



Stenungsunds kommun

**Kartläggning av processen för
utbetalning av leverantörsfakturor**

KPMG AB
8 december 2008
Antal sidor: 10

**Rapport - Stenungsunds kommun - Utbetalning av
leverantörsfakturor.doc**

Innehåll

1.	Sammanfattning	1
2.	Uppdraget	1
2.1	Bakgrund och granskningsmål	1
2.2	Syfte	1
2.3	Genomförande	2
2.4	Övergripande frågeställningar	2
3.	Kartläggning av processen	3
3.1	Processbeskrivning	3
3.2	Scannit	3
3.3	Gasell	4
3.4	Överföring av information till Aditro via DameWare	5
3.5	Aditro	6
3.6	Manuella fakturor	7

1. Sammanfattning

De större iakttagelser vi har observerat under vår granskning beskrivs kortfattat nedan. Risker och rekommendationer kopplat till dessa iakttagelser beskrivs i samband med respektive avsnitt i rapporten.

- Funktionalitet i Gasell för belopps-, samt tidsbegränsning vid attest används inte
- Det saknas en formell och dokumenterad rutin för hantering, samt periodisk genomgång, av användare med administratörsbehörigheter i Gasell
- Rutinen för utbetalning av leverantörsfakturer och manuella fakturer i Aditro hanteras av en och samma person
- Det krävs endast en person för att initiera betalning av leverantörsfakturer och manuella fakturer till bank- och plusgiro
- Flertalet personer på ekonomiavdelningen har tilldelats en användarroll med den högsta behörigheten i Aditro

2. Uppdraget

KPMG har på uppdrag av kommunrevisionen i Stenungsund genomfört en granskning av processen för utbetalningar av leverantörsfakturer inom kommunen. Granskningen har utförts under oktober och november månad 2008.

2.1 Bakgrund och granskningsmål

Stenungsunds kommun har infört ett system för att skanna leverantörsfakturer, vilket har inneburit förändringar i processen för hantering av kommunens fakturer och avstämning av leverantörsreskontra.

Som ett led i granskningen har vi kartlagt processen för utbetalningar av kommunens leverantörsfakturer. Granskningen fokuserar på i vilken utsträckning riskerna för brister i processen har begränsats, dels genom ändamålsenliga systembaserade kontroller och dels genom fungerande manuella kontroller och avstämningar.

2.2 Syfte

Syftet med granskningen är att resultatet ska vara en del av kommunrevisionens underlag för sina bedömningar och uttalanden.

2.3 Genomförande

Metoden som valts för uppdraget är genomläsning av dokumentation för, och genomgång av, systemapplikationer som ingår i processen för leverantörsfakturor, samt intervjuer med personal vid ekonomi- och IT-avdelningen. Vi har också genom att ta stickprov på fakturor i olika steg i processen verifierat att väsentliga kontrollmål enligt rutinbeskrivningar tillämpas.

I denna rapport sammanfattas våra väsentligaste iakttagelser från granskningen. Rapporten skrivs i avvikelseform, vilket innebär att i huvudsak förhållanden som vi anser bör uppmärksammas eller bli föremål för åtgärder redovisas.

2.4 Övergripande frågeställningar

- Vilka kontroller finns det i processen för betalning av leverantörsfakturor?
- Hur hanteras behörigheter i systemen?
- I vilken utsträckning beaktas risken för kritiska kombinationer av systembehörighet när användare skapas?
- Hur skiljer sig rutinen för utbetalningar av inskannade leverantörsfakturor jämfört med utbetalning av manuella fakturor?

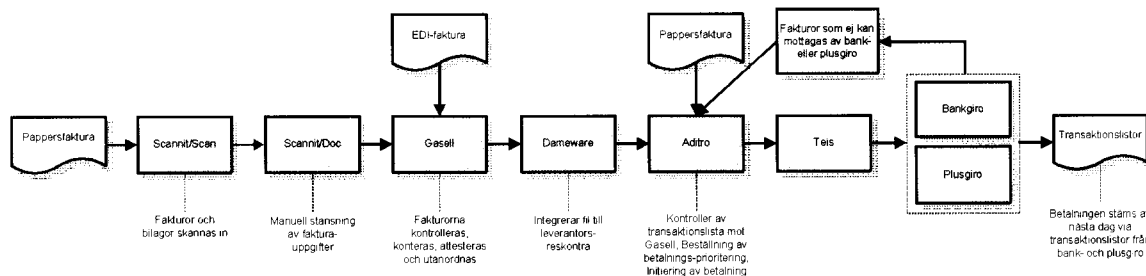
3. Kartläggning av processen

3.1 Processbeskrivning

—> Integrerade system

—> Filöverföring

—> Manuell registrering



System	Syfte
ScannitScan	Skanning av leverantörsfakturor
ScannitDoc	Registrering av information för skannade fakturor
Gasell	Elektroniskt fakturahanteringssystem
DameWare	Överföring av filer till Aditro
Aditro	Ekonomisystem

3.2 Scannit

Beskrivning

I nuläget skannas fakturor in manuellt av en handläggare på ekonomiavdelningen via applikationen ScannitScan. Fakturan förs sedan över till applikationen ScannitDoc där fakturauppgifterna matas in manuellt, t ex leverantör, totalbelopp, momsbelopp, fakturanummer, samt mottagarkod. Med mottagarkod avses den Gasellanvändare som ska ta emot fakturan vid importeringen av fakturor till Gasell. Under ett år hanteras ca 35 000 fakturor.

Ny eller uppdaterad leverantörsinformation som matas in i ScannitDoc förs över till ekonomisystemet Aditro via DameWare (se nedan). Handläggaren kontrollerar den leverantörsinformation som anges på fakturan, bl. a. information om F-skattsedel. I övrigt görs inga andra kontroller av leverantörer.

Iakttagelse, risk och rekommendation

Manuell stansning av fakturauppgifter vid skanningsförandet innebär en risk att fel information registreras och därmed en risk för felaktig hantering av leverantörsfakturor avseende t ex utbetalning och momsredovisning. Enligt uppgift är det vanligast förekommande felet att

momsbeloppet är felaktigt registrerat. Vid inmatningen av fakturauppgifter läggs momsen automatiskt på 25 % (ludvikamoms). Om en annan momssats ska gälla så måste handläggaren ändra momsbeloppet eller lägga momsen i ett annat momsält (affärsmoms vid fakturor som rör VA-verksamhet). Stenungsunds kommun håller för närvarande på att upphandla en lösning för extern fakturaskanning.

Vid registrering av en ny leverantör görs endast kontroller mot informationen som finns på fakturan, dvs. att leverantören har en F-skattesedel. Således görs ingen kontroll att momsregistreringsnummer finns eller att post- eller bankgironumret är korrekt angivet på fakturan. KPMG rekommenderar att kommunen inför utförligare kontroller av leverantörer vid registrering av leverantörsuppgifter för att undvika till exempel "bluff"-fakturor.

3.3 Gasell

Beskrivning

Det finns användarinstruktioner för Gasell och personal på ekonomikontoret genomför regelbundet utbildning för användarna i systemet.

Först importeras de inskannade fakturorna från ScannitDoc till Gasell. En lista över importerade fakturor stäms översiktligt av mot originalfakturorna.

Fakturorna passerar sedan fyra olika steg i Gasell: kontroll, kontering, attestering och utanordning. I systemet finns flera inbyggda kontroller, till exempel kan inte en och samma person kontrollera och attestera en faktura. Den användare som utanordnar fakturor för utbetalning kan heller inte utanordna fakturor som personen själv har attesterat.

Attesträttigheterna i systemet har begränsats till de ansvarsområden där personerna har beslutsattest enligt kommunens attestreglemente. Detta dokumenteras per ansvarsområde och attestant i för ändamålet avsedda pärmar. I Gasell har man lagt in attestbegränsningar per ansvar, verksamhet och konto, motsvarande den delegation som dokumenterats för den specifika attestanten enligt ovan. Detta innebär att en attestant endast kan attestera fakturor inom det ansvar som är definierat i systemet för denna person. I systemet går det att tidsbegränsa attesträtten, dock används inte alltid denna funktion vid tidsbegränsade attestmandat. Vidare går det att sätta beloppsgränser per attestant. Denna systembegränsning används inte i nuläget.

Varje verksamhetsekonom hanterar upplägg, borttag och förändringar av användarrättigheter inom sina verksamheter. Verksamhetsekonomen ansvarar också för att årligen göra en genomgång av samtliga användare i Gasell inom sitt verksamhetsområde.

Vid utanordning av fakturor till betalning genomför handläggaren stickprovskontroller av fakturor på specifika konton, vissa leverantörer, höga belopp (ca 800 tkr) etc. Är något oklart sätts fakturan "under utredning" för närmare granskning. Kontrollerna dokumenteras inte, men det finns en hanteringshistorik där man kan följa vidtagna åtgärder för varje enskild faktura.

En person med administrationsbehörigheter kan lägga upp nya och ta bort gamla användare, ändra behörigheter, samt göra konfigurationsändringar i systemet. Dock kan en administratör

aldrig ändra sin egen behörighet, t ex sätta sig själv som attestant. Sammanlagt elva personer på ekonomiavdelningen har administratörsrättigheter i systemet, dock har endast två av dessa också rätt att attestera fakturer. Ekonomichefen godkänner nya administratörer enligt en informell rutin.

Iakttagelse, risk och rekommendation

Gasell innehåller funktionalitet för att sätta beloppsgränser vid attest. Dock används inte denna funktionalitet i dagsläget, vilket innebär att möjligheten till fördelning eller begränsning av attesträtten för stora belopp inte utnyttjas. Personer som har beslutsattest för ett visst ansvar är formellt begränsade av tilldelad budgetram och som en kontroll att budgeten följs har budgetansvarig månadsvis uppföljning av budgetföljsamhet tillsammans med ekonom. KPMG rekommenderar dock att Stenungsunds kommun utvärderar möjligheten att använda funktionaliteten för beloppsgränser vid delegerat attestansvar, i syfte att tydliggöra detta ansvar vad gäller belopp. Vi rekommenderar också att funktionen för tidsbegränsad attesträtt i Gasell alltid bör användas när en attestant formellt har ett tidsbegränsat mandat.

Det finns ingen formell rutin för hantering av administratörsbehörigheter i Gasell. Det görs heller inte någon periodisk genomgång av administratörsbehörigheter i systemet. Detta innebär en risk att obehöriga personer tilldelas administratörsrättigheter, vilket ökar risken för felaktiga eller bedrägliga transaktioner i systemen. KPMG rekommenderar att rutinen för hantering av administratörsbehörigheter formaliseras och dokumenteras på liknande sätt som rutinen för administration av övriga behörigheter i Gasell, samt att det genomförs periodiska genomgångar av sådana användare.

Kritiska kombinationer av rättigheter uppstår när en person både kan ändra systemparametrar i systemet, attestera fakturer samt har behörighet att skanna in och betala fakturer. Detta innebär att en person skulle kunna ändra parametrar som möjliggör för personen att ensam genomföra hela kedjan av transaktioner för en faktura. KPMG rekommenderar att dessa roller inte kombineras i kommunen. Är det inte möjligt att skilja dessa behörigheter åt bör kommunen, som en kompletterande kontroll, genomföra regelbundna genomgångar av loggar över förändringar av systemparametrar.

3.4 Överföring av information till Aditro via DameWare

Beskrivning

Fakturainformationen från Gasell, samt i förekommande fall leverantörsinformation, förs över till Aditro genom att handläggare kopplar upp sig mot den server där filerna ligger. Handläggaren går in på server via DameWare och flyttar bokförings- och utanordningsfil, samt fil med leverantörsinformation, till korrekt mapp för inläsning i huvudbok, leverantörsreskontra, respektive leverantörsregister i Aditro.

Iakttagelse, risk och rekommendation

Det finns inga dokumenterade rutiner som beskriver hur DameWare fungerar och hur överföring av filer till Aditro genomförs, vilket innebär en risk för att kunskap om rutinen blir personberoende. Enligt uppgift från IT-avdelningen vid Stenungsunds kommun går det att

automatisera denna process. KPMG rekommenderar att en rutinbeskrivning tas fram, samt att kommunen utvärderar möjligheten att automatisera processen.

Personal på ekonomiavdelningen har tillgång till katalogen dit filerna från Gasell skrivs. Filerna är okrypterade, men innehåller kontroller som gör det svårare att ändra i filen utan att det upptäcks av mottagande system.

3.5 Aditro

Beskrivning

Filen med fakturainformation läses sedan in i Aditro. Den enda fakturainformation som går att ändra i Aditro är betalningsdatum. Det utförs en manuell kontroll av summan av fakturorna i Aditro mot utanordningsloggen från Gasell och resultatet signeras och dokumenteras. Efter detta initieras en betalning av fakturorna, vilket innebär att filer till bank- och plusgiro skapas och skrivs till en filserver. Ett betalningsförslag skrivs också ut som inkluderar de fakturor som kommer att överförs till bank-, respektive plusgiro. Detta betalningsförslag stäms av mot utanordningsloggen från Gasell.

Filerna hämtas från servern vid en bestämd tidpunkt varje dag och skickas via integrationsservern Teis vidare filerna till bank- respektive plusgiro. Ekonomiavdelningen informeras automatiskt via mail när filerna har skickats vidare.

Dagen efter det att betalningarna har gått iväg får ekonomiavdelningen utbetalningslistor från bank- och plusgirot. Det sker en manuell kontroll av dessa listor mot det betalningsförslag som skickades föregående dag och eventuella avvikelser utreds. Eventuellt felaktiga fakturor dokumenteras och läggs sedan in manuellt i Aditro. Beloppet för betalda fakturor bokas bort i leverantörsreskontran via en dagrapport.

Det finns dokumenterade instruktioner för hantering av fakturor i ekonomisystemet som beskriver bl. a. beställning av betalningsprioritering, utanordning av betalning samt överföring av betalningsförslaget till bank- och plusgiro.

Iakttagelse, risk och rekommendation

Det saknas dokumenterade rutiner för avstämningen av utanordnade fakturor från Gasell mot Aditro, samt för avstämningen mellan Aditro och bank- och plusgiro. Detta innebär en risk för att kunskapen om rutinen blir personberoende. KPMG rekommenderar därför att rutinen dokumenteras.

En och samma handläggare hanterar inläsning, eventuella justeringar, utanordning till bank- och plusgiro och manuella kontroller i Aditro. Detta innebär en ökad risk för felaktiga eller bedrägliga transaktioner, samt att dessa förblir oupptäckta under en längre period. KPMG rekommenderar Stenungsunds kommun att tydligare skilja på ansvarsfördelningen i Aditro, till exempel bör inte en handläggare kunna registrera leverantörsuppgifter, samt utanordna betalningen till bank- och plusgiro. Vi rekommenderar också kommunen att överväga möjligheten att införa en rutin där det

krävs minst två personer för att godkänna utbetalning av leverantörsfakturer till bank- och plusgiro.

Betalningsinstruktioner från Aditro skrivs till en okrypterad fil på en server som är tillgänglig för personal IT-avdelningen. Filerna innehåller kontroller vilket gör det svårare att ändra i filen utan att det upptäcks av mottagande system.

3.6 Manuella fakturer

Beskrivning

Fakturer som avvisas vid överföringen till bankgirot registreras på nytt i Aditro som en manuell utbetalning. Detta förfarande används också för olika sorters utlägg. När registrering är klar initieras en betalning av fakturorna, vilket innebär att filer till bank- och plusgiro skapas och skrivs till en filserver. Ett betalningsförslag skrivs ut som inkluderar de fakturer som kommer att överföras till bank-, respektive plusgiro. Ekonomichefen attesterar detta betalningsförslag i efterhand.

De manuella utbetalningarna registreras av samma handläggare som också skapar och överför betalningsförslaget till bankgirot.

De manuella utbetalningarna är kopplade till ett separat leverantörsregister som handläggaren administrerar i samband med att manuella utbetalningar registreras.

Iakttagelse, risk och rekommendation

Personal på ekonomiavdelning har den högsta behörighetsrollen i ekonomisystemet, DX_MAXI. En person med denna behörighet kan utföra en hel kedja av transaktioner i systemet, t ex lägga upp en leverantör, registrera en manuell betalning samt utanordna betalningen, vilket innebär en ökad risk för att felaktiga eller bedrägliga transaktioner utförs i systemet.

KPMG rekommenderar att Stenungsunds kommun begränsar antalet användare som tilldelas den högsta behörigheten i Aditro.

KPMG rekommenderar kommunen att tydligare skilja på ansvarsfördelningen i Aditro, till exempel bör inte en handläggare kunna registrera manuella utbetalningar, samt utanordna betalningen till bank- och plusgiro. Vi rekommenderar också kommunen att överväga möjligheten att införa en rutin där det krävs minst två personer för att godkänna utbetalning av manuella betalningar till bank- och plusgiro.

Göteborg, som ovan

KPMG AB



Pontus Axblom



Sofie Andersson