

# Granskning av IT-leveransen från IT-service till Malmö stad

Februari 2010



Stadsrevisionen  
Malmö stad  
Stadshuset, August Palms plats 1  
205 80 Malmö

2010-02-09

Bäste Lennart,

Bifogat rekommendationsbrev innehåller en sammanställning av identifierade förbättringsförslag avseende leveransen från IT-service till Malmö stad, vilka noterades vid utförandet av vår granskning, vilken har utförts mellan November 2009 och Januari 2010.

Iakttagelserna är avstämde med respektive ansvarig och de har också fått möjlighet att lämna en kommentar avseende eventuell planerad åtgärd.

Bifogat rekommendationsbrev inkluderar även kommentarer och förbättringsförslag för varje iakttagelse.



**Marcus Sörländer**  
Partner



**Christian Bengtsson**  
Senior Consultant



**Fredrik Lövgren**  
Senior Consultant

# Innehållsförteckning

<b>SAMMANFATTNING .....</b>	<b>2</b>
<b>INLEDNING .....</b>	<b>3</b>
BAKGRUND .....	3
OMFATTNING .....	3
METOD .....	3
AVGRÄNSNINGAR.....	4
<b>IAKTTAGELSER OCH REKOMMENDATIONER .....</b>	<b>5</b>
<b>ÖVERGRIPANDE OBSERVATIONER .....</b>	<b>5</b>
1. OTYDLIG ANSVARSFÖRDELNING .....	5
2. PÅGÅENDE IMPLEMENTERING AV ITIL-PROCESSER.....	6
<b>INFORMATIONSSÄKERHET.....</b>	<b>7</b>
1. UPPRÄTTANDE AV PROCESS FÖR KONTROLL AV TEKNISK EFTERLEVAD .....	8
2. BRISTANDE LÖSENORDSKRAV I KATALOGTJÄNSTEN ACTIVE DIRECTORY .....	9
3. BRISTANDE LÖSENORDSKRAV I ORACLE .....	10
4. BRISTANDE LÖSENORDSKRAV I SQL.....	11
5. BRISTANDE LÖSENORDSKRAV I UNIX .....	12
6. STANDARDKONTO I ORACLE MED STANDARDLÖSENORD.....	13
7. STANDARDKONTO I WINDOWS EJ NAMNÄNDRAT.....	14
8. BRISTANDE UPPFÖLJNING AV LOGGFILER I ORACLE .....	15
9. BRISTANDE LOGGNING I ACTIVE DIRECTORY .....	16
10. BRISTANDE NAMNSTANDARD I ORACLE .....	17
11. GRUPPKONTO ANVÄNDS FÖR ADMINISTRATION AV PASSERKORT TILL STADSHUSET .....	18
12. BRISTANDE ANVÄNDARADMINISTRATION.....	19
13. ANVÄNDARE MED HÖG BEHÖRIGHET I ORACLE .....	20
<b>DRIFT.....</b>	<b>21</b>
1. AVSAKNAD AV SERVICE LEVEL AGREEMENTS .....	21
2. BRISTER I FYSISK SÄKERHET I DATAHALLAR.....	22
3. STORT ANTAL PERSONER MED TILLGÅNG TILL DATAHALLAR.....	23
4. AVSAKNAD AV KONTINUITETSPLAN.....	24
5. AVSAKNAD AV ÅTERLÄSNINGSTEST AV BACKUP.....	25
6. BRISTANDE RUTIN FÖR UPPDATERING AV PROGRAMVAROR .....	26
<b>FÖRÄNDRINGSHANTERING .....</b>	<b>27</b>
1. AVSAKNAD AV GODKÄNNANDE AV FÖRÄNDRING .....	27
2. BRISTER I RUTIN VID PRODUKTIONSSÄTTNING AV FÖRÄNDRING .....	28
3. BRISTANDE SPÅRBARHET VID TESTNING .....	29
<b>BILAGA 1 INTERVJUADE PERSONER .....</b>	<b>30</b>

# Sammanfattning

Vi har granskat den interna kontrollen hos IT-service avseende leverans av IT tjänster inom Malmö stad. Granskningen har omfattat arbetssätt, rutiner och vissa tekniska inställningar för att utvärdera IT-service leverans till Malmö stad och identifiera riskområden som bör utredas samt åtgärdas.

Våra slutsatser är att det flesta generella rutinerna för god IT-leverans finns på plats, eller håller på att implementeras eller förbättras hos IT-service. Detta baserar vi på den testning som utförts under granskningen och innefattade områden så som ansvarsfördelning, informationssäkerhet, övervakning och mätning, incident- och problemhantering, förändringshantering samt avtal med underleverantörer.

Vi har dock identifierat ett antal brister som bör utredas och åtgärdas. Framst handlar det om ansvarsfördelning mellan IT-service och verksamheten, där ansvaret inte alltid är tydligt. Detta kan leda till driftavbrott och onödiga säkerhetsbrister. Vi har även noterat ett antal förbättringsmöjligheter gällande informationssäkerheten i IT-miljön, gällande bl.a. lösenordskrav och användande av standardkonton. Inom områdena drift och förändringshantering har vi också identifierat ett antal förbättringsmöjligheter gällande främst kontinuitetsplanering och spårbarhet vid implementering av förändringar.

# Inledning

Malmö Stadsrevision har beslutat genomföra en granskning av Malmö stads IT-leverantör IT-service som är ett affärsområde inom Serviceförvaltningen. För denna granskning har Malmö Stadsrevision tagit stöd av Deloitte, Enterprise Risk Services, som genomfört denna granskning i tätt samarbete med IT-service.

## Bakgrund

Granskningen är initierad av Stadsrevisionen i Malmö Stad baserat på den granskningsplan för IT som genomfördes under 2008. Drift hos IT-service var en av de identifierade områdena för riktade granskningar. Granskningen syftar till att gå igenom de rutiner och processer på IT-service för att kunna bedöma om det finns en ändamålsenlig intern kontroll över de tjänster som IT-service levererar.

## Omfattning

Granskningen av IT-service har i samråd med stadsrevisionen fokuserat på följande områden som bedöms vara centrala i leveransen av IT-drift inom Malmö stad:

- Ansvarsfördelning
- Informationssäkerhet
- Övervakning och mätning
- Incident- och problemhantering
- Förändringshantering
- Avtal med underleverantörer

## Metod

Intervjuer har utförts med ett stort antal medarbetare inom Malmö stad, se bilaga 1. Intervjuerna har genomförts för att skapa en förståelse för funktionalitet och rutiner avseende IT-service leverans till Malmö stad. Relevant dokumentation har också samlats in för de områden som granskas, vilket till exempel kan vara styrande dokument, så som IT-säkerhetspolicy samt regler och riktlinjer för IT-säkerhet inom Malmö stad.

Testning har sedan utförts för att bedöma om identifierade kontroller utförs på ett sätt som föreskrivs i eventuella fastslagna regler, riktlinjer eller motsvarande dokument inom Malmö stad samt om dessa möter förväntningar på god intern kontroll relativt stadens verksamhet. Insamlat material har analyserats enligt Deloitte's etablerade kontrollramverk och även jämförts med så kallad "best practice". Deloitte's kontrollramverk är bland annat baserade på COBIT, vilket är en förkortning för "Control Objective for Information and Related Technology". Detta är en allmänt accepterad standard för kontroller inom informationsteknologi, framtagen av IT Governance Institute (ITGI).

Avvikelser grupperas och rapporteras inom fyra områden, vilka presenteras närmare nedan.

## Övergripande observationer

Under denna rubrik presenteras iakttagelser som är gränsöverskridande över de övriga tre områdena och därför inte kan grupperas in under ett enskilt område.

## **Informationssäkerhet**

Området informationssäkerhet avser iakttagelser som avser påverkan på informationens tillgänglighet, integritet eller sekretess.

## **Drift**

Inom området drift rapporteras iakttagelser kopplat till den dagliga driften av IT-systemen, fysisk säkerhet, samt ansvar och förvaltningsfrågor. Detta område har precis som informationssäkerhetsområdet en stark koppling till informationens tillgänglighet, integritet och sekretess.

## **Förändringshantering**

Syfte med denna process är att få kontroll över vilka ändringar som utförs i IT-system och infrastruktur. Därmed är det möjligt att undvika oväntade konsekvenser och dessutom få en effektiv, verksamhetsanpassad och ändamålsenlig hantering av förändringar. Processen används till exempel vid:

- Införande av ny programvara, ny version eller buggrättningar
- Vid risk för driftavbrott vid mindre ändringar
- När en konfiguration ändras

## **Avgränsningar**

Denna granskning är begränsad till IT-service leverans (drift av IT) och därför har ingen granskning eller testning utförts på förvaltningar som hanterar sin egen IT miljö. Det finns också IT frågor som hanteras av IT avdelningen på Stadskontoret, vilka ej har varit föremål för granskning inom detta uppdrag.

Under granskningen pågick ett projekt med syfte att gå igenom processerna Incident, Problem och Change (vilka ingår i ramverket ITIL, IT Infrastructure Library), varför det inte varit fullt möjligt att testa att dessa fungerar som avsett. Samtliga processer var under granskningen inte helt färdiga och implementerade.

# Iakttagelser och rekommendationer

I de följande avsnitten kommer iakttagelser från områdena informationssäkerhet, drift samt förändringshantering att redovisas.

## Övergripande observationer

Under granskningen har vi även gjort observationer av mer övergripande karaktär, som vi redovisar i detta avsnitt då de inte går att sortera in under ett enskilt område bland de övriga observationerna inom informationssäkerhet, drift och förändringshantering nedan.

### 1. Otydlig ansvarsfördelning

#### Iakttagelse

Vi har noterat att ansvaret för IT inte alltid är tydligt inom Malmö stad, då förvaltningsorganisationerna ibland hänvisar till IT-service och IT-service i sin tur hänvisar till förvaltningsorganisationen. Dessutom finns IT-avdelningen inom Stadskontoret också inblandad. Detta är ett vanligt problem i outsourcing-liknande situationer, där ansvar och uppgifter måste vara tydligt avtalat och kommunicerat.

#### Risk:

Vid outsourcing och outsourcing-liknande situationer finns det en risk att ansvar kan bli otydligt. När ägarskap mellan två parter inte är helt klart finns en risk att en process eller uppgift inte blir utförd enligt plan, vilket bland annat kan leda till ökade kostnader och försämrat förtroende från intressenter, så som invånarna i Malmö stad.

#### Rekommendation

Vi rekommenderar att Malmö stad utvärderar ansvar kring processer och uppgifter i relationen mellan IT-service, IT Staben, och övriga förvaltningar.

## 2. Pågående implementering av ITIL-processer

### Iakttagelse

Vi har konstaterat att Malmö stad är mitt i ett projekt för att implementera ITIL-processerna Incident, Problem och Change. Under vår granskning har vi noterat brister som kan härledas till avsaknad av just dessa processer, till exempel har vi noterat att inte alla incidenter registreras i ärendehanteringssystemet samt att vi noterat brister i Change processen.

#### Risk:

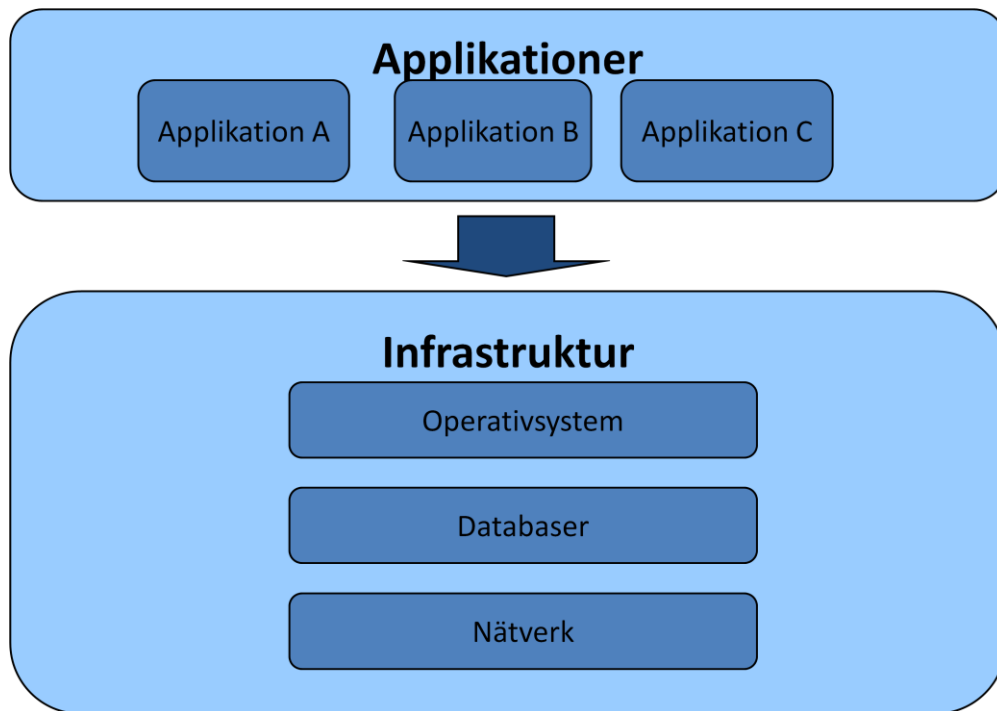
Brister i ITIL-processerna ökar risken att kunskap kring incidenter går förlorad, vilket kan skapa problem i onödan. Detta medför även att problem inte blir åtgärdade genom implementering av nya förändringar.

### Rekommendation

Vi rekommenderar att Malmö stad fortsätter implementeringen av ITIL-processerna fullt ut och följer upp hur processerna fungerar när samtliga processer är implementerade och någon/några incidenter, problem och förändringar har identifierats och hanterats.

# Informationssäkerhet

Informationssäkerhet skall upprätthållas inom samtliga områden för att säkerställa en god tillgänglighet, sekretess och integritet. Applikationer och system har ofta inbyggda kontroller som syftar till att stödja informationssäkerheten i applikationen. Dessutom nyttjar applikationer ofta de kontroller som finns i den underliggande infrastrukturen, så som operativsystem, databaser och nätverk.



Denna granskning har fokus på de kontroller som finns i infrastrukturen och skapar grunden för den leverans som IT-service utför.

## 1. Upprättande av process för kontroll av teknisk efterlevnad

### Iakttagelse

Vi har under granskningen noterat att det inte finns någon etablerad process för att regelbundet säkerställa att informationssystemen uppfyller de krav som finns från regler och riktlinjer fastslagna inom Malmö stad samt eventuella externa lagkrav och föreskrifter.

#### Risk:

Utan en fungerande process för kontroll av teknisk efterlevnad finns risk att informationssystem ej är konfigurerade korrekt eller uppfyller de krav och föreskrifter som är aktuella. Detta kan innebära en risk för påverkan av systemen och informationens tillgänglighet, integritet och sekretess.

### Rekommendation

Vi rekommenderar Malmö stad att upprätta standards exempelvis för konfiguration och installation av system. En process bör sedan etableras som har till uppgift att se till att alla system uppfyller de policys och tekniska standards som finns fastslagna. Kontrollen kan utföras manuellt av systemexpert och/eller genom automatiserat kontrollverktyg. Avvikelser bör dokumenteras och åtgärdas.

## 2. Bristande lösenordskrav i katalogtjänsten Active Directory

### Iakttagelse

Vi har noterat att lösenordskraven i den centrala katalogtjänsten Active Directory inte kräver komplexa lösenord och tvingade byte sker efter 180 dagar, vilket betyder att de ej uppfyller kraven enligt Malmö stads "Regler och riktlinjer för IT-säkerhet i Malmö stad".

#### Risk:

Bristande lösenordskrav ökar risken för intrång. Svaga lösenord utgör en säkerhetsrisk då risken för att obehöriga kommer åt känslig information väsentligt ökar, vilket kan innebära att data otillbörligen modifieras och/eller förstörs.

### Rekommendation

Vi rekommenderar Malmö stad att utvärdera lösenordsinställningarna för Malmö stads AD. Malmö stads "Regler och riktlinjer för IT-säkerhet i Malmö stad" säger att lösenord ska innehålla bokstäver, siffror samt symboler (komplexa lösenord).

Best practice är enligt Deloitte;

- Bytesintervall: 30 till 90 dagar
- Lösenordslängd: Minst 6 (om komplext) eller 8 (om ej komplext)
- Lösenordskomplexitet: Ja, lösenordet skall innehålla en blandning av versaler, gemener, numeriska samt andra tecken.
- Lösenords historik: 6 senaste lösenorden skall ej gå att återanvända
- Låsning av konto efter misslyckad inloggning: Efter 3 - 6 felaktiga försök.
- Låsningsperiod: Tills kontot låses upp av administratör, alternativt minst 30 minuter

### 3. Bristande lösenordskrav i Oracle

#### Iakttagelse

Vi har noterat att lösenordsinställningarna i Oracle-databasen för Procapita inte är i linje med Malmö stads policy. Det finns inget krav på tvingande byte av lösenord.

#### Risk:

Bristande lösenordskrav ökar risken för intrång. Svaga lösenord utgör en säkerhetsrisk då risken för att obehöriga kommer åt känslig information väsentligt ökar, vilket kan innebära att data otillbörligen modifieras och/eller förstörs.

#### Rekommendation

Vi rekommenderar Malmö stad att gå igenom lösenordshanteringen för användarkonton i Oracle-databaserna och utvärdera hur dessa konton ska hanteras för att lösenordspolicyn ska efterlevas.

## 4. Bristande lösenordskrav i SQL

### Iakttagelse

Vi har noterat att det finns användarkonton som loggar in direkt i SQL databasen utan autentisering genom den centrala katalogtjänsten Active Directory. Detta kan innebära att de ej hanteras enligt föreskrivna regler och rutiner med avseende på kontohantering och lösenord som regleras med hjälp av Active Directory.

#### Risk:

Bristande lösenordskrav ökar risken för intrång. Svaga lösenord utgör en säkerhetsrisk då risken för att obehöriga kommer åt känslig information väsentligt ökar, vilket kan innebära att data otillbörligen modifieras och/eller förstörs.

### Rekommendation

Vi rekommenderar att Malmö stad går igenom lösenordsinställningarna för SQL-servrar och validerar om de följer fastställda policys. Vi rekommenderar även Malmö stad att säkerställa lösenordshanteringen för SQL-konton med hög behörighet.

## 5. Bristande lösenordskrav i Unix

### Iakttagelse

Vi har noterat att lösenordskraven i Unix inte kräver komplexa lösenord och inget tvingade byte av lösenord.

#### Risk:

Bristande lösenordskrav ökar risken för intrång. Svaga lösenord utgör en säkerhetsrisk då risken för att obehöriga kommer åt känslig information väsentligt ökar, vilket kan innebära att data otillbörligen modifieras och/eller förstörs.

### Rekommendation

Vi rekommenderar Malmö stad att utvärdera lösenordsinställningarna för Unixmiljön. Malmö stad "Regler och riktlinjer för IT-säkerhet i Malmö stad" säger att lösenord ska innehålla bokstäver, siffror samt symboler (komplexa lösenord).

Best practice är enligt Deloitte;

- Bytesintervall: 30 till 90 dagar
- Lösenordslängd: Minst 6 (om komplext) eller 8 (om ej komplext)
- Lösenordskomplexitet: Ja, lösenordet skall innehålla en blandning av versaler, gemener, numeriska samt andra tecken.
- Lösenords historik: 6 senaste lösenorden skall ej gå att återanvända
- Låsning av konto efter misslyckad inloggning: Efter 3 - 6 felaktiga försök.
- Låsningsperiod: Tills kontot låses upp av administratör, alternativt minst 30 minuter

## 6. Standardkonto i Oracle med standardlösenord

### Iakttagelse

Vi har noterat att det finns ett standardkonto aktivt i Oracle-databasen för Procapita där lösenordet är detsamma som defaultvärdet som ställs automatiskt vid installation.

#### Risk:

När standardlösenord ej ändras för standardkonton ökar risken väsentligt för intrång. Standardkonton är ofta extra utsatta vid intrångsförsök och risken för att obehöriga kommer åt känslig information ökar väsentligt, vilket kan innebära att data otillbörligen modifieras och/eller förstörs. Detta kan också innebära att känslig information kan spridas okontrollerat.

### Rekommendation

Vi rekommenderar att Malmö stad går igenom Oracle-databaserna och säkerställer att inga standardkonton med standardlösenord är aktiva.

## 7. Standardkonto i Windows ej namnändrat

### Iakttagelse

Vi har observerat att standardkontot *Administrator* inte är namnändrat i Windows. Genom att ändra namnet försvåras eventuella försök att angripa systemet genom att lista ut lösenord för kontot.

#### Risk:

*Administrator* är det konto i Windows med högst behörighet och är därför speciellt utsatt vid eventuella intrångsförsök, vilket ökar risken för att obehöriga kommer åt känslig information. Detta kan innebära att data otillbörligen modifieras och/eller förstörs.

### Rekommendation

Vi rekommenderar Malmö stad att utvärdera om namnet på standardkontot *Administrator*, vilket är det kontot med högst behörighet i Windows, bör namnändras. Dessa konton är ofta särskilt utsatta vid eventuella intrångsförsök och bör därför hanteras med extra säkerhet och kontroll. Genom att byta namn på kontot kan ett eventuellt angrepp på systemet försvåras.

## 8. Bristande uppföljning av loggfiler i Oracle

### Iakttagelse

Vi har noterat att det är databasadministratören för Oracle-databaserna på IT-service som går igenom loggfilerna i Oracle. Detta kan innebära en brist i den interna kontrollen med avseende på uppdelning av arbetsuppgifter.

#### Risk:

Bristande uppföljning av loggfiler ökar risken för att medvetna eller omedvetna felaktiga förändringar kopplat till Oracle inte identifieras och utreds inom en lämplig tid, om de identifieras alls. Detta ökar risken för att data modifieras utan att tillfredställande spårbarhet finns för att upptäcka detta.

### Rekommendation

Vi rekommenderar att Malmö stad utvärderar rutinen för genomgång av loggfiler. En rutin bör implementeras för regelbunden genomgång av loggfiler och dessa bör inte granskas av de medarbetare som har höga behörigheter i Oracle-databaserna.

## 9. Bristande loggning i Active Directory

### Iakttagelse

Vi har noterat att det inte finns några riktlinjer kring vad som bör loggas i Windows-miljön. Stora mängder loggfiler kräver ofta ett strukturerat angreppssätt för lagring och analys av insamlade händelser.

#### Risk:

Avsaknad av eller bristande loggningsfunktionalitet ökar risken för att medvetna eller omedvetna felaktiga förändringar inte identifieras och utreds inom en lämplig tid, om de identifieras alls.

### Rekommendation

Vi rekommenderar Malmö stad att utvärdera vad som bör loggas i Windows-miljön och se över rutinen för genomgång av loggfiler.

Best practice är enligt Deloitte;

Audit Account Logon Events: Success, Failure

Audit Account Management: Success, Failure

Audit Logon Events: Failure

Audit Policy Change: Success, Failure

Audit Privilege Use: Failure

Audit Process Tracking: None

Audit System Events: Success, Failure

Vi rekommenderar också att lösningar för logganalys undersöks för att kunna dra slutsatser och kunna agera på insamlade händelser.

## 10. Bristande namnstandard i Oracle

### Iakttagelse

Vi har noterat att det inte finns någon namnstandard för databaskonton i Oracle. Vi har även noterat att det saknas kunskap kring de historiska inställningarna i Oracle.

#### Risk:

Bristande namnstandard ökar risken att felaktiga konton ej upptäcks och avaktiveras, eftersom att det är svårt för en databasadministratör (DBA) att avgöra vem som har tillgång till respektive konto samt vad konton används till.

### Rekommendation

Vi rekommenderar en genomgång av namnstandarderna av Oracle-konton samt att kunskap kring historiska inställningar skaffas för att säkerställa att det inte finns några risker med nuvarande inställning och att det finns kunskap kring Oracle-databaserna om någon incident skulle inträffa.

## 11. Gruppkonto används för administration av passerkort till Stadshuset

### Iakttagelse

Vi har noterat att administratörerna i passerkortssystemet RCO, vilket är vaktmästarna tillhörande Kommunteknik på Stadshuset, använder ett gruppkonto (ett personligt användarkonto är alltid inloggat och samtliga vaktmästare som administrerar systemet nyttjar detta konto) för att administrera tillgång till bland annat datahallen i Stadshuset. Vi noterade även att det finns totalt 11 administratörer (konton med hög behörighet) i RCO.

#### Risk:

Konton som inte är designerade till specifika användare minskar spårbarheten och därmed möjligheten att utreda orsakerna till eventuella felaktigheter.

### Rekommendation

Vi rekommenderar Malmö stad att se över vilka som har tillgång till IT-systemet RCO och säkerställa att samtliga medarbetare med tillgång använder personliga konton. Detta för att säkerställa spårbarhet vid tillägg och borttag av medarbetare med tillgång till datahallen i Stadshuset, samt säkerställa att endast behörig personal har tillgång till RCO.

## 12. Bristande användaradministration

### Iakttagelse

Vi har noterat att inte all personal som har slutat under 2009 har fått sitt användarkonto i AD inaktiverat. Vi har även noterat att en del konton inte blivit inaktiverade inom en rimlig tidsperiod.

#### Risk:

Brister i rutinerna för behörighetsadministration kan innebära att personer får eller bibehåller obehörig åtkomst till IT-system och information. Detta kan ge leda till otillbörlig spridning, manipulering eller otillgänglighet av information och resurser.

### Rekommendation

Vi rekommenderar Malmö stad att säkerställa att rutinen för behörighetsadministration efterlevs. Vi rekommenderar också Malmö stad att regelbundet säkerställa att varje användarkontos rättigheter i nätverk, operativsystem, databaser och applikationer är adekvat baserat på individernas arbetsuppgifter samt att användare som lämnat organisationen tas bort ur systemen. Denna aktivitet genomförs bäst regelbundet med hjälp av någon form av systemstöd men finns ej detta rekommenderar vi en manuell genomgång åtminstone en gång per år. Detta genomförs förslagsvis genom att delegera ansvaret för genomgången till respektive chef i organisationen vilka genomför granskningen och rapporterar sedan centralt.

## 13. Användare med hög behörighet i Oracle

### Iakttagelse

Vi har noterat att det finns användarkonton i Oracle med högre behörigheter än vad som är brukligt för dessa konton. Rollen "TOOROBKS" är tilldelad ett antal vanliga konton i Oracle (konton som vanliga användare nyttjar vid access till databasen via applikationen). Rollen har behörighet att bland annat skapa och förändra användare.

#### Risk:

När användare har högre behörighet än nödvändigt ökar risken att obehöriga kommer åt känslig information. Detta kan innebära att data otillbörligen modifieras och/eller förstörs.

### Rekommendation

Vi rekommenderar Malmö stad att utvärdera vilka konton som ska ha höga behörigheter i Oracle och säkerställa att endast behöriga användare har höga behörigheter.

# Drift

## 1. Avsaknad av Service Level Agreements

### Iakttagelse

Vi har noterat att Service Level Agreements inte är etablerade för samtliga förvaltningsorganisationer. Uppföljning av SLA sker även på ad hoc basis, där vissa förvaltningsorganisationer följer upp sina SLA kontinuerligt och andra förvaltningsorganisationer inte följer upp några SLA alls.

#### Risk:

Bristande uppföljning ökar risken att brister kan gå oupptäckta och eventuella incidenter skulle kunna leda till ökade kostnader och driftstopp. Avsaknad av SLA kan innebära oklarheter i tjänsteleveransen som en konsekvens av detta även påverka en tjänsts tillgänglighet.

### Rekommendation

Vi rekommenderar Malmö stad att etablera SLA med samtliga förvaltningsorganisationer och dessa bör följas upp på regelbunden basis.

## 2. Brister i fysisk säkerhet i datahallar

### Iakttagelse

Vi har noterat att datahallarna är utrustade med olika säkerhetsanordningar och miljöskydd. Datahallen i Stadshuset har inget upphöjt golv och i datahallen på Rönnen noterades det att bitar av taket lossnar. Vi har även förstått att datahallen i Stadshuset delas med utomstående leverantörer (till exempel Tele2). Datahallen i Stadshuset var tilltänkt som en temporär lösning, men används fortfarande och ytterligare en temporär datahall har etablerats genom hosting hos TDC via Kerfi.

### Risk:

Otillräcklig fysisk säkerhet kring datahallar och utrustningen i dessa ökar risken för avbrott i driften av IT-miljön.

### Rekommendation

Vi rekommenderar Malmö stad att se över miljöskyddet i datahallarna. Vi rekommenderar även Malmö stad att utvärdera vilka datahallar som ska användas som primära datahallar.

### 3. Stort antal personer med tillgång till datahallar

#### Iakttagelse

Vi har noterat att det totalt är 87 kort utfärdade med tillgång till datahallen i Stadshuset, vilket får anses vara ett mycket stort antal personer.

#### Risk:

När många personer har tillgång till datahallen minskar kontrollen kring vilka personer som är behöriga, vilket kan leda till att obehöriga personer kan vistas i datahallen utan att detta uppmärksammas.

#### Rekommendation

Vi rekommenderar Malmö stad att utvärdera vilka medarbetare som bör ha tillgång till datahallarna för att säkerställa att obehöriga inte har access till datahallarna. Det finns en risk att kontrollen av datahallarna minskar när många medarbetare (och eventuella konsulter) har tillgång till datahallarna. Risken att något oförutsett gällande datahallarna händer ökar också med antalet personer med tillgång. Endast personal som behöver tillgång till datahallar ska ha denna tillgång.

## 4. Avsaknad av kontinuitetsplan

### Iakttagelse

Vi har noterat att det inte finns någon etablerad kontinuitetsplan inom Malmö stad, vilket även påpekas i tidigare revisionsrapporten "Kontinuitetsplanering av IT-verksamheten" daterad i september 2009.

#### Risk:

Avsaknad av en kontinuitetsplan ökar risken att en katastrof eller incident leder till långvariga driftsstopp som inte kan hanteras inom en för Malmö stad acceptabel tidsram. Ett sådant avbrott kan även leda till förlust av kritisk information, vilket kan leda till ökade kostnader, intäktsförluster, missnöjda invånare och andra nackdelar för Malmö stad.

### Rekommendation

Vi rekommenderar att Malmö stad utvärderar om de bör skapa en kontinuitetsplan för verksamheten. Grunden i en kontinuitetsplan är riskanalyser, varför vi rekommenderar Malmö stad att utvärdera vilka risker som är viktigast att hantera för verksamheten.

## 5. Avsaknad av återläsningstest av backup

### Iakttagelse

Vi har noterat att det inte finns någon fastställd rutin eller strategi för periodiska återläsningstest av säkerhetskopierad data. Återläsningstester sker på ad-hoc basis, vid initiativ hos IT-service eller önskemål från förvaltningen.

#### Risk:

Avsaknad av återläsningstest av säkerhetskopierad data kan leda till att det tar lång tid att läsa tillbaka data och data kan även gå förlorad vid en eventuell incident.

### Rekommendation

Vi rekommenderar Malmö stad att revidera rutinen för återläsningstester av säkerhetskopierad data för att säkerställa att en fullständig återläsning är möjlig i en krissituation. Tester bör utföras och dokumenteras regelbundet för att säkerställa att data kan återställas inom en godtagbar tid.

## 6. Bristande rutin för uppdatering av programvaror

### Iakttagelse

Vi har noterat att det inte finns någon fastställd rutin för hantering av programvaruuppdateringar (patch management). Uppdateringar testas inte på några specifika testgrupper av klienter och servrar. Det finns ingen dokumentation kring patchnivåerna på servrarna. Vidare ses programvaruuppdateringar som ”pre-approved” av IT-service och Malmö stad, varför inget godkännande går att finna.

#### Risk:

Utan en fastställd rutin ökar risken att spårbarheten kring uppdateringen blir lidande. Utan tester ökar även risken att eventuella brister i en uppdatering tillför problem i IT-miljön. Utebliven uppdatering innebär också risker för IT miljön.

### Rekommendation

Vi rekommenderar att Malmö stad utvärderar om de bör etablera en rutinbeskrivning för hantering av uppdateringar av programvaror. Vi rekommenderar även att uppdateringar testas innan dess att de installeras i produktionsmiljön. Detta bör med fördel göras på specifika testklienter och servrar som har liknande installation som de i produktion.

# Förändringshantering

## 1. Avsaknad av godkännande av förändring

### Iakttagelse

Vi har noterat att godkännande av förändringar inte alltid fattas genom ett Change Advisory Board (CAB) eller av en Change Manager innan förändringen implementeras. Enligt rutinbeskrivningen "Processdokumentation Change Management" version 1.0.0 skall varje så kallad Request for Change (RFC) innehålla rekommendationer från CAB.

#### Risk:

Avsaknad av formellt godkännande av en förändring kan innebära att felaktiga förändringar produktionssätts samt ökat personberoende på grund av ofullständig dokumentation, vilket kan ha en negativ inverkan på IT-miljön och dess tillgänglighet.

### Rekommendation

Vi rekommenderar Malmö stad att utvärdera rutinen för förändringshantering och säkerställa att förändringar alltid blir formellt godkända enligt fastställd rutinbeskrivning. Det är viktigt att man kan följa hela flödet i förändringshanteringen från initiering till slutlig acceptans.

## 2. Brister i rutin vid produktionssättning av förändring

### Iakttagelse

Vi har noterat att inte alla löpande förändringar har ett acceptanstest samt en så kallad back-out plan för att avbryta en förändring och återgå till tidigare miljö, ifall något inte skulle fungera som avsett. Enligt rutinbeskrivningen "Processdokumentation Change Management" version 1.0.0 skall varje RFC innehålla en så kallad back-out plan. Vi har till exempel noterat att det inte finns någon etablerad back-out plan gällande det pågående Exchange-projektet som innebär byte av mail plattform i Malmö stad.

#### Risk:

Avsaknad av acceptanstest samt back-out plan av en förändring kan innebära att felaktiga förändringar produktionssätts samt ökat personberoende på grund av ofullständig dokumentation, vilket kan ha en fördömande effekt på IT-miljön.

### Rekommendation

Vi rekommenderar Malmö stad att säkerställa att rutinen för förändringshantering fungerar som avsett. Förändringar bör dokumenteras med information kring godkännande, testresultat, acceptanstest, back-out plan samt avslut och godkännande efter implementering.

### 3. Bristande spårbarhet vid testning

#### Iakttagelse

Vi har noterat att det finns brister i spårbarheten kring vilka tester som utförts för respektive förändring. Vi har även noterat att förändringar ibland kan implementeras innan tester är utförda.

#### Risk:

Bristande dokumentation av utförda tester och kontroller av förändringar kan innebära brister i kvalitet och spårbarhet, vilket kan leda till personberoende, driftsstörningar eller annan negativ påverkan på IT-miljön.

#### Rekommendation

Vi rekommenderar Malmö stad att utvärdera dokumentationskraven kring tester av förändringar för att säkerställa spårbarheten när förändringar implementeras i IT-miljön.

# Bilaga 1 Intervjuade Personer

Namn	Titel/Roll	Datum
Peter Johansson	Informationssäkerhetschef	4/11 – 2009
Harald Nilsson	Systemsamordnare	2-3/11 – 2009
Bert Blomqvist	Vaktmästeriet Stadshuset, Kommunteknik	10/12 – 2009
Göran Nilsson	Vaktmästeriet Stadshuset, Kommunteknik	10/12 – 2009
Jörgen Nilsson	Vaktmästeriet Stadshuset, Kommunteknik	10/12 – 2009
Peter K Andersson	Chef IT-service	2/11, 9/12 – 2009
Rolf Hjertsson	Chef Design & Transition IT-service	3/11 – 2009
Davor Peraic	Produktionschef IT-service	2/11, 9/12 – 2009, 20/1 – 2010
Marcus Öhlin	Chef Kund & Support	3/11, 8-10/12 – 2009
Christer Christensson	IT-Driftchef	4/11 – 2009
Peder Haak	Fysisk access, Kund & Support	4/11 – 2009
Johan Almqvist	TEIS admin, IT-Drift	2/11, 9/12 – 2009
Mathias Nilsson	IT-Drift	20/1 – 2010
Jesper Henning	IT-Drift	20/1 – 2010
Michael Ian Avella	Oracle DBA, IT-Drift	20-21/1 – 2010
Thomas Öberg	IT-Drift	8/12 – 2009
David Ravenna	AD, Design & Transition	21/1 – 2010
Peter Bergehamn	ITIL, Konsult BiTA	21/1 – 2010