Deloitte.

Rapport avseende granskning av IT-säkerhet

Östersunds kommun

November 2014

Innehåll

Sammanfattning

Uppdrag och bakgrund

En god intern kontroll är viktig för att kunna uppnå och upprätthålla en hög IT-säkerhetsnivå och minimera riskerna för att verksamheten ska drabbas av allvarliga störningar.

På uppdrag av de förtroendevalda revisorerna i Östersunds kommun har Deloitte granskat den interna kontrollen avseende IT-säkerhetsarbetet.

Revisionsfråga

Syftet med granskningen är att bedöma om den interna kontrollen avseende IT-säkerhetsarbetet är tillräcklig.

Revisionskriterier

I denna granskning har revisionskriterierna huvudsakligen utgjorts av:

- Kommunallag (1991:900)
- Interna styrdokument

Svar på revisionsfrågan

Vi bedömer att den interna kontrollen avseende IT-säkerhetsarbetet kan förbättras.

Iakttagelser

Ansvarsfördelningen för kommunens IT-system är klarlagd. Förteckningen över innehavare av olika ansvarsroller för systemen behöver uppdateras och hållas aktuella.

Det finns dokumenterade rutiner och mallar för hanteringen av behörigheter till kommunens IT-system.

Det finns dokumenterade rutiner för regelbundna och systematiska kontroller av hur systemen används.

Kommunen har dokumenterade rutiner för hantering av icke önskvärda incidenter.

Rutinerna för risk- och konsekvensanalyser vid förändringar i IT-system eller vid införande av nya lösningar behöver utvecklas.

Rekommendationer

Utifrån genomförd granskning rekommenderar vi:

- Att förteckningar över ansvarsroller uppdateras och ajourhålls.
- Att det klargörs när och hur risk- och konsekvensanalyser ska genomföras och vem som ansvarar för att de genomförs.
- Att systemförvaltare och/eller IT-samordnare involveras i riskanalysarbetet och framtagandet av internkontrollplaner.
- Att behovet av ett forum för hantering av olika systemfrågor och erfarenhetsutbyte mellan systemförvaltare utreds.

Östersund 2014-11-21
DELOITTE AB

Marianne Harr
Certifierad kommunal revisor
Uppdragsansvarig

Mattias Holmetun
Projektledare

1. Inledning

1.1. Uppdrag och bakgrund

Kommunstyrelsen har det yttersta ansvaret för IT-säkerheten. Nämnderna har ansvaret för IT-säkerheten inom sina verksamhetsområden.

En god intern kontroll är viktig för att kunna uppnå och upprätthålla en hög IT-säkerhetsnivå och minimera riskerna för att verksamheten ska drabbas av allvarliga störningar.

På uppdrag av de förtroendevalda revisorerna i Östersunds kommun har Deloitte granskat den interna kontrollen avseende IT-säkerhetsarbetet.

1.2. Revisionsfråga

Syftet med granskningen är att bedöma om den interna kontrollen avseende IT-säkerhetsarbetet är tillräcklig.

Inom ramen för granskningens övergripande syfte ska granskningen besvara följande kontrollmål:

- Är ansvarsfördelningen för kommunens IT-system aktuell, klarlagd och dokumenterad?
- Finns ändamålsenliga rutiner för behörighet och lösenord?
- Granskas användandet av kommunens IT-system systematiskt?
- Hanteras icke önskvärda incidenteter på ett ändamålsenligt sätt?
- Görs riskanalyser regelbundet och på ett systematiskt sätt?

1.3. Revisionskriterier

Revisionskriterierna är de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.

I denna granskning har revisionskriterierna huvudsakligen utgjorts av:

- Kommunallag (1991:900)
- Interna styrdokument

1.4. Avgränsning

Granskningen har omfattat kommunstyrelsen och socialnämnden.

1.5. Metod

Granskningen har genomförts genom intervjuer samt dokumentanalyser. De intervjuade framgår av bilaga.

2. Granskningsresultat

2.1. Är ansvarsfördelningen för kommunens IT-system aktuell, klarlagd och dokumenterad?

Kommunens gällande IT-säkerhetspolicy beslutades av kommunstyrelsen 2004-09-21. Denna policy reglerar hur kommunen, och andra nyttjare av kommunens IT-infrastruktur, ska arbeta med IT -säkerhet. Med IT-säkerhet menas skydd av utrustning och information.

Av policyn framgår bland annat att:

- Kommunstyrelsen har det yttersta ansvaret för IT-säkerheten.
- Nämnden har ansvaret för IT-säkerheten inom sitt verksamhetsområde.
- Resurser för kommunövergripande IT-säkerhetsarbete anvisas av kommunstyrelsen genom den centrala IT-budgeten.
- Arbetet med IT-säkerhet ska bedrivas systematiskt och omfatta alla verksamheter.
- IT-systemen ska skyddas mot obehörig åtkomst.
- Lagar och externa krav på kommunens informationssystem ska följas.
- Ansvarsfördelningen för samtliga IT-system inom kommunens verksamhet ska vara aktuell, klarlagd och dokumenterad.
- Säkerhetsfrågorna ska beaktas redan vid upprättande av kravspecifikation och anskaffning av informationssystem.

Kommunledningsförvaltningen har tagit fram underliggande rutiner till stöd policyn. Dessa beskrivs i *”rutiner för Östersunds kommuns IT-säkerhetsarbete”* (IT-säkerhetsrutin).

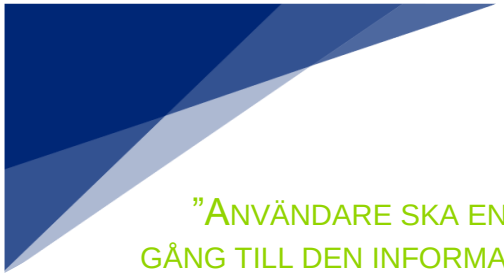
Av dessa rutiner framgår att förvaltningarna ansvarar för att verksamhetsrelaterade rutiner och rutiner för uppföljning av IT-säkerhetsarbetet tas fram.

För varje IT-system ska det utses en systemägare, en systemförvaltare och en systemadministratör. Ansvaret för samtliga roller framgår av dokumentet *”Systemförvaltningsorganisation Förvaltningsspecifika system”*.

En förteckning förs över kommunens system och vilka personer som innehar de olika rollerna (systemägare, systemförvaltare, systemadministratör). Vi har noterat att det saknas uppgifter om vem som är systemägare för ett par IT-system och vem som är systemadministratör för mer än hälften av systemen.

Tidigare fanns ett mötesforum för erfarenhetsutbyte och hantering av olika systemfrågor. Numer tas systemfrågor, i viss utsträckning, upp i IT-förändringsrådet och i säkerhetsforum. De intervjuade uppger dock att det finns ett behov av att arbeta mer strukturerat med informationssäkerhet överlag.

2.2. Finns ändamålsenliga rutiner för behörighet och lösenord?



”ANVÄNDARE SKA ENDAST FÅ TILLGÅNG TILL DEN INFORMATION SOM BEHÖVS FÖR ATT KUNNA UTFÖRA SINA ARBETSUPPGIFTER”

IT-säkerhetspolicy för Östersunds kommun

Av kommunens IT-säkerhetsrutin framgår de övergripande rutinerna för behörigheter och lösenordshantering.

Vid hanteringen av användarbehörigheter till kommunens IT-system används särskilda rutiner enligt kommunens behörighetsprocess. I behörighetsprocessen finns rutiner för upplägg-ning, ändringar och borttagning av behörigheter.

För att få tillgång till kommunövergripande IT-system krävs bland annat att personen är registrerad i kommunens personal- och lönesystem och att chefen eller en person som denne utsett fyller i ett särskilt, elektroniskt, behörighetsformulär med uppgifter om vilka system användaren ska ha tillgång till. Formuläret skickas till behörighetshanteringen vid datacenter som hanterar både upplägg och borttag av behörigheter.

När användaren tilldelats behörighet till IT-systemen krävs användar-id och lösenord för att logga in. Inom socialförvaltningen krävs separata inloggningar i kommunövergripande IT-system och de verksamhetsspecifika IT-systemen. Enligt de intervjuade förs dock diskussioner om möjligheterna för att införa ”single sign on”. Detta skulle innebära att användare endast behöver logga in en enda gång för att nå de system som användaren har behörighet till.

Användar-id och lösenord får inte lånas ut. Vid tillfälliga behov av tillgång till olika system, till exempel vid semestrar, ska tidsbegränsade behörigheter beställas.

Av IT-säkerhetsrutinen framgår generella rutiner för lösenordshanteringen. Lösenord innehåller minst 8 tecken med en blandning av siffror, bokstäver och andra tecken. I systemen finns inställningar/spärrar inlagda som gör att lösenord måste bytas efter en viss period. Det är även spärrat så att möjligheterna att återanvända samma lösenord är begränsade.

Service på system (de system som datacenter administrerar) får endast hanteras genom datacenter, på uppdrag av systemförvaltaren för det aktuella systemet.

Inom socialnämndens verksamhetsområde gäller så kallad inre sekretess. Detta innebär att uppgifter, som omfattas av sekretess, endast får lämnas mellan befattningshavare om det är nödvändigt för ett ärendes handläggning eller för verksamhetens bedrivande i övrigt.

Av kommunstyrelsens och socialnämndens internkontrollplaner för år 2014 framgår att det identifierats risker för att det finns brister i hanteringen av behörigheter. Socialnämnden har även identifierat att det finns en risk för att den inre sekretessen bryts. Av internkontrollplanerna framgår vilka kontroller/åtgärder som styrelsen och nämnden vidtar för att förhindra att riskerna inträffar.

2.3. Granskas användandet av kommunens IT-system systematiskt?

”ANVÄNDANDET AV KOMMUNENS IT-SYSTEM GRANSKAS SYSTEMATISKT”

IT-säkerhetspolicy för Östersunds kommun

Av 2014 års internkontrollplan som gäller för hela kommunförvaltningen framgår vilka kontroller av IT-användandet som kommer att genomföras under året. Under året genomförs bland annat:

- externt penetrationstest för att undersöka skyddet mot intrång i kommunens system,
- stickprov på hur personalen använder internet,
- uppföljning av hur systemens inbyggda kontrollfunktioner används. Detta är en återkommande kontrollpunkt i internkontrollplanen som även omfattar uppföljning av tidigare års åtgärdspunkter. Ett system per år väljs ut för kontroll. Valet av system görs av IT-förändringsrådet.
- kontroll av att det finns rutiner för att hantera personuppgifter på ett korrekt sätt.

Inom socialförvaltningen registreras all användning av det verksamhetsspecifika IT-systemet Viva i så kallade loggar. Logglistorna anger personnummer på registerledare, handläggare i ärendet, vilka användare som tittat på ärendet samt tidpunkt för detta.

I socialförvaltningen arbetar personalen i olika team och uppföljningen av logglistorna sker teamvis enligt följande:

- Systemförvaltaren tar varje månad ut logglistor för två slumpmässigt valda ärenden per team. För vissa ärendetyper tas logglistor ut kvartalsvis.
- Listorna överlämnas till respektive teamchef.
- Teamcheferna kontrollerar listorna, signerar och lämnar listorna till systemförvaltaren.
- Vid eventuella frågetecken vid kontroll av logglistorna, kontaktas systemförvaltaren för eventuell ytterligare kontroll av loggar.
- Vid misstanke om otillåten användning av systemet, kontaktas områdeschef. Beslut om vidare utredning fattas av förvaltningschef.

2.4. Hanteras icke önskvärda incidenteter på ett ändamålsenligt sätt?

”INCIDENTER SOM INTRÄFFAR SKA RAPPORTERAS ENLIGT KOMMUNENS GEMENSAMMA SKADE- OCH INCIDENTRAPPORTERINGSRUTIN.”

IT-säkerhetspolicy för Östersunds kommun

Respektive förvaltning ansvarar för att incidenter rapporteras i kommunens gemensamma skade- och incidentrapporteringssystem, Riskprio.

Alla incidenter, konstaterade eller misstänkta ska rapporteras och Datacenter ansvarar för att detta görs.

Säkerhetschefen och kommunens IT-strateg ansvarar för att sammanställa de skador- och incidenter som inträffar och föreslå förebyggande åtgärder.

Under våren 2014 drabbades kommunen av en driftstörning i IT-miljön som direkt påverkade cirka 700 medarbetare. Incidenten har analyserats och det har upprättats detaljerade redogörelser av händelseförloppet liksom en rapport över den konsekvensanalys som genomförts. Av dokumentationen framgår bland annat vad som hände, vilka åtgärder som vidtogs, vilka skador som konstaterats samt vilka risker som verksamheten utsattes för.

Rapporten över den konsekvensanalysen har presenterats för kommunledningsgruppen som gett säkerhetschefen i uppdrag utreda hur kommunen på ett mer strategiskt och strukturerat sätt ska kunna jobba med informationssäkerhet.

2.5. Görs riskanalyser regelbundet och på ett systematiskt sätt?

Som tidigare nämnts har kommunstyrelsen och socialnämnden analyserat risker som rör IT-säkerheten och internkontrollplaner med kontroller/åtgärder för att hantera dessa risker har upprättats. Inom socialförvaltningen har dock inte systemförvaltaren eller IT-samordnaren deltagit i riskanalysarbetet.

Enligt de intervjuade genomförs riskanalyser, utöver analyserna i samband med upprättandet av internkontrollplaner, i för liten omfattning. Det saknas tydliga direktiv för risk- och konsekvensanalyser vid förändringar i IT-system eller vid införande av nya lösningar, som till exempel införande av molntjänster.

3. Revisionell bedömning

Vi bedömer att den interna kontrollen avseende IT-säkerhetsarbetet kan förbättras. Det har framkommit att det finns ett behov av att arbeta på ett mer strukturerat sätt med informationssäkerheten.

Granskningen visar att ansvarsfördelningen för kommunens IT-system är klarlagd och att det finns dokumentation som beskriver ansvarsfördelningen. För varje IT-system utses en systemägare, en systemförvaltare och en systemadministratör. Förteckningen över vilka personer som innehar dessa roller för de olika systemen behöver dock uppdateras och hållas ajour.

Det finns dokumenterade rutiner och mallar för hanteringen av behörigheter till kommunens IT-system. Styrelsens och socialnämndens internkontrollplaner tyder på att det kan finnas brister i dessa rutiner eller i tillämpningen av rutinerna. Kontrollåtgärder har dock beslutats för att se över och kvalitetssäkra behörighetsrutinerna.

IT-säkerheten följs upp på ett systematiskt sätt och det finns dokumenterade rutiner för regelbundna och systematiska kontroller av hur systemen används.

Kommunen har dokumenterade rutiner för hantering av icke önskvärda incidenter. För att underlätta rapporteringen av konstaterade eller misstänkta incidenter används ett kommungemensamt skade- och incidentrapporteringssystem.

Granskningen visar att det till viss del genomförs riskanalyser som rör IT-säkerheten. Rutinerna för risk- och konsekvensanalyser vid förändringar i IT-system eller vid införande av nya lösningar behöver dock utvecklas. Den interna kontrollen skulle stärkas av att det klargörs när och hur risk- och konsekvensanalyser ska genomföras och vem som ansvarar för att de genomförs.

3.1. Rekommendationer

Utifrån genomförd granskning rekommenderar vi:

- Att förteckningar över systemägare, systemförvaltare och systemadministratörer uppdateras och ajourhålls.
- Att det klargörs när och hur risk- och konsekvensanalyser ska genomföras och vem som ansvarar för att de genomförs.
- Att systemförvaltare och/eller IT-samordnare involveras i riskanalysarbetet och framtagandet av internkontrollplaner.
- Att behovet av ett forum för hantering av olika systemfrågor och erfarenhetsutbyte mellan systemförvaltare utreds.

4. Bilagor

Intervjuade

Lars-Åke Wallin, Säkerhetschef, Kommunledningsförvaltningen
Eva Rodin Svantesson, IT-strateg, Kommunledningsförvaltningen
Kristina Paulsson, Systemförvaltare, Socialförvaltningen
Christer Ljungqvist, IT-/E-samordnare, Socialförvaltningen