Öhrlings

PRICEWATERHOUSECOOPERS

Revisionsrapport*

Intern kontroll och säkerhet vid elektronisk handläggning av skannade leverantörsfakturor, intern fakturering samt elektronisk handel

Vänersborg kommun

2008-01-14

Rolf Aronsson

Vilma Lisboa

*connectedthinking

Öhrlings

PRICEWATERHOUSECOOPERS

Innehållsförteckning

1 Sammanfattning av synpunkter

I vår granskning av skanning och elektronisk handel har vi konstaterat att kontrollmiljön och genomförda kontrollaktiviteter till stora delar fungerar bra . Det finns en medvetenhet om behovet av intern kontroll bl.a. genom bildande av den s.k. internkontrollgruppen.

Vi har dock funnit några områden som vi anser bör förbättras och förtydligas för att ytterligare förbättra den interna kontrollen.

- Vi anser att det är positivt att kommunen har en kontinuerlig dialog med WM-data gällande de inskannade fakturorna för att kunna meddela leverantören om vad som blivit fel och återkoppla felaktiga händelser.

  Dock kan vi se att det är många objekt som hamnar på fellistan beroende på att leverantören inte är registrerad i systemet. Vi föreslår därför att man gör en jämförelse av leverantörsregistret mot befintliga ramavtal för att se följsamheten vid inköp.

- Vi rekommenderar att man förstärker nuvarande kontroller med mer styrda efterkontroller genom stickprovsmässig och delvis styrt urval av leverantörsfakturor. Dessa kan lämpligen genomföras av den internrevision som finns vid ekonomiavdelningen och ute i verksamheterna.

  Vad som skall efterkontrolleras och i vilken omfattning bör bestämmas utifrån genomförda riskanalyser och bör variera över tiden, d.v.s. en period kan man ha bestämt att vissa typer av utgiftsslag kontrolleras och nästa period några andra utgiftsslag. Man kan också välja att göra selektiva efterkontroller av vissa leverantörer eller specifika konton.

  Felaktigheter som upptäcks vid efterkontrollerna bör alltid åtgärdas via kontakt med den som har gjort felet alternativt rapporteras till överordnad chef beroende på vilken typ av fel som påträffats.

  Enligt vår uppfattning bör man också överväga att upprätta någon form av ”statistik” över felaktigheter som upptäcks vid efterkontrollerna för att mäta typ av felaktigheter och kvaliteten i genomförda kontroller och attester. Det finns anledning att i statistiken också dokumentera vilka typer av efterkontroller som har gjorts. Detta blir då en del av den uppföljning av internkontrollen som sker i kommunen.

- Genomförda kontrollaktiviteter via internkontrollsgruppen

  Ekonomerna i verksamheterna har sedan flera år tillsammans med internrevisorn i nämnderna och KS internrevisor samt redovisningschefen bildat en internkontrollgrupp, som bland annat har genomfört en kontrollaktivitet under en vecka i september 2007 genom att granska cirka 800 fakturor som skannas in under vald period.

  Verksamheternas genomförda kontrollaktiviteter skall redovisas till nämnderna och kommunstyrelsen under december 2007. Vi rekommenderar därför att revisionen begär att få ta del av de redovisningar som lämnas till nämnder och styrelse.

- I nuvarande dokumenthanteringsplan finns inget beskrivet om hur skannade leverantörsfakturor skall arkiveras. Enligt avtal med WM-data (Raindance) så sker korttidsarkivering hos WM-Data, därefter överförs enligt uppgift leverantörsfakturorna för långtidsarkivering till Depona AB i Malmö.

  Frågan om långtidsarkivering enligt nuvarande avtal Med WM-data är mycket oklar. Vi har därför bett att få ta del av skanningsföretagets avtal med underleverantören Depona som enligt uppgift som underleverantör till WM-Data är den som hanterar långtidsarkivering av leverantörsfakturor i Vänersborgs kommun.

  Vi har vid granskning i andra kommuner inte - trots upprepade försök - kunnat få fram något avtal som reglerar långtidsarkiveringen av kommunens leverantörsfakturor, vilket vi finner mycket märkligt. Vad vi kan finna är förhållandet det samma i Vänersborgs kommun.

  Enligt vår uppfattning är detta en viktig fråga eftersom ansvaret för egna leverantörsfakturor som utgör räkenskapsmaterial ligger på kommunen. Avtal och rutiner med externa leverantörer måste därför vara kristallklart kring på vilket sätt som leverantörsfakturor arkiveras bl.a. med utgångspunkt från arkivlagen och kommunens arkivreglemente och Lag om kommunal redovisning, sekretesslagen mm.

  Åtgärder för att få fram ett tydligt avtal kring långtidsarkiveringen bör omgående vidtas.

  Nuvarande dokumenthanteringsplan måste också kompletteras med om hur arkivering och förvaring samt gallring skall ske av elektronisk information i ekonomisystemet Raindance.

  Vi har inte gjort någon mer omfattande analys av vilka filer och databaser som kan vara aktuella, men konstaterar exempelvis att skannade fakturor inkommer i elektroniskt textformat och bildformat (Tiff) och lagras i Raindance ekonomisystem. Dessa elektroniska fakturor uppdateras sedan med olika kontrollmoment i form av

ankomstregistrering (filinläsning) och attester (mottagning/granskning, beslutsattest och betalning) som måste sparas som räkenskapsmaterial. Det finns också ett antal olika tabeller över attestanter, behörigheter, kontoplaner m.m. som också är viktig elektronisk information i ekonomisystemet. Denna information finns i databasen i Raindance.

I en dokumenthanteringsplan bör också finnas beskrivet hur länge och på vilket sätt som olika loggar i systemet skall sparas.

Precis som för skannande fakturor så måste dokumenthanteringsplanen kompletteras med hur arkivering och förvaring samt gallring skall ske i elektroniskt arkiv i e-handelsystemet Marakanda samt erhållna CD/DVD.

- Behörigheter i Raindance (skanning av leverantörsfakturor): I den här typen av system så måste säkerhetsnivån vara mycket hög. Vi rekommenderar att man ser över nuvarande konfiguration av kraven på lösenord. Bl.a. bör antalet sparade gamla lösenord sättas till 12 stycken, vilket innebär att ett gammalt lösenord först kan användas efter 24 månader. Antalet försök med felaktigt lösenord bör ändras från 5 försök till 3 försök, vilket i dag är en vedertagen standard. Dessutom bör valideringsprofilen förstärkas genom krav på att lösenord måste innehålla både siffror och bokstäver, exempelvis krav på minst två siffror.

  Antalet ändrade tecken bör höjas något exempelvis till två tecken. Visa senast felaktiga inloggning och/eller visa senaste inloggning bör aktiveras för att den behöriga användaren skall kunna se när inloggning har skett senast.

  Se för övrigt rekommendation för lösenordshantering i bilaga 1.

- Behörigheter i Marakanda (elektronisk handel): Säkerhetsnivån i nuvarande konfigurationen av identiteter och lösenord är i dag mycket låg. Det finns inga krav på antal tecken för lösenord eller krav på definitiv utspärrning efter försök med felaktigt lösenord. Inga krav finns på en blandning av numeriska och alfabetiska tecken. Etc.

  Precis som vi påtalat ovan vad gäller Raindance så måste i den här typen av system säkerhetsnivån vara mycket hög. Nuvarande konfiguration måste ses över. Se för övrigt rekommendationer i bilaga 1.

- Loggning i ekonomisystemet Raindance: Samtliga loggar är aktiverade vilket är mycket bra och gör att möjligheter till uppföljningar kan ske. Någon systematisk uppföljning sker dock inte. Enligt uppgift sker ibland vissa uppföljningar.

Loggning och uppföljning av olika händelser har stor betydelse för kontroll av säkerheten i olika avseende och är dessutom en grundförutsättning för att skapa god intern kontroll genom planenliga uppföljningar och kontroller. Det finns därför anledning att tydliggöra nuvarande regelverk genom att ta fram riktlinjer/föreskrifter för ”när, hur, var” loggning och uppföljning skall ske. Detta gäller både säkerhetshändelser i inloggningsserverar, mailservrar och brandväggar och i detta fallet behandlingshistorik i ekonomisystemet Raindance..

- Loggning i Marakanda (elektronisk handel): Alla händelser loggas i Marakanda och det finns ett flertal olika loggar på olika nivåer, bl.a. statuslogg per order/fakturor som skickas ut/vem som gör order etc. Det finns ytterligare loggar i systemet men dessa tas fram till kund/ på begäran, man måste således göra en beställning till Marakanda.

  I dagsläget utför man ingen kontroll av de loggar som finns. Samma slutsatser som framförs vad gäller uppföljning av loggar i Raindance ovan gäller även för loggar i e-handelsystemet Marakanda.

2 Bakgrund, revisionsfråga och genomförande

En mycket stor del av kommunens utbetalningar sker utifrån inkommande fakturor som underlag. Kommunen har i november 2006 infört rutiner för skanning av inkommande fakturor. Därmed skapas elektroniska dokument för handläggning och utbetalning av leverantörsfakturor. Det förekommer också elektronisk handel (Marakanda) i begränsad omfattning.

Syftet med granskningen är granska säkerheten i rutinen samt om den interna kontrollen är tillfredsställande.

Revisionsfråga: Är kontrollmiljö och kontrollaktiviteter i systemet tillräckliga för att garantera hög säkerhet vid elektronisk handläggning och utbetalning av leverantörsfakturor? Sker arkivering och finns back- up system som är betryggande och i enlighet med lag och rekommendationer.

Granskningen har genomförts med hjälp av intervjuer med nuvarande redovisningschef, fakturahandläggare vid fakturacentralen samt systemförvaltaren för ekonomisystemet och upphandlingschef (EH). Genomgång har även skett av befintlig dokumentation som vi tagit del av.

Kartläggning och analys samt rapportdisposition sker utifrån två områden, dels rutiner/dokumatation vid skanning av leverantörsfakturor och dels elektronisk handel och

elektroniska leverantörsfakturor. Dessutom görs en översiktlig kartläggning och analys av rutiner kring interna fakturor.

3 Kartläggning och analys av rutiner vid skanning av leverantörsfakturor

3.1 Förstudie elektronisk fakturahantering

Vi har tagit del av projektgruppens förstudiedokument ”Elektroniskt fakturahanteringssystem” från 2006-07-18. I den står att ett av de viktigaste motiven till att införa elektronisk fakturahantering var för att ledtiden för fakturahanteringsprocessen skulle reduceras samt att säkerheten av fakturor skulle ökas.

Något som kan vara intressant i samband med implementeringsfasen av skanning är att se dröjsmålsräntornas utveckling då de tenderar att öka i samband med införandet av skanning.

2006		2007
1e kvartal	2 419	51 933
2e kvartal	7 706	14 053
3e kvartal	7 805	8055
4e kvartal	28 003	

Det som kan konstateras är att kostnaderna för dröjsmålsräntorna har ökat markant, då de gått från 7 805 kronor (3e kvartal 2006) till 28 003 kronor (4e kvartal 2006) och sedan till att kulminera 51 933 kronor (1a kvartalet 2007). Trenden tycks dock vända åt rätt håll då dröjsmålsräntorna sjunker igen 2 kvartalet 2007.

I dialog med ansvariga så tror de att denna ökning beror på att:

- Verksamheterna tyckte det var ”krångligare” i början att attestera en faktura elektroniskt och att det på så sätt tog längre tid.
- Att verksamheterna har blivit bättre på att sätta rätt konto för dröjsmålsräntor i och med skanningen.
- Att det var mycket samlingsfakturor i början och att det försvårade attestflödet

I Vänersborgs kommun hanteras idag drygt 50 000 leverantörsfakturor per år och uppdelningen ser ut enligt följande:

Förvaltning	Attestanter[1]	Reg.ställen idag	Fakturor
Samhällsbyggnadsförvaltningen	14	8	15 000
Gymnasieförvaltningen	155	2	7 300
Barn- och Ungdomsförvaltningen	148	17	12 400
Kommunstyrelseförvaltningen	13	2	3 300
Socialförvaltningen	152	2	13 300
Totalt	482	31	51 300

3.2 Leverantörsfakturor - tillämpningsanvisning

Från och med den 1 november 2006 hanteras kommunens alla leverantörsfakturor elektroniskt. En extern faktura måste vara utställd till kommunen och innehålla beställar- ID och vid varje beställning ska beställar- ID anges som referens på fakturan. Om fakturan är korrekt skickas den vidare automatiskt för mottagnings- och beslutsattest. Angivet beställar- ID avgör vem i organisationen som får fakturan.

Fakturan ska innehålla leverantörens namn och adress, mottagarens namn och adress, PG/BG, fakturadatum, totalbelopp samt beställar- ID. Av fakturan ska de även framgå att F-skatt och org-nr finns. Av fakturan ska även framgå vad som inköpts eller så ska följesedel bifogas. I tillämpningsanvisningar står det att fakturor för representation, kurs, konferens och resor alltid ska kompletteras uppgift om syfte och deltagare och att man inte attesterar en faktura om man själv deltagit.

Bilagor som skannats in, t.ex. kvitton och följesedlar, där det inte framgår av fakturan vad som avses ska sparas med nummersatt försättsblad hos respektive fakturacentral där de läggs i en arkivkartong som vid årsskiftet skickas till ekonomikontoret.
Vidare står i anvisningarna att fakturan ska vara fullständigt konterad d.v.s. innehålla ansvar, konto samt verksamhetskod .

Fakturor utställda till annan exempelvis när ett personnamn står först i adressen, får inte betalas av kommunen. Är fakturan felaktig ska den skickas tillbaka med begäran om en ny.

[1] Mottagnings- samt beslutsattestanter

Felaktig faktura på grund av att beställar- ID saknas ska returneras till leverantören med information om kommunens användning av beställar- ID[2].

3.3 Avtal med leverantör

Man har tecknat ett särskilt avtal mellan Vänersborgs kommun och WM- data Sverige AB (avtalsperiod gäller tom 20101231 och kan förlängas med 2+2 år) för skanning av leverantörsfakturor. Avtalet ser ut enligt följande beskrivning och sker i WM- datas lokaler:

1. Leverantören skickar fakturor till WM - data
2. Posten registreras, sprättas och plockas upp hos WM- data.
3. Sortering görs utifrån kommunadress hos WM- data.
4. Kontroll görs att informationen på fakturan är tillräcklig, om inte, skickas den tillbaka till leverantören [3].
5. Hos WM-data sätts en streckkod på varje faktura som innehåller kundkod + löpnummer för att vara unik. Ett försättsblad sätts på varje bunt med information om sortering, skanningdatum, antal fakturor och kund och skannas därefter.
6. För att minimera fel kontrolleras den tolkade informationen mot ett leverantörsregister, t.ex. namn, adress, bank- postgironummer, organisationsnummer och moms.
7. Överföringsfil sker av tolkade data till Vänersborgs kommun.
8. Kortidslagring av skannade dokument
9. Hantering av fel/returer till leverantörer

Felstatistik
Vänersborgs kommun har kontinuerlig kontakt gällande felstatistik med WM-data och den kan sägas vara uppdelad i två;

1. **Statistik för oregistrerade fakturor**
   Här ingår allt som hamnar på fellistan och framförallt leverantörer som inte är inregistrerade i systemet.

2. **Statiskt över antal felsända till WM-data.**
   En gång i veckan får Vänersborgs kommun en återrapportering från WM-data över

[2] Detta görs fr.o.m 2007-09-01 av WM-data i Malmö

[3] Se ovan

antal återsändningar som gjorts. Dvs. hur många fakturor som saknar Beställar-ID och som returnerats till avsändaren.

Vi tycker att det i avtalet framgår klart och tydligt vad specifika tjänster kostar .

Vi anser att det är positivt att kommunen har en kontinuerlig dialog med WM-data gällande de inskannade fakturorna för att kunna meddela leverantören om vad som blivit fel och återkoppla felaktiga händelser.

Dock kan vi se att det är många objekt som hamnar på fellistan beroende på att leverantören inte är registrerad i systemet. Vi föreslår därför att man gör en jämförelse av leverantörsregistret mot befintliga avtal för att se följsamheten vid inköp.

3.4 Ankomstregistrering och meddelanderutiner

Fakturan ankomstregistreras i samband med inläsningen som sker en till två gånger per dag, är den felaktig vid inmatningen hamnar fakturan som oregistrerad i systemet. Meddelande till användare som får fakturor sker olika beroende på hur många fakturor som kommer samt vilken inställning man valt. Det finns olika möjligheter att välja beroende på hur ofta man vill ha ett mejlmeddelande.

Man kan vid behov från fakturacentralerna även skicka e-postmeddelande till berörd fakturamottagare om obetalda, sena eller ofullständiga fakturor för att påskynda betalningsprocessen.

3.5 Kontering och attest

När fakturan kommer till användare ska den först mottagningsattesteras och det finns möjlighet att göra ett konteringsförlag (som dock är ändringsbar till dess att fakturan är beslutsattestserad). Efter detta går fakturan vidare till beslutsattestanten som konterar den (om det inte tidigare blivit gjort). För att underlätta processen kan man lägga in personliga och generella konteringsmallar.

Enligt reglementet för kontroll (attester) av ekonomiska transaktioner står att attestmoment ej får utföras av den som själv ska betala till kommunen och där ta emot transaktionen eller själv ta emot en betalning från kommunen. Det är därför viktigt att man dirigerar om till annan person om så skulle vara fallet.

Egna kostnader i samband med tjänsten, t.ex. personlig utrustning, representation, kurser, konferenser och liknande ska alltid beslutsattesteras av ansvarig chef. För förvaltningschef

beslutsattesterar kommunchefen och för den politiska organisationen finns särskilt beslutade attestanvisningar.

3.6 Filöverföringar och betalning

När fakturan har gått igenom attestflödet är den redo för betalning, då granskas den preliminära journalen och efter granskning definitiv sätts den. Varje dag gör ekonomikontoret en betalningsbearbetning där två betalfiler skickas, en till postgiro och en till bankgiro där de ligger kvar till fakturans förfallodatum. Ekonomiavdelningen får dagligen en återrapporteringsfil över de betalningar som gjorts.

4 Översiktlig beskrivning och analys av elektronisk handel

Elektronisk handel används i dag i begränsad omfattning vid samhällsbyggnadsförvaltningen och kommunstyrelsen och omfattar i huvudsak livsmedel, kontorsmaterial och telefonräkningar.

Vi har tagit del av nuvarande avtal med leverantören Marakanda Marknadsplats AB som beskriver bl.a. initialt anslutna leverantörer , systemkrav, priser, betalningsvillkor, tvister m.m.

Vi har också översiktligt analyserat upphandlingsprocessen i form av upprättat förfrågningsunderlag, inkommit anbud och utvärdering av anbuden. Vad vi kan finna är förfrågningsunderlag och anbudsutvärdering väl underbyggt.

4.2 Översiktlig systembeskrivning av Marakanda

Tjänsten Marakanda Inköp för hantering av elektroniska beställningar och leverantörsfakturor är helt webbaserad, vilket innebär att det inte krävs någon installation av extra programvara. Inköpstjänstgen är en komplett e-handelslösning via Internet utan krav på investeringar i maskinpark eller mjukvara.

Systemet har stöd för avtalsbunden handel, direktköp och direktupphandling enligt handelsprocesserna:

- Normalförfarande med beställning till faktura (beställning/godkänn leverans/faktura).
- Direktköp

Normalförfarandet omfattar hantering av avtal, prislistor och behörigheter, beställning/avrop med kontering och attest, mottagning av orderbekräftelse, inleveranskontroll och

fakturagranskning, arkivering av fakturaverifikat och gränssnittsfil för överföring till Vänersbors ekonomisystem..

Direktinköp omfattar funktioner för att skicka fritextorder via fax eller e-post.

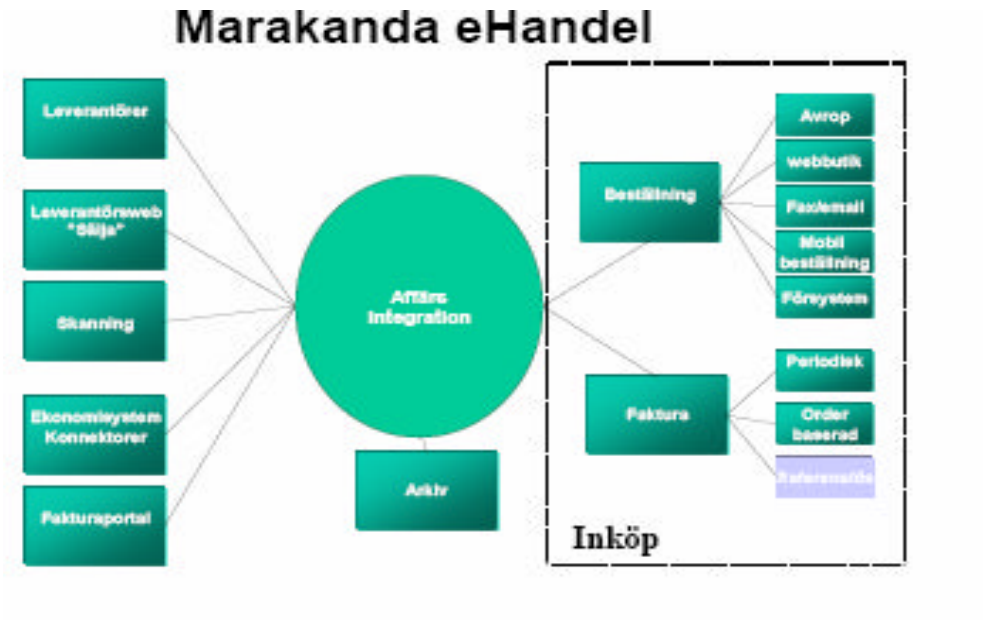
Informationen lagras i en för varje kund dedikerad databas i tjänsten.

Handelsmeddelanden som hanteras är följande:

Funktion	Internnamn/filer
Prislista	(PRICAT)
Order/avrop/beställning	(ORDERS)
Orderbekräftelse	(ORDRSP)
Orderändring	(ORDCHG)
Faktura	(INVOIC)

Tjänsten hanterar fullt automatiserad orderbaserad handel samt även handel via webbbutik. Dessutom kan man skicka order som fritextmeddelanden via e-post eller fax.

Marakanda ehandel kan grafiskt beskrivas enligt nedan:



Marakanda Affärsintegration

Detta är en komplett tjänst för affärsintegration, som möjliggör anslutning av alla typer av interna och externa parter.

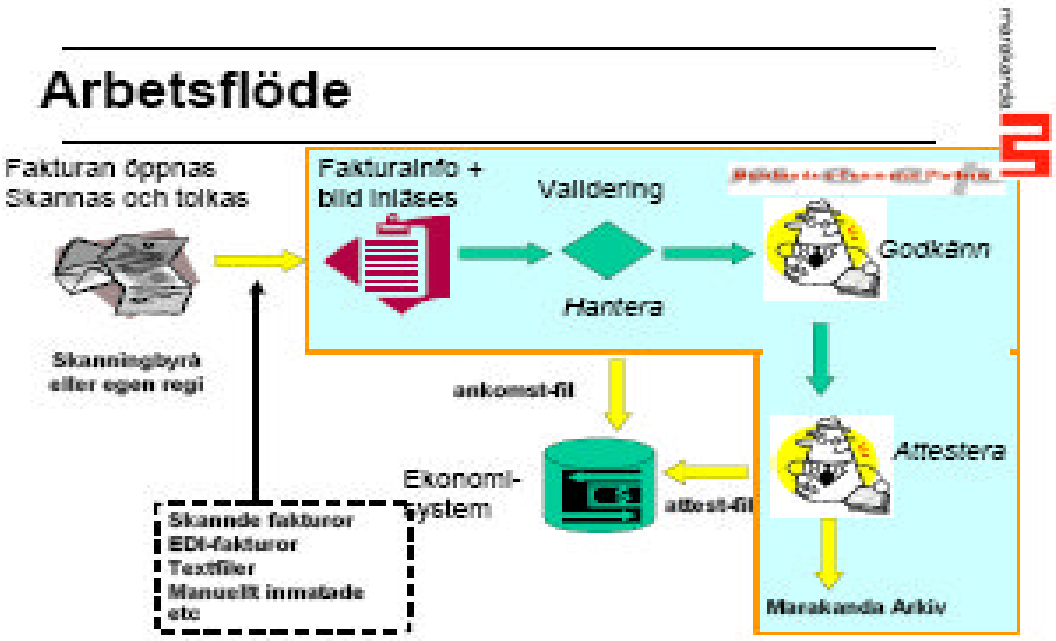
Vi gör ingen mer utvecklad beskrivning i denna rapport.

Elektronisk arkiv

Delsystem Arkiv är ett webbaserat elektroniskt arkiv som erbjuder komplett funktionalitet och är integrerat i Marakandas e-handelplattform. Detta innebär att meddelande flödet styrs i förekommande fall till arkivsystemet. Förutom själva meddelandet, dvs det elektroniska dokumentet, bifogas även attribut vid lagringen vilket gör att elektroniska dokument enkelt kan hämtas genom sökfunktioner via webbaserat gränssnitt. Arkivet säkerställer långtidslagring av EDI-dokument och det finns support för lagring på magnetiska och optiska media.

Översiktlig bild över fakturahanteringen

Nedan beskrivs översiktligt grafiskt arbetsflödet kring fakturahanteringen:



Vi gör ingen detaljerad beskrivning av flödet, men konstaterar följande kontrollaktiviteter::

- Fakturan valideras med avseende på innehåll. Här kontrolleras att mottagna uppgifter uppfyller minimimängden uppgifter och här sker även en matchning mot andra tillgängliga underlag som avtal och leverantörsuppgifter.

- I arbetsflödet hanteras i olika attest- och godkännandeflöde som överförs i form av attestfil till ekonomisystemet samt arkiveras elektroniskt tillsammans med fakturan i Marakanda Arkiv.

5 Översiktlig kartläggning och analys av rutiner kring interna fakturor

Vänersborgs kommun införde 1 september 2007 internfakturering i Raindanceportalen där systemansvarig är ansvarig för att utbilda berörda i det nya systemet.

Bakgrunden till den nya förändringen är att man vill få en resultatpåverkan så snabbt som möjligt. Genom direkt definitivsättning på säljsidan registreras intäkten hos säljaren. På mottagarsidan bokas en preliminärkostnad upp på ankomstbokningen. Vid slutkontering och attest av fakturan registreras kostnaden in på ”rätt” konto.

Interna fakturor går att söka fram i Portalen på samma sätt som de externa fakturorna. Användarna läggs upp i Raindance RAN med namn och e-mailadress med följande behörighetsnivåer:

1. Titta på fakturor
2. Kontera, attestera, och titta på fakturor (vanliga användare)
3. Registrera och kontera säljfaktura
4. Registrera samt ändra i kundregistret
5. Tillgång till attestregister
6. Allt annat (systemförvaltare)

Enligt uppgift av ekonomikontoret så fungerar rutinerna för interna fakturor bra. För övrigt gäller samma synpunkter kring intern kontroll som framförs i rapporten vid skanning och e-handel.

6 Generellt kring kontrollmiljö och kontrollaktiviteter

6.1 Reglemente för intern kontroll

Antaget av Kommunfullmäktige 2000-03-14. I detta reglemente fastställs ansvaret för den interna kontrollen samt på vilket sätt uppföljning av den interna kontrollen ska ske. Vidare står i reglementet att kontrollen har som mål att:

- Säkra att pengar och andra resurser används i överensstämmelse med tagna beslut
- Säkra en effektiv organisation och förvaltning
- Säkerställa en riktig och fullständig redovisning
- Skydda mot förluster till följd av fel eller oegentligheter
- Skydda politiker och anställda mot oberättigade

Detta reglemente avser inte att reglera vad som ska kontrolleras, vidare reglerar den inte heller hur uppföljning av kvalitet och kvantitet mot fastställda mål ska ske. Kommunstyrelsen (KS) har det övergripande ansvaret att tillse att det finns en god intern kontroll inom kommunens nämnder och förvaltningar. KS ansvarar för att kommungemensamma reglementen, regler och anvisningar upprättas samt att en organisation kring intern kontroll upprättas inom kommunen.

Det är dock nämnderna som har det yttersta ansvaret för den interna kontrollen inom respektive verksamhetsområde. Inom en nämnds verksamhetsområde ansvarar förvaltningschefen eller motsvarande för att förvaltningsspecifika konkreta regler och anvisningar utformas för att upprätthålla en god intern kontroll.

Nämnden ska därmed:

- Tillse att kommunövergripande reglementen, regler och anvisningar följs inom respektive verksamhetsområde
- Upprätta regler och anvisningar som kan behövas för de nämndspecifika verksamheterna
- Upprätta en organisation för den interna kontrollen

De verksamhetsansvariga cheferna på olika nivåer är skyldiga att följa antagna reglementen, regler och anvisningar om intern kontroll samt informera övriga anställda om innebörden i dessa. Vidare har cheferna att verka för att de arbetsmetoder som används bidrar till en god intern kontroll.

Nämnderna ska varje år godkänna en särskild plan för granskning och uppföljning av den interna kontrollen. KS ska utvärdera kommunens samlade system för intern kontroll utifrån nämndernas rapporter om uppföljning av internkontrollen och i de fall förbättringar behövs besluta om sådana.

6.2 Efterkontroll

I reglementet för intern kontroll står att det är nämnderna som har det yttersta ansvaret för den interna kontrollen inom respektive verksamhetsområde[4].

I våra intervjuer har vi preliminärt noterat följande kontrollaktiviteter:

1) Före betalning av skannade och attesterade leverantörsfakturor så gör kassahandläggare en genomgång och rimlighetskontroll av både den preliminära och den definitiva fakturajournalen. Därefter sker betalning.

2) I efterhand gör den centrala internrevisorn en kontroll av fakturajournalerna. Inriktningen och omfattningen styrs – vad vi kan finna – i stor utsträckning av internrevisors erfarenhet av områden som behöver granskas närmare.

Vi rekommenderar att man förstärker nuvarande kontroller med mer styrda efterkontroller genom stickprovsmässig och delvis styrt urval av leverantörsfakturor. Dessa kan lämpligen genomföras av den internrevision som finns vid ekonomiavdelningen och ute i verksamheterna.

Vad som ska efterkontrolleras och i vilken omfattning bör bestämmas utifrån genomförda riskanalyser och bör variera över tiden d.v.s. en period kan man ha bestämt att vissa typer av utgiftsslag kontrolleras och nästa period några andra utgiftsslag. Man kan även välja att göra selektiva efterkontroller av vissa leverantörer eller specifika konton.

En utgångspunkt kan också vara resultatet av de kontrollaktiviteter som gjorts under en vecka i september 2007. Se skrivningar nedan.

Vissa stickprovsmässiga kontroller bör alltid finnas och som exempel kan följande nämnas:

- Fakturabelopp
- Momsbelopp
- Pg/Bg/bankkontonummer
- Förfallodatum enligt kommunens regelverk
- F-skattesedel

Felaktigheter som upptäcks vid efterkontrollerna bör alltid åtgärdas via kontakt med den som har gjort felet alternativt rapporteras till överordnad chef beroende på vilken typ av fel som påträffats.

[4] I enlighet med kommunallagen 6 kap 7§.

Enligt vår uppfattning bör man också överväga att upprätta någon form av ”statistik” över felaktigheter som upptäcks vid efterkontrollerna för att mäta typ av felaktigheter och kvaliteten i genomförda kontroller och attester. Det finns anledning att i statistiken också dokumentera vilka typer av efterkontroller som har gjorts. Detta blir då en del av den uppföljning av internkontrollen som sker i kommunen.

Genomförda kontrollaktiviteter via internkontrollsgruppen

Ekonomerna i verksamheterna har tillsammans med internrevisorn i nämnderna ch KS internrevisor samt redovisningschefen bildat en intern- kontrollgrupp. De har bland annat haft till uppgift att granska de fakturor som skannats inunder en vald vecka i september 2007, vilket innebär att totalt har ca 800 fakturor stickprovsmässigt granskats.

Gruppen har utgått ifrån en särskild mall som beskriver 23 punkter som sedan har granskats.

Verksamheternas genomförda kontrollaktiviteter skall redovisas till nämnderna och kommunstyrelsen under december 2007. Vi rekommenderar därför att revisionen begär att få ta del av de redovisningar som lämnas till nämnder och styrelse.

6.3 Attest- och utanordningsreglemente

Vänersborgs kommun har ett särskilt reglemente[5] för kommunens ekonomiska transaktioner där KS utfärdar anvisningar till detta reglemente. I denna framgår följande;
Att alla ekonomiska transaktioner, både inbetalningar och utbetalningar ska attesteras. Attest kan ses som ett sammanfattande begrepp för ett antal olika kontrollåtgärder. Attest sker med ett skriftligt intygande eller elektronisk signatur av att kontrollen är utförd.

I attestanordningen ingår följande huvudmoment

1. Mottagningsattest- kontroll mot leverens/prestation
2. Granskningsattest- kontroll mot uträkning, pris och villkor
3. Beslutsattest- kontroll mot underlag/beställning/beslut
4. Behörighetsattest- kontroll av beslutsattestanter vid fakturaregistrering

1. **Mottagningsattest** är en kontroll av erhållen leverens/fullgjord tjänst mot beställning och faktura det vill säga, att leveransen hat mottagits alternativt presentationen fullgjorts. Mottagningsattest innebär att den som tar emot varan är skyldig att se till att:

[5] Reglemente för kontroll (attester) av ekonomiska transaktioner för Vänersborgs kommun, antagen av kommunfullmäktige 1993-05-25.

- varan har mottagits och att varorna stämmer med uppgifterna på följesedel eller liknande
- kvantitet och antal stämmer
- godset/varan är felfri, reklamation, restnoteringar och dyl. framförs till leverantör

(Vid elektronisk handel samt elektronisk fakturahantering, sker mottagningsattesten med en elektronisk signatur).

2. **Granskningsattest** innebär en kontroll av att pris, rabatter, betalningstider är rätt samt eventuella fakturerings- och expeditionsavgifter samt fraktkostnader följer ramavtal och upphandling. Granskningsattest tecknas med förnamn, efternamn eller signatur i avsedd ruta på konteringsblanketten (någon särskild granskningsattest förekommer ej vid elektronisk handel då granskning sker mot gällande tabeller och vid elektronisk fakturahantering övergår detta attestmoment till beslutsattestanten).

3. **Beslutsattest** är en kontroll av erhållen faktura mot beslut, plan eller direktiv för verksamheten som innebär att:

- beställning har skett hos leverantör av behörig person
- kontering är korrekt
- kontroll av priser, rabatter, betalningstider samt eventuella fakturerings- och expeditionsavgifter eller fraktkostnader följer ramavtal och upphandling
- infria en ekonomisk förpliktelse genom att frakturan blir klar för utbetalning

Vid elektronisk handel sker beslutsattesten med en elektronisk signatur. Vid hantering av elektroniska fakturor kan beslutsattest ske före mottagningsattest. Beslutsattesten sker då vid ordertillfället och avstämning sker vid inleverans.

Fakturor inom elektronisk handel ska vara försedda med både mottagningsattest och beslutsattest. Mottagningsattest och beslutsattest av fakturor inom elektronisk handel får inte utföras av samma person. Vid periodisk och orderlös fakturering inom ramen för elektronisk handel kan hela attestförfarandet ske genom en automatisk avstämning av fakturan mot den kontraktsinformation som finns registrerad i e-handelssystemet.[6]

Vid elektronisk fakturahantering sker beslutsattesten med en elektronisk signatur.
Fakturor inom elektronisk fakturahantering ska vara försedda med både mottagningsattest och beslutsattest och får inte utföras av samma person.

Behörighetsattest- intygar med sin signatur att den som beslutsattesterat är behörig. Vid elektronisk handel sker behörighetskontrollen mot den behörighetstabell som finns upplagd i

[6] Mer om e-handel kommer i del 2 av rapporten

systemet och vid elektronisk fakturahantering sker behörighetskontrollen mot den behörighetstabell som finns upplagd i systemet.

I reglementet för kontroll[7] (attester) kan man vidare läsa att *”Varje nämnd beslutar vilka befattningar och/eller funktioner som har rätt att attestera eller vara ersättare för dessa”*. Beslutsattestanter och behörighetsattestanter kan utses för viss tid eller tills vidare och en instruktion ska medfölja attestuppdraget där det framgår vilka uppgifter och skyldigheter som följer med uppdraget. Beslutsattestanter, behörighetsattestanter och mottagningsattestanter inom elektronisk handel ska underteckna ett attestuppdrag och för elektronisk fakturahantering ska beslutsattestanter och mottagningsattestanter underteckna ett attestuppdrag. Attestuppdragen ligger till grund för behörigheter inom system för elektronisk fakturahantering samt elektronisk handel.

Aktuella attestuppdrag över utsedda attestanter och ersättare för dessa med namnteckningsprov ska finnas hos respektive förvaltning. Vid det tillfälle attestuppdrag upphör ska uppdraget återkallas. Återkallande attestuppdrag ska förvaras under en tid av 10 år på respektive förvaltning eller i kommunens arkiv.

6.4 Arkivplan (arkivreglemente) och dokumenthanteringsplan

Förutom de i arkivlagen och i arkivförordningen antagna bestämmelser om arkivvård finns i Vänersborgs kommun ett ”Reglemente för kommunarkivet” antaget av kommunfullmäktige. Detta är reviderat 1996-03-26. Detta gäller för kommunfullmäktige och kommunens myndigheter. Med myndigheter avses kommunstyrelsen och övriga nämnder, kommunfullmäktiges revisorer samt andra kommunala organ med självständig ställning.

Av arkivreglementet framgår att varje myndighet ska redovisa sitt arkiv dels genom information om vilka slag av handlingar som kan finnas och hur arkivet är organiserat (arkivbeskrivning), dels i en systematisk förteckning över de handlingar som förvaras i myndighetens arkiv (arkivförteckning). Varje myndighet ska upprätta en dokumenthanteringsplan som beskriver myndighetens handlingar, hur dessa hanteras och regler för bevarande och gallring.

En viktig fråga – inte minst eftersom skanning av inkommande fakturor sker utanför kommunen – är formuleringar i arkivplan och dokumenthanteringsplan.

Med utgångspunkt från denna granskning har vi tagit del av kommunstyrelsens dokumenthanteringsplan med avseende på ekonomikontoret. Av denna framgår att

[7] Reglemente för kontroll (attester) av ekonomiska transaktioner för Vänersborgs kommun, antagen av kommunfullmäktige 1993-05-25.

verifikationer till bokföringen (inklusive leverantörsfakturor) skall arkiveras i pappersform i 10 år. Först sker förvaring i högst 3 år i närarkivet, därefter sker överföring till kommunarkivet. Eventuellt IT-material skall skrivas ut på arkivbeständigt papper.

Nuvarande dokumenthanteringsplan är inte fullt ut tillämpbart i nuvarande hantering av leverantörsfakturor (skanning och elektronisk handel) och beskriver inget om arkivering av elektronisk information. Se för övrigt kommentarer under nedanstående rubriker.

6.4.1 Arkivering av inkommande pappersfakturor som skannas

I nuvarande dokumenthanteringsplan finns inget beskrivet om hur skannade leverantörsfakturor skall arkiveras. Enligt avtal med WM-data (Raindance) så sker korttidsarkivering hos WM-Data, därefter överförs enligt uppgift leverantörsfakturorna för långtidsarkivering till Depona AB i Malmö.

Frågan om långtidsarkivering enligt nuvarande avtal Med WM-data är mycket oklar. Vi har därför bett att få ta del av skanningsföretagets avtal med underleverantören Depona som enligt uppgift som underleverantör till WM-Data är den som hanterar långtidsarkivering av leverantörsfakturor i Vänersborgs kommun.

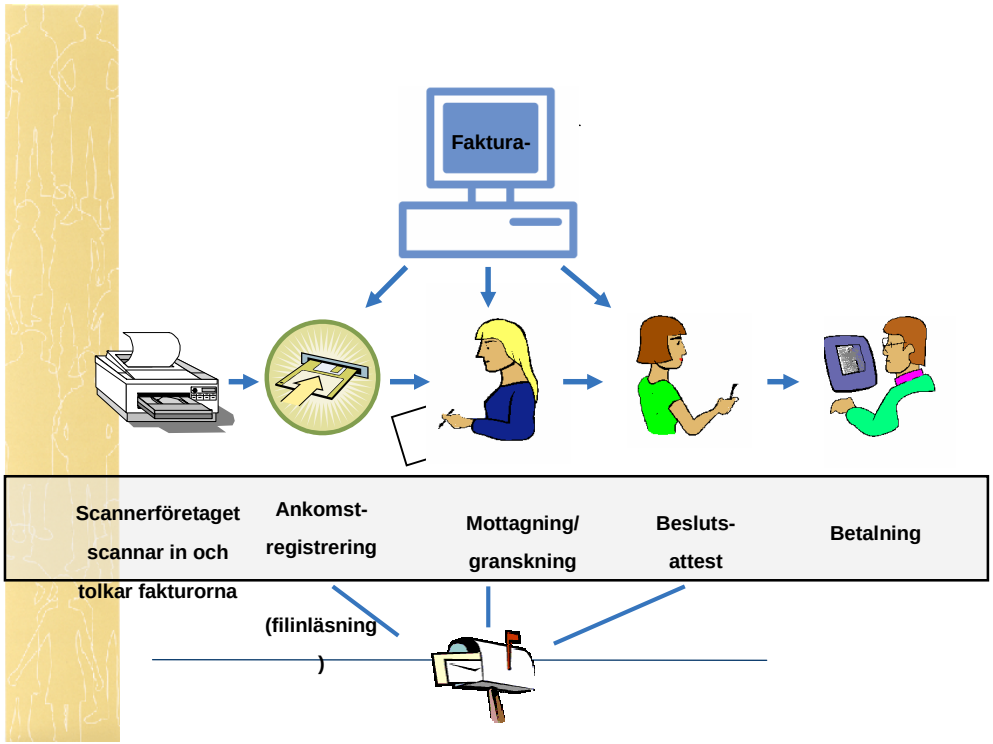
Vi har vid granskning i andra kommuner inte - trots upprepade försök - kunnat få fram något avtal som reglerar långtidsarkiveringen av kommunens leverantörsfakturor, vilket vi finner mycket märkligt. Vad vi kan finna är förhållandet det samma i Vänersborgs kommun.

Enligt vår uppfattning är detta en viktig fråga eftersom ansvaret för egna leverantörsfakturor som utgör räkenskapsmaterial ligger på kommunen. Avtal och rutiner med externa leverantörer måste därför vara kristallklart kring på vilket sätt som leverantörsfakturor arkiveras bl.a. med utgångspunkt från arkivlagen och kommunens arkivreglemente och Lag om kommunal redovisning. (se skrivning ovan).
Åtgärder för att få fram ett tydligt avtal kring långtidsarkiveringen bör omgående vidtas.

6.4.2 Arkivering av elektronisk information som skapas i Raindance vid hantering av skannade fakturor

I nuvarande dokumenthanteringsplan finns ingen beskrivning om hur arkivering och förvarande samt gallring skall ske av elektronisk information i ekonomisystemet Raindance.

Nedanstående bild beskriver översiktligt hur uppdatering sker av olika kontrollmoment som lagras elektroniskt:



Vi har inte gjort någon mer omfattande analys av vilka filer och databaser som kan vara aktuella, men konstaterar exempelvis att skannade fakturor inkommer i elektroniskt textformat och bildformat (Tiff) och lagras i Raindance ekonomisystem. Dessa elektroniska fakturor uppdateras sedan med olika kontrollmoment i form av ankomstregistrering (filinläsning) och attester (mottagning/granskning, beslutsattest och betalning) som måste sparas som räkenskapsmaterial. Det finns också ett antal olika tabeller över attestanter, behörigheter, kontoplaner m.m. som också är viktig elektronisk information i ekonomisystemet. Denna information finns i databasen i Raindance.

I en dokumenthanteringsplan bör också finnas beskrivet hur länge och på vilket sätt som olika loggar i systemet skall sparas. Se nedanstående avsnitt kring behörigheter och loggar.

Kommentarer:
Nuvarande dokumenthanteringsplan måste kompletteras med om hur arkivering och förvaring samt gallring skall ske av elektronisk information i ekonomisystemet Raindance.

6.4.3 Arkivering av elektroniska fakturor och annan skapad elektronisk information

Vad vi kan finna i dialog med ansvariga så arkiveras elektroniska fakturor i ehandel-systemet Marakanda innevarande år samt ytterligare 10 år. Dessutom erhåller kommunen en CD/DVD med arkiverade fakturor från Marakanda.

Precis som för skannade fakturor så måste dokumenthanteringsplanen kompletteras med hur arkivering och förvaring samt gallring skall ske i elektroniskt arkiv samt erhållna CD/DVD.

6.5 Offentlighet och sekretess

I avtalen med skanningsföretaget WM-data finns samt Markanda (E-handel) – vad vi kan finna – inga tydliga skrivningar om sekretess eller hantering av känsliga personuppgifter.

Vi har inte gjort någon mer detaljerade bedömning, men konstaterar att det bör finnas skrivningar kring vad som gäller för eventuell sekretess av fakturor. Nuvarande avtal bör kompletteras med mer tydliga skrivningar om hur sekretessbelagda uppgifter skall hangteras.

7. Behörigheter och loggning

7.1 Behörigheter i Raindance (skanning av leverantörsfakturor)

Behörighetsregistret i Raindance är integrerat med ett användarregister (Meta-katalog). Meta-katalogen läggs upp och hanteras av IT-avdelningen. En särskild blankett används och skall skrivas under både av närmaste chef och av användaren. Användaren undertecknar dessutom en sekretessförbindelse i samband med att denne ansöker om en användaridentitet. Blanketten lämnas först till IT-avdelningen som lägger upp ett användarkonto. Systemförvaltarna ansvarar sedan för att ange behörigheterna på applikationsnivå (Raindance och Marakanda).

Vi har tagit del av nuvarande konfiguration av användaridentitet och lösenordshantering. Vi har noterat att utspärrning sker efter 5 försök med felaktigt lösenord och att lösenorden måste bytas efter 60 dagar annars sker utspärrning efter 70 dagar. Minsta antal tecken måste vara 6 tecken. Antal ändrade tecken vid byte av lösenord är 1 tecken och antalet sparade lösenord är satt till ett, vilket innebär att ett gammalt lösenord kan återanvändas efter (60+60) 120 dagar.

Visa senast felaktiga lösenord är inte aktiverat. Användare får undantas från lösennordsbyte är aktiverat och gäller för kommunens revisorer. Vi föreslår att inget undantag från lösenordsbyte ska finnas för revisorerna då detta skapar möjligheter att i framtiden även undanta andra grupper/användare.

I den här typen av system så måste säkerhetsnivån vara mycket hög. Vi rekommenderar att man ser över nuvarande konfiguration av kraven på lösenord. Bl.a. bör antalet sparade gamla lösenord sättas till 12 stycken, vilket innebär att ett gammalt lösenord först kan användas efter 24 månader. Antalet försök med felaktigt lösenord bör ändras från 5 försök till 3 försök, vilket i dag är en vedertagen standard. Dessutom bör valideringsprofilen förstärkas genom krav på att lösenord måste innehålla både siffror och bokstäver, exempelvis krav på minst två siffror.

Antalet ändrade tecken bör höjas något exempelvis till två tecken. Visa senast felaktiga inloggning och/eller visa senaste inloggning bör aktiveras för att den behöriga användaren skall kunna se när inloggning har skett senast.

Se för övrigt rekommendation för lösenordshantering i bilaga 1.

7.2 Behörigheter i Marakanda (elektronisk handel)

Behörigheter läggs upp av en sk. ”företagsadministratör” på förvaltningen. Det är vanligen ekonomen i förvaltningen som administrerar behörigheter. Vid upplägg av en ny behörighet ska följande uppgifter fyllas i:

- Användar-id (skall vara 1-30 tecken långt)
- Lösenord
- Beställarkod, är fyra bokstäver (A-Z) och används för att identifiera avsända order
- Attestbelopp fylls i om personen i fråga ska vara orderattestant, dvs. ha rättighet att godkänna och skicka iväg en order till leverantör. (så länge ordervärdet inte överstiger användarens attestbelopp kommer denna förvalda orderattestant inte att vara inblandad i orderprocessen.)

Säkerhetsnivån i nuvarande konfigurationen av identiteter och lösenord är i dag mycket låg. Det finns inga krav på avtal tecken för lösenord eller krav på definitiv utspärrning efter försök med felaktigt lösenord. Inga krav finns på en blandning av numeriska och alfabetiska tecken. Etc.

Precis som vi påtalat ovan vad gäller Raindance så måste i den här typen av system säkerhetsnivån vara mycket hög. Nuvarande konfiguration måste ses över. Se för övrigt rekommendationer i bilaga 1.

7.3 Loggning i ekonomisystemet Raindance

Loggning sker i portalen samt i systemet Raindance. I den sistnämnda loggas även ändringar av pg/bg, leverantörer och ändringar i användarregister etc. Så fort det har skett en ändring loggas det i systemet.

Samtliga möjliga loggar i Raindance är vad vi kan finna aktiva, vilket är mycket bra och innebär stora möjligheter till kontroller både kontinuerligt (beslutade interna kontroller) och vid olika händelser som kräver närmare analyser.

Som exempel på viktiga loggar i ekonomisystemet och skanning (Raindance) som är aktiverade i systemet och som systematiskt bör användas vid uppföljningar kan nämnas:

- RK LV Nyregistrering och ändring av uppgifter om leverantörer, inklusive postgiro och bankgiro

- RAN – Funktionen loggar registrering av uppgifter för enskild användare, bl.a. behörigheter och rättigheter, tillgång till företag m.m.

- FLOGON – Loggar olika felaktigheter vid användning av identiteter och lösenord samt försök till åtkomst utan rättigheter.

Samtliga loggar är aktiverade vilket är mycket bra och gör att möjligheter till uppföljningar kan ske. Någon systematisk uppföljning sker dock inte. Enligt uppgift sker ibland vissa uppföljningar.

Loggning och uppföljning av olika händelser har stor betydelse för kontroll av säkerheten i olika avseende och är dessutom en grundförutsättning för att skapa god intern kontroll genom planenliga uppföljningar och kontroller. Det finns därför anledning att tydliggöra nuvarande regelverk genom att ta fram riktlinjer/föreskrifter för ”när, hur, var” loggning och uppföljning skall ske. Detta gäller både säkerhetshändelser i inloggningsserverar, mailservrar och brandväggar och i detta fallet behandlingshistorik i ekonomisystemet Raindance..

Som exempel på frågor kan noteras:

1) Hur länge[8] och på vilket media[9] skall loggfiler (behandlingshistorik) sparas?

2) Vad skall loggas och vilka kontrollmål gäller, d.v.s. av vilken anledning sparas uppgifterna?

3) Organisation för uppföljning och kontroll?

[8] Om inte lagstiftningen ställer högre krav bör loggade uppgifter sparas i två år.

[9] Vid lagring av loggar på exempelvis tapekassetter/CD/DVD är det viktigt att också förvara dessa med utgångspunkt från den sekretess som gäller.

4) Vilka krav på selektiv loggning (terminal, användare, register m.m.) skall finnas?

5) Vilka krav skall finnas på program för rapportuttag?

7.4 Loggning i Marakanda (elektronisk handel)

Alla händelser loggas i Marakanda och det finns ett flertal olika loggar på olika nivåer, bl.a. statuslogg per order/fakturor som skickas ut/vem som gör order etc. Det finns ytterligare loggar i systemet men dessa tas fram till kund/ på begäran, man måste således göra en beställning till Marakanda.

I dagsläget utför man ingen kontroll av de loggar som finns. Samma slutsatser som framförs vad gäller uppföljning av loggar i Raindance ovan gäller givetvis även för loggar i Marakanda.

Bilaga 1 Generella krav på användaridentiteter och lösenord

Användaridentitet och lösenord

Användaridentitet skall alltid vara **individuell** och kunna identifieras av systemet. Lösenord är alltid kopplade till unika användaridentiteter och kontrolleras i två faser.

Åtkomstregler (rättigheter) och bestämda behörighetsprofiler styr vilka möjligheter en användare har till åtkomst av olika resurser. **Åtkomstreglerna** bör alltid vara uppbyggda **utifrån behov** av att känna till samt vilka uppgifter som skall utföras. Det finns ett antal grundläggande typer av åtkomstmöjligheter:

Loggning (registrering) av åtkomster

Åtkomst till datorsystem och störningar skall loggas automatiskt och kunna rapporteras.

Frekvensen för uttag och granskning av rapporter av säkerhetsansvarig är beroende av hur känslig den skyddade informationen är.

Vid uppföljning skall den säkerhetsansvarige särskilt uppmärksamma:

1) Mönster och återkommande missförhållande som är kopplade till användare med höga åtkomstmöjligheter och tillgång till känslig information.

2) Störningar i form av upprepade försök till åtkomst av vissa datafiler eller applikationer av ej behöriga användare eller genom användande av felaktiga lösenord.

Grundläggande restriktioner för lösenord

1) Lösenord skall vara lätta att komma i håg, men svåra att gissa för obehörig. Egna regler för att ur "ramsor" ta ut vissa kombinationer av bokstäver är ett sätt att enkelt komma ihåg ett lösenord.

   Ex 1: *Hur komma ihåg detta lösenord = rmhee. Vid krav på viss kombination av bokstäver och siffror kan lösenordet bli: rm2he4e.*

   Ex 2: Använd alltid kombinationer av gemena och versala bokstäver och siffror. = R2fKj5.

2) Nya lösenord skall utlämnas mycket diskret med ovillkorligt krav att när användaren loggar på för första gången skall systemet tvinga användaren att lägga in ett eget hemligt lösenord.

3) Efter 3 försök med felaktigt lösenord spärras identiteten definitivt.

4) Frisläppande av spärrad identitet måste ske med iakttagande av hög säkerhet och i övrigt efter samma regler som vid nya lösenord.

5) Lösenord skall vara envägskrypterade och inte kunna förstås eller användas av någon annan person.

6) Lösenord får inte visas i någon form (bildskärm, rapporter eller nedskrivna på papper)

7) Lösenord skall ändras - krav från systemet - efter viss period, exempelvis 90 eller 180 dagar. Val av period är beroende av IT-miljö och känsligheten i hanterad information m.m., som bedöms i en riskanalys.

8) Regler för format på lösenord:

   a) Minst 6 – 8 tecken långt. Om lösenord kombineras med identifiering genom användande av kort i särskild läsare kan det räcka med färre tecken.

   b) Alltid en kombination av alfabetiska och numeriska tecken.

   c) Lösenord ska inte kunna identifieras med viss person, exempelvis genom att härleda till identitet eller namn.

   d) När lösenord ändras skall systemet inte godkänna att samma lösenord används igen under en viss period (exempelvis 6 generationer). Det bör också finnas krav på att ett lösenord har en tydlig förändring.

   Vid höga krav på säkerhet skall också finnas möjlighet att lägga in en spärrlista som hindrar användning av s k vanliga ord (ex.vis förnamn, månadsnamn, bilmärke, produktnamn etc).

9) Användaridentitet som inte har använts under en förutbestämd period (exempelvis 60 dagar) skall automatiskt spärras.

10) Uppkopplad användare skall automatiskt kopplas ner om inte systemet har använts under viss tid (exempelvis under 30 minuter). Efter hur lång tid är beroende av vilken applikation som används och i vilken miljö som användaren verkar samt hur känsliga uppgifterna är. Det är därför viktigt att det finns möjlighet att använda denna funktion individuellt för olika användare.