Kommunrevisorerna granskar

UMEÅ KOMMUN
Granskning av IT- och informationssäkerhet.

Sammanfattning

Bakgrund

På uppdrag av de förtroendevalda revisorerna i Umeå har EY genomfört en granskning av IT- och informationssäkerhet vad gäller policyer, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå i kommunen samt specifikt för ett antal verksamhetskritiska system och hantering av molntjänster. Syftet med revisionsprojektet har varit att granska på vilket sätt kommunen jobbar för att upprätta en god IT-säkerhet. Granskningen har gjorts mot utvalda delar av Myndigheten för samhällsskydd och beredskaps ramverk för informationssäkerhet, BITS.

Övergripande slutsatser

Av samtliga 71 granskningspunkter är fördelningen av bedömningarna följande:

Kontrollen finns och fungerar tillfredsställande:	66,2%
Kontrollen finns och fungerar delvis:	11,3%
Kontrollen finns ej eller fungerar ej tillfredsställande:	21,1%
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	1,4%

Iakttagelser

Nedan listas våra mest väsentliga iakttagelser och rekommendationer. Fullständiga iakttagelser och rekommendationer återfinns i kapitel 4.

#	Iakttagelse och rekommendation	Prioritet
1.	Kommunens informationssystem har ej klassats avseende hur kritiska de är	Hög
2.	Kommunen har ej genomfört systemsäkerhetsanalys eller fastställt längsta acceptabla tid för avbrott för samtliga system	Hög
3.	Inga penetrationstester genomförs regelbundet	Hög
4.	Kommunen har ingen rutin för hur utomstående leverantörers tjänster följs upp	Hög
5.	Kommunen har ej satt upp regler för åtkomst/tillträde till tredjepart till information eller informationssystem	Hög
6.	Brister i avtal med leverantörer	Hög

Innehåll

1. Bakgrund

Idag bedrivs så gott som all verksamhet i en kommun med någon form av datoriserat stöd. Stödet har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet och antalet olika programvaror är stort. För att uppnå målen för en kommuns verksamhet krävs att informationen i verksamhetsstödet är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

Inom Umeå kommun hanteras IT-verksamheten av IT-funktionen. Tekniska nämnden ansvarar för den verksamhet som bedrivs inom IT-funktionen. IT-funktionens uppdrag är att med hög kompetens, delaktighet och god serviceanda erbjuda ett brett utbud av IT-tjänster som stödjer arbetet för välfärd och ett gott liv i Umeå. Detta görs i form av:

- Strategiskt stöd: IT-funktionen levererar modeller, principer, tekniska plattformar, informationssäkerhet och följer upp IT-verksamheten.
- IT-tjänster: Tjänsterna är utredningar, processkartläggningar, projektledning, kravspecifikationer/förberedelser inför upphandling, förvaltning och systemutveckling, installation, drift och support av verksamhetssystem, infrastruktur och arbetsplats-utrustning. Servicenivå och innehåll i tjänsterna fastställs i överenskommelser med kommunens verksamheter.
- Telefonitjänster: IT-funktionen levererar en telefonifunktion som omfattar teknisk plattform, telefonist- och upplysningstjänst till kommunens verksamheter, bolag, stiftelser och Umeåregionens kommuner.

Under 2013 genomförde revisorerna en förstudie med syftet att beskriva ett antal delområden inom Umeå kommuns IT-verksamhet, för att därmed skapa ett underlag till revisorernas risk- och väsentlighetsanalys. I förstudien noterades utvecklingsområden avseende IT-säkerhet och i hanteringen av molntjänster. Flera av verksamheterna hanterar direkt konfidentiell information där IT-säkerheten är av stor vikt.

Revisorerna har i sin riskbedömning för 2015 identifierat en risk avseende att Tekniska nämnden inte fullt ut säkerställt en fungerande IT-säkerhet varför EY kontaktats för att genomföra en granskning.

1.1 Syfte

Syftet med granskningen har varit att bedöma hur effektivt Umeå kommun arbetar med IT-säkerhet i dag. För att besvara granskningens syfte och bedöma nämndernas rutiner har granskningen utgått från följande revisionsfråga:

- Hur ändamålsenlig är IT-säkerheten för de behov kommunens verksamhet har?

1.2 Metod

Revisionsfrågan har besvarats genom en granskning mot så kallad god praxis inom IT-säkerhetsområdet. Granskningen har gjorts mot utvalda delar av Myndigheten för samhällsskydd och beredskaps ramverk för IT- och informationssäkerhet, BITS. Ramverket bygger på den svenska och internationella standarden ISO/IEC 27001. EY har genomfört en övergripande kartläggning av rutiner och kontroller samt granskat IT-säkerheten specifikt för två verksamhetskritiska system.

Granskningen genomfördes genom insamling av bakgrundsinformation inför intervjuer. Relevant information utgjordes av befintliga styrande dokument, instruktioner, avtal etc. Därefter genomfördes intervjuer med relevant personal för djupare förståelse för övergripande rutiner och kontroller. Under granskningen har dock inga stickprovstester utförts i syfte att granska efterlevnad av kommunens interna regler och processer. Under granskningen intervjuade vi:

- IT-chef
- IT-säkerhetsansvarig
- Systemansvarig och systemförvaltare för de två utvalda systemen
- IT-tekniker

Därefter har denna rapport utformats som underlag för revisorernas bedömning av hur ändamålsenlig IT-säkerheten är i kommunen. Rapporten beskriver vår bedömning av kommunens mognadsgrad per huvudområde, inkluderat iakttagelser och rekommendationer.

Följande huvudområden har granskats och utvärderas:

- Säkerhetspolicy
- Säkerhetsorganisation
- Hantering av tillgångar
- Personal och säkerhet
- Styrning och kommunikation av drift
- Styrning av åtkomst
- Systemutveckling och underhåll
- Incidenthantering
- Kontinuitetsplanering
- Efterlevnad
- Hantering av information i molnet

1.3 Avgränsningar

Granskningen avser, för de systemspecifika revisionsfrågorna, de två verksamhetskritiska systemen Treserva och Lärum. Systemen valdes ut i samråd med IT-chef och valet av system har därefter godkänts av kommunrevisorerna.

2. Granskning

2.1 IT-system

Kommunen har totalt ca 300 verksamhetssystem. De system som centralt inom Umeå kommun anses vara mest kritiska är:

Namn	Typ av system
Treserva	Verksamhetssystem för socialtjänsten
Lärum	Läroplattform
Heroma	Personalsystem
VMWare	Driftsystem

Nedan följer beskrivningar av de två system som valts ut för vidare granskning. För en lista på alla kommunens system hänvisas till kommunens IT-avdelning.

2.1.1 Treserva

Treserva är ett verksamhetssystem som används av socialtjänsten inom Umeå kommun. Systemet har ca 4 500 användare som arbetar inom socialtjänstens alla verksamhetsområden. Socialtjänsten använder systemet för alla typer av ärenden och därmed innehåller systemet stora mängder känslig information. Systemet har inför granskningen bedömts som kritiskt på grund av sitt innehåll av känslig information samt på grund av att en av kommunens viktigaste verksamheter är beroende av systemet.

Systemet är uppdelat i två delar, ett som rör individ- och familjeomsorg, och ett som rör vård och omsorg. I nära anslutning till granskningen genomfördes en större uppdatering av den del av systemet som rör vård och omsorg. Treserva är ett standardsystem som levereras av CGI.

2.1.2 Lärum

Lärum är en läroplattform för pedagoger, elever och vårdnadshavare på alla Umeå kommuns skolor. Lärum fungerar som ett pedagogiskt verktyg för pedagoger och elever, men möjliggör också kommunikation mellan pedagog, elev och vårdnadshavare. Plattformen innehåller känslig information såsom personuppgifter och individuella utvecklingsplaner och har valts ut för granskning på grund av att det innehåller viss känslig information samt på grund av att systemet är ett av de system vars information lagras i molnet.

Lärum är en standardlösning från Tieto. Under tidpunkten för granskningen implementerades systemet fortfarande på flertalet skolor i kommunen.

2.2 Granskningsprotokoll

Granskningspunkt		Kommentar	Utvärdering
1 Säkerhetspolicy			
1.1	Har kommunen en informations-/IT-säkerhetspolicy?	Kommunen har en informationssäkerhetspolicy. Policyn fastställdes 2009-04-27 och reviderades 2013-06-17. Dokumentet beslutas av kommunfullmäktige. Policyn beskriver övergripande omfattning, syfte och mål med informationssäkerhetsarbetet. Det finns ingen uppsatt rutin för regelbunden översyn av dokumentet.	Ja
2 Organisation av säkerheten			
2.1	Finns det en informationssäkerhetssamordnare/-funktion för informationssäkerhet?	Kommunen har en IT- och informationssäkerhets-samordnare i form av en IT-säkerhetssamordnare. Därtill har Umeå kommun en kommungemensam IT-samordning som består av tre personer, en för varje område inom kommunen. Kommunen är uppdelad i områdena Unga, Vuxna och Samhällsbyggnad.	Ja
2.2	Finns det utsedda systemägare för samtliga informationssystem?	Samtliga system i kommunen har en utsedd systemägare. Alla kommunens system finns registrerade i applikationen RegIT i vilken det framgår vem som är systemägare. Det är systemägarna som är ansvariga för att hålla informationen i listan uppdaterad. Kommunen arbetar även med att införa PM3 i syfte att tydliggöra rollerna för systemägare och systemansvarig. **Treserva** För systemet Treserva är kommunens socialdirektör systemägare. **Lärum** För systemet Lärum är kommunens skoldirektör systemägare.	Ja
2.3	Finns det utsedda systemansvariga för samtliga informationssystem?	Samtliga system i kommunen har en utsedd system-ansvarig. Som nämnts ovan finns kommunens samtliga system registrerade i applikationen RegIT, där det även framgår vem som är systemansvarig. **Treserva** Treserva har nyligen genomgått en stor uppdatering och systemets förvaltningsmodell är ej klar. Systemet har en tillförordnad systemansvarig som förvaltar systemet till dess att förvaltningsmodellen är fastställd. **Lärum** Lärum har tre systemansvariga, kallade systemförvaltare, som arbetar centralt på kommunen inom område Unga.	Ja
2.4	Har ansvaret för informationssäkerheten reglerats i avtal för informationsbehandling som lagts ut på en utomstående organisation?	Umeå kommun har avtal med de utomstående organisationer som hanterar information tillhörande kommunen. Ansvaret för informationssäkerhet regleras i de fall informationen som behandlas innehåller person-uppgifter. I de fallen skrivs ett personuppgiftsbiträdes-avtal. Enligt IT-chef och IT-säkerhetssamordnare föreligger dock en risk att detta ej är reglerat i äldre avtal. Vidare regleras inte ansvar för informationssäkerhet hos tredjepart utöver sådant som rör personuppgifter.	Delvis
3 Hantering av tillgångar			
3.1	Har samtliga informationssystem identifierats och dokumenterats i en aktuell systemförteckning?	Umeå kommuns samtliga informationssystem finns registrerade i applikationen RegIT. I RegIT registreras information om systemet, systemägare och systemansvarig samt när systemet togs i drift. Ansvaret för att hålla informationen i RegIT uppdaterad ligger på systemägaren.	Ja

Granskningspunkt		Kommentar	Utvärdering
3.2	Har organisationens informationssystem klassats avseende hur kritiska de är?	I RegIT framgår huruvida systemen innehåller personuppgifter. I samband med att ett system registreras kan den som registrerar välja att fylla i om systemet är verksamhetskritiskt eller ej. Det är dock inte obligatoriskt att fylla i detta. Det finns ingen övergripande formell klassificering avseende hur kritiska kommunens informationssystem är. Dock har gjorts en klassificering av vilken verksamhet som klassas som samhällsviktig och därmed ska prioriteras vid kris och katastrof. **Treserva** Systemet har ännu ej klassats avseende hur kritiskt systemet är. Klassning kommer att genomföras i samband med planerad systemsäkerhetsanalys i augusti. **Lärum** Lärum har ej klassats avseende hur kritiskt systemet är.	Nej
4 Personalresurser och säkerhet			
4.1	Finns det framtagna dokumenterade säkerhetsinstruktioner för användare?	Kommunen har tagit fram en informationssäkerhets-policy, regler och instruktioner för informationssäkerhet för verksamheten samt regler och instruktioner för informationssäkerhet för användare. Dessa dokument är tillgängliga på kommunens hemsida. Vidare kommuniceras dokumenten till nyanställda vid tidpunkten för anställningens början. Ansvaret för att informera användare ligger på respektive verksamhet. **Treserva** Användarna i Treserva får säkerhetsinstruktioner i de användarhandledningar och utbildningar som distribueras. **Lärum** För systemet Lärum finns säkerhetsinstruktioner för användare, såsom instruktioner om vad som är lämpligt att skriva och inte. Det finns också ett färdigt informationsbrev som skickas till vårdnadshavare.	Ja
4.2	Får inhyrd/inlånad personal information om vilka säkerhetskrav och instruktioner som gäller?	Inhyrd/inlånad personal får ta del av informations-säkerhetspolicy, regler och instruktioner för informations-säkerhet för verksamheten samt regler och instruktioner för informationssäkerhet för användare. Inhyrd/inlånad personal får även skriva på ett dokument där de intygar att de tagit del av de säkerhetskrav och instruktioner som gäller. **Treserva** Inlånad personal eller externa utförare får samma information om säkerhetskrav som vanliga anställda. Alla anställda inom socialtjänsten skriver dessutom under sekretessavtal. **Lärum** Inhyrd och inlånad personal såsom exempelvis vikarier får samma information som andra anställda. Om vikarien ska vara på plats i mindre än två veckor ges ingen tillgång i systemet utan all verksamhet sköts helt manuellt. Ska däremot vikarien vara där mer än två veckor skapas ett eget AD-konto och en egen användare i systemet.	Ja

Granskningspunkt		Kommentar	Utvärdering
4.3	Genomförs utbildningsinsatser inom informationssäkerhet regelbundet?	Kommunen genomför inga utbildningsinsatser inom informationssäkerhet regelbundet. Det är upp till verksamheten att initiera och efterfråga utbildning. Kommunen har tillgång till utbildningsmaterial att använda vid behov. **Treserva** Utbildningar inom informationssäkerhet genomförs ej regelbundet för användare i Treserva. Utbildningar genomförs då ett behov identifieras. Under granskningen noterades att utbildning i hälso- och sjukvårdslagen och social dokumentation genomförs vid nyanställning samt vid behov. **Lärum** Systemförvaltarna ansvarar för att utbilda representanter för de olika enheterna, som i sin tur ansvarar för att utbilda personalen på skolorna. Utbildning sker kontinuerligt. Under utbildning täcks vad man bör skriva och inte samt hur känslig information ska hanteras. Utöver detta berörs inte informationssäkerhet.	Nej
4.4	Har systemägaren definierat vilka krav som ställs på användare som får tillgång till informationssystem?	De krav som ställs på användare är definierade i dokumentet *Informationssäkerhet – Regler och instruktioner för användare*. Dokumentet täcker instruktioner kring åtkomst till information, användarens arbetsplats, hantering av information, Internet, e-post, incidenter samt avslutning av anställning. I de fall systemägaren ställer högre krav än vad som definierats i instruktionen definieras dessa per system. **Treserva** Krav på användaren utöver de som nämns i det kommungemensamma dokumentet *Informationssäkerhet – Regler och instruktioner för användare* finns i utbildningsmaterial för användare och chefer. Därtill måste alla användare skriva på ett sekretessavtal i samband med anställning. **Lärum** Lärum definierar krav på sina användare genom förväntansdokument för användare. I övrigt ställs inga krav på användarna.	Ja
4.5	Finns det användarhandledning för informationssystem att tillgå?	Inom kommunen har systemförvaltaren ansvar för att upprätta användarhandledning för informationssystem. **Treserva** För Treserva finns användarhandledning samt utbildningsmaterial för chef och medarbetare. **Lärum** Alla olika typer av användare i systemet har användarhandledning för systemet Lärum att tillgå.	Ja
4.6	Dras åtkomsträtten till information och informationsbehandlings-resurser in vid avslutande av anställning eller vid förflyttning?	Kommunen har ett gemensamt Active Directory (AD) som styr behörigheterna i kommunens samtliga system. Active Directory är integrerat med personalsystemet vilket innebär att då en anställd slutar och användaren tas bort ut personalsystemet inaktiveras användaren även i Active Directory. Då en anställd byter roll inom kommunen är det upp till respektive chef att säkerställa att användaren har rätt behörigheter. **Treserva** För Treserva är närmaste chef ansvarig för att göra avbeställning av behörigheter. Även då en användare byter roll i organisationen är det ansvarig chef som ansvarar för att omdirigera behörigheten. **Lärum** Om en anställd slutar är det upp till närmaste chef att göra en avbeställning av behörigheten. Även vid förflyttning är det upp till närmaste chef att beställa förflyttning av behörigheter. Behörigheter för elever och vårdnadshavare i Lärum bygger på vad som är registrerat i systemet ProCapita, som i sin tur bygger på uppgifter från folkbokföringsregistret. Kopplingar mellan lärare och elev görs av en elevregistrerare på respektive skola. När en klass byter årskurs försvinner läraren från klassen automatiskt.	Ja

Granskningspunkt		Kommentar	Utvärdering
5 Styrning och kommunikation av drift			
5.1	Finns det driftdokumentation för verksamhetskritiska informationssystem?	Umeå kommun hanterar driftdokumentation för samtliga system på den kommungemensamma drift-wikin. Drift-wikin är en SharePoint-lösning och innefattar all drifts-information för systemen. Nivån på driftsinformationen varierar beroende på systemets storlek och komplexitet. Vanligt är att drift-wikin innehåller information om daglig drift, lösning på tekniska problem, instruktioner för driftsättning samt kontaktuppgifter till systemansvariga. **Treserva** Driftdokumentation för Treserva finns i den kommun-gemensamma drift-wikin. **Lärum** Den driftdokumentation om Lärum som finns internt på Umeå kommun finns i den kommungemensamma drift-wikin. Majoriteten av driften sköts dock av leverantören Tieto.	Ja
5.2	Sker system-/programutveckling samt tester av modifierade system åtskilt från driftmiljön?	Testning av modifierade system sker åtskilt från driftsmiljön, förutom då förändringen är av mycket liten och ej väsentlig art. **Treserva** De förändringar som görs i Treserva är oftast omkonfigurationer och verksamhetsanpassningar. Tester genomförs i regel åtskilt från driftmiljön. Är det en mindre konfigurering sätts den ibland i drift utan testning. **Lärum** Leverantören Tieto genomför all utveckling och testar den internt. I de fall Tieto initierar en standardändring har kommunen ej möjlighet att testa denna utan ändringen går in som en programuppdatering. Då förändringen kommer av en förfrågan från Umeå kommun och är av större karaktär testas den av Umeå kommun innan driftsättning. Testning sker då skilt från driftmiljö.	Delvis
5.3	Finns rutiner för hur utomstående leverantörers tjänster följs upp och granskas?	Kommunen har inga gemensamma rutiner för hur utomstående leverantörers tjänster granskas och följs upp. **Treserva** Leverantören CGI lägger upp systeminformation i sin kundportal, vilken systemförvaltningen prenumererar på. Dock finns inga rutiner för formell uppföljning av CGI:s aktiviteter. **Lärum** Lärum har inga formella rutiner för att följa upp Tietos drift och hantering av Lärum. Vid incidenter krävs dock en incidentrapport in. Umeå kommun har även regelbundna möten med Tieto.	Nej
5.4	Godkänner lämplig personal (systemägaren) driftsättningar av förändrade informationssystem?	Förändringar godkänns i regel av systemansvarig innan driftsättning. **Treserva** Förändringar i Treserva godkänns av systemansvarig innan driftsättning. **Lärum** Umeå kommun äger inte funktionaliteten i Lärum och har således inte mandat att godkänna driftsättning av förändringar, om inte förändringen beställts av kommunen.	Ja
5.5	Finns det för både servrar och klienter rutiner för skydd mot skadlig programkod?	Umeå kommun har för samtliga servrar och klienter skydd mot skadlig programkod i form av virusskydd. Kommunen har även brandväggsskydd både utifrån och in, mellan nät samt på enskilda servrar. Kommunen använder sig av skydd mot skadlig programkod på klienterna. Därtill scannas all inkommande mail av tre antivirusmotorer.	Ja
5.6	Har organisations nätverk delats upp i mindre enheter (segmentering), så att en (virus) attack enbart drabbar en del av nätverket?	Organisationens nätverk har delats upp i mindre enheter för att minska risken för att en attack på en del av nätverket får inverkan också på övriga delar av nätet.	Ja

Granskningspunkt		Kommentar	Utvärdering
5.7	Genomförs säkerhetskopiering regelbundet?	Kommunen använder sig av två metoder för säkerhetskopiering. Dels tas klassisk filbackup på alla servrar. Backupperna lagras i ett separat backuprum. Därtill görs också en imagebackup, dvs en ögonblicksbild, av VMWare varannan dag. Utöver detta replikeras all data synkront mellan Umeå kommuns två datahallar vilket ger möjlighet till en s.k. failover, där man låter redundansservern ta över driften vid en större incident eller katastrof såsom brand.	Ja
5.8	Genomförs regelbundna tester för att säkerställa att informationssystem kan återstartas från säkerhetskopior?	Återläsningstester genomförs regelbundet. Frekvensen beror på vilket system det rör sig om. Kommunen använder sig av ett verktyg för att verifiera att det går att återläsa backuper automatiskt.	Ja
5.9	Finns det en aktuell förteckning över samtliga externa anslutningar?	Kommunen har en aktuell förteckning över samtliga externa anslutningar i form av kommunens nätverkskarta.	Ja
5.10	Saknas alternativa vägar vid sidan av organisationens brandvägg in till det interna nätverket?	Kommunens nätverk är uppsatt för att minska risken för att obehöriga kommer åt nätverket via andra vägar än kommunens brandväggar.	Ja
5.11	Finns det riktlinjer avseende förvaringstid för datamedia?	Datamedia förvaras i stadsarkivet i enlighet med gällande lagkrav.	Ja
5.12	Gäller det för e-postsystem och andra viktiga system att de är isolerade från externa nät? (DMZ) t.ex. genom någon form av brandväggsfunktion?	E-postsystem och andra viktiga system är isolerade från externa nät. Det går att logga in externt men servrarna är skyddade genom kommunens lösning.	Ja
5.13	Sparas revisionsloggar för säkerhetsrelevanta händelser?	Revisionsloggar för säkerhetsrelevanta händelser sparas. Loggarna sparas olika länge beroende på applikation/server/databas. För Active Directory gäller att skapande, borttag och förändringar i behörighetsgrupper, användarkonton (inklusive utelåsning, lösenordsbyte, datorkonton samt förändring av grupprincipobjekt) sparas för evigt. DHCP-loggar sparas i 100 dagar. **Treserva** För systemet Treserva sparas loggar för: ▸ vilken användare som har loggat in ▸ vilken användare (användarnamn) som registrerar och läser ärenden ▸ beslut ▸ insatser ▸ vilken användare (användarnamn) som läser text, skapar text, och ändrar text, ▸ för vilken brukare/klient (namn och personnummer) i dokumentationssystemet det sker, samt ▸ tidpunkt för ovanstående aktiviteter Enligt ett dokument i utkastformat ska systematisk kontroll av loggar genomföras månadsvis. Loggar för specifikt ärende eller användare kan också kontrolleras. Därtill kan chef beställa kontroll av loggning vid behov. Dokumentet ska fastställas av systemägare då det färdigställts. **Lärum** I Lärum loggas om en användare skriver något. Det loggas inte om en användare söker på något eller tittar på något. Loggarna sparas.	Ja
5.14	Finns det rutiner för incidenthantering?	Under dagtid hanteras incidenter av supporten. Supporten har en skriftlig rutin med flödesschema för hantering av incidenter. Dygnet runt finns beredskap för att hantera incidenter avseende kritisk infrastruktur samt nät. Ingen uppföljning görs av inträffade incidenter. Respektive system kan även ha separata rutiner för incidenthantering. **Lärum** Lärum har ett dokument i utkastformat, *Rutin vid driftstörning eller avbrott Lärum*, som beskriver hur olika typer av driftstopp ska hanteras.	Ja

Granskningspunkt		Kommentar	Utvärdering
6 Styrning av åtkomst			
6.1	Har organisationen satt upp dokumenterade regler för åtkomst/tillträde för tredjeparts åtkomst till information eller informationssystem?	Då en tredjepart behöver hög åtkomst till kommunens IT går förfrågan alltid via IT-avdelningen. Det finns dock inga formellt uppsatta regler avseende åtkomst/tillträde för tredjepart till information eller informationssystem.	Nej
6.2	Tilldelas användare en behörighetsprofil som endast medger åtkomst till informationssystem som krävs för att lösa arbetsuppgifterna?	**Treserva** I Treserva tilldelas användaren endast den behörighets-profil som krävs för att kunna lösa arbetsuppgifterna. I samband med den stora uppdatering som genomfördes nyligen stramades behörighetsprofilerna för Treserva Vård och Omsorg åt. **Lärum** Behörigheter i Lärum läses in från systemet ProCapita vars information baseras på folkbokföringsregistret. Elevregistrerare på varje skola kopplar ihop lärare och mentorer med rätt klass och ämne så att lärare endast kan se sina elever och sitt ämne. Vårdnadshavare kan endast se information om sina egna barn i Lärum. Denna koppling är även den baserad på folkbokförings-uppgifterna i ProCapita.	Ja
6.3	Har samtliga administratörer fullständiga systembehörigheter eller endast i den utsträckning som krävs för arbetsuppgifterna?	De tekniker som arbetar centralt på kommunen tilldelas behörigheter efter behov. **Treserva** I Treserva har alla systemadministratörer fullständiga behörigheter. De kan se allt, med viss begränsning inom hälso- och sjukvård. Allt systemadministratörerna gör i systemet loggas. I Treserva finns 13 personer med systemadministratörsrättighet. **Lärum** Systemadministratörer har endast behörighet i den utsträckning som krävs för arbetsuppgifterna. De kan se all struktur i systemet, men kan inte se uppgifter om klasser eller personer.	Ja
6.4	Begränsas rätten att installera nya program i nätverket samt den egna arbetsstationen till endast utsedd behörig personal?	Inom kommunen kan verksamheter beställa datorer inom konceptet *Dator som tjänst*. I de fallen är användaren inte administratör på sin egen dator och kan därmed inte installera program på den egna arbetsstationen. Användaren kan välja att installera vissa redan godkända program. Ett stort antal användare, främst inom skola, har dock inte dator som tjänst. De är därmed administratörer på sin egen dator och kan således installera nya program på sin egen arbetsstation. Rätten att installera nya program begränsas till utsedd personal från IT och Telefoni alternativt personal utsedd av verksamheten enligt dokumentet *Informationssäkerhet – Regler och instruktioner för användare*. En användare är enligt instruktionen inte tillåten att installera program i kommunens datorer.	Delvis
6.5	Har organisationen en dokumenterad rutin för tilldelning, borttag eller förändring av behörighet? Är de kommunicerade till ansvarig för behörigheter?	Kommunen har en rutin för tilldelning, borttag och förändring av behörigheter som täcker konton i Active Directory samt vissa kommungemensamma system. Den generella rutinen för borttag är att användaren inaktiveras i Active Directory i samband med att användaren försvinner från lönesystemet. För tilldelning och förändring av behörigheter i övriga system måste användaren gå via närmaste chef som lägger en beställning till systemförvaltare.	Ja

Granskningspunkt		Kommentar	Utvärdering
6.6	Får nya användare ett initialt lösenord som de måste byta, till ett eget valt lösenord vid första användning?	Byte av lösenord vid första inloggning i Active Directory är ej standard. **Treserva** Användare behöver inte byta lösenord i Treserva vid första användningen. Treserva använder single-sign on via Active Directory för individ- och familjeomsorg samt tvåpartsauktorisering med kort för de användare som arbetar inom vård och omsorg. **Lärum** Olika skolor hanterar lösenordsfrågan olika. Byte av lösenord i Active Directory vid första användning rekommenderas men är inte tvingande. Då många av eleverna är unga krävs inte att lösenordet byts vid första inloggningen. Lösenord för elever byts automatiskt en gång per år.	Nej
6.7	Genomförs kontinuerlig (minst en gång per år) kontroll av organisationens behörigheter?	Ansvaret för periodisk genomgång av behörigheter ligger hos systemförvaltarna. **Treserva** Treserva ska börja genomföra periodisk genomgång två gånger per år. Ansvariga chefer ska då kontrollera och verifiera att deras medarbetare har rätt behörigheter. Genomgången börjar med att säkerställa att cheferna är rätt för respektive enhet då personalomsättningen är hög. **Lärum** Samtliga klasser görs om en gång per år i samband med nytt läsår. Genomgången görs i juni varje år och resultatet blir detsamma som en periodisk genomgång.	Delvis
6.8	Har systemadministratörer/-tekniker/-användare individuella unika användaridentiteter?	Systemadministratörer, tekniker och användare har individuella användaridentiteter. Systemtekniker har även flera konton till olika delar av IT-miljön för att minska omfattningen av skada vid ett eventuellt intrång.	Ja
6.9	Öppnas låsta användarkonton först efter säker identifiering av användaren?	Låsta användarkonton öppnas av kommunens gemensamma IT-support. Innan byte av lösenord görs sker alltid en verifiering av användarens identitet. Detta sker genom att användaren uppger personnummer och om möjligt användar-ID. Supporten söker fram användaren via applikationen eGuide för att verifiera användarens identitet. Dessutom görs en kontroll av namn och det nummer som syns på telefondisplayen hos supporten. Vid osäkerhet är alternativet att verifiera med användarens närmaste chef. **Treserva** För de användare som loggar in med kort kan de själva låsa upp sitt konto genom att använda kortets PUK-kod. Övriga användare får vända sig till IT-supporten för att låsa upp kontot. **Lärum** Användare får vända sig till IT-supporten vid låst konto.	Ja
6.10	Finns en gemensam lösenords-policy?	Kommunen har en gemensam lösenordsinstruktion, som en del i dokumentet *Informationssäkerhet – Regler och instruktioner för användare*. Reglerna anger krav på längd, komplexitet och byte. Utöver lösenordsreglerna finns ytterligare bestämmelser för delar av socialtjänsten, som måste logga in genom en tvåfaktorsautentisering. Skolan har egna regler för lösenord för elever som inte har lika höga krav som skolans övriga personal.	Ja
6.11	Sker automatisk aktivering av skärmsläckare och automatisk låsning av obevakade arbets-stationer efter visst givet tidsintervall? Upplåsning kan endast ske med lösenord.	Automatisk aktivering av skärmsläckare sker efter 15 minuter. Därefter måste användaren logga in igen med lösenord alternativt med lösenord och kort.	Ja
6.12	Är brandväggsfunktionen den enda kanalen för IP-baserad datakommunikation till och från organisationen?	Brandväggsfunktionen är den enda kanalen för IP-baserad kommunikation till och från organisationen.	Ja

Granskningspunkt		Kommentar	Utvärdering
6.13	Finns en dokumenterad brandväggspolicy där det beskrivs vilka tjänster brandväggen skall tillhandahålla?	Umeå kommun har ingen dokumenterad brandväggspolicy.	Nej
6.14	Används trådlösa lokala nät? I så fall, finns det åtgärder mot obehörig avlyssning och obehörigt utnyttjande av resurser?	Kommunen använder trådlösa nät. Kommunen har vidtagit åtgärder mot obehörig avlyssning och obehörigt utnyttjande av resurser.	Ja
6.15	Finns det en karta över nuvarande säkerhetsarkitektur (tekniska anvisningar) för interna och externa nät och kommunikationssystem?	Umeå kommun har en karta över nuvarande säkerhets-arkitektur som visar nät och kommunikationssystem. För ytterligare information kring kartan hänvisas till kommunens IT-avdelning.	Ja
6.16	Har organisationen upprättat dokumenterade riktlinjer avseende lagring?	Kommunen har upprättat dokumenterade riktlinjer avseende lagring av backuper.	Ja
6.17	Har verksamheten ställt och dokumenterat tekniska säkerhetskrav och krav på praktisk hantering avseende användandet av mobil datorutrustning och distansarbete?	En stor andel av de anställda har möjlighet att arbeta på distans. Kommunen har olika lösningar för distansarbete. Primärt autentiseras användaren genom webinloggning med dosa eller genom sms. För att få högre behörighet till t.ex. fjärrskrivbord och filareor krävs förutom användarnamn och lösenord ett engångslösenord via sms. Instruktionen *Informationssäkerhet – Regler och instruktioner för användare* fastställer inte några krav på användaren vad gäller praktisk hantering av mobil datorutrustning.	Delvis
6.18	Har systemägaren eller motsvarande beslutat om att ett informationssystems information ska få bearbetas på distans med stationär eller mobil utrustning?	**Treserva** Chefer måste godkänna att medarbetare får arbeta på distans. **Lärum** Lärum är en webbaserad applikation och frågan är ej applicerbar.	Ja
6.19	Finns det aktuell dokumentation med regler för distansarbete?	Kommunen har ingen aktuell dokumentation med regler för distansarbete.	Nej
7 Anskaffning, utveckling och underhåll av informationssystem			
7.1	Har en systemsäkerhetsanalys upprättats och dokumenterats för varje informationssystem som bedöms som viktigt?	Systemsäkerhetsanalyser har ej upprättats och dokumenterats för varje informationssystem som bedöms som viktigt. För att en systemsäkerhetsanalys ska upprättas krävs att verksamheten beställer detta av IT-säkerhetssamordnaren. Då kommunen ej har klassificerat system utefter hur kritiska de är finns inte heller något naturligt sätt för kommunen att från centralt håll välja ut vilka system som bör analyseras. Vid tillfället för granskningen hade ett tiotal systemsäkerhetsanalyser upprättats. **Treserva** Ingen systemsäkerhetsanalys har genomförts för den nyligen uppdaterade delen av Treserva. Dock är en systemsäkerhetsanalys av den nyligen uppdaterade delen av Treserva planerad i augusti. En systemsäkerhetsanalys har genomfördes för ett antal år sedan för den delen av Treserva som berör individ- och familjeomsorgen. **Lärum** Lärum är fortfarande i implementeringsfasen och kommer vara i full drift i samband med nästa läsårsstart. Av denna anledning har någon analys ännu ej upprättats. En risk- och sårbarhetsanalys genomfördes dock i förstudien innan systemet avropades från ramavtal.	Delvis
7.2	Krypteras persondata som förmedlas över öppna nät?	Persondata som förmedlas över öppna nät, inom eller mellan kommunens olika system, krypteras.	Ja
7.3	Finns det angiven personal som ansvarar för systemunderhåll?	Servergruppen på IT-avdelningen, bestående av 12 personer, ansvarar för systemunderhåll. Det finns dock vissa applikationer som hanteras av konsulter eller andra grupperingar på IT. Ett fåtal system underhålls även av arbetsplatstekniker ute i verksamheten. Kommunikationsavdelningen inom IT underhåller sina egna system.	Ja

Granskningspunkt		Kommentar	Utvärdering
7.4	Finns det regler för hur system- och programutveckling ska genomföras?	Regler för hur system- och programutveckling ska genomföras finns i kommunens dokument *Systemförvaltning i Umeå kommun*.	Ja
7.5	Finns det regler och riktlinjer avseende beslut om programändringar?	Regler och riktlinjer avseende beslut om programändringar finns i kommunens dokument *Systemförvaltning i Umeå kommun*.	Ja
8 Hantering av informationssäkerhetsincidenter			
8.1	Finns det dokumenterade instruktioner avseende vart användare skall vända sig och hur de skall agera vid funktionsfel, misstanke om intrång eller vid andra störningar?	I instruktionen *Informationssäkerhet – Regler och instruktioner för användare* samt på Umeå kommuns hemsida och intranät finns skriftliga instruktioner för vart användare skall vända sig vid funktionsfel, misstanke om intrång eller andra störningar. Kommunen har en central IT-support dit alla användare kan vända sig. Vidare finns särskilda rutiner för hur användare ska agera vid misstanke om brott. I dessa fall blir det chefens ansvar att föra frågan vidare till IT-chefen. Tillsammans bedömer de därefter om polis ska kopplas in.	Ja
9 Kontinuitetsplanering i verksamheten			
9.1	Finns det en gemensam kontinuitetsplan dokumenterad för organisationen?	Kommunen har en gemensam kontinuitetsplan som är dokumenterad för organisationen. Under granskningen har denna dock ej delgetts på grund av dess känsliga innehåll.	Ja
9.2	Har systemägaren eller motsvarande beslutat om den längsta acceptabla tid som informationssystemet bedöms kunna vara ur funktion innan verksamheten äventyras?	I kommunen finns ingen sammanställning av längsta acceptabla tid som informationssystem kan vara ur funktion innan verksamheten äventyras. Dock har det gjorts en klassificering av vilken verksamhet som klassas som samhällsviktig och därmed ska prioriteras vid kris och katastrof. **Treserva** Inget beslut har fattats om längsta acceptabla tid som systemet kan vara ur funktion innan verksamheten äventyras. Beslut om längsta acceptabla tid systemet kan vara ur funktion kommer fattas vid planerad systemsäkerhetsanalus i augusti. **Lärum** Inget beslut har fattats om längsta acceptabla tid som systemet kan vara ur funktion innan verksamheten äventyras.	Nej
9.3	Finns det en dokumenterad avbrottsplan med återstarts- och reservrutiner för datadriften som vidtas inom ramen för ordinarie driften?	Kommunen har ingen övergripande avbrottsplan för samtliga applikationer. Umeå kommun har dock en handlingsplan vid avbrott som berör telefoni samt en teknisk instruktion för hur drift ska flyttas över från en datahall till en annan.	Delvis
9.4	Har omständigheter som ska betecknas som kris/katastrof (extraordinära händelser) för verksamheten kartlagts?	De omständigheter som ska betecknas som kris och extraordinär händelse har kartlagts i dokumentet *Umeå kommuns program för säkerhet och trygghet*.	Ja
10 Efterlevnad			
10.1	Används endast programvaror i enlighet med gällande avtal och licensregler?	Programvaror används i enlighet med gällande avtal och licensregler. Licensrevision genomförs för individuella företag och produkter.	Ja
10.2	Genomförs interna och externa penetrationstester kontinuerligt?	Penetrationstest genomfördes för ett par år sedan, men kommunen har ingen plan för regelbunden penetrationstestning. Under granskningen har noterats att ett säkerhetsprojekt genomfördes under 2014, där kommunen på en övergripande nivå gick igenom möjliga sätt för en angripare ta sig in i kommunens informationssystem.	Nej
10.3	Granskar ledningspersoner regelbundet att säkerhetsrutiner, -policy och -normer efterlevs?	Ledningspersoner granskar inte regelbundet att säkerhetsrutiner, -policy och -normer efterlevs.	Nej
11 Hantering av molntjänster			

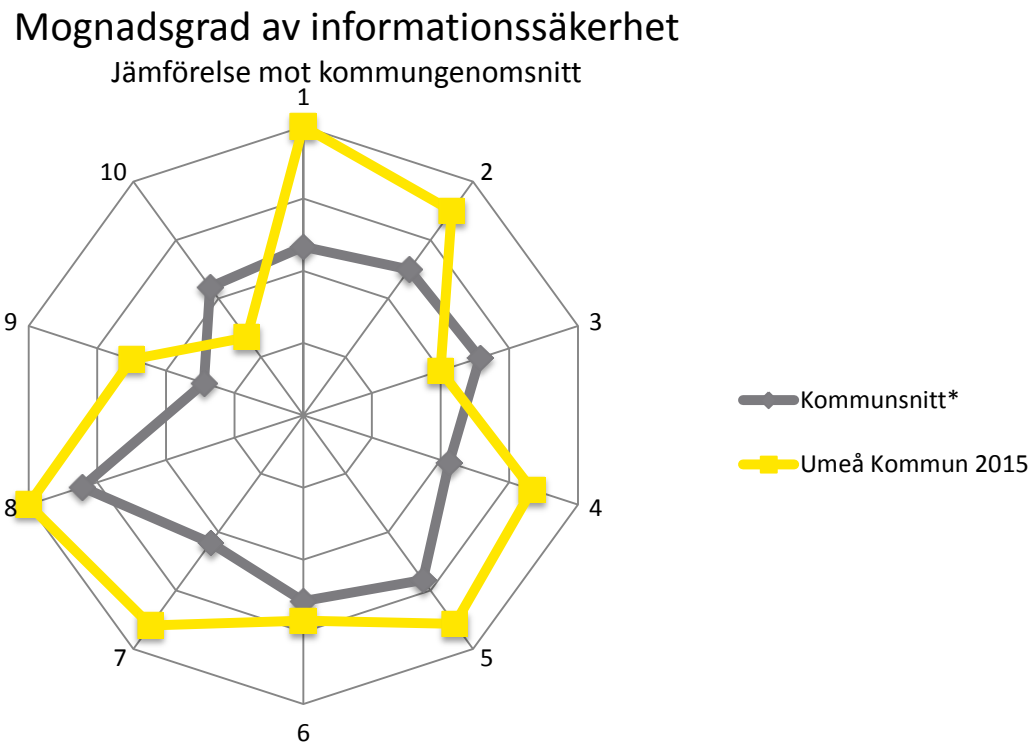
Granskningspunkt		Kommentar	Utvärdering
Umeå kommun använder sig i låg utsträckning av molntjänster. Systemet Lärum som levereras av Tieto är en molnbaserad tjänst. Lärum är inköpt genom ett avrop på Kammarkollegiets ramavtal med Tieto. Därmed regleras en stor del av hanteringen och driften av Lärum genom Kammarkollegiets avtal. Inom ramen för Lärum lagras kommunens information i databaser som delas med andra kommuner. All information från Lärum, förutom personuppgifterna i ProCapita lagras i molnet.			
11.1	Hanteras personuppgifter i molnet? Beaktas personuppgiftslagens bestämmelser, bl.a. vad avser när behandling av personuppgifter är tillåten, att lagens säkerhetskrav är uppfyllda? Finns det ett skriftligt avtal som reglerar molntjänstleverantörens behandling av personuppgifterna?	**Lärum** Lärum hanterar inga personuppgifter såsom personnummer i molnet. Dock hanteras registrerade uppgifter av vilka det direkt eller indirekt kan framgå vem uppgiften rör, vilket enligt Skatteverkets definition klassas som personuppgifter. I bilaga till avtalet med Tieto anges att i de fall personuppgifter hanteras ska detta göras i enlighet med gällande lagstiftning.	Ja
11.2	Beaktas regler om sekretess i offentlighets- och sekretesslagen (2009:400) i kommunens avtal med leverantören? Förvaras sekretessbelagda uppgifter i molnet? Säkerställs då att denna information skyddas?	**Lärum** Ingen sekretessbelagd information förvaras i molnet.	E/T
11.3	Finns en fastställd sourcing-strategi för molntjänster?	Kommunen har ingen fastställd sourcing-strategi för molntjänster.	Nej
11.4	Har ansvarsområden mellan kommunen och leverantören av molntjänsten fastställts?	**Lärum** Ansvarsområden mellan kommunen och leverantören av Lärum är fastställda i de bilagor som följer med avtalet.	Ja
11.5	Har det i avtal reglerats att leveranfören genomför olika typer av säkerhetsaktiviteter, som exempelvis regelbundna tester med återläsning av kopior, penetrations-tester och skydd mot skadlig kod?	**Lärum** Kommunen har i avtalet för Lärum ej reglerat att leverantören ska genomföra säkerhetsaktiviteter. I förfrågningsunderlaget för ramavtalet från Kammarkollegiet framgår dock att fullständig säkerhetskopiering ska göras och att återläsningstester ska ske minst en gång per år.	Delvis
11.6	Har det i avtal reglerats i vilka fall leverantören får använda sig av underleverantörer?	**Lärum** I avtalet mellan kommunen och Tieto regleras ej i vilka fall Tieto får använda sig av underleverantörer. Ej heller i Kammarkollegiets allmänna villkor framgår detta. Dock framgår av Kammarkollegiets allmänna villkor att avtal med underleverantör måste finnas och att Tieto fullt ut ansvarar för leveransen av systemet.	Nej
11.7	Har analys genomförts avseende på vilket sätt en eventuell migrering av data ska ske från molnet och ställt krav på leverantören utifrån detta?	**Lärum** Hur data ska kunna migreras från molnet och vilka krav som ställs på leverantören är fastställt i avtalets bilaga 2.	Ja
11.8	Inkluderas information i molnet i kommunens kontinuitetsplanering?	Information som lagras i molnet inkluderas ej i kommunens kontinuitetsplan.	Nej
11.9	Har kontinuitetsplan inkluderats i avtalet med leverantören?	**Lärum** I bilaga till avtalet med Tieto framgår att leverantören ska ha en kontinuitetsplan att tillämpa vid större avbrott eller katastrof så att tjänsten snabbt kan vara i drift för användarna.	Ja
11.10	Har krav på gallring och arkivering förts in i avtalet med leverantören?	**Lärum** Kommunen har ej fört in krav på gallring och arkivering i avtalet med leverantören.	Nej
11.11	Har det i avtalet med leverantören tydliggjorts vilket rättsligt regelverk som ska tillämpas vid en eventuell tvist? (Avser exempelvis immateriella tillångar och personuppgifter i de fall data lagras i annat land)	**Lärum** I bilaga till avtalet framgår att svensk lag ska tillämpas vid eventuell tvist.	Ja
11.12	Har det i avtalet fastställts var (land) information får lagras?	**Lärum** I avtalet framgår ej var (land) informationen tillåts lagras.	Nej

3. Jämförelse mot andra kommuner

EY har gjort ett flertal gapanalyser mot BITS-ramverket hos svenska kommuner. Tack vare detta kan vi mäta Umeå kommuns mognadsgrad rörande informationssäkerhet mot ett genomsnitt av de kommuner vi granskat.

I diagrammet nedan representerar ytterkanten 100 % måluppfyllnad, medan mittpunkten anger 0 % måluppfyllnad. Varje nummer representerar ett granskningsområde i enlighet med granskningsprogrammet i kapitel två, samt listan nedan. Området avseende hantering av molntjänster ingår ej i jämförelsen.

1. Säkerhetspolicy
2. Organisation av säkerheten
3. Hantering av tillgångar
4. Personalresurser och säkerhet
5. Styrning och kommunikation av drift
6. Styrning av åtkomst
7. Anskaffning, utveckling och underhåll av informationssystem
8. Hantering av informationssäkerhetsincidenter
9. Kontinuitetsplanering i verksamheten
10. Efterlevnad



*Kommunsnitt baseras på 20 granskningar genomförda mellan 2009 – 2015.

Det framgår från diagrammet att Umeå kommun ligger högre än kommungenomsnittet på majoriteten av kontrollpunkterna. Dock ligger kommunen under genomsnittet på punkterna *3. Hantering av tillgångar* och *10. Efterlevnad*.

4. Slutsatser och rekommendationer

4.1 Slutsatser

Av samtliga 71 granskningspunkter är fördelningen av bedömningarna följande:

Kontrollen finns och fungerar tillfredsställande:	66,2%
Kontrollen finns och fungerar delvis:	11,3%
Kontrollen finns ej eller fungerar ej tillfredsställande:	21,1%
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	1,4%

Hur ändamålsenlig är IT-säkerheten för de behov kommunens verksamhet har?

Granskningen har visat att Umeå kommun har goda förutsättningar för ett effektivt och ändamålsenligt arbete med informationssäkerhet. Kommunen har interna regelverk och processer som verkar för god säkerhet. Kommunens starka sidor finns inom områdena, säkerhetspolicy, organisation av säkerheten, personalresurser och säkerhet, styrning och kommunikation av drift, anskaffning, utveckling och underhåll av informationssystem samt hantering av incidenter. Förbättringsområden har identifierats främst inom hantering av tillgångar, styrning av åtkomst, kontinuitetsplanering i verksamheten samt efterlevnad.

Nedan har samtliga identifierade förbättringsområden och rekommendationer beskrivits.

4.2 Rekommendationer

Nedan följer våra rekommendationer samt vårt förslag på prioritering utifrån bedömd risk och väsentlighet. Rekommendationerna är prioriterade enligt följande:

Hög	Observation av kritisk karaktär som kan riskera kommunens möjlighet att driva verksamhet eller leda till materiella förluster för kommunen. Observation som graderas som "hög" bör omedelbart åtgärdas.
Medel	Observation som anses kunna ha påverkan på verksamhetens mål, rykte, finansiell information, materiella tillgångar och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av kommunens resurser. Bristen bör åtgärdas för att säkerställa god intern kontroll på lång sikt.
Låg	Observation som ej direkt påverkar verksamhetens mål, men kan medföra ineffektiv verksamhet, mindre fel i information, mindre brister i efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.

#	Iakttagelse och rekommendation	Prioritet
1.	**Kommunens informationssystem har ej klassats avseende hur kritiska de är** Kommunen har ej analyserat samtliga system och därefter klassificerat dem utefter hur kritiska de är ur ett verksamhets- och säkerhetsperspektiv. Detta innebär att ingen prioritering finns för systemen vid ett eventuellt avbrott. Kommunen har gjort en typ av urskiljning av systemen då det i kommunens lista över system framgår huruvida systemet innehåller personuppgifter eller ej. **Risk** Att inte klassificera system utefter hur kritiska de är ökar risken för att systemen prioriteras felaktigt vid ett eventuellt avbrott vilket kan äventyra verksamheten. En klassificering av system bör ligga till grund för kommunens avbrottsplan. **Rekommendation** Kommunen rekommenderas att klassificera samtliga informationssystem avseende hur kritiska de är för verksamheten. Detta kan med fördel införas i RegIT och därefter ligga till grund för kommunens avbrottsplan och prioritering för systemsäkerhetsanalys.	Hög
2.	**Kommunen har ej genomfört systemsäkerhetsanalys eller fastställt längsta acceptabla tid för avbrott för samtliga system** Verksamheten har möjlighet att efterfråga en systemsäkerhetsanalys av IT-avdelningen. Dock har endast ett fåtal systemägare efterfrågat denna tjänst och en stor andel av systemen är därmed ej analyserade ur ett systemsäkerhetsperspektiv. En del av att genomföra en systemsäkerhetsanalys bör vara att fastställa längsta acceptabla tid för avbrott. Detta är inget som ingår i systemsäkerhetsanalysen i dagsläget utan det är istället upp till systemägare eller motsvarande att besluta om längsta acceptabla tid systemet kan vara ur funktion utan att verksamheten äventyras. Detta hade ej gjorts för de system som ingått i granskningen. **Risk** En systemsäkerhetsanalys syftar till att kartlägga vilka säkerhetskrav som ska ställas på ett system. Vid avsaknad av systemsäkerhetsanalys ökar risken för att säkerheten ej är tillräcklig för att exempelvis upprätthålla sekretessen, säkerställa att informationen i systemet är riktig samt att informationssystemets information och funktion ej är åtkomligt vid behov. Då längsta acceptabla tid för avbrott ej har fastställts finns en risk att systemen ej prioriteras i rätt ordning vid ett eventuellt avbrott och att verksamheten på så vid äventyras. **Rekommendation** Kommunen rekommenderas att efter att ha klassat samtliga system utefter hur kritiska de är, genomföra en systemsäkerhetsanalys för samtliga system som bedömts som viktiga. Analysen bör utgå från vilka hot som finns mot systemet, sannolikheten för att de inträffas samt konsekvenserna de realiserade hoten skulle få för verksamheten. Kommunen rekommenderas därtill att i samband med systemsäkerhetsanalys fastställa längsta acceptabla tid för avbrott och därefter inkludera denna information i en avbrottsplan.	Hög
3.	**Inga penetrationstester genomförs regelbundet** Penetrationstester syftar till att identifiera tekniska sårbarheter som kan vara blottade för en eventuell angripare. Kommunen genomför i dagsläget inga externa penetrationstester, dvs tester utifrån ett externt angreppsutfall, och inga interna penetrationstester, dvs tester utifrån ett insiderperspektiv. Kommunen har genomfört tester tidigare men senaste gången ett penetrationstest genomfördes var för ett par år sedan. **Risk** Att inte regelbundet genomföra penetrationstester medför en risk att system och infrastruktur inte följer kommunens uppsatta säkerhetspolicyer och säkerhets-standarder och att man inte upptäcker eventuella säkerhetsbrister som gör det möjligt för utomstående att komma åt kommunens information. **Rekommendation** Kommunen rekommenderas att införa regelbundna penetrationstester. Under granskningen har noterats att utförande av nytt penetrationstest är under diskussion.	Hög

#	Iakttagelse och rekommendation	Prioritet
4.	**Kommunen har ingen rutin för hur utomstående leverantörers tjänster följs upp** En del av kommunens system levereras av externa leverantörer, däribland Lärum som levereras av Tieto. Ingen uppföljning görs av exempelvis leverantörernas avtalsefterlevnad. Kommunen har inga gemensamma rutiner för att följa upp leverantörer utan överlåter detta till respektive systemförvaltare. För de system vi granskat skedde ingen formell uppföljning av leverantör. **Risk** Att inte följa upp leverantörers tjänster medför en risk att leverantören ej har den nivå på informationssäkerhet som avtalad och lämplig. Det finns också en risk att kommunen inte får det som avtalats vad gäller drift, funktionalitet och service. I de fall kommunen ej hanterar driften själv blir det viktigare att säkerställa att leverantören utför avtalade aktiviteter på ett tillfredställande sätt. **Rekommendation** Umeå kommun rekommenderas att införa en rutin för uppföljning av utomstående leverantörers tjänster.	**Hög**
5.	**Kommunen har ej satt upp regler för åtkomst/tillträde till tredjepart till information eller informationssystem** Det finns tillfällen då en utomstående part behöver åtkomst till kommunens system eller information, vid exempelvis förändringsutveckling av system. I de fall någon utomstående behöver tillträde eller åtkomst går förfrågan alltid via IT. Det finns dock inga regler som styr hur detta ska gå till och vilken åtkomst som får tilldelas. **Risk** Utan formella regler för åtkomst/tillträde till tredjepart finns en risk att beslut avseende tilldelandet av behörigheter till kommunens system inte utförs på ett kontrollerat och spårbart sätt. Det kan i sin tur innebära en ökad risk för att utomstående felaktigt får tillgång till känslig information. **Rekommendation** Kommunen rekommenderas att ta fram formella regler för hur tredjeparts åtkomst/tillträde till information eller informationssystem bör hanteras för att säkerställa att rätt åtkomst ges. Kommunen rekommenderas därtill att säkerställa att spårbarhet finns i tilldelandet av behörigheter.	**Hög**
6.	**Brister i avtal med leverantörer** Informationssäkerhet regleras endast i avtal för informationsbehandling som lagts ut på en utomstående organisation i de fall personuppgifter är inblandade. Detta regleras genom ett personuppgiftsbiträdesavtal. Under granskningen framkom också att det är oklart hur informationssäkerhet och hantering av personuppgifter hanteras i äldre avtal. Även vad gäller avtalet kommunen har med Tieto som levererar Lärum har ett antal brister identifierats. I avtalet framgår ej var informationen får lagras (land). Därtill har kommunen ej fört in krav på gallring och arkivering i avtalet. Avtalet reglerar inte heller i vilka fall Tieto får använda sig av underleverantörer, vilket inte heller inkluderats i Kammarkollegiets allmänna villkor. Dock framgår av Kammarkollegiets allmänna villkor att avtal med underleverantör måste finnas och att Tieto fullt ut ansvarar för leveransen. **Risk** Avtalsbrister medför risker för att kommunen ej efterlever gällande lagstiftning samt risk att brister i säkerheten kan uppstå. I och med avtalsbristerna föreligger även en risk att kommunen tappar kontroll över sin information. **Rekommendation** Umeå kommun rekommenderas att alltid reglera ansvar för informationssäkerhet i avtal för informationsbehandling som lagts ut på en utomstående organisation. Kommunen rekommenderas även att se över hur avtalen ser ut för de äldre systemen. Kommunen rekommenderas därtill att se över avtalet med Tieto i syfte att säkerställa att avtalet lever upp till de krav på säkerhet och kontroll kommunen ställer samt att avtalet medför att kommunen efterlever lagar och regler.	**Hög**

#	Iakttagelse och rekommendation	Prioritet
7.	**Kommunen genomför inga regelbundna utbildningsinsatser inom informationssäkerhet** Umeå kommun har från centralt håll inga regelbundna utbildningsinsatser inom informationssäkerhet. För att utbildning ska genomföras krävs att verksamheter efterfrågar det, vilket i dagsläget inte görs i så stor utsträckning. Varje verksamhet kan ha separata utbildningar inom informationssäkerhet. **Risk** Utan regelbunden utbildning inom informationssäkerhet ökar risken för att kunskapen om informationssäkerhet samt säkerhetsmedvetandet minskar. Det ökar också risken för att organisationen tappar motivationen för att upprätthålla säkerheten. **Rekommendation** Kommunen rekommenderas att genomföra utbildningsinsatser inom informationssäkerhet regelbundet. Utbildningsinsatser kan ske både genom fysisk utbildning samt genom webbaserade utbildningar.	**Medel**
8.	**Brister i kontinuitetsplan samt avsaknad av avbrottsplan för kritiska informationssystem** Umeå kommun har en övergripande kontinuitetsplan som beskriver krishantering i stora drag. Denna kontinuitetsplan är dock ej fullständig då den ej täcker hantering av information som finns i molnet. Därtill har kommunen inte skapat någon avbrottsplan med bestämd prioritering för IT att ta till hjälp för att säkerställa effektivt återgående till normal drift vid ett eventuellt avbrott. Avbrottsplan med återstarts- och reservrutiner för datadriften som vidtas inom ramen för ordinarie drift finns framtaget för telefoni och för den övergripande tekniska driften av kommunens IT-miljö. En förutsättning för att kunna skapa en avbrottsplan för IT är genomförda systemsäkerhetsanalyser, klassificering av hur kritiska systemen är samt fastställd längsta tillåtna tid för avbrott, i enlighet med rekommendation 1 och 2. **Risk** Att ej ha en dokumenterad avbrottsplan innebär en risk för att system och applikationer ej startas upp enligt rätt prioritering samt på ett effektivt och ändamålsenligt sätt vid ett eventuellt avbrott. Detta innebär att verksamheten kan äventyras. **Rekommendation** Kommunen rekommenderas att uppdatera kontinuitetsplanen så att den även täcker informationen i molnet. Kommunen rekommenderas vidare att upprätta en avbrottsplan för kritiska informationssystem, innehållande de åtgärder som ska säkerställa fortsatt verksamhet vid störning eller avbrott i IT-driften inom en viss tid och redovisa de reserv- och återstartsrutiner för IT-driften som krävs för detta. Planen bör omfatta åtgärder för områden såsom dokumentation, roller och ansvar, bemanning, brand, skydd mot skadlig programkod, elförsörjning samt säkerhetskopiering och förvaring av datamedia. Avbrottsplanen bör baseras på kommunens klassificering och längsta acceptabla tid varje system kan vara ur funktion.	**Medel**
9.	**Kommunen har ingen dokumenterad brandväggspolicy** Umeå kommun har brandväggar som säkerställer en viss säkerhetsnivå. Dock finns inga interna regler avseende brandväggar att luta sig mot, i syfte att säkerställa att rätt säkerhetsnivå uppnås för kommunens samtliga verksamheter. **Risk** Utan en brandväggspolicy finns risk att vissa verksamheter ej får sina säkerhetskrav tillgodosedda. Brandväggen är en gemensam resurs för organisationen och bör därmed vara anpassad för alla verksamheter. **Rekommendation** Kommunen rekommenderas att skapa en brandväggspolicy och i skapandet av denna bland annat ta med i beräkningen vilka tjänster brandväggen ska tillhandahålla, vilka uppgifter som ska döljas av brandväggen, exempelvis strukturen på det egna nätet, egna IP-adresser och användaridentitet, om e-post ska kontrolleras i brandväggen samt hur brandväggsadministrationen ska ordnas.	**Medel**

#	Iakttagelse och rekommendation	Prioritet
10.	**Kontinuerlig kontroll av behörigheter genomförs ej för samtliga system/Active Directory** Ansvaret för periodisk kontroll av behörigheter ligger på respektive systemförvaltare. Inom kommunen finns ingen regelbundenhet i att initiera en kontroll från centralt håll. Vid avslut av anställning förlitar sig kommunen på den koppling som finns mellan personalsystemet och Active Directory. Kopplingen medför att en användare låses automatiskt vid avslutad anställning. Det genomförs dock ingen periodisk genomgång för att säkerställa att användare har rätt behörigheter samt för att säkerställa att inga behörigheter ligger kvar efter avslutad anställning. **Risk** Då ingen kontinuerlig kontroll görs av samtliga system och Active Directory finns en risk att personer som inte längre jobbar kvar eller har fått ändrade arbetsuppgifter har kvar gamla behörigheter i systemet. Detta kan utnyttjas för att t.ex. förvanska eller radera information i kommunens kritiska applikationer. Felaktig åtkomst ökaräven risken för oegentligheter eller oavsiktliga fel på grund av att medarbetare har behörigheter som medger otillåtet handlande t.ex. genom brister i ansvarsfördelningen. **Rekommendation** Kommunen rekommenderas att införa en årlig kontroll av samtliga behörigheter. Kontrollen bör initieras centralt men bör utföras av verksamheten.	Medel
11.	**Testning av system- och programutvecklingar sker inte alltid** Umeå kommun testar alla större system- och programutvecklingar innan de sätts i drift. Vid mindre förändringar sker dock inte alltid testning i testmiljö utan förändringen sätts i drift utan att ha testats. Det finns inga interna regler som fastställer i vilka fall en utveckling kan driftsättas utan att testas. **Risk** Bristande kontroll i hanteringen av programförändringar i viktiga system kan innebära ökad risk för att otillräckligt testade förändringar införs i produktionsmiljön. Detta kan leda till fel i systemets funktionalitet och därmed allvarliga störningar för verksamheten. **Rekommendation** Kommunen rekommenderas ta fram interna regler som fastställer vilken typ av ändringar som kan sättas i drift utan testning. Syftet med ett sådant dokument är att säkerställa att de ändringar som kan påverka säkerhet eller funktionalitet alltid testas åtskilt från produktionsmiljö innan driftsättning.	**Medel**
12.	**Rätten att installera nya program på den egna arbetsstationen begränsas inte till endast utsedd behörig personal** En stor andel av kommunens anställda har egna arbetsstationer. Därtill har många elever i skolan bärbara datorer som tillhör kommunen. Inom kommunen finns ett koncept som heter *Dator som tjänst*. De medarbetare som har en dator inom *Dator som tjänst* har inte möjlighet att installera nya program på datorn, utöver ett antal program som är fördefinierade och godkända. De som har fått dator tilldelad utanför *Dator som tjänst*, vilket främst är inom skolan, har möjlighet att installera program på sin dator. **Risk** Att användare kan installera program på sin egen arbetsstation ökar risken för att skadlig programvara som kan störa övriga funktioner och nät, medvetet eller av misstag, installeras. Det leder också till en risk att obehöriga kan komma åt och sprida känslig information. **Rekommendation** Kommunen rekommenderas att i så stor utsträckning som möjligt frånta användare möjligheten att installera programvara på sina arbetsstationer samt säkerställa att alla programvaror som ska kunna installeras på arbetsstationen är godkända. Detta kan exempelvis göras genom att arbeta för att få över fler medarbetare till konceptet *Dator som tjänst*.	**Medel**

#	Iakttagelse och rekommendation	Prioritet
13.	**Byte av lösenord vid första inloggning är ej ett krav** Kommunen har inte som standard att byte av lösenord vid första inloggning är tvingande. Detta innebär att en användare kan tilldelas ett lösenord vid första inloggning på Active Directory eller vid första inloggningen på en applikation och att det inte finns krav på att byta detta. I en del verksamheter har kommunen bedömt att det ej är lämpligt att ha tvingande byte av lösenord vid första inloggning. **Risk** Avsaknad av tvingande lösenordsbyte vid första inloggning kan innebära att standardlösenord används eller att lösenord som skickas i klartext plockas upp av utomstående. Detta ökar risken för att obehöriga kan få tillgång till system och därmed eventuell känslig information. **Rekommendation** Kommunen rekommenderas att ha lösenordsbyte vid första inloggning som standard, med anpassning för de verksamheter där initialt lösenordsbyte ej är lämpligt.	Medel
14.	**Ingen strategi för molntjänster** Umeå kommun använder sig av molntjänster, bland annat för systemet Lärum. Användning av molntjänster ställer krav på kommunen att se över vilka säkerhetskrav som ska ställas och för vilka verksamheter och funktioner molntjänster får användas. Kommunen har dock inte utformat någon strategi för i vilka fall och för vilka verksamheter molntjänster kan vara aktuellt, samt vilka krav som ska ställas på säkerhet. **Risk** En sourcing-strategi för molntjänster bör vara i linje med IT-strategin och beskriva krav och inriktning på informationssäkerhet i de tjänster som ska upphandlas. Utan en sådan strategi ökar risken att kommunen bortser från viktiga säkerhetsaspekter vid upphandling eller inköp av molntjänster. **Rekommendation** Kommunen rekommenderas att skapa en sourcing-strategi för molntjänster i syfte att skapa en säkrare upphandling av outsourcing och molntjänster. Strategin bör beskriva i vilka delar de långsiktiga behoven och målen för verksamheten kan uppnås med hjälp av outsourcing alternativt molntjänster, samt vilka krav på informations-säkerhet som ska ställas i samband med upphandlingen.	Medel
15.	**Kommunen har inga aktuella regler för distansarbete** En stor andel av kommunens anställda har möjlighet att arbeta på distans. Varje chef har möjlighet att ge sina medarbetare tillåtelse att arbeta på distans. Dock har kommunen inga regler som rör distansarbete eller regler kring vilka krav som finns på användaren vad gäller praktisk hantering av utrustning. De regler som finns rör hur uppkoppling ska ske. **Risk** Utan dokumenterade regler för distansarbete finns en risk att användaren omedvetet agerar oaktsamt och att användaren därmed utgör en säkerhetsrisk. **Rekommendation** Kommunen rekommenderas att införa dokumenterade regler för distansarbete. I samband med framtagandet av regler bör kommunen se över vilka krav som ska ställas på bland annat fysiskt skydd (stöldrisk och brandrisk) i eller utanför hemmet, logiskt skydd, hantering av utskrifter samt hur eventuella hjälpinsatser utifrån ska ske.	Låg
16.	**Ledningspersoner granskar inte att rutiner, policyer och normer efterlevs** Kommunen har ett antal interna regler och policyer som samtliga anställda och andra användare måste följa. Dock sker ingen uppföljning och granskning av att medarbetare följer de interna regelverk avseende informationssäkerhet som finns. **Risk** Att inte regelbundet följa upp och granska att medarbetare följer de interna regelverk avseende informationssäkerhet som finns medför en risk att kommunen ej identifierar brister i efterlevnad av säkerhetspolicyer och säkerhetsstandarder och att kommunen därmed ej uppmärksammar behov av utbildningsinsatser. **Rekommendation** Kommunen rekommenderas att regelbundet följa upp och granska att medarbetare följer de interna regelverk avseende informationssäkerhet som finns. Granskningen kan genomföras genom central initiering där efterlevnad följs upp med respektive systemförvaltare.	Låg

5. Källförteckning

5.1 Kommungemensamma dokument

- Informationssäkerhetspolicy för Umeå kommun
- Bevissäkring vid IT-relaterad brottslighet
- Incidentrapport mall
- Umeå kommuns program för säkerhet och trygghet
- Skiss på principiell uppbyggnad av kommuninternt nät
- Skiss över fysiskt spridningsnät
- Avbrottsplan telefoni
- Systemförvaltning i Umeå kommun
- Checklista för introduktion
- Dokumentation kring TjänsteID/SITHS-kort
- Informationssäkerhet: Regler och instruktioner för användare
- Informationssäkerhet: Regler och instruktioner för verksamheten
- Umeå kommuns datacenter
- GAP-analys: Genomlysning av ledningssystem för informationssäkerhet
- Snapshotschema
- Incidenthantering flödesschema
- Rutinbeskrivning ärendehantering – Incident

5.2 Lärum

- Avtal Tieto, inklusive bilagor
- Riskanalys Lärum
- Rutin vid driftstopp eller avbrott, Lärum

5.3 Treserva

- Flöde för anmälan utbildning och behörighet till Treserva utförare
- Beslutsunderlag behörigheter
- Presentation utbildningsdag
- Integrationer Treserva
- Checklista Treserva
- Loggningsrutiner