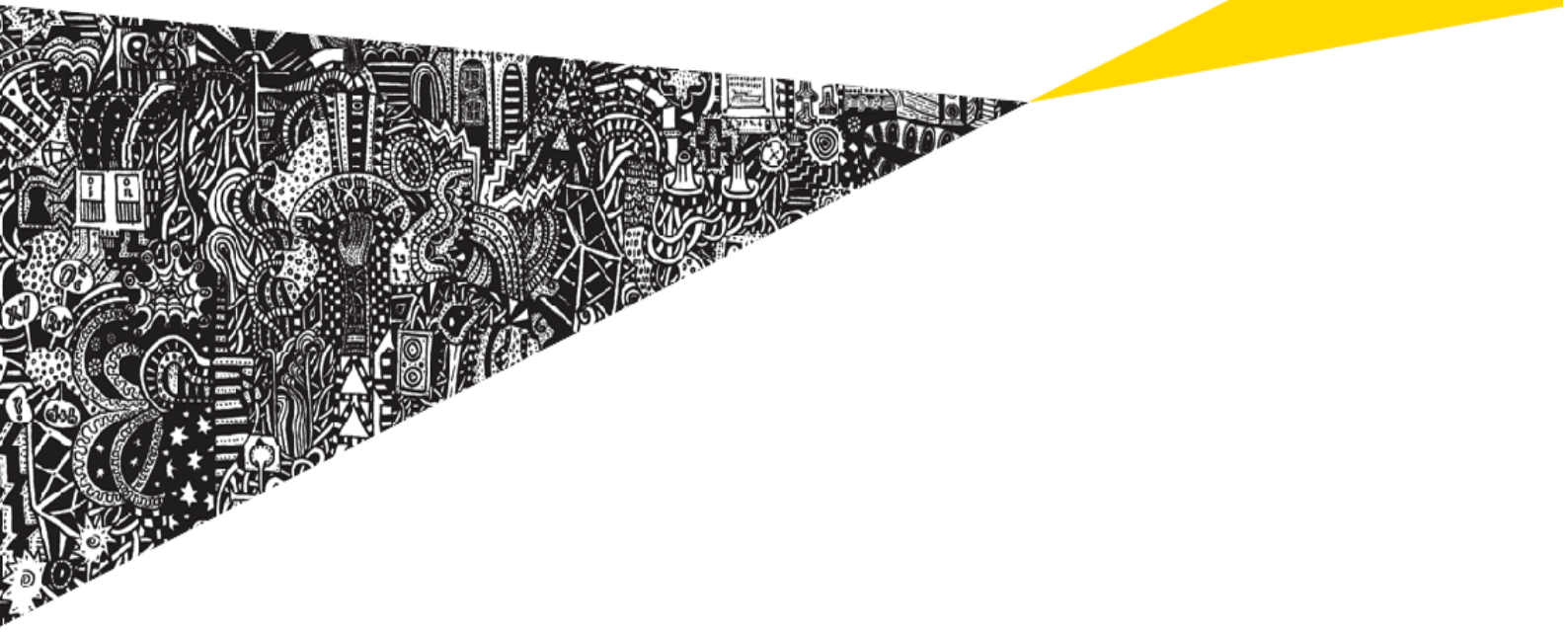
**Revisionsrapport 2010**
Genomförd på uppdrag av revisorerna
i Jönköpings kommun

# Jönköpings kommun

## Granskning av användaradministrationen



# Innehåll

# 1. Bakgrund och syfte

Jönköpings kommun och dess olika förvaltningar har stort behov av olika IT-system i den dagliga verksamheten. Ansvaret för användaradministrationen, avseende många av systemen, finns vanligtvis ute hos förvaltningarna som använder systemen. IS/IT-avdelningen ansvarar för användaradministrationen rörande de centrala nätverken, servrar m.m. Detta innebär att många personer på olika nivåer i kommunens organisation är inblandade.

Syftet med granskningen har varit att bedöma om användaradministrationen är ändamålsenlig och tillräcklig.

# 2. Metod och avgränsning

Följande system har valts ut tillsammans med IS/IT-avdelningen:

- Ett internsystem som tillhandahåller kraftfulla behörigheter - Helpdesk.
- Ekonomisystemet Aditro.
- Upphandlingssystemet/avtalsdatabasen Tendsign.

Dessa system har valts ut p.g.a.

- Att de belyser användaradministration som sker både på förvaltningsnivå och på central nivå
- Att ett system (ekonomisystemet Aditro) finns på servrar i kommunens regi och ett system (Tendsign) är ett webbaserat system där drift köps från extern part
- Ett system (Helpdeskfunktionen) är centraliserat till användare enbart IS/IT-avdelningen, medan främst Aditro är ett system där många användare finns på de olika förvaltningarna inom kommunen.

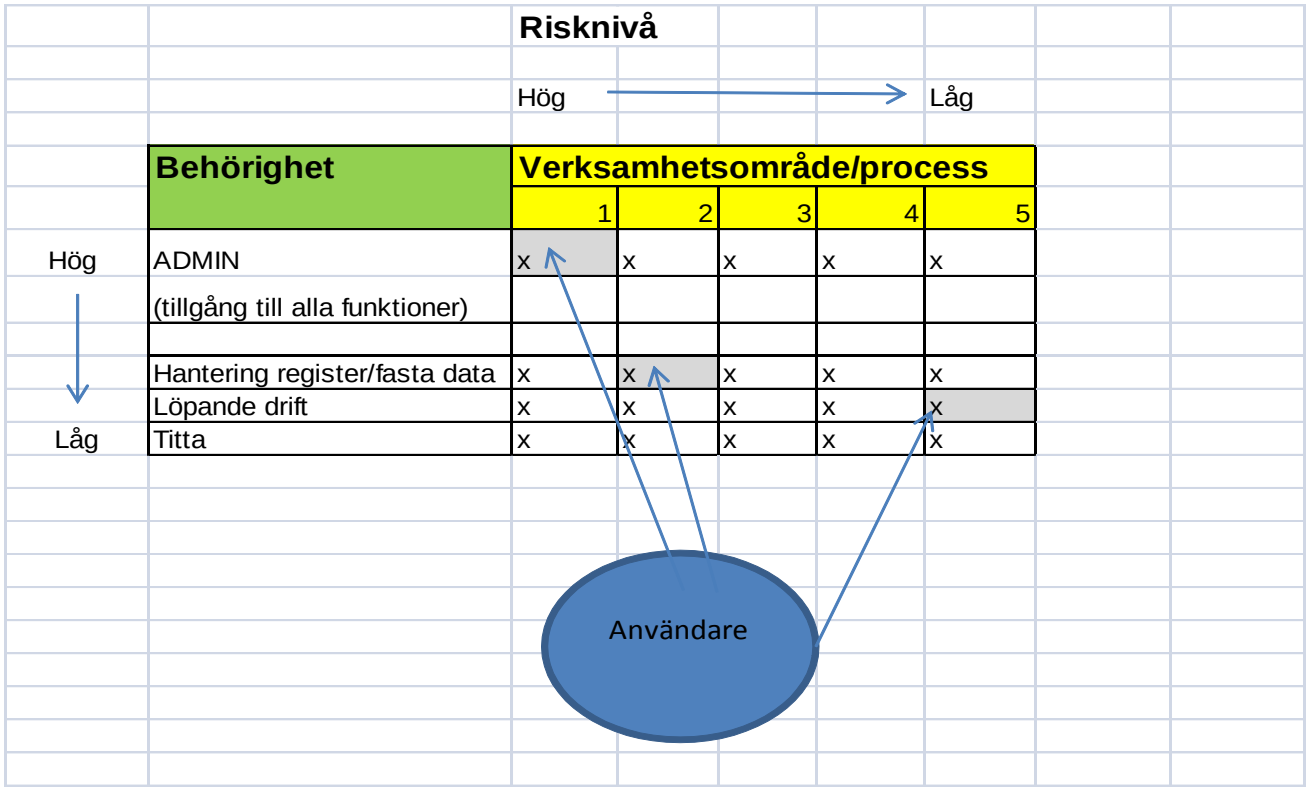
Systemen har valts ut för att kunna visa om det finns skillnader i rutiner och kontroller då de olika systemen har olika förutsättningar.

Följande granskningsmoment har genomförts för ovanstående system:

- Identifiering och verifiering av fem användarkonton som skapats under 2010. Granskning har skett av dokumentation som styrker att användarkontot skall skapas, om aktuell behörighet är relevant, att godkännande finns från behörig person osv.
- Identifiering av vilka personer som har de kraftfullaste användarkontona i respektive system. Det kan förekomma personer som har obegränsade behörigheter i systemen. Bedöma om dessa är rimliga vad gäller antal personer, deras funktioner osv.
- Urval av tre behörighetsprofiler i systemet. Analysera behörigheternas omfattning och verifiera att de följer riktlinjer/beslut.

## 3. Begreppsförklaringar

Nedanstående figur beskriver ett antal begrepp som används i rapporten.




I en organisation finns ett antal verksamhetsområden/processer t.ex. löneprocess, inköpsprocess m.m. Verksamhetsområdena/processerna kan delas in utifrån olika risknivåer. En högre risknivå bör fastställas när det gäller **känsliga system** som hanterar ex. sekretessbelagd information (t.ex. inom socialtjänsten). Det kan också vara system som hanterar funktioner som kan påverka mycket, t.ex. stänga ner ett värmekraftverk eller flytta obegränsat med pengar till externa konton. En lägre risknivå kan fastställas för exempelvis kommunens anläggningsregister. Riskklassificeringen bör utgå från den skada som kan uppstå om obehöriga får tillgång till information/funktioner i systemet. För verksamhetsområdena/processerna används olika IT-stöd (system). Ovanstående figur utgår från antagandet att det endast är ett IT-stöd som används för varje verksamhetsområde.

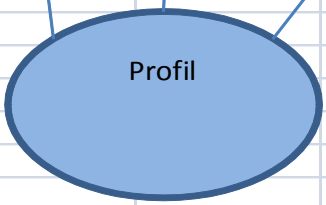
För att nå en hög säkerhet inom IT-systemen är det en grundläggande förutsättning att systemstrukturen byggs på ett säkert sätt så att det finns klara skiljelinjer mellan de olika systemen, dvs. det får inte finnas möjlighet att nå ett system via en behörighet i ett annat system. Systemstrukturen mellan kommunens olika IT-system har inte behandlats i denna granskning.

I det enskilda systemet finns olika behörigheter, dessa beskriver vilken information och vilka funktioner användaren har tillgång till. Den lägsta nivån är tittarbehörigheten. I det fallet kan användaren inte ändra något i den information som finns lagrad i systemet. Motsatsen är **ADMIN-behörigheten**, som innebär att användaren har tillgång till samtliga funktioner och information i systemet. Denna behörighet bör begränsas i så stor utsträckning som möjligt.

Användare som har tillgång till denna behörighet eller har motsvarande behörigheter som är mycket omfattande kallas i rapporten **kraftfulla användare**.

Inom varje system finns olika delsystem. Nedanstående figur visar delsystem inom ett ekonomisystem.

| | **Delsystem** | | |
|---|---|---|---|
| | Leverantörs-reskontra | Kund-reskontra | Anläggnings-register |
| ADMIN | x | x | x |
| (tillgång till alla funktioner) | | | |
| | | | |
| Hantering register/fasta data | x | x | x |
| Löpande drift | x | x | x |
| Titta | x | x | x |




Delsystemen kan delas upp ytterligare i ett antal funktioner/arbetsuppgifter. I leverantörsreskontran ingår normalt bl.a. att registrera leverantörsuppgifter, registrera fakturor och utföra betalningar.

En användare kan få tillgång till olika behörigheter i delsystemen. Man kan t.ex. ha tittarbehörighet i ett delsystem och ADMIN behörighet i ett annat. Kombinationen av behörigheter kallas i rapporten för **profil**.

# 4. Utförd granskning

I detta avsnitt presenteras de väsentligaste iakttagelserna som noterats i granskningen.

## 4.1. Riskklassificering av processer / IT-system

*Iakttagelse:*
Det noteras att det saknas rutiner för att på ett systematiskt sätt riskklassificera IT-system inom kommunen.

*Kommentar:*
Rutiner för tilldelning av behörigheter, lösenord, uppföljningar m.m. bör utgå från varje enskilt systems identifierade risknivå. Kommunen har nu inlett ett arbete med att klassificera systemen utifrån ett riskperspektiv. Hänsyn måste tas till att det finns system med känslig information (t.ex. system på socialförvaltningen) och att systemen måste vara tillgängliga (t.ex. system som styr dricksvattentillförsel).

*Förbättringsområde:*
Som nämns ovan har kommunen startat ett arbete med att klassificera system. Vi rekommenderar att det fastställs rutiner för att riskklassificera varje enskilt IT-system som kommunen använder. Riskklassificeringen bör uppdateras med en viss frekvens, t.ex. årligen, för att säkerställa att inga väsentliga förändringar skett av verksamheten som påverkar risknivån för aktuellt system.

Fastställd risknivå bör påverka all hantering av systemet, hur ofta lösenord ska bytas, vilka kontroller som skall utföras vid tilldelning av nya behörigheter, vilka kontroller som skall utföras vid systemuppdatering m.m.

## 4.2. Kraftfulla användare

Ett urval av användare i berörda system har granskats för att få en bild av vilka som kan klassificeras som kraftfulla användare. Granskning har även skett av dessa användares funktioner i organisationen samt omfattningen av antalet kraftfulla användare.

*Iakttagelse:*
Det noteras att det finns ett antal personer inom den operativa verksamheten som kan definieras som kraftfulla användare. Dessa personer använder systemen i sitt dagliga arbete för att utföra löpande arbetsuppgifter. Vissa av dessa personer har nyckelbefattningar i organisationen. Det noterades även en person som slutat sin anställning inom kommunen.

Kommentar:
Kraftfulla användare bör så långt det är möjligt vara avgränsade från den operativa verksamheten.

Förbättringsområde:
Det är väsentligt att det på ett tydligt sätt framgår för varje enskilt system vilka personer som identifierats som kraftfulla användare. Om det inte är möjligt att avskilja kraftfulla användare från den operativa verksamheten bör kompletterade kontroller fastställas.

### 4.3. Profiler

*Iakttagelse:*
I vissa av systemen är behörigheterna detaljanpassade efter användarna, medan andra system har mer standardiserade behörigheter. I granskningen har det noterats att ansökan om behörigheter till en ny användare ibland önskas utifrån en medarbetares befintliga behörighetsstruktur.

Det noteras även att många av de profiler som skapats utgår enbart från vad en användare behöver ha tillgång till för att sköta det dagliga arbetet. Det saknas en dokumenterad riskbedömning som utgår från vad som är lämpligt utifrån ett intern kontrollperspektiv.

*Kommentar:*
Det är svårare att upprätthålla en god kontroll på användarna och deras behörigheter om de är för detaljerat uppsatta till specifika tjänster. Om nya behörigheter begärs utifrån en annan användare, finns det en risk att den personen har kraftfullare behörigheter än vad den nya personen verkligen behöver.

*Förbättringsområde:*
Behörigheter bör standardiseras och följa en enhetlig struktur. Behörigheter ska tilldelas utifrån ansvarsområden men även utifrån systemets riskklassificering. Vid beställning och godkännande av behörigheter är det väsentligt att analys och bedömning sker av både medarbetarens ansvarsområde och om det är rimligt ur ett internkontroll perspektiv (stödjer två-personshantering, dvs. en person ska inte ensam hantera alla moment i verifieringskedjan). I de fall tilldelning av en behörighet innebär en ökad risk ur internkontroll synpunkt är det väsentligt att identifiera detta och täcka in eventuella riskområden med ex. manuella kontroller.

### 4.4. Beställning och godkännande av behörighet

*Iakttagelse:*
De granskade systemen skiljer sig åt vad gäller struktur och antal användare. Det finns en tydlig huvudägare till behörighetstilldelningen på IS/IT-avdelningen, men det saknas tydliga regler för vem som har rätt att beställa behörigheter ute i förvaltningsorganisationen. I de flesta fall är det en avdelningschef eller motsvarande som gör beställningen till IS/IT-avdelningen.

*Kommentar:*
Det finns en risk att personal erhåller en felaktig behörighet om det finns tveksamheter kring vem som har rätt att beställa nya behörigheter/förändra villkoren i befintliga behörigheter.

*Förbättringsområde:*
Det bör finnas fastställda rutiner där det tydligt framgår vem som har rätt att:

- godkänna behörigheter
- beställa nya behörigheter alternativt/förändra befintliga behörigheter
- begära borttagning av behörigheter när de inte längre är aktuella

Det är väsentligt att den person som har rätt att beställa behörigheter är väl insatt i vad medarbetaren har för ansvarsområden och arbetsuppgifter. Den person som har rätt att godkänna behörigheter bör har god kunskap om hur behörigheterna är strukturerade i det aktuella systemet.

### 4.5. Ansökan av en behörighet

*Iakttagelse:*
Det finns ingen gemensam policy avseende användaradministrationen inom kommunen. Det noteras att det även saknas systemspecifika policys/riktlinjer för de system som ingår i granskningen. Det finns inget fastställt dokument som anger vilka uppgifter som krävs vid en beställning av en ny behörighet/förändring av en befintlig behörighet.

*Kommentar:*
Avsaknad av riktlinjer kring användaradministrationen ökar risken för olikartad hantering och att det är den enskilda personens riskmedvetande som styr vilka kontroller som utförs i samband med behörighets- och lösenordstilldelning.

*Förbättringsområde:*
En mall för behörighetsansökan bör tas fram. Den kan med fördel vara webbaserad och innehålla följande uppgifter:

- vem ansökan gäller
- vem som är ansvarig för ansökan
- aktuellt system
- datum för ansökan
- startdatum och i vissa fall även slutdatum (slutdatum ska alltid anges gällande ”känsliga behörigheter”. I dessa fall ska en begäran om förnyelse ske efter viss fastställd period.
- en tydlig struktur för vilka system, behörigheter m.m. som avses
- vem som godkänt och utfört behörigheten
- om ansökan gäller en ”känslig behörighet” kan ev. ytterligare godkännande krävas

### 4.6. Inloggning

*Iakttagelse:*
Som nämnts tidigare finns det ingen generell policy som fastställer gemensamma rutiner avseende användaradministrationen för kommunens system. Det förekommer system som har tvingande lösenordsbyte varje månad men det förekommer även system som saknar denna rutin.

Det noteras att lösenord till ett nytt system skickats till ansvarig chef. Det finns även fall där standardlösenord använts.

*Kommentar:*
Lösenordet till inloggningen, som skall vara personligt och hemligt, skall säkerställa att det är rätt användare som loggar in i systemet/på kontot. Om det saknas riktlinjer för inloggning ökar risken för felaktig hantering och obehörig åtkomst.

*Förbättringsområde:*
Det finns en mängd teorier kring säker inloggning och byte av lösenord. Ett sätt är att ha ”enkla” lösenord och byta ofta och ett alternativ är att ha mycket komplicerade lösenord med byte mer sällan.

Branschstandarden rekommenderar att standardsystem har lösenord som består av minst åtta tecken och att byte sker var 90:e dag. För system som kräver en ökad säkerhet bör det krävas komplicerade lösenord, dvs. innehålla minst ett specialtecken, en siffra och en bokstav.

Byte av lösenord som sker mer frekvent än var 90:e dag, kan resultera i att lösenordet skrivs ner, vilket minskar säkerheten. Vidare bör det inte vara möjligt att byta tillbaka till tidigare använt lösenord och det bör finnas krav på att ha lösenordet ska innehas minst en dag. Efter ett fastställt antal misslyckade inloggningsförsök bör kontot låsas och endast kunna låsas upp med hjälp av Helpdesk. Det är viktigt att någon annan part blir medveten om orsaken till låsningen.

Lösenordet bör alltid lämnas direkt till aktuell användare.

### 4.7. Uppföljning

*Iakttagelse:*
Det saknas rutiner för periodiska uppföljningar som säkerställer att rätt användare och rätt behörigheter är kopplat till kommunens system.

Vid vår granskning noterades konton som borde låsts eller plockats bort p.g.a. att användaren slutat sin anställning eller bytt arbetsuppgifter.

*Kommentar:*
När en medarbetare slutar eller byter arbetsuppgifter och ansvarsområden och erhåller nya behörigheter är det viktigt att det finns rutiner för att de gamla behörigheterna plockas bort. Detta kan resultera i icke önskade kombinationer av behörigheter som inte är förenat med god intern kontroll.

*Förbättringsområde:*
Rutiner för systematiska uppföljningar av samtliga IT-system bör fastställas. Det är väsentligt att fastställa en tidplan för uppföljningarna som bör vara kopplade till systemets fastställda risknivå.

## 5. Sammanfattande bedömning

I vår granskning har det noterats ett par gamla konton och behörigheter som inte avslutats på korrekt sätt. I övrigt görs bedömningen att det finns en informell kontrollstruktur avseende användaradministrationen. Det saknas dock skriftliga rutiner och dokumentation som gör det möjligt att i efterhand verifiera att kontroller utförts. Vår sammanfattande bedömning är att användaradministrationen kan utvecklas för att bli mer ändamålsenlig och enhetlig inom kommunen.

Följande utvecklingsområden har identifierats i granskningen:

- Ett system för att på ett systematiskt sätt riskklassificera samtliga system/processer som används inom kommunen bör införas. Fastställd risknivå bör omprövas enligt fastställd tidsplan för att ta hänsyn till ev. förändringar i verksamhet m.m.

- Det är väsentligt att det på ett tydligt sätt framgår för varje enskilt system vilka personer som identifierats som kraftfulla användare. Om det inte är möjligt att avskilja kraftfulla användare från den operativa verksamheten bör kompletterade kontroller fastställas.

- Behörigheter bör standardiseras och följa en enhetlig struktur. Behörigheter ska tilldelas utifrån ansvarsområden men även utifrån systemets riskklassificering.

- Det ska finnas tydliga riktlinjer som anger vem i organisationen som har rätt att beställa nya/förändra befintliga behörigheter samt vem/vilken funktion som har rätt att godkänna behörigheter.

- Vid beställning och godkännande av behörigheter är det väsentligt att det finns kontrollmoment som beaktar rimligheten i behörigheten utifrån medarbetarens ansvarsområden och fastställda krav på intern kontroll.

- En mall för ansökan om ny behörighet/förändrig av befintlig behörighet bör tas fram för att säkerställa ett likformigt arbetssätt.

- Riktlinjer kring lösenordstilldelning bör fastställas. Dessa bör kopplas till systemets fastställda risknivå.

- Det bör fastställas riktlinjer som anger hur lösenord för olika typer av system ska utformas och hur ofta byte av lösenord ska ske. Även här bör koppling till systemets risknivå ske.

- Rutiner för systematiska uppföljningar av samtliga IT-system bör fastställas. Uppföljningar bör ske med viss fastställd frekvens.

Jönköping 24 februari 2011

Per Magnusson

## Källförteckning

Intervjuer har skett med följande befattningar:

- IS/IT- chef
- Informationssamordnare
- Upphandlingschef
- Systemägare för Aditro ekonomisystem
- Systemförvaltare för Aditro ekonomisystem
- Teknikgruppschef inom IS/IT-avdelningen
- Dokument avseende användare i berörda system och servrar
- Dokument över behörigheter för ett urval av användare
- Skärmbilder som visar exempel på inloggning och lösenordslängder