

Granskning av informations- integrationer inom 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 informationsintegrationer inom Malmö stad. Iakttagelserna har noterats vid utförandet av vår granskning under perioden November 2009 till och med Januari 2010.

Iakttagelserna är avstämnda 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

SAMMANFATTNING	2
INLEDNING	3
BAKGRUND.....	3
OMFATTNING	3
METOD	4
AVGRÄNSNINGAR	4
IAKTTAGELSER OCH REKOMMENDATIONER	5
INFORMATIONSSÄKERHET	5
1. BRISTANDE LÖSENORDSKRAV PÅ TEIS-SERVERN	5
2. BRISTANDE SÄKERHET I ÖVERFÖRINGAR	6
3. MELLANLAGRING AV FILER VID ÖVERFÖRING	7
DRIFT	8
1. AVSAKNAD AV RUTINBESKRIVNINGAR	8
2. AVSAKNAD AV SYSTEMÄGARE FÖR INTEGRATIONSMOTORN TEIS	9
3. BRISTANDE SPÅRBARHET KRING ÖVERVAKNING AV INTEGRATIONER	10
4. AVSAKNAD AV REDUNDANT LÖSNING FÖR TEIS.....	11
5. AVSAKNAD AV SUPPORT EFTER KONTORSTID	12
FÖRÄNDRINGSHANTERING	13
1. BRISTANDE FÖRÄNDRINGSHANTERING AV SCHEMALAGDA JOBB	13
BILAGA 1 INTERVJUADE PERSONER	14

Sammanfattning

Deloitte har granskat informationsintegrationer i Malmö stad som utförs med hjälp av integrationsmotorn TEIS. Granskningen har undersökt både tekniska inställningar samt arbetssätt och rutiner hos IT-service och andra inblandade parter.

I vår granskning har vi identifierat kontroller baserat på de risker som vanligtvis är aktuella vid integrationer. Rapporten visar de avvikelser vi har noterat i vår testning av de identifierade IT-kontrollerna. Våra slutsatser är att informationsintegrationerna i Malmö stad samt funktionaliteten i TEIS är fungerande. Det finns däremot ett antal identifierade riskområden som bör utredas samt åtgärdas. Främst handlar det om svagheter i ansvaret för TEIS. Detta innebär att förvaltningen av TEIS blir otydlig vilket kan påverka systemets tillgänglighet och i förlängningen påverka informationsflödet både internt och externt. Det finns också förbättringspotential i rutinerna kring förändringshantering samt kontinuitetsplanering för att ytterligare säkerställa stabilitet och tillgänglighet.

Inledning

Deloitte har genomfört en granskning avseende informationsintegrationer mellan system inom Malmö stad, vilka hanteras i integrationsmotorn TEIS. Många av integrationer är mycket kritiska för verksamheten inom Malmö stad. Bristande övervakning och/eller bristande hantering av eventuella fel eller avbrott kan leda till att information inte finns tillgänglig eller är fullständig när den behövs. Detta kan leda till att Malmö stad inte kan ge den service som förväntas av Malmöns invånare eller utföra det arbete som förväntas. En god intern kontroll är därför en förutsättning för att information skall kunna användas på ett sådant sätt att det stödjer verksamhetens behov och krav. Det är också viktigt att kunna upprätthålla informationens sekretess, tillgänglighet och integritet. På uppdrag av Stadsrevisionen har därför Deloitte granskat om informationsintegrationer hanterade av TEIS samt beroenden till denna kan anses fungera på ett tillfredsställande sätt.

Bakgrund

Malmö stad har köpt en produkt för systemintegration, TEIS. Leverantören av TEIS är Tieto, som är behjälpliga med konsultation när detta behövs. IT-service ansvarar för driften av TEIS, som körs på en fysisk server med operativsystemet Windows Server 2003. Merparten av alla integrationer (ca 1800) inom Malmö stad hanteras via den granskade TEIS implementationen. De flesta integrationerna innebär att ett systemkonto i TEIS, efadec, flyttar filer från en mapp till en annan och på så sätt gör filerna tillgängliga för att annat IT-system. Tillgång till dessa mappar begränsas till endast detta konto. Det sker även en del konverteringar av filer, då TEIS ändrar filformatet för att det mottagande IT-systemet ska kunna ta del av filerna. Integrationer eller förändringar i konfiguration av integrationer verkställs av IT-service, efter beställningar från respektive förvaltning och systemägare.

Omfattning

Granskningen av TEIS har fokuserat på följande områden som bedöms som centrala för god intern kontroll över informationsintegrationer:

- Ansvarsfördelning
- Informationssäkerhet
- Incident- och problemhantering
- Övervakning
- Förändringshantering

I denna granskning har IT-kontroller testas gällande operativsystem samt ett antal applikationer utvalda efter deras betydelse inom Malmö stad, baserat på antalet integrationer. Rutiner och IT-kontroller kring informationsintegrationer är generella för samtliga integrationer, varför de applikationer som valts ut i denna granskning kan anses vara ett representativt urval för att granska den interna kontrollen av informationsintegrationer.

De applikationer där ett antal integrationer valts ut för närmare granskning är:

- Origo (Vård och omsorg)
- Raindance (Malmö stads ekonomisystem)
- Prima (Personalsystem)
- Procapita (Individ och familjeomsorg)

Metod

Intervjuer har utförts med ett antal medarbetare inom Malmö stad, se bilaga 1. Intervjuerna har genomförts för att skapa en förståelse för funktionalitet och rutiner avseende TEIS och integrationerna i 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, rutiner eller andra styrande dokument inom Malmö stad samt att kontrollerna utformats så att de möter de risker som de är avsedda att adressera. 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 tre områden, vilka presenteras närmare nedan.

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 samt ansvar och förvaltningsfrågor. Iakttagelser gällande IT-driften kan ha påverkan på informationens tillgänglighet och integritet.

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

Programutveckling och mjukvaruförändringar avseende informationsintegrationssystemet sker hos leverantören av TEIS, Tieto, och har inte varit föremål för granskning.

I denna granskning har vi valt ut fyra applikationer vars integrationer har varit i fokus under testningen. Applikationerna valdes i samråd med IT-service, för att identifiera centrala integrationer med många integrationer. Informationsintegrationssystemet är centralt och IT-kontroller gällande integrationerna är av generell karaktär, varför de 4 centrala applikationerna bedöms utgöra tillräckligt underlag för att göra mer generella iakttagelser och rekommendationer.

IT-system och kataloger för avlämning och hämtning av filer har inte varit föremål för denna granskning, som fokuserar på TEIS och miljön där TEIS körs.

Iakttagelser och rekommendationer

I de följande avsnitten presenteras iakttagelser från områdena informationssäkerhet, drift samt förändringshantering.

Informationssäkerhet

1. Bristande lösenordskrav på TEIS-servern

Iakttagelse

Vi har noterat att lösenordskraven för användarkonto på TEIS servern är svaga. Lösenord behöver endast bestå av 2 tecken, bytas efter 170 dagar och det finns inget krav på komplexa lösenord, vilket betyder att de inte uppfyller kraven enligt Malmö stads "Regler och riktlinjer för IT-säkerhet i Malmö stad".

Risk:

Bristande lösenordsinställningar 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 TEIS servern. 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

2. Bristande säkerhet i överföringar

Iakttagelse

Information kan överföras på ett antal sätt mellan TEIS samt respektive för- och eftersystem. Ett av dessa sätt är med hjälp av så kallad FTP, File Transfer Protocol. FTP är ett filöverföringsprotokoll som i grunden är oskyddat för avlyssning. Det finns idag även alternativ som är skyddade mot denna typ av svagheter. Vi har i vår granskning noterat att vissa överföringar använder den nyare tekniken, så kallad Secure FTP, vilket innebär att överföringen är krypterad och på så sätt skyddad mot eventuell avlyssning.

Vi har under granskningen noterat att inte all överföring via TEIS sker med SFTP (Secure File Transfer Protocol).

Risk:

När data skickas utan okrypterad ökar risken att data, till exempel personuppgifter, kan hamna i orätta händer.

Rekommendation

Vi rekommenderar Malmö stad att utvärdera säkerheten i de filöverföringsprotokoll som används för att säkerställa att den motsvarar de krav förvaltningarna har på säker datahantering.

3. Mellanlagring av filer vid överföring

Iakttagelse

Vi har noterat att filer mellanlagras i integrationsmotorn TEIS, samt att det tas en backup av filer som flyttas med hjälp av TEIS. Filer som mellanlagras och sparas via backup kan innehålla känslig information.

Risk:

Det finns en risk att filer som mellanlagras av TEIS (i mappar och backup) inte hanteras enligt de krav som ställs av respektive förvaltning baserat på lagkrav och förordningar. Det finns dessutom en teoretisk risk att data oönskat ändras då säkerhetskraven på lösenord till TEIS-servern är låga, se rekommendation nr 1 ovan.

Rekommendation

Vi rekommenderar Malmö stad att utvärdera säkerheten kring mellanlagringen av dessa filer och säkerställa att det motsvarar de krav förvaltningarna har på säker datahantering. Det är också mycket viktigt att förvaltningarna informerar IT-service om eventuella restriktioner och lagkrav i samband med skapandet av integrationen. Se även rekommendation nr 1 under avsnittet "Förändringshantering".

Drift

1. Avsaknad av rutinbeskrivningar

Iakttagelse

Vi har noterat att det inte finns några rutinbeskrivningar för upplägg av nya integrationer samt borttagning och förändring av befintliga integrationer. Det finns inte heller några rutinbeskrivningar gällande processen för att starta om ett schemalagt jobb eller dokumentation av hur fel och avbrott i schemalagda jobb skall hanteras eller eskaleras.

Risk:

Avsaknad av rutinbeskrivningar ökar personberoende och kunskap kan gå förlorad när personal försvinner från organisationen. Det ökar även risken att mänskliga fel inträffar på grund av bristande kunskap av hur den specifika situationen skall hanteras. Detta kan påverka tillgängligheten av information, till följd av till exempel driftstopp och felaktiga prioriteringar.

Rekommendation

Vi rekommenderar Malmö stad att utvärdera om rutinbeskrivningar gällande TEIS och hanteringen av schemalagda jobb bör upprättas och fastställas. Rutinbeskrivningar hjälper till att minska personberoenden och skapar en enhetlig process som är lättare att följa. TEIS har en nyckelroll inom Malmö stad och det är därför av högsta prioritet att tillgänglighet och funktionalitet kan säkerställas.

2. Avsaknad av systemägare för integrationsmotorn TEIS

Iakttagelse

Vi har noterat att det inte finns någon systemägare av integrationsmotorn TEIS. Det tekniska ansvaret för TEIS finns hos IT-service med hjälp av konsulter från Tieto. Den information som hanteras i TEIS ägs av respektive förvaltning. Avsaknaden av systemägare innebär också att det saknas ett så kallat Service Level Agreement (SLA), dvs ett avtal som reglerar IT-service ansvar för driften av systemet. Det kan också påverka en strukturerad förvaltning (löpande underhåll, uppgraderingar och kontroll av säkerhetsinställningar) av systemet som till exempel kan innebära försenade insatser och investeringar som kan påverka systemets tillgänglighet.

Risk:

När ägarskap inte är helt klart finns en risk att en process eller uppgift inte blir utförd enligt plan. Detta kan påverka informationens tillgänglighet, fullständighet och sekretess, vilket i förlängningen kan leda till ökade kostnader och försämrat förtroende från allmänheten.

Rekommendation

Vi rekommenderar Malmö stad att se över ägarskapet av integrationsmotorn TEIS. Malmö stad bör utvärdera om det ska finnas en systemägare för TEIS inom någon förvaltningsorganisation alternativt om TEIS ska erbjudas som en tjänst av IT-service.

3. Bristande spårbarhet kring övervakning av integrationer

Iakttagelse

Vi har noterat att fel, avbrott och åtgärder kring schemalagda jobb inte dokumenteras på ett tillfredsställande sätt. Det finns ingen spårbarhet kring vad som inträffat och åtgärdats när ett schemalagt jobb inte slutförs korrekt som det skulle.

Risk:

Bristande dokumentation av incidenter kan resultera i att återkommande fel inte motverkas, vilket kan orsaka extra kostnader och driftstopp. Det finns också en risk att det inte går att utläsa huruvida jobbet någonsin avslutades, vilket kan ha påverkan på informationens fullständighet och integritet.

Rekommendation

Det är viktigt att alla incidenter registreras i ett ärendehanteringssystem, både för att kunna ha tillgång till historik och möjligheter till felsökning, men även till exempel för att IT-service skall kunna mäta de faktiska insatserna som görs samt att skapa möjligheter för proaktiva insatser. Vi rekommenderar därför att Malmö stad säkerställer att det finns en spårbarhet kring de avbrott och åtgärder som inträffar gällande integrationer via TEIS. Det är också ett viktigt steg i det pågående införandet av ITIL där ett grundläggande krav är att alla incidenter loggas i ett ärendesystem.

4. Avsaknad av redundant lösning för TEIS

Iakttagelse

Vi har noterat att det inte finns någon redundant lösning i det fall att hårdvara eller mjukvara fallerar för integrationsmotorn TEIS. Då TEIS hanterar cirka 1 800 integrationer och är en vital länk mellan en mängd olika IT-system, både internt i Malmö stad samt externt med myndigheter, banker och andra intressenter är det av högsta vikt att tillgängligheten är mycket god och att till exempel kontinuitetsplaner är upprättade.

Risk:

Det finns en risk att Malmö stad inte kan leverera önskvärd service till sina invånare och tillhandahålla korrekt information till sina anställda om en incident skulle slå ut TEIS-servern, då denna är en central knutpunkt i Malmö stads IT-miljö.

Rekommendation

Vi rekommenderar Malmö stad att inom ramen för sitt kontinuitetsarbete utvärdera hur kritisk TEIS integrationsmotor är för verksamheten och hur eventuella driftstopp av TEIS och servern som hanterar TEIS skulle påverka Malmö stad och dess invånare.

5. Avsaknad av support efter kontorstid

Iakttagelse

Som tidigare nämnts saknas ett SLA för TEIS. Vi har noterat att IT-service inte har dygnet runt support eller kontinuerlig övervakning för integrationer via integrationsmotorn TEIS. Vi har noterat att det finns schemalagda jobb som går dygnet runt vilket också innebär att övervakning bör finnas tillgänglig under samma period, förutsatt att de är kritiska avseende när i tid de utförs. För systemen som utnyttjar funktionaliteten i TEIS finns ofta SLA upprättade med en service nivå som innebär att IT-service åtar sig support under kontorstid.

Risk:

När det inte finns support dygnet runt gällande integrationer via TEIS ökar risken att incidenter som inträffar utanför arbetstid inte blir åtgärdade i tid, vilket kan skapa extra kostnader och längre driftstopp.

Rekommendation

Vi rekommenderar Malmö stad att utvärdera om integrationsmotorn TEIS ska vara under support dygnet runt. Vi rekommenderar även Malmö stad att säkerställa att förvaltningarna är införstådda i betydelsen av att integrationer körs under perioder då ingen support tillhandahålls och utvärdera betydelsen av detta.

Förändringshantering

1. Bristande förändringshantering av schemalagda jobb

Iakttagelse

Vi har noterat brister gällande spårbarhet av förändringar av de schemalagda integrationsjobben i TEIS. Det finns inte spårbarhet kring alla nya, förändrade och borttagna schemalagda jobb i TEIS vilket kan försvåra till exempel felsökning.

Risk:

Bristande förändringshantering av schemalagda jobb ökar risken att inte alla jobb går som avsett. Jobb kanske inte implementeras i tid, på rätt sätt och gamla jobb kan fortsätta köra trots att de inte längre ska vara aktiva. Detta kan bl.a. skapa felaktiga utbetalningar och skicka felaktig information mellan olika IT-system.

Rekommendation

Vi rekommenderar Malmö stad att utvärdera rutinen för tillägg, borttagning och förändring av schemalagda jobb och säkerställa att det finns en spårbarhet kring vilka jobb som ska köras. Användare behöver utbildning och mer information kring hur rutinen ska fungera och vilken information som är nödvändig vid tillägg, borttagning och förändring av integrationer.

Bilaga 1 Intervjuade personer

Namn	Titel/Roll	Datum
Harald Nilsson	Systemsamordnare	2-3/11 – 2009
Peter K Andersson	Chef IT-service	2/11 – 2009
Davor Peraic	Produktionschef IT-service	2/11 – 2009
Christer Christensson	IT-Driftchef	2/11 – 2009
Johan Almqvist	TEIS admin, IT-Drift	2/11 – 2009
Kaj Persson	Systemförvaltare Procapita	2/11 – 2009
Per Nilsson	Raindance	2/11 – 2009
Per-Olof Jansson	Prima	3/11 – 2009
Per-Evald Nilsson	Prima	3/11 – 2009