www.pwc.se

Revisionsrapport

Granskning av IT-säkerhet

Kommunalförbundet ITSAM

Martin Westholm
Mattias Wittbom

Augusti 2016

pwc

Innehållsförteckning

1. Inledning

1.1. Bakgrund

Ett fungerande IT-stöd är av stor betydelse i den kommunala verksamheten. Den moderna informationsteknologin ger möjligheter att höja kvalité, säkerhet och effektivitet i de olika verksamheterna, sprida och öka tillgängligheten till information m m. IT är en förutsättning för att verksamheten skall fungera på ett effektivt och säkert sätt och en central fråga är hur väl IT tillgodoser användarnas behov.

En fungerande IT-säkerhet är en förutsättning för att verksamhetens integritet skall upprätthållas samt för att information ej ska spridas till obehöriga. IT-säkerheten i IT-miljön i dess helhet påverkas av en mängd olika faktorer, t ex ändamålsenlig infrastruktur, IT-avdelningens förmåga, tillräckligt bra och säkra system, tekniska skyddsmekanismer, processer, rutiner samt fysiskt skydd av hårdvaran.

1.2. Uppdrag

De förtroendevalda revisorerna för ITSAM har identifierat IT-säkerhet som ett riskområde och uppdragit PwC att genomföra en översiktlig granskning av ITSAM:s hantering av IT-säkerheten enligt nedan granskningsmål.

Denna granskning avser att besvara följande revisionsfråga:

- **Säkerställer direktionen att ITSAM har en tillfredsställande IT-miljö och rutiner för att upprätthålla IT-säkerheten i driften och leveransen av IT mot medlemskommunerna?**

Vidare omfattar granskningen följande revisionskriterier:

1. Det finns aktuella styrande och stödjande dokument med avseende på IT-säkerhet och är dessa kända och tillämpas.
2. ITSAM arbetar strukturerat med riskhantering avseende IT-säkerhet utifrån en formaliserad riskhanteringsprocess
3. Det finns fungerande skydd mot fysisk åverkan på IT-resurserna, i form av skalskydd samt ändamålsenliga datahallar
4. Det finns ändamålsenligt skydd mot obehörigt intrång i IT-miljön samt rutiner för att hantera attacker
5. Det föreligger god intern kontroll vad gäller att ge, ändra och ta bort behörighet till IT-miljön samt till centrala/kommungemensamma system

1.3. Metod och avgränsning

Granskningen har utförts genom intervjuer med i huvudsak IT-säkerhetsansvarig inom ITSAM. Vidare har stödjande och styrande dokumentation såsom rutinbeskrivningar och policys inspekterats och vi har även genom inspektion testat att de kontrollmoment som innefattas av våra revisionskriterier är effektiva och fungerar som väntat.

Granskningsobjektet är i första hand ITSAM och de områden och rutiner inom IT-säkerheten som ligger inom ITSAM:s ansvar. Rutiner i respektive kommun kommer ej att innefattas. Då det är medlemskommunerna som är informationsägare är det de som formellt ansvarar för informationssäkerheten och ITSAM ansvarar för den mer tekniska IT-säkerheten.

Baserat på omfattningen av granskningen och revisionsfrågan kan granskningen och eventuella observationer inte förväntas inkludera alla möjliga förbättringar i den interna kontrollen och förvaltningen av IT-miljön.

2. *Sammanfattning och revisionell bedömning*

De förtroendevalda revisorerna för kommunalförbundet ITSAM har gett PwC uppdraget att översiktligt granska hanteringen av IT-säkerhet inom ITSAM. Granskningen besvarar revisionsfrågan ” **Säkerställer direktionen att ITSAM har en tillfredsställande IT-miljö och rutiner för att upprätthålla IT-säkerheten i driften och leveransen av IT mot medlemskommunerna?”**

Vår granskning visar att det finns en god intern kontroll vad gäller hanteringen av IT-säkerhet inom ITSAM, att styrande och stödjande dokumentation finns på plats samt att ändamålsenliga rutiner till stor del finns dokumenterade och implementerade. De iakttagelser som gjorts i samband med granskningen, redovisas under avsnitt 3 och nedan redovisas en kortfattad bedömning per revisionskriterie:

- Det finns aktuella styrande och stödjande dokument med avseende på IT-säkerhet och är dessa kända och tillämpas. Revidering av dessa bör dock ske årligen, vilket ej görs konsekvent.
- ITSAM arbetar strukturerat med riskhantering avseende IT-säkerhet utifrån en formaliserad riskhanteringsprocess.
- Det finns fungerande skydd mot fysisk åverkan på IT-resurserna, i form av skalskydd samt ändamålsenliga datahallar.
- Det finns ändamålsenligt skydd mot obehörigt intrång i IT-miljön samt rutiner för att hantera attacker.
- Det finns formaliserade rutiner vad gäller att ge, ändra och ta bort behörighet till IT-miljön samt till centrala/kommungemensamma system, däremot finns dessa rutiner ej tydligt dokumenterade.

Vår sammanfattande bedömning är att den interna kontrollen rörande IT-säkerheten är god, med endast mindre förbättringsområden. Detta främst när det gäller att dokumentera rutinen för behörighetstilldelning. Vår observation är dock ej av den grad att vi bedömer den som kritisk, med en allvarlig inverkan på IT-enhetens möjlighet att fullfölja sina åtaganden kopplat till IT-tjänsten som levereras till medlemskommunerna. Därför är slutsatsen att IT hanteras på ett säkert sätt, med viss förbättringspotential enligt rekommendationerna i denna rapport.

3. Granskningens resultat

Granskningen genomfördes under juni till augusti 2016. Nedan har vår bedömning och eventuella observationer per revisionskriterie sammanställts på aggregerad nivå. Observationerna har bedömts efter dess väsentlighet, graderingen illustreras med hjälp av följande definition:

Röd – En brist med så stor påverkan på system, processer eller intern kontroll vilken kan medföra att verksamheten exponeras för betydande förluster eller väsentliga fel i den finansiella rapporteringen.

Gul – Mindre brister eller fel där risken för otillbörlig användning och/eller felaktigheter i bokföringen är lägre, men där det ändå bedöms finnas utrymme för förbättringar.

Grön – Inga eller ej väsentliga brister noterade.

För detaljer, kommentarer och bedömning, se respektive avsnitt.

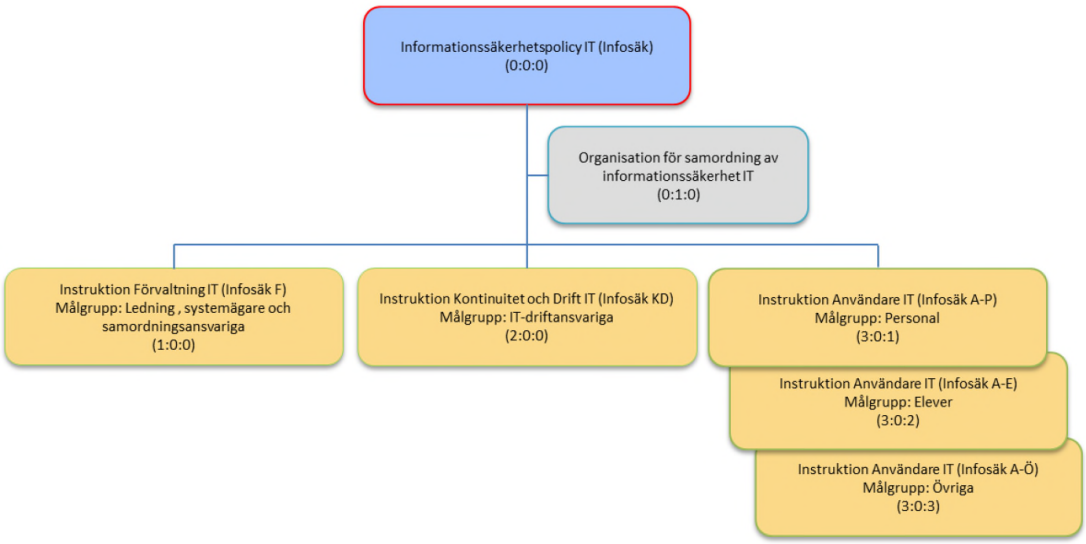
Ref.	Revisionskriterier	Bedömning
3.1	**Det finns aktuella styrande och stödjande dokument med avseende på IT-säkerhet och är dessa kända och tillämpas.**	
3.2	**ITSAM arbetar strukturerat med riskhantering avseende IT-säkerhet utifrån en formaliserad riskhanteringsprocess**	
3.3	**Det finns fungerande skydd mot fysisk åverkan på IT-resurserna, i form av skalskydd samt ändamålsenliga datahallar**	
3.4	**Det finns ändamålsenligt skydd mot obehörigt intrång i IT-miljön samt rutiner för att hantera attacker**	
3.5	**Det föreligger god intern kontroll vad gäller att ge, ändra och ta bort behörighet till IT-miljön samt till centrala/kommungemensamma system**	

3.1. Finns det aktuella styrande och stödjande dokument avseende IT-säkerhet och är dessa kända och tillämpas?

Under granskningen konstaterades att det finns styrande och stödjande dokument som kommuniceras till verksamheten samt internt inom IT-funktionen. ITSAM arbetar efter MSB:s riktlinjer vad gäller IT-säkerhet, processer och riskhantering och följer till stora delar kvalitetsstandarden ISO 27000 för informationssäkerhet. ITSAM har i grunden en IT-strategi vad gäller den övergripande leveransen till medlemskommunerna och hur ITSAM ska stödja dem med hjälp av IT och IT-kompetens.

Som nämnts i avsnitt 1.3 ligger ansvaret för informationssäkerheten hos medlemskommunerna medan ansvaret för IT-säkerheten ligger på ITSAM. Det är viktigt att här poängtera den gränsdragningen.

Vad gäller IT-säkerhet specifikt så finns en informationssäkerhetspolicy som syftar till att klarlägga viljeinriktning och mål med IT-säkerhetsarbetet på ITSAM samt för medlemskommunerna. Medlemskommunerna ansvarar för informationssäkerheten och informationsägarens roll/ansvar framgår av informationssäkerhetspolicyn. Kopplat till den övergripande policyn finns tre olika instruktioner enligt bilden nedan.



Källa: Informationssäkerhetspolicy IT - ITSAM

Alla dokument (Informationssäkerhetspolicy samt instruktioner för Förvaltning IT, Kontinuitet och Drift samt Användare) ligger ute på hemsidan och är tillgängliga för alla medlemskommuner och användare i nätverket. Utöver dokumenten ovan finns även ett antal policys gällande åtkomstkontroll, hantering av sekretessbelagd information samt användning av mobila enheter.

Vi har i vår granskning tagit del av ovanstående dokument och genom inspektion bedöms de innehålla väsentlig och relevant information. Revidering av dokumenten ska enligt plan ske årligen för att säkerställa att dokument och instruktioner hålls aktuella och i linje med det övergripande informationssäkerhetsarbetet.

3.1.1. Vår kommentar och bedömning

Vår sammanfattande bedömning är det finns aktuella styrande och stödjande dokument gällande IT-säkerhet, för arbetet internt på ITSAM såväl som för användarna ute i medlemskommunerna. Dokumenten innehåller väsentlig information och finns tillgängliga för samtliga medarbetare och användare av IT-resurserna.

De dokument vi granskat är dock ej reviderade årligen i samtliga fall, det finns policys/instruktioner som är reviderade senast 2013. Även om dokumenten fortfarande är aktuella finns det en poäng i att ha en årlig revideringsrunda och i och med det sätta nya revisionsdatum på dokumenten för att visa att en översyn skett.

3.2. ITSAM arbetar strukturerat med riskhantering avseende IT-säkerhet utifrån en formaliserad riskhanteringsprocess?

ITSAM har en formaliserad och dokumenterad rutin för hur de tillsammans med verksamheten, medlemskommunerna, skall arbeta med riskhantering avseende IT (”Rutin Risk- och Sårbarhetsanalys – Verksamhet”). Risk och sårbarhetsanalyser (RSA) genomförs för att kartlägga eventuella sårbarheter i informationsbärande system och för att eliminera eller reducera identifierade risker till en acceptabel nivå. Risk- och Sårbarhetsanalyser utförs kontinuerligt i verksamheterna och är i många fall ett krav då kritiska system används eller där personliga informationsuppgifter hanteras.

RSA genomförs dels ur ett IT-perspektiv, med fokus på de tekniska aspekterna av IT-leveransen, samt ur ett verksamhetsperspektiv, med fokus på säkerhet och tillgänglighet kopplat till informationen i systemen. RSA:n godkänns av verksamheten/systemägaren och den efterföljande åtgärdsplanen hanteras av verksamheten och ITSAM gemensamt i syfte att hantera eventuella hot och risker.

Vi har i detta arbete granskat den rutinbeskrivning som finns framtagen och som beskriver hur arbetet med RSA ska bedrivas inom medlemskommunerna och anser att den täcker in väsentliga områden samt är skriven på en rimlig nivå.

Vi har även som en del av vår granskning inhämtat resultatrapporter från utförda RSA:s under de senaste åren i syfte att säkerställa att analyserna utförs för verksamhetskritiska system samt att resultatet av analyserna hanteras. I detta har vi granskat analyser för systemen Procapita samt CosmicLink för att säkerställa att analyserna innehåller relevanta moment samt att det finns åtgärdslistor för identifierade risker.

3.2.1. *Vår kommentar och bedömning*

Vår sammanfattande bedömning är att det finns en formaliserad och dokumenterad rutin för hur ITSAM tillsammans med medlemskommunerna skall arbeta med riskanalyser vad gäller IT-säkerhet samt att dessa rutiner efterlevs. Vår granskning av faktiskt utförda analyser visar även på att de följer rutinerna samt att åtgärdsförslag tas fram som ett resultat av analyserna, i syfte att hantera de risker som identifieras.

3.3. Det finns fungerande skydd mot fysisk åverkan på IT-resurserna, i form av skalskydd samt ändamålsenliga datahallar?

ITSAM hanterar driften av IT i två fysiska datahallar; en i ITSAM-huset i Kisa och en i Vimmerby. Datahallen i Vimmerby moderniserades 2014 medan datahallen i ITSAM:s byggnad i Kisa är något äldre och saknar brandsläckningsutrustning. Det har dock inletts en process för att upphandla det under 2016.

Datahallarna innehåller följande skydd mot fysisk åverkan:

Larm: Kommunalförbundet ITSAMs kontor samt serverhallar är utrustade med brand- och inbrottslarm. Inbrottslarmet styrs normalt via manöver från passagesystemet. In-brottslarmet är kopplat till G4S larmcentral som vid larm vidtar åtgärd enligt åtgärdslista. Dagtid kontaktas Servicedesk, övrig tid kontaktas i första hand kontaktpersoner och i andra hand skickas väktare till platsen. I serverhallarna är inbrottslarmet även ett drift-larm då det är utrustat med sensorer för bl.a. hög temperatur, vattenläckage, nätavbrott m.m.

Klimatutrustning: Serverhallar samt teknikbodar är beroende av dess utformning och innehåll och är utrustade med aktiva klimatanläggningar för att hålla rätt temperatur.

Brandskydd: I serverhallen i Vimmerby finns Argonite släcksystem med tillhörande brandlarm. Brandlarmet är sammankopplat med fastighetens automatlarm som i sin tur är kopplat till SOS-Alarm och räddningstjänst. I serverhallen i Kisa finns i dagsläget endast brandlarm, ej släckningsutrustning.

Tillträdeskontroll/skalskydd: Samtliga dörrar till Kommunalförbundet ITSAMs kontor är larmade och utrustade med beröringsfria kortläsare med knappsats. Serverhallar och andra noder beroende av klassificering är och de utrustade med aktiv passagekontroll och larm. Behörigheterna är begränsade utifrån roll och ansvar och finns dokumenterade i passersystemet. Olika behörigheter gäller för kontorsutrymmen, serverhallar och noder. I nödsituation

kan dörrar öppnas med nyckel som finns hos ett ytterst begränsat antal medarbetare, vaktbolaget och räddningstjänsten.

Som en del av vår granskning har vi fysiskt inspekterat datahallen i ITSAM-huset i Kisa för att verifiera uppgifterna om de skyddsmekanismer som finns och kan konstatera att ovan beskrivning stämmer överens med faktiska förhållanden. Vi har även kontrollerat vilka personer som har access till datahallen och konstaterat att datahallen kräver en särskild behörighet i systemet till vilken passerkort är kopplad.

3.3.1. Vår kommentar och bedömning

Vår sammanfattande bedömning är att det finns ett tillräckligt skydd mot fysisk åverkan på IT-resurserna i form av de skyddsmekanismer som beskrivs ovan. Det saknas dock idag brandsläckningsutrustning i datahallen i Kisa och vår rekommendation är att ITSAM säkerställer att den upphandling som nu pågår slutförs som planerat och att utrustningen installeras så snart som möjligt.

Access till datahallen kräver en särskild behörighet i systemet vilken säkerställer att endast behöriga personer kan ha åtkomst till datahallen. Det är även ett begränsat antal personer som har den särskilda behörigheten.

3.4. Det finns ändamålsenligt skydd mot obehörigt intrång i IT-miljön samt rutiner för att hantera attacker?

ITSAM har installerat tekniska skydd för att förhindra obehörigt intrång i IT-miljön samt för att förhindra andra typer av skadliga virusattacker. Vi har i vår genomgång identifierat skydd på ett antal olika nivåer, med olika syften beroende på vad man vill skydda sig mot.

Det tekniska skyddet som appliceras och används inom Kommunalförbundet ITSAM är:

- **Identifierings- och autentiseringskontroll** – hanterar inloggningskontroller av användare som ska logga in i IT-miljön. Styr om och vilken access användaren får till system och information i IT-miljön.

- **Kryptering av vilande data såsom filer etc.** – hanterar kryptering av känslig data som lagrats i arkiv/filer. Styrs av en dokumenterad krypteringspolicy.

- **Kryptering av data i rörelse såsom VPN, trådlös uppkoppling etc.** – hantering av krypterad data som används i någon form av process. Inom kommunalförbundet finns möjlighet att kryptera datatransmission data med hjälp av certifikat.

- **Antivirusskydd -** Inom kommunalförbundet ITSAM tillämpas två nivåer för skydd mot skadlig kod; 1) Skydd mot skadlig kod på slutanvändares utrustning såsom datorer etc. samt 2) Skydd mot skadlig kod i perimeterskyddet, dvs i organisationens centrala brandväggsmiljö.

- **Brandväggsskydd -** Förutom antivirusskydd appliceras ett komplext regelverk vilka anslutningar som får eller inte får kommunicera med andra enheter eller datanät. Det finns även ett DDoS-skydd för att förhindra överbelastningsattacker mot IT-miljön.

Som ett led i vår granskning har vi verifierat ovan skyddsmekanismer genom intervju med säkerhetsansvarig samt genom inhämtande av teknisk dokumentation och dokumentation som beskriver hur ITSAM implementerat dessa skydd. All aktivitet loggas och kan följas upp, men det finns dock idag inget aktivt övervakningssystem som larmar vid en potentiell attack.

3.4.1. Vår kommentar och bedömning

Vår sammanfattande bedömning är att ITSAM har ändamålsenligt skydd mot obehörigt intrång i IT-miljön. Detta i form av autentiseringssystem för inloggning till generell IT-miljö samt applikationer, samt även i form av virusskydd och brandväggar som skydd mot skadliga attacker.

Vi har noterat att det saknas ett aktivt övervakningssystem som larmar vid försök till obehörigt intrång, det anses dock ej vara nödvändigt då det ej är en särskilt utsatt verksamhet.

3.5. Det föreligger god intern kontroll vad gäller att ge, ändra och ta bort behörighet till IT-miljön

ITSAM ansvarar för tilldelning av behörighet till den generella IT-miljön samt till kommungemensamma system. Vad gäller förvaltningsspecifika system så tilldelas behörighet av systemansvarig ute i verksamheten.

Tilldelning, ändring och borttag av behörighet sker via webformulär på ITSAM:s webportal, till vilken endast chefer och deras administratörer/assistenter har behörighet. Ansvarig chef fyller i personnummer samt vilka system användaren ska komma åt och behörighetsansökan tas emot av ITSAM servicedesk. Systemet gör automatiskt en körning av personnummer mot Skatteverket och identifieras inget avvikande skapas ett AD-konto med tillhörande access utifrån det som beställaren fyllt i. Beställaren kan endast välja access utifrån det område denna tillhör. Vid ändring eller skapande av konto får behörig chef per automatik ett mejl om att så skett. Det är således en automatisk process utan direkt inblandning från ITSAM.

Vi har granskat rutinen för behörighetsadministration genom att inspektera befintlig dokumentation samt genom test av rutinen för tilldelning av behörighet. Test har utförts genom ett slumpmässigt urval av 20 användare i IT-miljön och verifiering av att dessa användares tilldelning har föregåtts av ett formellt godkännande av ansvarig chef. För samtliga kommuner, förutom Vimmerby, sker det formella godkännandet i Webportalen genom att beställaren har den aktuella behörigheten för detta. Krav finns att beställaren ska kryssa i en ruta där denne bekräftar att kontoinnehavaren har läst igenom policy och information för användande av kontot. Vid beställning av konto i Vimmerby kommun skickar beställaren en fysisk beställning med underskrift där ITSAM:s servicedesk sedan skapar kontot. Stickproven utfördes slumpmässigt med tio stickprov av användare i Åtvidabergs kommun, fem stickprov av användare i Boxholm kommun och fem stickprov av användare i Kinda kommun. Genom att kontrollera användaren mot logg för senaste ändringen av kontot kontrollerade vi att den person som gjort ändringen hade rätt behörighet att göra detta. Samtliga konton hade skapats av behöriga användare.

Vår granskning visar att processen är formaliserad men inte finns tydligt dokumenterad vad gäller hur behörighetsadministrationen ska hanteras av ITSAM.

3.5.1. Vår kommentar och bedömning

Våra tester av rutinen för behörighetstilldelning visar att systemet sätter begränsningar i behörighet och att endast behörig person kan skapa ett konto.

Det finns en etablerad rutin för tilldelning/ändring/borttag av behörighet, däremot finns ingen tydligt dokumenterad instruktion som beskriver hanteringen. Det bör tas fram för att tydliggöra den process som följs idag.

2016-08-18

Martin Westholm
Projektledare/kvalitetsansvarig
PwC