätt. Systemförvaltning innebär också att det finns en tydlig organisation, ansvars- och rollfördelning för att säkerställa en effektiv och ändamålsenligt styrning och uppföljning av systemstödet.

Vår granskning visar att Personalavdelningens förvaltning av de personaladministrativa systemen idag sker informellt och att personalen utför arbetsuppgifter, inklusive kontroller, mer på grundval av personlig erfarenhet och ett väl inarbetat arbetssätt än på tillämpningen av en

övergripande förvaltningsstruktur baserat på risk och väsentlighet. Vår granskning visar även på ett nyckelpersonberoende avseende systemförvaltning samt att dokumentationen av systemmiljön, gränssnitt, driftrutiner och uppföljning av utförda kontroller behöver förbättras.

Vi har i samband med granskningen informerats dels om ett förslag på riktlinjer för förvaltningsmodell för administrativa system inom universitetsadministrationen som utarbetades 2008, dels om att IT-avdelningen har utvecklat en modell för förvaltning av de administrativa system som IT har ansvar för.

Risk
Svagheter i rutiner för systemförvaltning kan innebära en risk för att systemen inte hanteras effektivt, ändamålsenligt och säkert.

Brister i dokumentation av systemmiljö och gränssnitt med andra objekt innebär risk att SLU inte har tillräcklig kännedom om arkitektur och säkerhetslösningar samt att förändringar i miljön försvåras.

Nyckelpersonberoende i kombination med svagheter i dokumentation kan innebära risk för bristande tillgänglighet och tillförlitlighet beroende på att avstämningar, felsökning, rättningar etc. tar längre tid om inte nödvändig kompetens finns tillgänglig. Risk finns även att avsiktliga eller oavsiktliga fel inte upptäcks inom rimlig tid.

Rekommendation
Vi rekommenderar att universitetet fastställer en förvaltningsmodell att tillämpas för alla universitetsadministrativa system.

Vi rekommenderar vidare att ansvar och mandat för att förvalta modellen fastställs.

Vi rekommenderar slutligen att Personalavdelningen, med utgångspunkt i beslutad modell, inför tillämpliga delar i sin verksamhet.

Iakttagelse II
Vi har i samband med granskningen tagit del av avtal som SLU har med Evry avseende förvaltning och drift av Primula. Vår granskning visar att innehållet i avtalen är begränsat vad gäller beskrivningar och krav på leverantörens åtaganden samt krav avseende säkerhet och intern kontroll. Vår bedömning är att det är svårt att få en uppfattning om vilka åtaganden som leverantörerna har att leva upp till. Vi har även noterat att det inte finns några SLU-gemensamma, fastställda, styrande dokument kring informationssäkerhet vilket försvårar möjligheterna att styra leverantörerna mot önskad säkerhetsnivå.

Vår granskning visar vidare att det vid granskningstillfället inte fanns ett formellt giltigt avtal mellan SLU och Evry då avtalet som gick ut per sista augusti inte hade förlängts. Vi har blivit uppmärksammade på att det finns ett nytt ramavtal mellan ett antal lärosäten (bl a SLU) och Evry men att SLU inte gjort något avrop enligt detta nya avtal.

Risk
Ofullständiga avtal kan innebära risk för att tjänster inte levereras i tillräcklig omfattning eller

med fel inriktning. Svagheter i avtalsutformning avseende säkerhetsfrågor innebär risk att SLU:s förväntade säkerhetsnivåer inte upprätthålls.

Rekommendation
Vi rekommenderar att SLU reviderar avtalen med leverantörerna så att det tydligt framgår vilka åtaganden som leverantören har samt att avtalen kompletteras med mer detaljerade formuleringar kring kraven på tillgänglighet, riktighet, skydd och spårbarhet. Vi har inom ramen för den nu gjorda granskningen inte gjort någon bedömning av det nya ramavtalet.

Vi förslår även att Personalavdelningen tillsammans med system- och driftleverantören etablerar en gemensam styrmodell där roller, ansvarsområden och mötesforum beskrivs utifrån termer av strategisk/taktisk/operativ nivå samt gränssnitt för underhåll/förvaltning/utveckling och drift.

Stockholm 2013-11- 11

…….

Roger Karlsson
Senior manager CISA, CRISC, KPMG

Bilaga A - Intervjuer

Granskningen har omfattat intervjuer med nyckelpersoner och genomläsning av relevant dokumentation.

Intervjuerna har genomförts med följande personer.

Namn	Uppdrag/befattning
Stefan Cederqvist	Personalchef
Åsa Stiernström	Lönechef
Göran Åkerman	Systemutvecklare
Stefan Edholm	IT-chef
Anette Lindberg	Informationssäkerhetschef
Cecilia Wolkert	IT-avdelningen
Fredrik Berg	Evry
Karin Johannesson	Evry
Thomas Nilsson	Evry

Bilaga B - Källförteckning

Dokumentation som haft betydelse för vår granskning och rapportering

Internrevisionens rapport 2013 inkl ledningens kommentarer

IT-policy

IT-säkerhetspolicy

Riktlinjer för informationssäkerhetsklassning

Instruktioner för säkerhetsklassning

Systemförvaltningsmodell

Riksrevisionens material 2013-08-23

IT-säkerhetsgranskning av SLU:s IT-system Baltzar och Agresso, 2012-02-12

Leveransavtal avseende Primula, AU 21042004-11-08

Avtal IT-drift, 2004-11-06

Tilläggsavtal Agressodrift SLU (Primula)

Avtal avseende Kundstöd till SLU för Primula, AU 2304, 2004-11-06

Universitetsadministrationens verksamhetsplan 2013, 2012-12-20

Förvaltningsplan för SystemX,

Systemförvaltningsmodell för SLU, 2008-09-22

Organisation och ansvarsfördelning inom universitetsadministrationen, 1 november 2012

Utveckling programvara, Evry

Kvalitetsledningssystem, Evry

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

2014-01-28

Åtgärdsplan gällande internrevisionsrapport om informationssäkerhet

Sammanfattning av åtgärdsplanen

1. Förutsättningarna för införande av en SLU-övergripande förvaltningsmodell ska utredas närmare(klart: 2014-11-30, Ansvarig: IT chef)

2. Nytt avtal med Evry tecknas med avseende på Primula (klart: 2014-10-30, Ansvarig: Personalchefen).

3. En katastrof och avbrottsplan för Primula kommer att utarbetas av personalavdelningen (klart: 2014-09-30), Ansvarig: Personalchefen)

4. Personalavdelningen tar fram säkerhetrutiner för hur högre behörigheter i Primula ska hanteras och dokumenteras (klart: 2014-06-30, Ansvarig: Personalchefen)

5. Säkerhetsrevisioner genomförda på SLU görs tillgängliga för systemägare (klart: 2014-10-30, Ansvarig: IT chef i samråd med informationssäkerhetsansvarig)

6. En kopia av backupen på Primulas databas förs över och lagras på media inom SLU (klart: 2014-10-30, Ansvarig: Personalchefen)

Rekommendationspunkter från IR-rapport med åtgärdsanalys

2.1 Rekommendationer

Vi rekommenderar att SLU genomför en riskanalys i syfte att definiera vilka tillgänglighetskrav som bör gälla för Primula och att dessa krav formuleras i avtalen med berörda leverantörer.

Vi rekommenderar att SLU genomför en riskanalys i syfte att upprätta en sammanhållen avbrottsplan för Primula och tillhörande administrativa rutiner inklusive rutiner för löpande underhåll och test av planen. Vi ser det som väsentligt att planen inte bara avser IT-driften utan även övriga berörda verksamheter och där

verksamheternas behov av tillgänglighet till systemet får styra omfattning och inriktning på valda lösningar.

Vi rekommenderar även att avtalen med berörda systemleverantörer, baserat på ovantstående riskanalys, kompletteras med avbrottsplanering så att tillgängligheten kan säkerställas över tid.

2.1 Kommentar

Tillgängligheten för Primula kan delas upp i två separata spår, ett för klientanvändarna och ett för webbanvändarna. Enbart personalavdelningen, med några få undantag, använder klienten och resten av administratörerna och anställda använder webben. Ingen separat övergripande riskanalys kommer att göras för Primula utan en riskbedömning kommer att göras i samband med att en katastrof och avbrottsplan utarbetas för systemet. Katastrof och avbrottsplanen kommer att utarbetas av personalavdelningen, vid behov även i samverkan med IT.

Primulas webbapplikation är beroende av både Primulas webbserver och SLU:s egen internwebb. Tillgängligheten för enskild anställd till Primula anses inte vara av så pass kritisk natur att det motiverar en drastisk handlingsplan. Löneutbetalningarna som är systemets mest kritiska uppgift är inte beroende av tillgängligheten för de anställda. Katastrof och avbrottsplanen som ska behandla rutiner kring systemets nedgång räcker alltså för att säkerställa att löneutbetalningarna fortfarande kan göras. Alla andra transaktioner i systemet så som reseräkningar går att göra i efterhand när systemet åter är i drift.

Ett prioriterat projekt för personalavdelningen är att 2014 teckna nytt avtal med Evry med avseende på Primula (Örebro:s upphandling av PA/lönesystem 2013). En genomgång kommer då att göras av de delar av avtalet som belyser tillgänglighet.

Åtgärder

En katastrof och avbrottsplan kommer att utarbetas för Primula.
Ett nytt avtal med Evry med avseende på Primula kommer att tecknas. I samband med detta kommer de delar av avtalet som belyser tillgänglighet att belysas.

Ansvarig: Personalchefen
Tidsplan: 2014-09-30

2.2 Rekommendationer

Vi rekommenderar att universitetet stärker den interna kontrollen genom att formalisera och dokumentera principer och regler för administration och tillämpning av behörigheter i Primula.

Vi rekommenderar även att universitetet analyserar på vilket sätt som kontrollen av användningen av kraftfulla behörigheter kan förstärkas och därefter införa tillförlitliga och ändamålsenliga kontroller. Vi ser det också som väsentligt att SLU ökar insynen hos Evry om vilken personal som har kraftfulla systembehörigheter.

Vi har under granskningens gång fått information om att universitetet genomfört en säkerhetsrevision som avsåg driftmiljön av ett annat administrativt system. I den mån resultat från sådana säkerhetsanalyser kan vara användbara för andra enheter inom universitetet än den närmast berörda, bör Informationssäkerhetsansvarig svara för att sådan information delas.

2.2 Kommentar
Administrativa behörigheter på högsta nivån internt på SLU i Primula är redan idag högst begränsat. Endast ett fåtal personer på löneenheten har tillgång till övergripande konton som inte är personbundet. För test och verifiering så är de opersonbundna kontona väsentliga. Vid lägre behörigheter så finns redan idag en rutin för hur behörigheterna sätts och en arkivering görs av underlagen för dessa.

Inom ramen för arbetet med katastrofplanen och avbrottsplanen kommer personalavdelningen även att gå igenom säkerhetsrutiner internt vad gällande lagring av lösenord och hantering av högre behörigheter. Arbetet kommer även innefatta fastställda rutiner om vem som får högre behörighet och hur detta ska dokumenteras.

Materialet och resultatet av säkerhetsrevisioner kommer framöver att göras tillgängliga och spridas till tänkbara interna intressenter.

En dialog hålls redan idag med Evry om hur behörigheterna är uppsatta för dem i Primula och hur SLU kan verifiera att godtagbar loggning av deras aktivitet syns i systemet.

Åtgärder
Säkerhetsrutiner för hur högre behörigheter i Primula ska hanteras och dokumenteras utarbetas.

Ansvarig: Personalchefen
Tidsplan: 2014-06-30

Säkerhetsrevisioner genomförda på SLU görs tillgängliga för systemägare.

Ansvarig: IT-chef i samråd med informationssäkerhetsansvarig.
Tidsplan: 2014-10-30

2.3 **Rekommendationer**
Vi rekommenderar att Personalavdelningen, med utgångspunkt i SLU:s Arkivplan, dokumenterar och inför rutiner som säkerställer att arkivplanen efterlevs.

2.3 Kommentar

Arkiveringen av transaktioner och data i Primula arkiveras i Primula så ingen vidare åtgärd behövs för att åstadkomma detta. Detta är mer en fråga om backuperna av Primulas databas förvaras på ett säkert och tillförlitligt sätt.

Ett mål för 2014 är att upprätta ett överföringsschema av backuper så att de förutom hos Evry även finns att tillgå på en server hanterad av IT-avdelningen på SLU. Med backuper menas här en kopia på databasen där all information i Primula finns lagrad.

Åtgärder
En kopia av backupen på Primulas databas förs över och lagras på media inom SLU.

Ansvarig: Personalchefen
Tidsplan: 2014-10-30

2.4 Rekommendationer

Vi föreslår att universitetet fastställer en förvaltningsmodell att tillämpas för alla universitetsadministrativa system.

Vi förslår vidare att ansvar och mandat för att förvalta modellen fastställs.

Vi föreslår slutligen att Personalavdelningen, med utgångspunkt i beslutad modell, inför tillämpliga delar i sin verksamhet.

Vi föreslår att SLU reviderar avtalen med leverantörerna så att det tydligt framgår vilka åtaganden som leverantören har samt att avtalen kompletteras med mer detaljerade formuleringar kring kraven på tillgänglighet, riktighet, skydd och spårbarhet. Vi har inom ramen för den nu gjorda granskningen inte gjort någon bedömning av det nya ramavtalet.

Vi föreslår även att Personalavdelningen tillsammans med system- och driftleverantören etablerar en gemensam styrmodell där roller, ansvarsområden och mötesforum beskrivs utifrån termer av strategisk/taktisk/operativ nivå samt gränssnitt för underhåll/förvaltning/utveckling och drift.

2.4 Kommentar

Ett arbete kommer att påbörjas för att skapa en SLU-övergripande förvaltningsmodell. I första hand kommer detta bli ett samarbete mellan IT-säkerhetsansvarig och IT. Förvaltningsmodellen blir ett stöd för systemägarna och kan användas i dialog med externa parter. Hur styrande den framtagna förvaltningsmodellen blir bedöms från fall till fall då den måste viktas mot fördyringar av systemen. Kunskap om den övergripande förvaltningsmodellen kommer att spridas till berörda parter inom organisationen. För upphandlade/avropade system så måste dock den interna förvaltningsmodellen ses som ett önskat läge och inte som ett direkt styrande krav.

I samband med det nya avtalet gällande Primula kommer en dialog att föras med Evry om hur den strategiska dialogen mellan SLU och Evry kan utvecklas och förbättras.

Åtgärder

Förutsättningarna för införande av en SLU-övergripande förvaltningsmodell ska utredas närmare

Ansvarig: IT-chef
Tidsplan: 2014-11-30