www.pwc.se

Revisionsrapport

Styrning och ledning av IT och informationssäkerhet

Sollefteå

Göran Persson-Lingman

Robert Bergman

Mars/2017

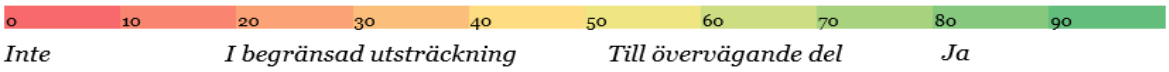
pwc

Innehåll

Sammanfattning

På uppdrag av de förtroendevalda revisorerna har PwC granskat om kommunens interna styrning och kontroll av hantering av IT och informationssäkerhet är tillfredställande.

Revisionell bedömning har skett utifrån följande skala/gradering:



Vår sammanfattande bedömning är att den interna styrningen i begränsad utsträckning är tillfredställande och att den interna kontrollen är bristande. Bedömningen grundar sig på följande:

Kontrollmål	**Bedömning**
Aktuella styrande dokument som berör kommunens informationssäker finns och är tillräckligt kommunicerade till de roller som berörs.	*I begränsad utsträckning*
Det sker uppföljning att styrande dokument som berör hantering av IT är kända och efterlevs.	*Inte*
Ansvar och roller avseende hanteringen av IT är tydlig (ansvar och roller).	*I begränsad utsträckning*
IT-relaterade risker analyseras på ett systematiskt sätt	*I begränsad utsträckning*
Det finns en tillfredställande övergripande behörighetshantering	*Till övervägande del*
Användare har tillräcklig kunskap för en effektiv och säker användning av IT.	*Till övervägande del*
Förekomsten av störningar och problem då IT används är rimliga.	*Till övervägande del*
Det finns en tillfredställande hantering av Backuper.	*I begränsad utsträckning*

Iakttagelser och bedömningar av respektive kontrollmål redovisas närmare i rapporten.

I syfte att utveckla verksamheten lämnas följande rekommendationer:

- Kommunstyrelsen bör säkerställa att styrande dokument är aktuella, kommunicerade och tillämpade i tillräcklig grad. Detta innebär bl.a. att uppföljning och utvärdering av IT och informationssäkerheten utvecklas samt att ansvar och roller förtydligas.

- Kommunstyrelsen bör utveckla arbetet med riskanalys för kommunens IT/informationssäkerhet bl.a. i syfte att tydliggöra vilka hot och brister som finns i kommunens IT-miljö och informationssäkerhet (inklusive backuphantering) samt för att få en överblick över kommunens system och dess väsentlighet.

1. Inledning

1.1. Bakgrund

Kommunens revisorer har med hänsyn till väsentlighet och risk bedömt det angeläget att genomföra en granskning avseende IT hanteringen och informationssäkerheten inom kommunen.

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 samt sprida och öka tillgängligheten till information med mera. IT är en förutsättning för att verksamheten skall fungera på ett effektivt och säkert sätt.

Brister kring hantering av IT och användning av IT i olika aktiviteter medför även risker att verksamheten och deras kunder och intressenter kan påverkas negativt.

En effektiv hantering av IT påverkas av flera olika faktorer, till exempel bra processer[1] inklusive organisation och ansvarsfördelning, tillräcklig infrastruktur, IT-systemen, användares kunskap, IT-funktionen och andra IT-resursers förmåga.

Informationen måste skyddas mot obehörig åtkomst samtidigt som den ska finnas tillgänglig och vara tillförlitlig - *rätt information i rätt tid och för rätt personer*. Detta innebär t ex att det krävs ett kontinuerligt informationssäkerhetsarbete.

1.2. Syfte och Revisionsfråga

Syftet med granskningen är att bedöma om den interna styrningen och kontrollen av hantering av IT är tillfredställande.

- Aktuella styrande dokument som berör kommunens informationssäker finns och är tillräckligt kommunicerade till de roller som berörs.
- Det sker uppföljning att styrande dokument som berör hantering av IT är kända och efterlevs.
- Ansvar och roller avseende hanteringen av IT är tydlig (ansvar och roller).
- IT-relaterade risker analyseras på ett systematiskt sätt *(innefattar t ex att man vet hur kritiskt systemet är för verksamheten (avbrott, informationen känslig m.m.)*
- Det finns en tillfredställande övergripande behörighetshantering *(till det gemensamma nätet, yttre och inre skydd)*
- Användare har tillräcklig kunskap för ett effektiv och säker användning av IT. *(innefattar om det sker utbildning inom informationssäkerhet)*
- Förekomsten av störningar och problem då IT används är rimliga.
- Det finns en tillfredställande hantering av Backuper.

[1] T ex processer för att kommunicera verksamhetskraven, systematiskt analysera risker, uppföljning och hantering av avvikelser. Hantering av inköp och att förändringar sker kontrollerat.

1.3. Revisionskriterier

- Kommunallagen
- Offentlighet och sekretesslagen
- Personuppgiftslagen
- Arkivlagen
- Kommuninterna styrdokument

1.4. Metod och avgränsning

Granskningen har skett genom dokumentanalys, intervjuer med IT-chef, kommunchef, verksamhetschefer för grundskolan, individ- och familjeomsorgen samt äldreomsorgen. Vidare har intervjuer genomförts med systemförvaltare inom ovan nämnda verksamheter samt att en enkät har ställts till kommunens användare, dvs. samtliga medarbetare.

I tid är granskningen avgränsad att i huvudsak gälla kalenderåret 2016. Verksamheter som främst berörs i granskningen är förutom kommunledningsförvaltningen även utbildning, IFO och äldreomsorg/omvårdnad.

2. Iakttagelser och bedömningar

2.1. Styrande dokument

En förutsättning för att kunna kommunicera hur information ska hanteras i kommunen på ett säkert sätt och i enlighet med lagar och förordningar är att det finns dokumenterad styrning i form av planer, policys, regler och riktlinjer. Dessa styrande dokument behöver vara kända av användarna, dvs. medarbetare och brukar som använder kommunen system och utrustning. Av styrningen bör det vidare framgå vilka roller som finns och vilka ansvar som gäller för de som verkar inom kommunens IT-miljö. På detta sätt skapas förutsättningar till att rätt person har tillgång till rätt information, dvs. informationssäkerhet.

2.1.1. Iakttagelser – Styrande dokument

Kommunövergripande styrning

Granskningen visar att det finns en Policy för informationssäkerhet upprättad (KF 2011-04-26). Policyn innehåller bl.a. en allmän beskrivning av policyns roll i informationssäkerhetsarbetet, mål samt revidering och uppföljning. Av intervju med IT-chef framgår att informationssäkerhetsplanen inte är aktuell, att informationssäkerhetssamordnare inte har utsetts och att dokumentet hänvisar bl.a. till dokument som inte finns upprättade.

Vidare framgår av intervju med IT-chef att kommunens strategi utgår från olika typer av rutiner och regler som finns upprättade och publicerade på kommunens intranät. Från intervjuer med företrädare för verksamheterna konstateras att det kan vara svårt att hitta dokumenten på kommunens intranät.

Resultatet av enkätundersökning visar att ca 63 % av de som svarat på enkäten instämmer helt eller i huvudsak till påståendet att de känner till vilka policys och riktlinjer som finns kring IT. De som *inte instämde* i påståendet uppmanades att utveckla detta i fritext. Fritextsvaren framgår bl.a. att de inte känner till eller har tagit del av policys och riktlinjer och/eller att de är inaktuella.

Vidare framgår att ca 43 % instämmer till viss del eller inte alls till att policys och riktlinjer kring IT och informationssäkerhet är tillräckligt kommunicerade inom kommunens organisation.

Verksamhetsspecifik styrning

Styrning som är specifik för respektive verksamhet är främst *Verksamhetsplan för pedagogiskt utvecklingsarbete med IT som stöd 2015-2017* som gäller för- och grundskolan samt gymnasieskolan. Planen är fastställd av barn- och skolnämnden (2014-11-17) och syftar till att ge stöd i användningen av datorer i verksamheten. Planen ska även vara ett stöd vid inköp och utveckling av utrustning.

Inom äldreomsorgen har främst riktlinjer och rutiner för behörigheter upprättats. Av intervju med systemförvaltare framgår att rutinerna berör chefer och att det är dessa som rutinerna kommuniceras till, främst när det har konstaterats att rutinerna inte har följts.

Övriga verksamheter har inte upprättat motsvarande styrande dokument. Vi kan vidare konstatera att det saknas en samlad bild över vilka dokument som finns.

2.1.2. Iakttagelser uppföljning av styrande dokument

Av policy för informationssäkerhet framgår hur uppföljning och revidering ska ske, bl.a. att policys och instruktioner ska vid behov revideras samt att regler efterlevs.

Granskningen har inte kunnat styrka att det sker någon uppföljning av tillämpning och efterlevnad av kommunövergripande styrande dokument för hantering av IT. När det gäller styrande dokument i form av riktlinjer, mallar och regler sker heller ingen systematisk uppföljning i vilken utsträckning dessa tillämpas och efterlevs.

Den pedagogiska utvecklingsplanen ska följas upp och utvärderas inom ramen för det systematiska kvalitetsarbetet. Detta finns reglerat i planen och rapportering ska ske till utskottet för lärande och unga. Av intervju med kvalitetsutvecklare (biträdande verksamhetschef) framgår att detta inte har skett enligt plan utan kommer ske under våren 2017. Detta beror främst på förändringar som skett inom organisationen. Tankar finns att löpande utvärdera vissa utvalda delar av utvecklingsplanen istället för att utvärdera hela planen vid ett tillfälle.

Tidigare år har det skickats ut enkät till personal inom skolan, vid nästa utvärdering av den pedagogiska utvecklingsplanen ska uppföljning ske genom att respektive rektor samtalar med sina arbetslag.

Resultatet av enkätundersökning visar att ca 41 % av respondenterna instämmer till viss del eller inte alls att det skett någon uppföljning av exempelvis efterlevnad av riktlinjer. Ca 43 % uppger att de saknar uppfattning eller vet ej om uppföljning har skett. Av fritextsvar framgår att arbetsplatsträffar är det huvudsakliga forumet för att fånga upp hur IT fungerar i verksamheterna. Många av svaret visar dock att det inte sker någon uppföljning.

2.1.3. Bedömning

Aktuella styrdokument som berör kommunens informationssäkerhet finns i begränsad utsträckning. Bedömningen baseras på att den policy som finns för området inte är aktuell.

Uppföljning av styrande dokument bedöms inte ske i tillräcklig utsträckning. Bedömningen baseras på att uppföljning av kommunövergripande styrning på området inte sker. Vidare tyder enkätundersökningen på att användarna tillfrågas i syfte att följa upp hur rutiner och riktlinjer efterlevs.

När det gäller skolans IKT-plan kommer denna att följas upp under våren 2017 och att det är reglerat i planen att regelbunden uppföljning ska ske. Enkätresultat indikerar på att uppföljningen är mer utvecklad inom skolans område.

2.2. Ansvar och roller

2.2.1. Iakttagelser – Ansvar och roller

Granskningen visar att roller och ansvar främst har reglerats i kommunens informationssäkerhetspolicy. Av policyn framgår bl.a. att kommunchefen är övergripande ansvarig för kommunens informationssäkerhetsarbete som bl.a. ska utse en informationssäkerhetsansvarig, direkt underställd kommunchefen. Vidare framgår att IT-chefen ansvarar för att uppfylla kommunens kontinuitetsplan (informationssäkerhet, kontinuitet och drift) för IT-stödet. Av policyn beskrivs även systemägarens respektive systemförvaltarens roller översiktligt.

Policyn hänvisar vidare till olika instruktioner för mer detaljerad beskrivning av roller. Som nämnts under 2.1.1 saknas dokument som policyn hänvisar till i stor utsträckning. Vår granskning visar vidare att policyn är i behov av uppdatering bl.a. utifrån att kommunens organisation har förändrats och att funktioner inte längre finns kvar.

Av intervju med IT-chef framgår att tydlig dokumentation över vilka som är systemägare och systemförvaltare saknas i dagsläget.

Intervjuer med systemförvaltare visar bl.a. att det inte upplevs vara tydligt vad som ska ingå i rollen som systemförvaltare.

Enkätresultatet visar att 52 % instämmer helt eller i huvudsak till påståendet att de känner till vem som är systemansvarig eller systemförvaltare för de system som de använder mest.

Ca 56 % av respondenterna i enkätundersökningen instämmer helt eller i huvudsak att det är tydligt vem som har det övergripande ansvaret för IT-hanteringen inom kommunen. Ca 52 % instämmer helt eller i huvudsak att det är tydligt vem som ansvarar för olika *områden* inom respektive förvaltning. Fritextsvar visar att flera kontaktar IT-enheten vid problem då de inte med säkerhet vet vem som är ansvarig eller kan hjälpa till.

53 % upplever att det är tydligt (helt eller i huvudsak) vem som ansvarar för kommunens gemensamma system. Av fritextsvar framgår bl.a. följande;

- *”Det är otydligt vem man specifikt ska vända sig till”*
- *”Varför olika support beroende på verksamhet?”*
- *”Saknas dokumentation kring vem/vilka som sköter systemen”*
- *”Organisationsförändringar har gjort det otydligt vem man ska vända sig till”*

Sker kommunikationen på ett tillräckligt sätt?
En förutsättning för att verksamheternas system ska fungera på ett ändamålsenligt sätt är det viktigt att det finns kanaler och/eller forum för att kommunicera utvecklingsbehov och förväntningar kring varandras roller.

Vår granskning visar att det i dagsläget inte finns något forum med fokus på utveckling och IT. Idag hanteras dessa frågor främst i ledningsgruppsmöten och mellan IT och systemförvaltarna. Av intervju med IT-chef framgår att ett forum för utvecklingsfrågor, IT-råd, planeras att inrättas under 2017. Planen är att representanter från verksamheterna ska finnas med och att rådet bl.a. ska jobba med uppföljning och utvärdering av verksamheternas IT-hantering.

Vidare kan vi konstatera att inom verksamheterna har förekommit att hanteringen av IT har diskuterats i bl.a. ledningsmöten och på chefsdagar.

Resultatet från enkätundersökningen visar att 58 % av respondenterna upplever att det är tydligt vilket stöd som IT-enheten kan erbjuda.

2.2.2. Bedömning

Ansvar och roller avseende hanteringen av IT bedöms i begränsad utsträckning vara tydlig. Bedömningen baseras på att roller till viss del har reglerats i olika styrande dokument. Dock visar både intervjuer och enkätundersökning att det finns roller som inte är tydligt utformade samt att ansvar för support och förvaltning av olika system inte har reglerats och kommunicerats på ett tillräckligt sätt.

2.3. Riskanalys

2.3.1. Iakttagelser - Riskanalys

I policy för informationssäkerhet framgår mål för informationssäkerhetsarbetet. Bl.a. ska hotbilden för varje enskilt informationssystem av vikt analyseras fortlöpande. Granskningen har inte kunnat verifiera att detta har skett, exempelvis genom en dokumenterad analys. Av intervju med IT-chef framgår att vid större förändringar sker riskanalyser och tester. Om det är nödvändigt har IT-enheten tagit hjälp utifrån, exempelvis med projektledning för att införa Windows 10 i organisationen.

Granskningen visar att en riskanalys för Google Apps, som används inom skolans verksamheter, har upprättats 2014-10-06. Analysen innehåller en lista på olika scenarier samt bedömningar av konsekvenser om dessa skulle inträffa. Vidare finns slutsatser utifrån den analys som genomförts.

Utifrån vår granskning kan vi konstatera att varken kommunstyrelsen eller kommunledningen har efterfrågat någon analys av de risker som finns i kommunens IT-hantering.

Granskningen har i övrigt inte kunnat styrka att det skett någon prioritering av vilka system eller ärenden som bör prioriteras vid ett eventuellt avbrott. Av intervju med bl.a. IT-chef framgår att det inte finns någon dokumenterad prioritering av kommunens olika system men att det är främst system inom socialförvaltningens verksamheter som i första hand prioriteras vid eventuella avbrott eller störningar. IT-enheten har koll på kritiska tider, exempelvis när utbetalning av löner ska ske, vilket kan spelar in vilka system som ska prioriteras för stunden.

I enkätundersökning som användarna i kommunen fått möjlighet att besvara framgår att ca 52 % av respondenterna till *viss del eller inte alls instämmer* i påståendet att IT-relaterade risker analyseras i verksamheterna. 32 % har svarat att de *inte vet eller inte har någon uppfattning*. Av fritextsvar där respondenterna fick möjlighet att beskriva hur risker analyseras och vilka förbättringsbehov de såg framkom bl.a. följande;

- *Riskbedömning sker inom ramen för internkontroll*
- *Förslag på åtgärder utifrån internkontroll har inte genomförts*
- *Låg prioritet att jobba med IT-relaterade risker*
- *Riskbedömning hur störningar påverkar undervisningen sker*
- *Informationssäkerhet diskuteras inom vissa verksamheter*
- *Det finns brister i kommunikationen mellan verksamheten och IT*

Inom ramen för vår granskning ska vi bedöma om användarnas kunskap är tillräcklig för att kunna använda system och utrustning samt hantera information på ett effektivt sätt. Av enkätundersökning och intervjuer med bl.a. systemförvaltare framgår bl.a. följande;

- Ca 80 % instämmer helt eller i huvudsak till påståendet att de har tillräcklig kunskap och datorvana för att hantera dator och andra hjälpmedel på ett effektivt sätt.
- Ca 90 % instämmer helt eller i huvudsak till att kunskap och datorvana är tillräcklig för att kunna utföra arbetsuppgifter med hjälp av de program som används mest.
- att introduktion till olika system är ett utvecklingsområde

Respondenter som i olika grad inte instämde i ovan påståenden fick möjlighet att i fritext kommentera detta. Av dessa kommentarer framgår bl.a. att utbildning i både program och utrustning är ett utvecklingsområde. Ca 30 % instämmer till viss del eller inte alls i påståendet att de har fått tillräcklig introduktion/utbildning för att kunna jobba effektivt.

Däremot framgår det av intervju med IT-chef att användarnas kunskaper och rutiner för att använda utrustning och system på ett säkert sätt är låga. Med detta menas exempelvis att användarna loggar ut/låser sin dator regelbundet för att hindra obehöriga åtkomst till system eller information.

Av fritextsvar från enkäten framgår bl.a. följande:

- Rutiner är okända
- Rutiner finns men tillämpas inte
- Glömmer logga ut/låsa datorn
- Användare förlitar sig på att utloggning/skärmsläckning sker automatiskt

Inom ramen för den enkät som användarna fått möjlighet att besvara framkommer följande angående förekomsten av störningar och problem när IT-används.

- 79 % upplever, helt eller i huvudsak, att den generella driftsäkerheten är god
- 71 % upplever, helt eller i huvudsak, att driftsäkerheten i system är tillräckligt god för att inte kunder/brukare/elever ska påverkas
- 67 % upplever att de förlorar mindre än 20 minuter per vecka pga. avbrott, väntetider och problem med den dator de arbetar med.
- Ca 80 % upplever, helt eller i huvudsak, att dator och annan kringutrustning är tillräckligt bra för att kunna arbeta effektivt och säkert.

2.3.2. Bedömning

IT-relaterade risker analyseras endast i begränsad utsträckning på ett systematiskt sätt. Bedömningen baseras på att vår granskning inte kunnat verifiera att verksamheten gjort någon dokumenterad riskanalys, att riskanalys främst sker vid större förändringar samt att intervju och enkät indikerar på att detta inte sker regelbundet. I sammanhanget noteras att det finns viss systematik inom skolans verksamheter när det gäller kartläggning av risker.

Användarnas kunskaper för ett effektivt och säkert användande av IT bedöms till övervägande del vara tillräcklig. Bedömningen baseras på enkätresultatet som indikerar på att användarnas generella kunskaper är goda. Dock finns utvecklingsområden i form av introduktion och utbildning när det gäller användning i system samt hur säker användning av utrustning och system ska säkerställas.

Vidare bedömer vi att förekomsten av störningar och problem då IT används till övervägande del är rimliga.. Bedömningen baseras på enkätresultat som visar att användarna till övervägande del upplever att driftsäkerheten är god och att datorer och annan utrustning är tillräckligt bra för att arbetet ska kunna utföras effektivt och säkert.

2.4. Behörighetshantering och backuper

2.4.1. Iakttagelser - Behörighetshantering

Granskningen visar att när en ny användare ska få behörighet till system i kommunen sker det via en beställning i E-summit av arbetsledare till IT-avdelningen. IT-avdelningen går sedan in i varje system som den nya användaren ska få tillgång till och ger där behörighet. Samma procedur gäller när det ska ske förändringar i en användares behörigheter. Anställande chef ansvarar för att ge respektive medarbetare rätt typ av behörighet.

I samband med anställning tilldelas användaren ett s.k. AD-konto som gör det möjlig för användaren att logga in på kommunens nät. Vid avslutad anställning stängs AD-kontot automatiskt ned två veckor efter anställningsavtalets utgång. Behörigheter till särskilda system behöver dock stängas ned manuellt. Av intervju med tekniker inom IT-avdelningen förekommer det att detta inte hanteras på rätt sätt, vilket kan medföra risk för obehörigt intrång.

Lösenordshantering är ett viktigt område för att säkerställa rätt behörighet. Av intervju med tekniker inom IT-avdelningen framgår att det finns vissa krav på hur lösenorden ska vara utformade och att lösenorden till AD-kontot byts ut varje månad. Många frågor som kommer in till Helpdesk handlar om lösenord, vilket indikerar att användarna inte tagit till sig av de instruktioner som finns, exempelvis hur lösenord ska formuleras.

Vidare konstateras utifrån intervju att det finns fungerande rutiner/sätt att säkerställa att anställda inom kommunen får behörighet till kommunens nät utifrån. Däremot är ett utvecklingsområde att se över rutinerna för att ge behörighet till externa, exempelvis konsulter och extern support, som ska in i kommunens system.

När det gäller attacker utifrån på kommunens nät kontaktas i första hand kommunens internetleverantör för att stänga ner uppkopplingen. Någon dokumenterad rutin har inte upprättats som närmare beskriver hur detta område ska hanteras.

2.4.2. Bedömning – Behörighetshantering

Det finns till övervägande del en tillfredställande övergripande behörighetshantering. Bedömningen baseras på att ansvarig för tilldelning av behörigheter är tydligt, det finns krav på lösenord samt rutiner för att säkerställa att anställda kan få tillgång till nätverk och system exempelvis från hemmet. Vi kan dock konstatera att rutiner för att säkerställa att behörigheter återtas, att säkerställa externa användares behörigheter samt nå ut med information till användarna kring, exempelvis lösenord, är områden som behöver utvecklas.

2.4.3. Iakttagelser - Backuper

Kommunens hantering av backuper bygger främst på följande tekniker:

- *Filbackuper*
- *Backuper av databaser*
- *Exporter av filer*
- *Kloning av servrar*

Av intervju med tekniker på IT-avdelningen framgår att servar som innehåller information från backuper av systemen förvaras i två separata kylrum. Vidare framgår att en server som behöver återställas är åter i bruk inom ca 15 minuter. Vid större fel har kommunen supportavtal som säkerställer att tekniker kan vara på plats nästkommande dag. Verksamheterna har signalerat att de klarar ett avbrott upp till tre arbetsdagar.

Backuper av systemen sker varje natt och IT-avdelningen får då rapport om något fel har inträffat, exempelvis att det saknats åtkomst till den information som ska kopieras.

Granskningen visar att verksamheternas krav på säkerhetskopiering och backuphantering inte har dokumenterats, dvs. hur långt tillbaka vill verksamheterna ha möjlighet att kunna återskapa information. Av intervju med tekniker inom IT-avdelningen framgår att information sparas ett år tillbaka, men att det finns signaler om att behov finns att kunna gå ännu längre tillbaka. Det finns heller ingen tydlig förteckning över vilka system som det sker backuper. Av intervju med tekniker inom IT-avdelningen sker backuper på alla system/servar. Detta kan medföra att det blir platsbrist på servrar vilket i sin tur kan leda till onödiga investeringar.

Som vi konstaterat tidigare (se avsnitt 2.3.1) sker inte något systematiskt arbete med riskanalyser, dvs. vilka system är mest kritiska vilket är en förutsättning för att få information om det är nödvändigt att anpassa backuprutinerna. Kommunicering kring brister och förbättringar sker främst mellan tekniker och systemförvaltare.

2.4.4. Bedömningar – Behörighets- och backuphantering

Backuphanteringen bedöms i begränsad utsträckning ske på ett tillfredställande sätt. Bedömningen baseras på att olika tekniker används för att genomföra backuper av systemet. Däremot saknas en tydlig överblick över verksamheternas krav och vilka system som behöver backup. Vidare sker inte utvärdering/analys över vilka system som är mest kritiska och därmed i störst behov att göra backuper på.

2017-03-01

Anneth Nyqvist	***Göran Persson-Lingman/Robert Bergman***
Uppdragsledare	*Projektledare*