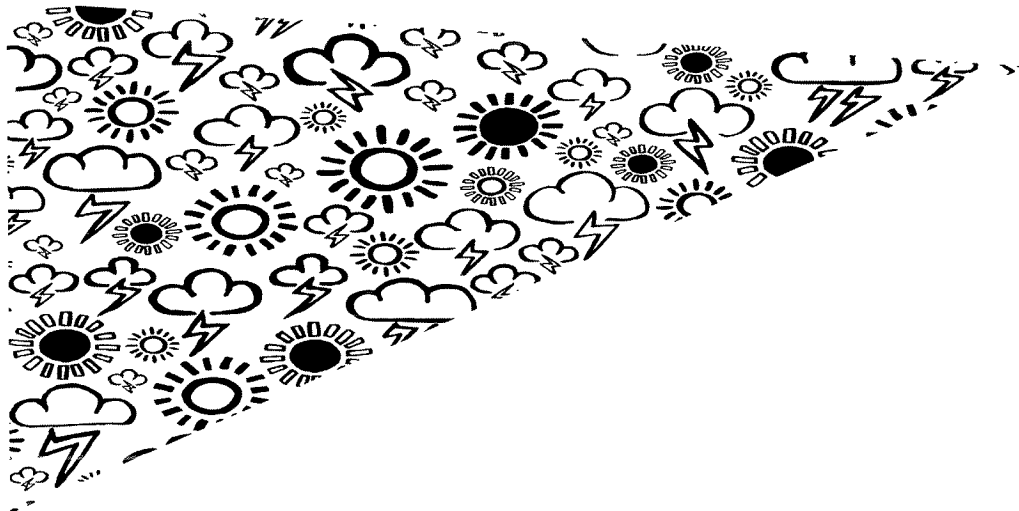


# Kalmar kommun

## Övergripande IT genomgång



## Innehåll

<b>1. Inledning.....</b>	<b>2</b>
1.1. Bakgrund .....	2
1.2. Metod och genomförande .....	2
<b>2. Genomförd granskning .....</b>	<b>4</b>
2.1. Policy-dokument och styrning .....	4
2.2. Förändringskontroller .....	4
2.3. Access till data och program .....	6
2.4. Drift och övriga kontroller .....	9
<b>3. Sammanfattande bedömningar och rekommendationer.....</b>	<b>11</b>

# 1. Inledning

## 1.1. Bakgrund

Kalmar kommuns olika bolag och förvaltningar har i sin verksamhet ett stort beroende av sina IT-system. Vi har fått i uppdrag att granska IT-generella kontroller som berör både dotterbolagen och kommunen avseende följande centrala system;

- Active Directory (AD)
- Aditro Affärslösningar
- Inköp och Faktura (modul i Aditro Affärslösningar)
- Personec P

Det är väsentligt att IT-system hanteras på ett tillfredsställande och korrekt sätt för att alla beroende parter skall kunna lita på den information systemen genererar och veta att den finns tillgänglig när det behövs. Som ett led i revisionen har vi granskat de generella IT-kontroller som avser IT-styrning, systemförändringar samt kontroller av behörighetsåtkomst, det vill säga access till data och program.

Syftet med granskningen har varit att verifiera att generella IT-kontroller finns på plats och att de är formellt dokumenterade.

## 1.2. Metod och genomförande

Vi har granskat policies och rutinbeskrivningar samt genomfört intervjuer med berörd personal. I vissa fall har vi gjort utdrag från system för att verifiera de parametersättningar som styr säkerheten. Vi har också tagit fram rapporter som visar på hur till exempel användare har satts upp i systemen.

I vår granskning har följande områden ingått:

### ***Policydokument och styrning***

- Översiktlig genomgång av att IT-policy, strategi mm finns på plats, att innehåll är rimligt ändamålsenliga och av hur kommunikation till berörda personer görs.

### ***Förändringskontroller***

- Översiktlig genomgång av att metodik och policy för förändringar i applikationer och system finns.
  - Hur godkänns förändringar och hur görs testning av förändringar?
  - Finns det separat utvecklings- och/eller testmiljö?

### ***Access till data och program***

- Översiktlig genomgång av rutinen för att hantera användare i systemen.
  - Var och hur administreras behörigheter och applikationer, sker genomgång av kraftfulla användare i system?
  - Hur säkerställer kommunen att användarkonton stängs ner inom rimlig tid för personer som slutat?
  - Sker det regelbundna användargenomgångar av samtliga användare och behörigheter?
  - Används loggning och sker det någon genomgång av aktiviteter som loggas?

### ***Drift och övriga kontroller***

- Översiktlig genomgång av säkerhetskopieringsrutiner.
  - Finns rutiner för backuper av och återläsningstest för systemet?
  - Finns rutiner för hur integrationer mellan systemen ska hanteras och övervakas?
  - Finns kontrollmoment på plats för att säkerställa att överföring av kritisk/ finansiell information är fullständig och korrekt?
  - Finns beroenden till externa leverantörer/ konsulter – om ja, vad ingår i den externa partens tjänsteleverans och hur sker uppföljning av extern part?

## **2. Genomförd granskning**

### **2.1. Policy-dokument och styrning**

Vi har tagit del av Kalmar kommuns IT-policies för att få en övergripande bild av kommunens styrning gällande IT. Vi har granskat IT-policies och instruktioner utefter vad som framkommit i de intervjuer vi genomfört med IT-avdelning, systemägare och systemförvaltare. Kommunens "Informationssäkerhetspolicy Säkerhetsinstruktion: Förvaltning" benämns nedan informationssäkerhetspolicy.

Kommunens IT-policy finns i dess verksamhetshandbok. När en person börjar på Kalmar kommun får denne en checklista som ska fyllas i. En del av checklistan avser en IT/introduktionskurs som är obligatorisk för samtliga nyanställda. På introduktionskursen behandlas delar av IT-policyn. Kommunen gör ingen kontinuerlig genomgång av IT-policyn efter introduktionen, detta sker endast vid nyanställning samt vid uppdateringar av policyn. Enligt IT-chefen revideras IT-policyn årligen.

I den säkerhetsinstruktion som finns upprättad i informationssäkerhetspolicyn stipuleras att det ska finnas en systemsäkerhetsanalys. I denna analys ska det framgå "de enskilda IT-systemens krav på avbrotts- och katastrofplanering. Kraven ska vara sammanställda i systemsäkerhetsanalysen för den tekniska infrastrukturen".

#### **2.1.1. Kommentarer**

Vi noterar att den systemsäkerhetsanalys som nämns i informationssäkerhetspolicyn inte upprättats och att det därmed inte finns några upprättade katastrofplaner för organisationen. Vi har fått uppgift om att det finns en plan för att komma igång med denna process under 2016. Kommunen håller på att upprätta systemsäkerhetsanalys som kommer inkludera väsentliga delar gällande loggar och katastrofplaner.

En väsentlig del av en styrning av IT-system och dess användning är en dokumenterad förändringsprocess. Dokumentationen utgör en viktig del i en IT-policy. Vi konstaterar att det finns ett behov av att se över dokumentationen kring styrning av förändringsprocessen för väsentliga system, och ställa krav på dokumentation efter en form av riskanalys. Detta för att säkerställa kontrollen kring förändringar i väsentliga system.

Utöver de noteringar vi gjort i detta avsnitt får flera av de områden som vi behandlar nedan påverka på kommunens IT-policy och styrning. I dessa fall framgår detta av de iakttagelser och rekommendationer som vi lämnar nedan.

### **2.2. Förändringskontroller**

Vi har genom våra intervjuer med systemägare samt genom dokumentation i form av styrdokument, processbeskrivningar, avtal och skärm-dumpar ur systemen fått en övergripande bild av de förändringskontroller som finns etablerade för Kalmar kommun. I våra samtal med berörda framkommer att inga större förändringar har implementerats gällande ekonomisystemet, Aditro Affärslösningar eller lönesystemet, Personec P, med undantag av förändringen som nämns nedan.

I lönesystemet har en något större förändring genomförts som bland annat har inneburit en implementering av en ny självserviceportal för frånvaroregistrering. Ytterligare applikationer som implementerats är en modul för att lägga in arvoden till förtroendevalda och en modul kopplat till löneförhandling. Vidare har kommunen gjort en analys och kvalitetskontroll av

systemtabeller. Det omfattande projektet har krävt en projektdokumentation i syfte att möjliggöra en uppföljning. Kommunen har tagit hjälp av konsulter med den projektstyrning som ansetts lämplig för projektets storlek. Förutom detta finns det inte någon generell dokumenterad förändringsprocess gällande systemförändringar.

### ***Aditro Affärlösningar***

För systemet Aditro Affärlösningar finns ingen formell dokumentation kring hur förändringar i systemet ska hanteras och dokumenteras. Förändringar görs direkt i produktionsmiljön. Förändringar dokumenteras inte avseende varför de implementeras, av vem de beslutats eller när förändring gjorts samt vad för typ av testning som utförts i samband med förändringen. Anledningen till att inte testmiljön används uppges vara att den inte är uppdaterad.

Mot bakgrund av att kommunen inte uppges utföra några större förändringar i systemet har systemägare inom kommunen bedömt att det inte krävs någon dokumenterad process för detta. När det gäller systemförändringar som görs av tredje part finns en ansvarsmatris där dokumentationskrav för Aditro Affärlösningar gällande systemförändringar är reglerade.

På kommunens centrala ekonomienhet finns några personer som i Aditro Affärlösningar har rollen som administratörer. Dessa personer har möjligheter att ändra kontroller i systemet, till exempel attestrutiner. Vi har tagit del av en skärmbild på administratörsrätter i Aditro Affärlösningar och noterar att åtta personer har möjlighet att göra ändringar i systemet.

Vid implementering direkt i produktionsmiljön sker också all testning i produktionsmiljön. Skulle förändringen gå fel eller orsaka problem, läser kommunen tillbaka senaste backupen och börjar om. Detta uppges aldrig ha inträffat. Vid större uppgraderingar av affärssystemet anlitas konsulter. Systemet stängs då ner och testning görs ihop med konsult. Kommunen uppges aldrig upplevt att de tappat redan inläst information vid uppgraderingar. Uppgraderingarna är välplanerade och konsulter informerar ett år i förväg om kommande uppgraderingar. De får tre dagar på sig att testa systemet och utbilda kommunens personal.

Under vår diskussion kring systemförändringar som påverkar finansiell rapportering diskuteras även rapporteringsmoduler. Kalmar kommun använder sig av något som kallas för HyperGene. Detta är ett system för rapportering som plockar information från ekonomisystemet. Kommunens budgetchef ansvarar för de rapporter som hanteras i systemet. Enligt budgetchefen görs inte mycket förändringar och det är sällan det skapas nya rapporter i systemet. Kommunen har valt att endast ha en rapport per förvaltning där linjeförvaltningen är målgruppen. Det är generellt sett enkla rapporter för att kunna ge chefer en snabb lägesbild. Vid förändringar av rapporter testas man rapporterna mot ekonomisystemet. Budgetchefen är ansvarig för testningen vilket görs ihop med en konsult. I övrigt är det varje förvaltnings ansvar att deras system visar korrekt data.

### ***Personec P***

Enligt systemägare och systemförvaltare för lönesystemet Personec P görs inga större förändringar i lönesystemet som kräver någon dokumentation eller projektbeskrivning. Det enda som görs är uppgraderingar av systemet vilket sker två gånger per år. Vid uppgraderingar skickar Aditro material till IT-avdelningen avseende förberedelseprocessen och implementeringen. Kommunen genomför sedan uppgraderingen i samarbete med Aditros konsulter, likt processen för uppgradering av Aditro affärssystem. Oftast görs inga särskilda tester vid dessa tillfällen.

De förändringar som görs avseende inbyggda kontroller i lönesystemet kan endast ändras av Aditros konsulter, inte av kommunens systemadministratörer. De inbyggda kontrollerna påverkar hur systemet tar sig och behandlar information, exempelvis hur lönen beräknas utifrån inbyggd formel och inputparametrar.

Kommunen har genomfört ett större projekt, vilket berördes i tidigare avsnitt, som krävt projektstyrning och som finns dokumenterat. Projektet, som pågått i ca 1,5 år, avser att bygga upp systemet från början och säkerställa samtliga tabeller. Dokumentationen är enligt standard gällande IT-projekt och har upprättats med hjälp av konsulter från Aditro. Systemförvaltaren är ansvarig för att information hanteras säkert i projektet.

### **2.2.1. Kommentarer**

Kalmar kommun saknar en riskanalys som hanterar vilka typer av förändringar som anses som större och därmed bör ha en dokumenterad förändringsprocess, och vilka typer av förändringar som anses vara mindre och som inte kräver lika omfattande dokumentation men ändå någon form av spårbarhet. Med hjälp av klara riktlinjer dokumenteras systemförändringar i den omfattning ledningen förväntar sig att den ska dokumenteras utifrån den risk som bedöms föreligga. Vi rekommenderar att kommunen utformar denna typ av riskanalys. Därtill noterar vi att Kalmar kommuns informationssäkerhetspolicy reglerar att system ska vara väldokumenterade, men att den inte tydligt indikerar något kring att förändringsprocessen bör vara formellt dokumenterad.

I informationssäkerhetspolicyn regleras även att testmiljö ska finnas tillgänglig vid behov och bör därför vara uppdaterad. Mot bakgrund av detta, samt att testmiljö är nödvändig vid alla typer av förändringar för att kunna verifiera att systemet efter ändringen fortfarande presterar enligt önskemål och att förändringen inte påverkat andra delar av systemets funktioner, anser vi att testmiljö bör användas. Testmiljön bör också vara uppdaterad inför testningsförfaranden för att spegla produktionsmiljön i största möjliga mån.

Vid användning av testmiljö är det viktigt att tänka igenom segregering av arbetsuppgifter i förändringsprocessen så att det inte är samma person som beslutar om förändring som också är den som testar samt implementerar förändringen. Detta för att undvika implementering av förändringar som är tillräckligt testade, eller som har oegentligheter som syfte.

### **2.3. Access till data och program**

Vi har genom våra intervjuer med IT-avdelningen fått en övergripande bild av hur tilldelning av behörigheter sker i Kalmar kommun med dotterbolag samt hur strukturen för användarkonton ser ut.

Användare har unika ID och lösenord som styrs av ADt (Active Directory, Microsofts katalogtjänst för nätverk), det vill säga användare loggar in på nätverket med unika användarnamn och lösenord. Så kallad singel sign-on används, det vill säga det krävs ingen ytterligare inloggning än Windows-inloggning för att komma åt de system och behörigheter man blivit tilldelad. Personalen använder vanlig standard avseende inloggningspolicy. Vi har tagit del av hur inloggningspolicyn ser ut och hur denna sker och gör bedömningen att det avseende intrångsrisk kan anses vara något svagt.

IT-avdelningen ger access till systemen i ett första skede genom ett konto i ADt, medan det är systemägarna/förvaltarna som sedan styr själva behörighetstilldelningen. Nya användare beställs via ITs ärendehanteringssystem vilket måste ske via en verksamhetsansvarig chef. Rutinen stöds av Kalmar kommuns IT-policy. IT-avdelningen gör en preliminär bedömning av åtkomsten och enligt enhetschefen på kundservice sker alltid en uppföljning och extra kontroll om något inte ser rimligt ut. Samtliga anställda på kommunen kommer åt Aditro Affärslösningars portal, men har bara begränsad åtkomst eller titt-funktion fram till dess att systemägaren tilldelat personen en riktig behörighet i systemet.

Lönesystemet fungerar som mastersystem för användare och synkroniserar fyra gånger dagligen mot ADt. Detta innebär att om man blir borttagen från lönesystemet och inte får någon

lön utbetald längre, blir man automatiskt borttagen från ADt och kan inte logga in och komma åt några system. Löneavdelningen blir alltid informerad av verksamhetsansvarig chef när en anställning upphör och lägger då in ett avslutningsdatum i Personec P. Användarkontot avslutas automatiskt i samband med detta avslutningsdatum. När en person med tillfällig anställning påbörjar sin anställning registreras alltid ett slutdatum manuellt i systemet. Mot bakgrund av dessa rutiner har kommunen inte några rutiner för periodiska genomgångar av behörigheter. De har inte bedömt det som nödvändigt att gå igenom konton av den anledningen att de stängs ner automatiskt med hjälp av synkroniseringen mellan lönesystemet och ADt.

Bild 2.3-1 visar Kalmar kommuns processflöde för att lägga upp nya anställda i lönesystemet innan lön kan utbetalas.

#### Lägga upp nyanställd – process

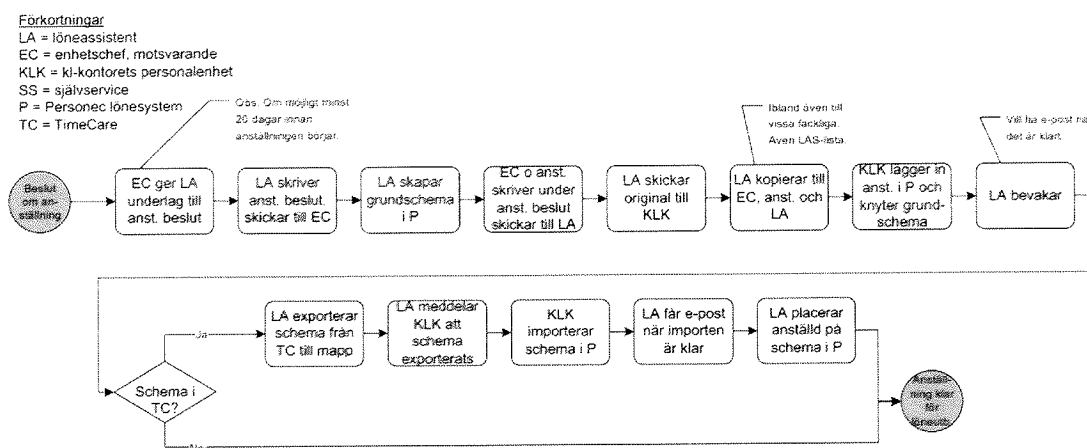


Bild 2.3-1

Bild 2.3-2 visar Kalmar kommuns processflöde för hur någon avslutar sin anställning och tas bort från lönesystemet.

#### Avsluta anställning – process

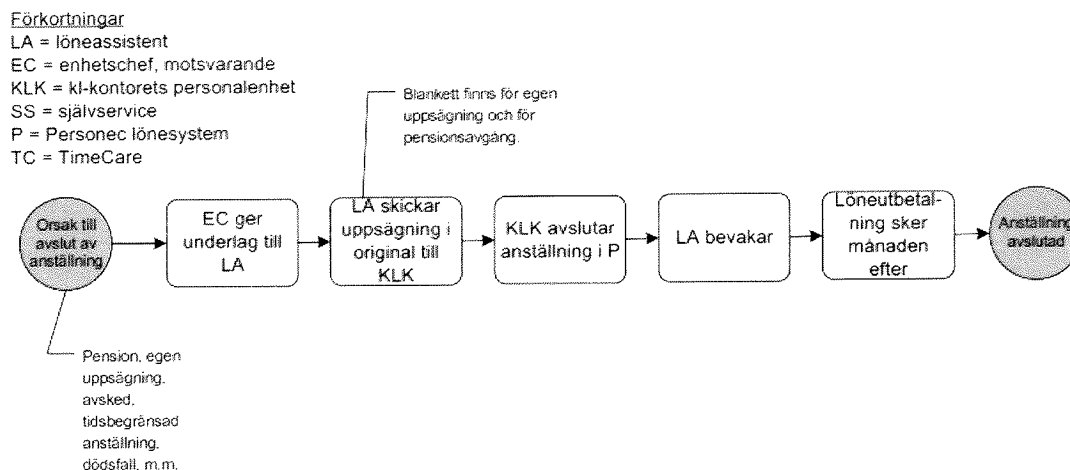


Bild 2.3-2



Vi har intervjuat systemägare för Aditro Affärslösningar för att få en övergripande förståelse kring hur behörighetshanteringen fungerar gällande redovisningssystemet Aditro Affärslösningar.

En förfrågan om behörighet till systemet kommer oftast från verksamhetsansvarig chef via mail till systemägare/förvaltare. Högre behörigheter måste godkännas, antingen av nämnden eller på delegation av berörd chef. En nyanställd måste, som nämnts tidigare, först få ett konto uppsatt i ADt av IT-avdelningen för att systemägaren ska kunna tilldela behörighet i affärssystemet. Systemägaren kopplar sedan användarkontot i ADt till den behörighetsgrupp som den nyanställda ska ha i affärssystemet. Det finns instruktioner framtagna för hur man lägger upp behörigheter. En kortare och övergripande beskrivning av detta finns också dokumenterat i Kalmar kommuns informationssäkerhetspolicy. Policyn för behörighetsadministration saknar dock tydlighet kring hur behörighetsförändringar hanteras.

Kalmar kommun har gjort en större uppgradering av affärssystemet under året som bland annat inneburit att de flertal individuella behörigheter de haft i systemet nu sätts upp i grupper istället. I samband med omstruktureringen och uppsättningen av de nya grupperna i affärssystemet ska intern kontroll ha varit i fokus.

Mot bakgrund av den automatiska synkroniseringen som finns mellan lönesystemet och ADt, som ska säkra att inga personer som slutat ska ha tillgång till kommunens system, finns ingen etablerad rutin kring att ekonomiavdelningen ska meddelas när någon avslutar sin anställning hos kommunen. Ekonomiavdelningen gör en informell genomgång av kontona i affärssystemet då de anser att det emellanåt krävs en rensning i systemet. Genomgång görs oregelbundet och de konton som inte använts på ett år stängs ner.

### ***Personec P***

Vi har intervjuat systemägare och systemförvaltare för lönesystemet för att få en övergripande förståelse kring hur behörighetshanteringen fungerar gällande lönesystemet Personec P. Precis som för ekonomisystemet behöver nya användare först få ett konto uppsatt i ADt för att behörigheter ska kunna tilldelas av systemägare/förvaltare. Det finns en beställningsblankett som används för nyanställda där verksamhetsansvarig chef specificerar system samt behörighet som denne ska ha tillgång till. Denna skickas till IT-avdelningen för att skapa ett användarkonto.

Verksamhetsansvarig chef mailar systemägare efter att IT lagt upp ett konto i ADt. Systemägaren kopplar då användarkontot i ADt till den behörighetsgrupp den nya användaren ska ha i lönesystemet. Genomgång av konton görs precis som för ekonomisystemet på ett informellt sätt, endast för att rensa användarkonton i lönesystemet. Lönehandläggaren brukar gå igenom användarbehörigheterna under sommarmånaderna då det är lite mindre att göra, men som tidigare nämnts dokumenteras inte detta.

Förändringar av behörigheter inom lönesystemet är inte lika formellt som vid nyanställning och avslutande av tjänst. Enligt systemförvaltare kan detta ske via telefon. Rutinen är att man tar bort tidigare behörigheter vid förändring, men detta finns inte dokumenterat. I informationssäkerhetspolicyn regleras att "beslut om och beställa (skriftligt) enskilda användares behörighet till IT-system", vilket vi tolkar som att även denna del av processen borde vara formell.

### **2.3.1. Kommentarer**

Vi har tagit del av hur inloggningspolicyn ser ut och hur denna sker och gör bedömningen att det avseende intrångsrisk kan anses vara något svagt. Mot bakgrund av detta rekommenderar vi Kalmar kommun att stärka sin inloggningspolicy med färre inloggningsförsök för att minska risken för att obehöriga ska kunna logga in på användarkonton.

Vidare rekommenderar vi att Kalmar kommun har en mer tydlig policy kring processen för att sätta upp nya användare och deras behörigheter samt förändringar därav för att på ett klart och tydligt sätt styra utifrån hur ledningen vill att behörighetsstyrningen ska hanteras och dokumenteras.

#### **2.4. Drift och övriga kontroller**

Vi har genom våra intervjuer med IT avdelningen på Kalmar kommun fått en övergripande bild av kommunens drift och övriga kontroller.

Backuper tas en gång per dygn för virtuella servrar. Loggar skapas när funktionen inte fungerar och på så vis meddelas IT-avdelningen om något skulle gå fel med backupen. Återläsning av enstaka filer görs ett par gånger i veckan och IT har inte upplevt några problem med återläsningen. Kalmar kommun uppges inte ha haft några större incidenter under året och upplever inte mycket störningar i allmänhet. I de fåtal fall kommunen har drabbats av mindre inträngsförsök har man fått testa sina återställningsfiler och inte haft några problem med detta.

Viruskydd och brandväggar finns och bevakas av enheten för infrastruktur. Kalmar kommun har viruskydd och IT får notiser genom mail ifall någon misstanke om virus finns. Brandväggarna bevakas både manuellt och via automatgenererade larm direkt från brandvägg eller IDS. Larm i lägre nivå syns enbart i övervakningsverktygen, emedan mer kritiska larm sker via mail till sändlistor för övervakning. Kalmar kommun har även logghanteringsserver som samlar loggar med larm som också går ut via mail till sändlistor för övervakning. Kontroll av dessa loggar sker enligt IT-chef dagligen.

Kalmar kommun använder sig av separerade serverrum som är utrustade med bevakningskameror, samt övervakning av väktare. Anläggningarna är tillträdesskyddade och strömförsörjning bevakas kontinuerligt.

Under vår genomgång av drift och övriga kontroller noterar vi att kommunen inte har några upprättade kontinuitetsplaner. Enligt IT-chefen är anledningen att man ännu inte tagit fram någon tillräckligt specifik riskanalys. Kalmar kommun tillsätter nu en ny systemförvaltningsmodell och jobbar med de olika rollerna och grupperna så att ansvar och mandat blir tydligare. Årliga möten kommer att införas och i och med denna omstrukturering kommer de att titta på kontinuitetsplaner för de viktigaste systemen. Ambitionen är att få igång arbetet under 2016.

Kalmar kommun har ett flertal sidofaktureringsystem och ett personalflödesystem som är integrerat med Aditro Affärssystem. En tredje part hanterar överflytt av filerna från server som driftas av extern part. Dessa filer hämtas och förflyttas var tredje minut. Betalningsfiler till banken avseende lön hanteras på samma sätt. Kommunen har inte upplevt några problem avseende inkompleta filer eller liknande. Serviceavtalet med den externa parten innehåller applikationsdrift, beredskap, integrationer, affärsvillkor samt ansvarsfördelning mellan parten och Kalmar kommun. Möten hålls varje kvartal där de går igenom om något hänt eller kommande förändringar.

Vi noterar efter våra samtal med kommunens IT-chef samt systemförvaltare att inga aktiviteter loggas för vidare övervakning, vilket finns reglerat i Kalmar kommuns informationssäkerhetspolicy. Förklaringen till detta är att det ska hanteras i systemsäkerhetsanalysen som ännu inte upprättats.

#### **2.4.1. Kommentarer**

Informationssäkerhetspolicyn inkluderar en utvärdering kring hur information ska loggas utifrån den systemsäkerhetsanalys som ska upprättas. Den inkluderar även hur loggar ska följas upp. Då det i dagsläget inte loggas några aktiviteter måste IT-avdelningen tillse att detta sker i enlighet med instruktionerna. Vidare bör Kalmar kommun tillsätta de resurser som behövs för att utföra den riskanalys som bas för katastrofplanerna som regleras i kommunens policy.

### 3. Sammanfattande bedömningar och rekommendationer

Under vår granskning har vi noterat ett flertal områden där vi ser avvikelser från Kalmar kommuns dokumenterade informationssäkerhetspolicy. Därtill har vi noterat ett antal förbättringsområden. Informationssäkerhetspolicyn nämner en systemsäkerhetsanalys som ska inkludera styrning av ett flertal moment. Denna systemsäkerhetsanalys ska exempelvis inkludera katastrofplan för verksamhetssystemen, hantering kring hur aktiviteter i verksamhetssystemen ska loggas samt att testmiljö ska finnas uppdaterad och användas.

Vidare noterar vi att informationssäkerhetspolicyn saknar tydlighet kring förändringsprocessen av behörighetsadministration. Det är viktigt att styrdokumentet i sin tydlighet beskriver hantering kring väsentliga processer, såsom behörighetstilldelning, och inte lämnar utrymme för tolkning. Det har i vår granskning framkommit att nya behörigheter följer en formell process, och när någon avslutar sin anställning är processen formell. Däremot är processen informell när förändring sker av behörigheter.

Vi ser heller inte att det finns en tydlig styrning eller reglering genom IT-policyn hur förändringar i verksamhetssystemen ska hanteras. Vi rekommenderar att detta regleras genom en riskanalys som hanterar vilka typer av förändringar som anses större och därmed bör vara mer formella, medan andra förändringar kan bedömas som mindre och därmed kräver mindre dokumentation. Viktigt att notera är dock att spårbarhet i samtliga förändringar bör finnas. Detta för att man lätt ska kunna gå tillbaka och se varför, av vem och när förändringen gjordes. Dessutom minskas personberoendet i organisationen.

Testmiljö används inte i enlighet med informationssäkerhetspolicyn. Beroende på den riskanalys som bör upprättas, kan förändringar kräva mer eller mindre testning. Det är viktigt att testning dokumenteras, dels för spårbarhetens skull, dels så att testning utförs för att minska risken för felaktigheter i produktionsmiljön.

Slutligen rekommenderar vi att Kalmar kommun stärker sin inloggningspolicy med färre inloggningsförsök för att minska risken för att obehöriga ska kunna logga in på användarkontot. Detta gäller såväl som skydd mot externa inloggningsförsök och interna försök som för att minska risken för oegentligheter.

Carin Ljung  
*IT-revisor*

Kristina Lindstedt  
*Certifierad kommunal revisor*