



**Sundsvallas kommun**

**Ytterligare uppföljning av IT-säkerhet  
Revisionsrapport**

KPMG  
*10 december 2004*  
*Antal sidor 6*

272395 GrskRpt04\_Def.doc

## **Innehåll**

1.	Bakgrund	1
1.1	Allmänt	1
1.2	Risk och väsentlighet	1
1.3	Tidigare rapportering	1
2.	Uppdraget	2
3.	Noteringar	2
3.1	Från den kommuninterna rapporteringen	2
3.2	Från intervju och redogörelse	3
4.	Kommentarer och rekommendationer	3

## **1. Bakgrund**

### **1.1 Allmänt**

KPMG fick av Sundsvalls kommuns revisorer redan hösten 2001 i uppdrag att granska kommunens rutiner för hur den styr, utreder, inför, upprätthåller och kontrollerar IT-säkerheten i sin verksamhet.

### **1.2 Risk och väsentlighet**

Revisionen bedömde 2001 att det fanns risk för att det förelåg brister i de rutiner som skall säkerställa en god IT-säkerhet och att det därför var väsentligt att klarlägga på vilket sätt och i vilken form kommunfullmäktige, -styrelse och -ledning samt operativt ansvariga styr IT-säkerhetsarbetet. Det ansågs vidare vara väsentligt att veta vilka riskbedömningar IT-säkerhetsarbetet vilade på, hur regler, anvisningar etc rörande säkerhetsarbetet kommunicerades, implementerades, underhölls samt hur efterlevnaden av beslutad IT-säkerhet kontrollerades.

### **1.3 Tidigare rapportering**

Revisionen har för åren 2001, 2002 och 2003 genomfört och lämnat uppföljande rapporter från sin granskning. Vår sammanfattande kommentar till kommunens IT-säkerhetsarbete i 2003 års rapport löd:

”Trots ambitionen att införa en modern IT-policy och högt prioritera IT-säkerhet så har kommunledningen i Sundsvall stora problem med att skapa trovärdighet med sitt IT-säkerhetsarbete. Kommunen är i betydande omfattning beroende av ett effektivt och säkert datoriserat verksamhetsstöd för att nå sina mål och uppfylla medborgarnas förväntningar och krav. I det sammanhanget är det förvånande att i princip inget IT-säkerhetsarbete utförts under ett år.

Oavsett hur man väljer att organisera/samordna kommunens totala IT-säkerhetsarbete är ansvaret för sekretess, tillgänglighet, riktighet och funktionalitet i och till verksamhetsstöden fortfarande tillhörigt desamma som för den verksamheten som de stöder. En försening i tillsättandet av en sammanhållande funktion får inte hindra att det kontinuerligt, tydligt och enkelt sprids ett allmänt budskap om IT-säkerhet i form av regler och riktlinjer samt att kontroller utförs för att säkra efterlevnaden.”

## 2. Uppdraget

KPMG fick av Sundsvalls kommuns revisorer för räkenskapsåret 2004 i uppdrag att följa upp och rapportera om kommunens fortsatta IT-säkerhetsarbete.

Uppdraget har utförts genom att:

- Studera kommunintern skriftlig rapportering rörande IT-säkerhetsarbetet.
- Tillsammans med de förtroendevalda revisorerna intervjua kommunens IT-chef samt få en redogörelse för 2004 års IT-säkerhetsarbete av den konsult som på halvtid anlits av kommunen (IT-chefen) för att fungera som central IT-säkerhetssamordnare.

Rapporten har varit föremål för saklighetskontroll utförd av IT-chef.

## 3. Noteringar

### 3.1 Från den kommuninterna rapporteringen

I föreliggande rapporter från april till november kan noteras att:

- IT-säkerhetsrådet bestående av representanter från förvaltningar och bolag med uppgift att ansvara för att ta fram säkerhetsinstruktioner och metoder för IT-säkerhetsarbetet hade inte sitt första möte förrän i maj 2004
- Engagemanget från förvaltningar och bolag är per maj femtioprocentigt. Endast hälften av förvaltningarna och bolagen skickade representanter. En process för identifiering av samtliga system startas.
- Den anlitade IT-samordnaren påbörjar sitt arbete i april och har fram till november 2004 inventerat IT-säkerhetsläget, informerat förvaltningarna om sitt ansvar och sin uppgift samt initierat och stimulerat till IT-säkerhetsarbete. Han har vidare allmänt deltagit i det övergripande säkerhetsarbetet som ingår i en IT-enhets ansvar.
- Några förvaltningar har påbörjat sitt arbete och det efter en ordning överenskommen i IT-säkerhetsrådet. Man prioriterar definition av IT-system och rollbesättning vilket skall följas av informationsklassning, upprättandet av systemsäkerhetsplaner, planering av åtgärder, avbrottsplanering samt framtagande av IT-säkerhetsinstruktioner.
- Per novemberrapporten så är uppslutning till senaste mötet med IT-säkerhetsrådet ”mycket dålig”. De som medverkar upplever ändå mötena som konstruktiva.
- Det framgår inte med tydlighet om någon förvaltning/bolag för något system med säkerhet har slutfört, eller är i den omedelbara slutfasen av, det prioriterade arbetet.

## 3.2 Från intervju och redogörelse

Vid intervju och redogörelse framkommer att:

- Engagemang och förståelse för IT-säkerhetsarbete inom kommunen får bedömas som lågt.
- Den allmänna IT-kompetensen inom kommunen, från medarbetaren till chefsnivån, bedöms även den som låg.
- Incidenter har inträffat under året vilka alla kunnat åtgärdas om än med merkostnader för kommunen. Här nämns främst bristen på tillgänglighet till ekonomisystemet under början av året samt driftsättning av system som inte varit driftgodkända.
- IT-säkerhetspolicyn har utan att i nämnvärd grad varit tillämpad nu blivit så gammal att den är i behov av en revidering.
- Anlitandet av den externa IT-säkerhetsamordnaren har varit IT-chefens bidrag till att göra något för IT-säkerhetsarbetet även om den huvudsakliga delen av det ansvaret inte skall ligga inom IT-enheten.
- IT-chefen anser sig ha nödvändiga resurser för att under kommande år kunna finansiera en fortsättning av det externt anlitade IT-säkerhetsstödet.

## 4. Kommentarer och rekommendationer

Den externt anlitade IT-säkerhetsamordnaren har som det framgår av rapporter och intervju tillfört kommun en kompetens som uppenbarligen tidigare saknats. Vi kan dock inte finna att respons och initiativkraft från kommunens sida fullt ut stått i proportion till vad som tillförts.

Under fyra år har vi nu följt kommunens IT-säkerhetsarbete. Kommunen styr verksamheten såtillvida att de 2002 beslutat om en policy som nu måste revideras för att nå ändamålsenlighet. Utreder och undersöker gör man i så ringa omfattning att det inte lett till konkreta resultat i någon nämnvärd grad. Upprätthållande och kontroll av IT-säkerheten blir i konsekvens av detta inte tillämpligt. Om tillförd kompetens inte placeras ändamålsenligt i organisationen, utnyttjas målinriktat och ges ett tydligt mandat kommande år bedömer vi risken som stor för att arbetet utvecklas långsamt och ofullständigt som under 2004 eller går i stå som under 2003. Vid bruket av de datoriserade verksamhetsstöden innebär detta enligt vår mening en ökad risk för:

- Fel
- Effektivitetsförluster
- Rationaliseringsförluster
- Fördyringar
- Förtroendeskada
- Oegentligheter

Vi rekommenderar att revisorerna hos ytterst ansvariga tjänstemän och förtroendevalda söker svar på följande frågor:

- Vilket engagemang för IT-säkerheten man kan förvänta sig av ledningen samt motivet för detta.
- Vilka riskanalyser de genomfört och vilka konsekvenser dessa fått på behovet av skyddsåtgärder.
- Hur ansvarsfördelningen för IT-säkerheten har beslutats och hur detta har kommunicerats till de ansvariga.
- Vilka administrativa regler (policies, riktlinjer, systemsäkerhetsplaner etc.) och rutiner som finns samt behöver införas.
- Vilka regelbundna kontroller av beslutad säkerhetsnivå gentemot införda skyddsåtgärder kommer att genomföras.

Falun datum som ovan

KPMG

Lars Anteskog