Kommunrevisorerna granskar

IT- och informationssäkerhet

2020-11-30

Angående granskningen

Revisionsuppdraget är ett kommunalt förtroendeuppdrag och revisorerna är direkt ansvariga inför kommunfullmäktige och därmed indirekt inför medborgarna genom den representativa demokratin. Revisionen har uppdrag att granska de verksamheter som styrelser, nämnder och kommunala bolag bedriver.

I formell mening är varje revisor en egen myndighet, men i det praktiska revisionsarbetet sker arbetet gemensamt.

Ytterst syftar revisionen till att undersöka om verksamheten bedrivs i enlighet med uppställda mål och på ett från ekonomisk synpunkt tillfredsställande sätt.

- Revisorernas uppdrag regleras i kommunallag, aktiebolagslag, god revisionssed, ägardirektiv och reglemente.
- Revision ska utföras på ett oberoende sätt.
- Revisorerna genomför grundläggande granskning, granskning av delårsrapport och årsredovisning och fördjupade granskningar.

Revisorerna ska därför objektivt, opartiskt och sakligt, självständigt granska den verksamhet som styrelse, nämnder och beredningar bedriver. Revisorerna ska också bedöma om de förtroendevalda ledamöterna i nämnder och styrelser har tillräcklig styrning och kontroll över verksamhetens ekonomi, prestationer och kvalitet.

Revisorernas uttalanden och bedömningar finns i revisionsberättelser och granskningsrapporter. En ambition i revisorernas arbete är att deras rekommendationer i samband med granskning ska kunna användas av verksamheterna för att åstadkomma effekter i deras förbättringsprocess.

Kontaktuppgifter

Om kommunrevisorernas uppdrag

kommunrevisionen@umea.se

Ordförande i kommunrevisionen

Ewa Miller, ordförande
ewa.miller@umea.se

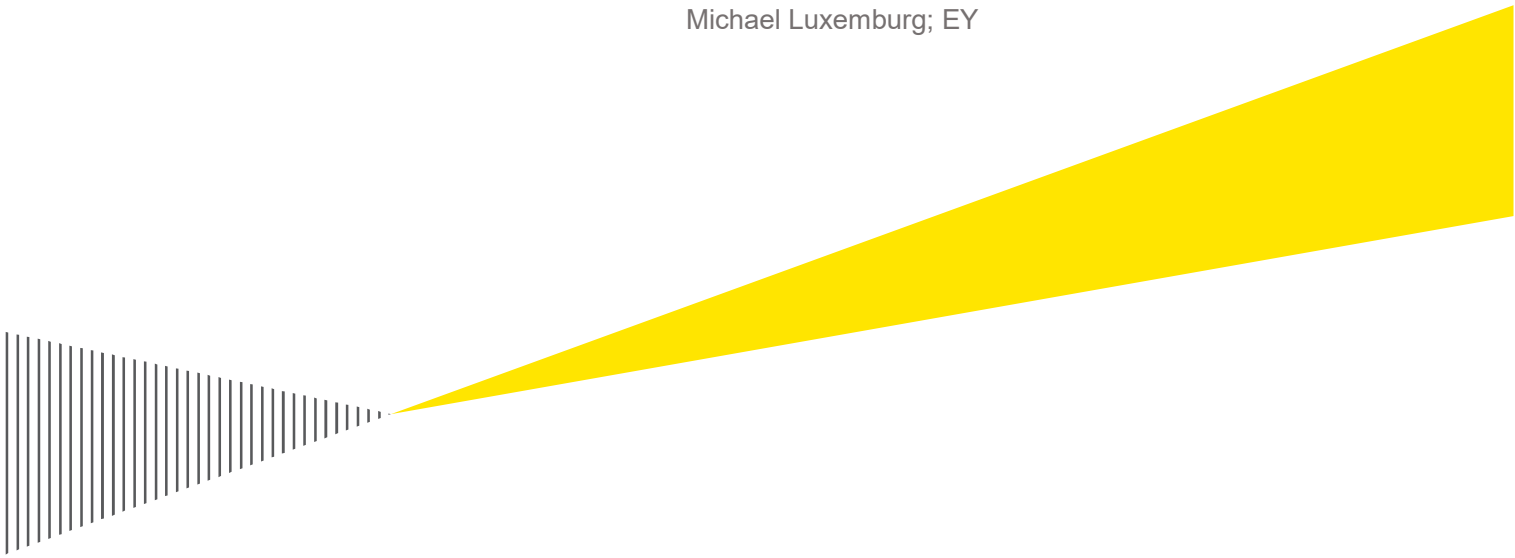
Umeå kommun

Granskning av IT- och informationssäkerhet

2020-11-30

Oscar Rydén; EY

Michael Luxemburg; EY



Sammanfattning

Genomförd granskning

EY har på uppdrag av Umeå kommuns förtroendevalda revisorer genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Granskningens syfte har varit att övergripande granska huruvida kommunen har tillsett att arbetet kring IT- och informationssäkerhet med fokus på styrning, uppföljning och incidenthantering är ändamålsenligt.

Som bedömningsunderlag för granskningen användes följande revisionskriterier:

- Myndigheten för samhällsskydd och beredskaps (MBSs) styrningsmodell för offentliga organisationers IT- och informationssäkerhet, LIS.
- Den internationella standarden för informationssäkerhet, ISO/IEC 27000.
- God praxis och EY:s erfarenhet inom IT-, Cyber – och informationssäkerhet.

Granskningen genomfördes under juni 2020 och baserades på intervjuer med identifierade nyckelpersoner i kommunens IT- och informationssäkerhetsarbete samt genomgång av insamlad styrdokumentation. Granskningens metod har utgått ifrån EY:s metodstöd, Granskningsprogram för Cyber och Informationssäkerhet (GCI), med fokus på offentlig verksamhet. Intervjuade representanter har beretts tillfälle att faktagranska rapporten och lämna synpunkter på dess innehåll. Granskningen har även kvalitetssäkrats internt av EY:s utsedda kvalitetsgranskare.

Granskningsresultat

Umeå kommun har etablerat ett grundläggande ramverk i form av systemförvaltningsmodell, policy, riktlinjer och instruktioner för arbetet med informationssäkerhet. Det har dock noterats att den övergripande styrningen i vissa hänseenden saknar tydlighet avseende ansvar, mandat och uppföljning för att säkerställa ändamålsenligt arbete med informationssäkerhet i alla kommunens verksamheter. Detta medför en risk att kommunens policyer och riktlinjer inte följs. Baserat på denna iakttagelse rekommenderar vi att Umeå kommun överväger att införa ett ledningssystem för informationssäkerhet (LIS) för att möjliggöra ett mer strukturerat och systematiskt arbete som har ledningens uttalade stöd och engagemang. Vi föreslår även att Umeå kommun definierar och tillsätter den roll i nämndernas förvaltningar som ska ansvara för att samordna och driva respektive nämnds arbete med IT- och informationssäkerhet. Vi noterar även att kommunen skulle dra nytta av att etablera en långsiktig strategi och tydliga mål för kommunens informationssäkerhetsarbete. Detta skulle hjälpa verksamheterna att fokusera på rätt aktiviteter och även samverka med digitaliseringsarbetet.

Granskningen visar också på att Umeå kommun tillsett ett grundläggande arbete med operationella rutiner för informationssäkerhetsarbete, men att det finns potential till förbättring. VI rekommenderar Umeå att förbättra processen för granskning av behörigheter till informationssystem, implementera en kommungemensam kontinuitetsplan, och accelerera arbetet med informationsklassning och riskanalyser.

Definitioner

Active Directory (AD): Katalogtjänst vilken lagrar information om resurser (såsom användare). Separata IT-system kan kopplas till Active Directory och både inloggning och behörighetsroller i systemen kan således styras genom inställningar och rolluppsättning i Active Directory. Detta möjliggör för central användarhantering och automatisk inloggning.

Säkerhetskopiering: Kopia av den information som finns i en databas eller på en server.

Återläsningstest: För att säkerställa att en säkerhetskopia fungerar som den ska och inte är sönder eller ofullständig så är det god praxis att genomföra tester av de säkerhetskopior som genomförts. Testet går ut på att återläsa in kopian in på servern eller databasen igen och granska innehållets korrekthet och fullständighet.

Förvaltningsobjekt: Styrande enhet inom vilken ett antal olika informationssystem för en viss typ av kommunens verksamhet innefattas. Förvaltningsenheten styrs av en styrgrupp som beslutar om förvaltningsplan och budget. System är uppdelade på olika förvaltningsgrupper inom ett förvaltningsobjekt.

Systemförvaltare: Ansvarar för att operativt sköta ett systems förvaltning inom givna ekonomiska ramar.

Systemägare: Verksamhetens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.

Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.

Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.

Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.

SLA (Service Level Agreement): Servicenivåavtal mellan beställare och tjänsteleverantör där överenskomna krav som ställs på tjänsten definierats.

KLASSA: Klassa är ett verktyg för att genomföra en kombinerad informationsklassning, riskanalys och åtgärdsplan, framtagen av Sveriges Kommuner och Regioner (SKR). Verktyget är framtaget i enlighet med ISO27001.

Applikation: Datorprogram med olika typer av funktionalitet beroende på applikationens syfte. Applikationen finns lagrad på en dator eller en server.

Databas: En databas är en katalogtjänst med indexerad information om resurser (såsom tex. användare).

Server: En server är ett datorprogram som bidrar med funktionalitet till ett annat program via en nätverksuppkoppling.

Nätverk: Ett nätverk administrerar koppling mellan olika resurser såsom olika program.

Ärendehanteringssystem: Ett ärendehanteringssystem är en typ av informationssystem som används för att dokumentera information rörande genomförandets av olika processer eller rutiner inom verksamheten, såsom exempelvis förändringsprocessen eller incidenthanteringsprocessen. Exempel på ärendehanteringssystem som Lunds kommun använder är Servis, TFS och Stratsys.

Innehåll

1. Inledning

1.1 Bakgrund

Umeå kommun och dess olika nämnder och förvaltningar hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

I tidigare granskningar har kommunens revisorer identifierat risker relaterat till kommunens övergripande arbete med IT- och informationssäkerhet samt sårbarheter kopplat till verksamhetskritiska system inom kommunen. Revisorerna har därför valt att genomföra en granskning för att kartlägga kommunens arbete med IT- och informationssäkerhet. Riskerna inom dessa områden är inte specifikt relaterade till Umeå kommun utan gäller hela den offentliga sektorn.

1.2 Syfte

Granskningens syfte är att bedöma om det finns brister i kommunens interna kontroll kopplat till säkerställande av att arbetet med IT- och informationssäkerhet är ändamålsenligt. Vidare är syftet också att bedöma i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. För att uppnå granskningens syfte besvaras följande frågor:

- Kan styrningen av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?
- Är arbetet med att följa upp att beslut och styrningsdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?
- Är Umeå kommuns incidenthanteringsprocess ändamålsenlig?

1.3 Genomförande och revisionskriterier

Granskningen har genomförts genom intervjuer med identifierade nyckelpersoner för kommunens IT- och informationssäkerhetsarbete samt av relevant styrdokumentation. Granskningen är utförd mot god praxis inom informations- och IT-säkerhetsområdet och bygger på EY:s granskningsprogram Cyber och Informationssäkerhet (GCI), med fokus på offentlig verksamhet.

GCI baseras på erkända ramverk såsom ISO/EC27000-serien och Myndigheten för Samhällsskydd och Beredskaps (MSBs) metodstöd för informationssäkerhet.

Intervjuer har genomförts med:

- IT-driftchef
- Informationssäkerhetssamordnare
- Samordnare för systemförvaltningsmodell

Samtliga intervjuade har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta.

Fullständig källförteckning framgår av bilaga 1.

1.4 Avgränsning

Granskningen är avgränsad till att ge en övergripande bild av området och kan i första hand användas till att utgöra en lägesbild och kunskapsunderlag i det fortsatta IT- och informationssäkerhetsarbetet. Således syftar granskningen inte till att kontrollera att arbetet, såsom det är utformat, har genomförts, och rapporten syftar heller inte till att bedöma den faktiska informationssäkerheten i enskilda system eller hos enskilda verksamheter inom kommunen.

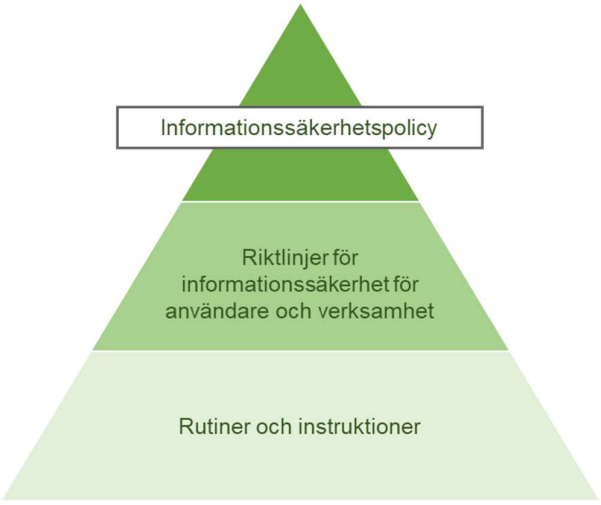
Granskningen syftar till att genomföra en bedömning och tillhandahålla en översiktsbild av hur Umeå kommun har utformat sitt arbete med IT- och informationssäkerhet. Granskningen täcker således inte enskilda IT-system eller applikationer. Vidare omfattar granskningen endast hantering av incidenter kopplat till IT- och informationssäkerhet och inte kommunens incidenthanteringsprocess i sin helhet.

2. Strategi, styrning och organisation

2.1 Styrdokument

Arbetet med IT- och informationssäkerhet i Umeå kommun kan illustreras genom en pyramidstruktur av styrningsdokument där *informationssäkerhetspolicyn* är tänkt att definiera kommunens mål och viljeinriktning med informationssäkerhetsarbetet som sedan förtydligas i *Riktlinjer för informationssäkerhet – användare* samt *Riktlinjer för informationssäkerhet – verksamhet* för den enskilde respektive för kommunens verksamheter, se schematisk representation nedan. Policyn beskriver syftet med kommunens informationssäkerhetsarbete, sätter upp ett antal mål för informationssäkerhetsarbetet, samt definierar vilka som har det övergripande ansvaret. Ett tydliggörande av ansvarsfördelningen görs också i riktlinjerna för kommunens verksamheter som även innehåller kortfattade rollbeskrivningar. Riktlinjerna för användare och verksamheter berör huvudområdena inom IT- och informationssäkerhet såsom Lösenordspolicy, behörighets-, förändrings- och incidenthantering m.m. Mer detaljerade styrande dokument så som rutiner och instruktioner för att säkerställa att verksamheternas processer efterlever riktlinjerna är i huvudsak vardera nämnds ansvar att tillse. Från kommungemensam IT-samordning har man dock tagit fram vissa rutiner och instruktioner för att stödja informationssäkerhetsarbetet i enlighet med riktlinjerna, så som metodstöd för informationsklassning, regler för e-post användning, informationshantering i molntjänster m.m.

Informationssäkerhetspolicyn är framtagen av kommungemensam IT-samordning och är fastställd av Kommunfullmäktige. Riktlinjerna är framtagna inom kommungemensam IT-samordning och är godkända av IT-chef.



Figur 1 - Schematisk bild över strukturen på Umeå kommuns styrande dokument för IT- och informationssäkerhet

För att få hela bilden av informationssäkerhetsarbetet bör även *Systemförvaltningsmodellen* nämnas. Kommunen har arbetat för att definiera en gemensam systemförvaltningsmodell. Modellen innehåller en beskrivning av de

samlade åtgärder som görs för att kontinuerligt administrera, underhålla, och vidareutveckla IT-systemen och de tillhörande processerna vilket även involverar IT- och informationssäkerhetsprocesser. Modellen för systemförvaltning, som bygger på pm3-modellen, har utformats av Kommungemensam IT-samordning och fastställts av högsta tjänstemannaledningen (hette då Stadsdirektörens ledningsgrupp).

Inom kommunen finns utöver ovan nämnda policyer och riktlinjer beslutade styrande dokument, både kommungemensamma och nämndspecifika, som berör informationssäkerhet i olika grad. Diskussioner har förts kring det, men det har dock inte implementerats något mer formaliserat Ledningssystem för Informationssäkerhet som innebär att kommunen från centralt håll eller inom förvaltningarna jobbar strukturerat och systematiskt med informationssäkerhet med ledningens uttalade stöd. Just ledningens stöd och involvering har dock setts som en viktig del i informationssäkerhetsarbetet och kommunen har därför inkluderat informationssäkerhet som en del i högsta ledningens genomgång för kvalitet, miljö och arbetsmiljö, där förvaltningschefer årligen skall gå igenom och diskutera status på arbetet. Dock har inte samtliga förvaltningar implementerat det ledningssystem för kvalitetsledning som inkluderar högsta ledningens genomgång, och dessa granskar inte heller informationssäkerhet inom internkontrollen.

2.2 Ansvarsfördelning och organisation

Organisationen och dess ansvar för Umeå kommuns informationssäkerhetsarbete beskrivs i kommunens informationssäkerhetspolicy, riktlinjer för informationssäkerhet, modell för systemförvaltning, samt ett dokument framtaget av samordnare för systemförvaltning kallat ”Ansvar och roller för ägande och förvaltande av informationssystem”.

Umeå kommuns informationssäkerhetspolicy beskriver att ansvaret för informationssäkerhet följer verksamhetsansvaret. Det vill säga att alla har ett ansvar för informationssäkerheten utifrån gällande delegationsordning och ansvarsfördelning, samt att den som upptäcker informationssäkerhetsbrister har ett ansvar att rapportera detta till chef eller säkerhetsfunktionen. Vidare beskriver informationssäkerhetspolicyn att chefer har ett ansvar att aktivt bidra till en positiv attityd till säkerhetsarbetet.

Som riktlinjerna för informationssäkerhet detaljerar, faller det faktiska ansvaret för informationen och informationssäkerheten inom ett verksamhetsområde på nämnderna och dess förvaltningar. Inom förvaltningarna är det huvudsakliga ansvaret fördelat över chefer, informationsägare, systemägare, och andra medarbetare. Det är enligt riktlinjerna upp till varje chef att ansvara för att förutsättningar för informationssäkerheten inom den egna organisationen finns och fungerar, samt att medvetandegöra informationsanvändare på deras ansvar. Vidare beskrivs det centrala ansvar som verksamheten kommungemensam IT-samordning under tekniska nämnden har i att definiera kommungemensamma informationssäkerhetskrav samt stötta arbetet med dessa. Kommungemensam IT-samordning, och primärt informationssäkerhetssamordnaren leder och koordinerar

kommunens arbete med att uppnå informationssäkerhetspolicyns mål, samt initierar och stöttar verksamheternas arbete.

Riktlinjerna för informationssäkerhet fastslår även att varje system i kommunen ska ha dels en juridisk systemägare (ansvarig nämnd) som innehar det övergripande ansvaret för alla aktiviteter som bedrivs inom respektive ansvarsområde utifrån reglemente och delegationer, och dels en operativ systemägare/objektägare i form av en person som är övergripande operativt ansvarig för informationssystemet i organisationen. Detta innebär även ansvar för att systemet ska uppfylla de informationssäkerhetskrav som ställs på systemet utifrån rådande lagar och riktlinjer, samt säkerställa att informationsklassning genomförs, att kontinuitetsplaner tagits fram och fastställts, att ändringshantering genomförs kontrollerat och strukturerat m.m.

Även kommunens modell för systemförvaltning beskriver roller som är relevanta utifrån ett informationssäkerhetsperspektiv. Modellen antogs av kommungemensam IT-samordning 2009 (reviderades senast under 2020) och beskriver att alla system som hämtar in och lagrar information digitalt och där informationen ägs av kommunal myndighet kommunens system ska organiseras i så kallade förvaltningsobjekt med en förvaltningsorganisation med representanter från både verksamheten och IT, se tabell nedan.

Part / Nivå	Verksamhetsnära förvaltning	IT-nära förvaltning	Beslutsforum
STRATEGISK	Organisationens ledning		Förvaltningsportfölj-styrgrupp
TAKTISK/ BUDGET	objektägare	objektägare IT	Objektstyrgrupp
TAKTISK/ BESLUT	förvaltningsledare	förvaltningsledare IT	Objektledning
OPERATIV	Objektspecialister, t.ex.: systemförvaltare, systemadministratörer	IT-specialister	

Tabell 1 - Roller enligt Umeå kommuns systemförvaltningsmodell

Ur ett informationssäkerhetsperspektiv är förvaltningsobjekten relevanta när det kommer till forum för uppföljning av förvaltningsarbetet samt beslut och genomförande av förändringar i system. Objektstyrgruppen och objektledningen agerar på taktisk nivå. Genom det planerings- och prioriteringsarbete som sker där skall säkerställas att den operativa förvaltningsverksamheten bidrar till de mål med informationssäkerhetsarbetet som finns definierade i kommunens policy och riktlinjer för informationssäkerhet.

2.3 Personal och utbildning

Vid perioden för denna granskning (Juni, 2020) så är det kommunens uppfattning att man i nämndernas förvaltningsorganisationer har kommit olika långt med att

implementera ansvar och organisationsstrukturer i enlighet med riktlinjer och modellen för systemförvaltning.

Organisationen rörande informationssäkerhet är slimmad. Informationssäkerhetssamordnaren inom kommungemensam IT-samordning leder och koordinerar kommunens arbete med att uppnå informationssäkerhetspolicyns mål, samt initierar och stöttar förvaltningarnas arbete. Dock saknas det personer i förvaltningarna som arbetar operativt med informationssäkerhet . I samband med inträdet av GDPR har personuppgiftskoordinatorer i varje nämnds förvaltningsorganisation utsetts, vilka är kontaktpunkter och ansvariga för att koordinera arbetet med GDPR i deras verksamheter. Det saknas emellertid utsedda personer som ansvarar för koordinering, uppföljning, och kontroll av övrigt ansvar rörande IT- och informationssäkerhet inom förvaltningsobjekten och övriga delar av de olika förvaltningsorganisationerna.

Detta tros vara en följd av att resurstillsättningen samt kunskapen om informationssäkerhet varierar mellan kommunens olika verksamheter och mellan de olika förvaltningsobjekten. Det varierar i vilken utsträckning de känner ett ansvar för information- och informationssystem och att arbeta med skyddsåtgärder för information som behandlas i systemen. Detta innebär en varierande grad av genomförande av viktiga delar i informationssäkerhetsarbetet som definieras i kommunens riktlinjer för informationssäkerhet, t.ex. riskanalyser, informationsklassificering, kontinuitetsplanering, m.m.

Utbildning- och informationsinsatser för att öka kunskapsnivån och medvetenheten genomförs, men det har konstaterats att det är en utmaning att nå ut till samtliga medarbetare. I tillägg till löpande dialog i olika forum informationssäkerhetssamordnare, dataskyddsombud, samordnare för systemförvaltning, och andra samordnande personer har med förvaltningsorganisationerna för att dela kunskap och expertis informerar informationssäkerhetssamordnare och dataskyddsombud 15 minuter vardera varje halvår vid introduktionsdagar för nyanställda. Under 2017 började även en webbaserad så kallad nano-utbildningslösning användas vilken skickas ut till samtliga kommunens medarbetare som innehar en mailadress. Nano-utbildningarna är korta utbildningar på olika teman inom IT- och informationssäkerhet vars grundmall är utformad av en extern leverantör och innehållet anpassat utifrån kommunens förutsättningar. Cirka två lektioner i veckan skickas ut till kommunens medarbetare under en period av 1 ½ månad under höstterminen. Kommunen upplever att dessa är mycket välgjorda och möjliggör en god grundförståelse för olika aspekter av säkerhet. Dock är det inte obligatoriskt för medarbetare att genomgå utbildningarna, och vid de uppföljningar som har gjorts har det noterats en generellt låg grad av genomförande inom kommunens olika verksamheter.

2.4 Externa leverantörer och hantering av leverantörsavtal

Upphandlingar av IT-system i Umeå kommun underordnar sig lagen om offentlig upphandling och själva upphandlingen hanteras av kommunens centrala inköpsfunktion Upphandlingsbyrån. Mycket arbete har lagts senaste åren på att ta fram riktlinjer och metodstöd vid upphandling av nya IT-system. För att verka för att

upphandlat IT-stöd levererar så mycket verksamhetsnytta som möjligt, att det följer de krav kommunen har kring säkerhet, samt att kritiska moment som informationsklassning och riskanalys genomförs, har en IT-upphandlingsmodell utarbetats av kommungemensam IT-samordning. Kommunfullmäktige har i kommunens IT-strategi beslutat att IT-upphandlingsmodellen ska tillämpas vid alla upphandlingar av IT-system och det är den som verksamheten har utsett att leda arbetet i analysfasen som har ansvar att se till att ingående moment inkluderas i förstudien. Trots detta beslut förekommer det upphandlingar som inte följer IT-upphandlingsmodellen även om förbättring har skett då andelen upphandlingar som följer modellen har ökat från 74% 2017 till 89% 2020.

Enligt IT-upphandlingsmodellen skall först en analysfas genomföras där arbete genomförs för att konkretisera tänkt verksamhetsnytta med IT-systemet man vill upphandla, samt dokumentera tekniska krav samt informationssäkerhetskrav i en förstudierapport. Själva upphandlingen leds av upphandlare från upphandlingsbyrån. Förstudierapporten används som underlag för att ta fram avtalsvillkor och för att beskriva funktionella och icke-funktionella (tekniska och informationssäkerhetsmässiga) krav som ska ingå i förfrågningsunderlaget till potentiella leverantörer.

Som en del av förstudiefasen i IT-upphandlingsmodellen skall alltid en riskanalys och informationsklassning av datan som kommer att behandlas i systemet genomföras för att säkerställa att systemet (och leverantören) följer de krav på IT- och informationssäkerhet man har. Kommunens informationssäkerhetssamordnare involveras ofta i dessa moment eftersom förvaltningarna inte har någon operativ informationssäkerhetsresurs i den egna organisationen. Hon upplever att det i nuläget fungerar väl för att öka följsamheten gentemot policy och riktlinjer för informationssäkerhet för nya system som sätts i drift i kommunen. I IT-upphandlingsmodellen anges att en ansvarig för avtalsuppföljningen ska utses med ansvar för att säkerställa att kommunen faktiskt får det som har upphandlats, avtalats och betalats för. Samt att det skapas ett formellt underlag för godkännande av leveransen innan leveransprojektet avslutas. För löpande kontroll av leverantörer av upphandlade system har inga särskilda centrala riktlinjer för uppföljning av att leverantören följer avtalat ansvar för informationssäkerhet eller servicenivåavtal (SLA) definierats. Det ingår i förvaltningsobjektens ansvar att ha en kontinuerlig dialog med leverantören rörande driften och säkerheten i systemen men det genomförs sällan några formaliserade leverantörsgranskningar eller uppföljningar från förvaltningsobjekten. Upphandlingsbyrån har däremot nyligen fått i uppdrag att ta fram ett verktyg och en modell för avtalsuppföljning.

2.5 Operationella rutiner

2.5.1 Behörighetshantering

Grundåtkomst till Umeå-kommuns gemensamma Active Directory (AD) som möjliggör åtkomst till majoriteten av kommunens system administreras av IT. Active Directory är integrerat med personalsystemet vilket innebär att då en anställd börjar tilldelas han eller hon ett konto med grundbehörighet för att kunna logga in på sin

dator, och komma åt vissa gemensamma resurser som intranätet och liknande. Då en anställd slutar och användaren tas bort ut personalsystemet inaktiveras användaren även i Active Directory.

Även om ett Active Directory-konto möjliggör åtkomst till majoriteten av kommunens system krävs att användaren aktivt ges åtkomst till varje specifikt system och att användarrollen i systemet definieras. Detta hanteras vanligtvis inom förvaltningsobjekten. De krav som ställs på användare och verksamhet i processen för tilldelning av åtkomst till system är definierade i *Riktlinjer för informationssäkerhet – användare* samt *Riktlinjer för informationssäkerhet – verksamhet.* I det förstnämnda dokumentet stipuleras att användaren har ett ansvar att upprätthålla starka lösenord för sina konton till informationssystem, som inte delas med till andra och som uppfyller kommunens lösenordspolicy. I *riktlinjer för informationssäkerhet – verksamhet* anges att det är närmsta chefs ansvar att besluta om och godkänna behörigheter till informationssystem. Det definieras även att det är ansvarig chefs ansvar att beställa inaktivering av behörigheter samt besluta om åtkomst till system från distans för anställda. Processen för tillägg och borttag hanteras i praktiken av förvaltningsobjekten som administrerar behörigheter efter godkännanden från användares chefer. Periodiska granskningar av att aktuella behörigheter i system är lämpliga genomförs inom varje förvaltningsobjekt om de ser ett behov för det. Det finns dock inga riktlinjer som kravställer att sådana granskningar ska göras enligt given frekvens.

2.5.2 Drift och IT-incidenthantering

IT-funktionen inom Umeå kommun ansvarar för driften av informationssystem som inte tillhandahålls av extern leverantör. Kontinuerlig säkerhetskopiering genomförs för att säkerställa att data inte går förlorad. Utöver detta replikeras all data synkront mellan 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. Återläsningstester genomförs regelbundet. Frekvensen beror på vilket system det rör sig om.

IT-funktionen har utformat en väldokumenterad kontinuitetsplan som beskriver rutiner för katastrofhantering och reservrutiner vid större avbrott. Krav på frekvens för säkerhetskopiering, acceptabel återställningstid osv. bör komma som krav från verksamheten t ex utifrån gjorda informationssäkerhetsklassningar men i många fall där dessa klassningar ännu inte är gjorda så är dessa krav istället definierade av IT. Strukturerade tester av kontinuitetsplanen genomförs två gånger per år där strömmen stängs av helt och hållet.

Kommunen har en central process för hantering av IT- och informationssäkerhetsrelaterade incidenter. Användare kan antingen rapportera incidenter själva via IT-självservice, alternativt ringa eller maila in incidenter till IT-support, som sedan registrerar ett ärende i kommunens ärendehanteringssystem Easit. Utifrån detta prioriteras och eskaleras ärendet så att incidenten hanteras enligt lämplig tidsram och av rätt person. Informationssäkerhetssamordnaren sammanfattar årligen en rapport om informationssäkerhet som går till förvaltningsledningarna.

Rapporten innefattar en sammanfattning av det kontinuerliga arbetet med rutiner för att upptäcka och hantera incidenter.

2.5.3 Programförändringar

Kommunen har efter medvetet övervägande ingen kommungemensam rutin för genomförande av programförändringar för IT-system. Man har gjort försök att ta fram och använda sig av en sådan, men upplevde att det i många fall blev för styltigt. För vissa system är det viktigt att processen är rigorös och inkluderar noggrann testning och godkännanden, medan det för andra mindre system har upplevts vara onödigt och bidrar till för långa ledtider på grund av administration.

Det är varje förvaltningsobjekts ansvar att tillse att lämpliga rutiner finns och efterlevs för införande av ändringshantering i förvaltningsobjektens system. Modellen för systemförvaltning i kommunen innehåller en beskrivning av process för ändringshantering som förvaltningsobjekten uppmuntras att efterleva. Enligt denna process skall ändringshantering innefatta följande moment och kontrollpunkter:

1. Framtagande av ändringsförslag och önskemål – Förvaltningsledare och objektspecialister dokumenterar på ett systematiskt sätt föreslagen ändrings syfte, typ och kategori
2. Beredning och prioritering – Vidare analys av ändringsförslaget för att komplettera med nödvändiga uppgifter för att kunna fatta beslut om ändringen är genomförbar. Kan inkludera moment så som ytterligare kravspecifikation, konsekvensbedömning avseende vilken påverkan ändringen får vid införande (eller icke-införande), nyttouppskattning av ändringen för verksamheten, samt beräknad kostnad och tidsåtgång.
3. Beslut - Beslut om ändring tas utifrån de underlag som har arbetats fram i tidigare steg. Beslut eller avslag dokumenteras med kort motivering. Förvaltningsledaren ansvarar för att beslutade ändringar beställs genomförs med de medel som finns avsatta.
4. Beställning från externa leverantörer - I dessa fall ska kontroll ske av eventuella ramavtal eller om det är fråga om en upphandling enligt lagen om offentlig upphandling innan beställningen görs. Beställningsdokumenten med kravspecifikation och ev. kostnadsofferter ska sparas av förvaltningsledaren.
5. Genomförande - Systemleverantören (extern eller intern) ansvarar för genomförandet och initial testning av ändringen och att ändringsdokumentation upprättas. Förvaltningsledaren ansvarar ytterst för att det görs eventuella anpassningar och förändringar i arbetsprocesser som kan bli effekter av systemförändringar.
6. Test - När leverantören levererat systemändringen ska den alltid först testas, helst i separat testmiljö. Förvaltningsledare/systemförvaltare ansvarar för att både test av ändringens funktionalitet samt att den fungerar i Umeå kommuns driftmiljö genomförs. Efter godkänt test sker en formell produktionssättning i produktionsmiljön.

7. Beslut om införande - Förvaltningsledare beslutar (i normalfallet) efter samråd med t.ex. objektspecialister och IT-specialister, i vissa fall även tillsammans med förvaltningsledare IT, om lämpligt datum för driftsättning av ändringen.
8. Införande, information och utbildning - Driftsättning utförs enligt beslut i tidigare steg. Förvaltningsledaren och/eller objektspecialister eller systemförvaltare har ansvar att planera informations- och utbildningsinsatser.
9. Uppföljning - Förvaltningsledaren ansvarar för att göra en utvärdering av genomförda åtgärder utifrån uppnådd effekt och nedlagd resursåtgång samt kostnad.

2.5.4 Informationsklassning och riskanalys

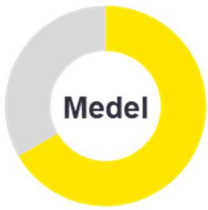
Informationsklassning är en metod som hjälper organisationer att välja rätt åtgärder för att skydda informationen. Umeå kommun har inom kommungemensam IT-samordning utformat en instruktion för som är baserat på SKR:s modell KLASSA, vilken har tagits fram för att förenkla kommuners och regioners informationsklassning. Verktyget används i arbetet att identifiera vilka av kommunens informationssystem som innehåller skyddsvärd information och vilken skyddsnivå informationen som behandlas i systemet bör ha. Kommunens instruktion beskriver bland annat syftet med informationsklassningar, när sådana ska göras, vem som ansvarar för dem och hur de ska dokumenteras, samt förklaringar till de olika skyddsnivåerna. Det är informationsägaren för informationen som behandlas som ansvarar för klassificering av verksamhetens information. Enligt årshjulet för systemförvaltning ska IT-system med informationsklassning nivå 2 eller högre genomgå en KLASSA-analys med stöd av informationssäkerhetssamordnaren. För klassificering av IT-system är det ytterst systemägare som har ansvar att säkerställa att systemen är rätt klassade och har det skydd som krävs. Mycket av ansvaret faller alltså på förvaltningsobjekten. Från kommungemensam IT-samordning har informationssäkerhetssamordnare och samordnare för systemförvaltning drivit informationsklassning som ett prioritetsområde för att öka medvetenheten hos förvaltningsobjekten och stödja dem i genomförandet av klassningarna. Dock har man kommit olika långt i olika förvaltningsobjekt och verksamheter, och det återstår fortfarande ett stort antal objekt och verksamheter där informationsklassning är delvis eller ej ännu genomförd.

En riskanalys genomförs för att identifiera och bedöma sådana risker som skulle kunna äventyra säkerheten för informationen i kommunens system. Kommunen har tagit fram en modell för riskanalys. Som en del av förstudiefasen i IT-upphandlingsmodellen skall alltid en riskanalys för att bedöma risker för datan som kommer att behandlas i systemet genomföras. Detta bedöms av kommunen fungera väl. Även för befintliga system och informationen i dessa skall riskanalyser genomföras för att säkerställa att information har rätt skyddsnivå. Dock är genomförandegraden för befintliga system och informationen i dessa låg i förhållande till för nya system.

4. Iakttagelser och rekommendationer

Under granskningen har vi identifierat iakttagelser inom granskade områden. För varje iakttagelse har vi lämnat rekommendationer som syftar till att stödja Umeå kommun i dess framtida arbete med IT- och informationssäkerhet. Identifierade iakttagelser har klassificerats enligt tre prioritetsnivåer avseende hur omfattande dess eventuella inverkan anses vara:

Prioritering låg: Observation som ej direkt påverkar verksamhetens mål, men som kan medföra ineffektiv verksamhet, mindre brister i IT- och informationssäkerhet, efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.



Prioritering medel: Observation som anses kunna ha påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av verksamhetens resurser.

Prioritering hög: Observation av större karaktär som anses kunna ha hög påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer.

4.1 Strategi, styrning och organisation – IT- och informationssäkerhet

4.1.1 Överväg att införa ett Ledningssystem för Informationssäkerhet

Iakttagelse

Långsiktig informationssäkerhet kräver ett helhetsgrepp och fungerande arbetssätt för att säkerställa att kommunens information ges ändamålsenligt skydd. Umeå kommun har etablerat ett grundläggande ramverk i form av systemförvaltningsmodell, policy, riktlinjer och instruktioner för informationssäkerhetsarbetet. Det har dock noterats att den övergripande styrningen av arbetet med informationssäkerhet i vissa hänseenden saknar tydlighet avseende ansvar, mandat och uppföljning för att säkerställa ändamålsenligt arbete med informationssäkerhet i alla kommunens verksamheter. Initiativ har dock tagits för att höja förvaltningsledningarnas medvetandehet i form av att informationssäkerhet har inkluderats som en punkt i högsta ledningens genomgång.

Risken med otydligt ansvar, mandat och uppföljning är att kommunens policyer och riktlinjer inte efterlevs och att skyddsåtgärder genomförs på en ojämn nivå runtom i kommunen.

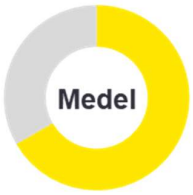
Ett ledningssystem för informationssäkerhet möjliggör ett mer strukturerat och systematiskt arbete med informationssäkerhet som har ledningens uttalade stöd och engagemang. Det ger ett verktyg för att formalisera ansvar och ägandeskap för mål, policies, och riktlinjer samt tillse att modeller och rutiner utarbetas för att kontinuerligt kontrollera, utvärdera, och förbättra informationssäkerhetsarbetet i organisationen.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Överväga att införa ett ledningssystem för informationssäkerhet samt ta fram ett förslag på tillvägagångssätt för införande. Detta skulle möjliggöra ett mer strukturerat och systematiskt arbete med informationssäkerhet med ledningens uttalade stöd och engagemang.

4.1.2 Tydliggör ansvar för IT- och informationssäkerhetsarbete i nämndernas förvaltningsorganisationer



Iakttagelse

Tekniska nämnden, och primärt kommungemensam IT-samordning leder och koordinerar kommunens arbete med att uppnå riktlinjer för IT- och informationssäkerhet, samt initierar och stöttar nämndernas förvaltningar i deras arbete. Det är dock förvaltningschefers ansvar att besluta och se till att rätt förutsättningar finns och fungerar inom den egna organisationen. Kapaciteten finns inte inom kommungemensam IT-samordning att både samordna och stötta samt ansvara för att arbete enligt riktlinjer alltid utförs. Då de är placerade under tekniska nämnden och inte centralt har man heller inte ansvar för, eller mandat att besluta kring, prioritering av IT- och informationssäkerhetsinsatser i övriga nämnder.

En brist på ansvar för att bedriva IT- och informationssäkerhetsarbete i nämndernas förvaltningsorganisationer medför en risk att riktlinjer inte efterlevs och att aktiviteter inte genomförs enligt den frekvens och omfattning som är önskvärd. Även om sådana aktiviteter genomförs av förvaltningsobjekt, personuppgiftskoordinatorer, och andra ansvariga inom nämnderna har noterats en varierande genomförandegrad av exempelvis riskanalyser, informationsklassningar, kontinuitetsplaner m.m. i de olika verksamheterna.

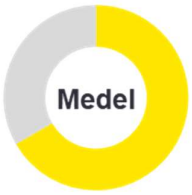
Rekommendation

Kommunstyrelsen rekommenderas att:

- Säkerställa att nämndernas förvaltningar har en funktion som ansvarar för att samordna och driva respektive nämnds arbete med IT- och informationssäkerhet Rollen kan sammanföras med rollen personuppgiftskoordinator.
- Säkerställa att rollen har ett tydligt mandat kring prioritering av IT- och informationssäkerhetsinsatser inom nämnden och att den har nära kontakt med förvaltningsledningen.
- Etablera processer och instruktioner för att i rollen bedriva uppföljning av verksamhetens IT- och informationssäkerhetsarbete kopplat till de riktlinjer, rutiner, och instruktioner som finns framtagna centralt
- Tydliggöra informationsägares och personuppgifts-ansvariges ansvar att se till att samtliga medarbetare genomför nano-utbildningarna. Inför formella uppmaningar att genomgå utbildningarna och säkerställ att varje chef följer upp de medarbetare som inte genomfört utbildningen.

4.1.3 Etablera en långsiktig strategi och tydliga mål för kommunens IT- och informationssäkerhetsarbete

För att ändamålsenlig IT- och informationssäkerhet ska kunna uppnås är det viktigt att kommunen har strategiska mål som definierar viljeriktning för arbetet både på lång och kort sikt. Umeå kommun har i informationssäkerhetspolicyn som antogs av KF 2009 beskrivit syfte, mål, och viljeriktning med kommunens informationssäkerhetsarbete, men detta är mycket generellt hållet och kopplas inte till andra strategiska mål inom kommunen inom till exempel IT- och digitalisering.



Iakttagelse

För att viljeriktningen ska vara tydlig för organisationen och för att kontinuerligt fokusera på rätt aktiviteter är det viktigt att konkreta långsiktiga, samt kortsiktiga mål som definierar hur den långsiktiga strategin ska realiseras de kommande 1-2 åren, är formulerade. Kommunen har formulerat krav som ställs på användare och verksamheter i riktlinjer för informationssäkerhet, men inte tydligt definierat mål som är mätbara och kan stämmas av för att utvärdera kommunens utveckling.

Avsaknaden av en tydlig strategi med mätbara mål på lång och kort sikt kan påverka IT- och informationssäkerhetsarbetets effektivitet och följsamhet gentemot andra strategiska målsättningar och initiativ.

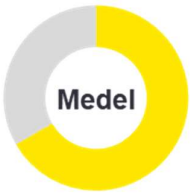
Rekommendation

Kommunstyrelsen rekommenderas att:

- Tydligt definiera och prioritera det kommunövergripande IT- och informationssäkerhetsarbetets innehåll, omfattning, kortsiktiga och långsiktiga mål och vision samt säkerställa att förvaltningarnas mål med avseende på den dagliga verksamheten är i enlighet med denna övergripande strategi.
- Etablera en process för utvärdering, uppföljning och utveckling av definierade mål.

4.2 IT-drift, förändringar samt behörigheter

4.2.1 Tydliggör förvaltningsobjektens ansvar att säkerställa lämpligheten av användare och deras behörighetsnivåer i informationssystem



Iakttagelse

Ansvaret för att löpande säkerställa att behörigheter i kommunens informationssystem är lämpliga utifrån användares anställningsstatus, roller och ansvar i organisationen faller på förvaltningsobjekten för de olika systemen. Det genomförs ingen centralt initierad periodisk genomgång för att säkerställa att användare har rätt behörigheter samt för att säkerställa att inga behörigheter ligger kvar efter avslutad anställning, utan detta ansvar förväntas tas av förvaltningsobjekten. Det har dock noterats att detta ansvar inte är tydliggjort i de kommungemensamma riktlinjerna för informationssäkerhet, eller i beskrivningen av systemförvaltningsmodellen vilket ökar risken att löpande kontroller inte genomförs enligt önskvärd frekvens.

Avsaknad av periodisk kontroll av behörigheter medför en risk att personer som inte längre jobbar kvar eller har fått ändrade arbetsuppgifter har kvar gamla behörigheter i systemen. Detta ökar risken för oegentligheter eller oavsiktliga fel på grund av att medarbetare har behörigheter som tillåter aktiviteter som användaren inte borde ha tillgång till i sin arbetsroll.

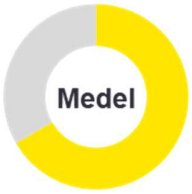
Rekommendation

Kommunen rekommenderas att säkerställa att förvaltningsobjektens ansvar att periodvis (minst årligen) kontrollera användare och deras behörighetsnivåer i informationssystemen tydliggörs i relevant styrdokumentation, förslagsvis i riktlinjerna för informationssäkerhet samt i modellen för systemförvaltning.

För att säkerställa god kvalitet på genomgångarna rekommenderas kommunstyrelsen att upprätta riktlinjer som tydliggör att:

- Granskade behörigheter ska baseras på ett utdrag som är systemgenererat, dvs har tagits ut från systemet i fråga och inte är baserad på en manuell förteckning eller liknande
- Både förekomsten av användarkontot samt de roller användare har ska granskas, för att säkerställa både att det är rätt användare som har åtkomst samt att de har korrekta behörighetsnivåer

4.2.2 Definiera och implementera en kommungemensam kontinuitetsplan för att säkerställa lämpliga reservrutiner och åtgärder vid avbrott



Iakttagelse

Inom IT-funktionen har man en väl utformad och dokumenterad kontinuitetsplan som beskriver rutiner för katastrofhantering och reservrutiner vid större avbrott som har påverkan för IT-driften. Strukturerade tester av denna plan genomförs två gånger per år för att säkerställa att man har rutiner och kapacitet för att upprätthålla driften och återställa system vid behov. I dessa tester är även externa leverantörer med.

Det har dock noterats att prioritetsordning och aktiviteter i kontinuitetsplanen är definierat av IT utifrån bedömning av vilka system och tjänster som är mest kritiska. Krav på exempelvis frekvens för säkerhetskopiering, acceptabel återställningstid, och data som behöver återläsas är definierade av IT och kommer inte som krav från verksamheten eller förvaltningsobjekten. Detta medför en risk att, även om IT har möjlighet att hantera ett avbrott och återställa systemen efter ett sådant, prioritetsordning och säkerhetsåtgärder inte följer verksamhetens behov.

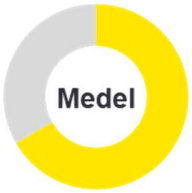
Rekommendation

Kommunstyrelsen rekommenderas att säkerställa att:

- IT-funktionen tillsammans med informationssäkerhetsamordnare (eller andra personer som bedöms vara lämpade) driver genomförandet av en gemensam kontinuitetsplan för kommunen i samråd med lämpliga representanter från verksamheter och/eller förvaltningsobjekt. Den gemensamma kontinuitetsplanen bör föregås av en analys av informationssäkerhetsrelaterade risker, samt bedömning av känslighet av system och tjänster för att säkerställa att prioritetsordning och aktiviteter i IT:s kontinuitetsplan är lämpligt definierade. Vidare bör kontinuitetsplanen även innefatta av verksamheterna dokumenterade reservrutiner som verksamheten ska tillämpa vid eventuella avbrott för att säkerställa kontinuitet i verksamheter och deras tjänster.

4.3 Incident-, risk- och informationshantering

4.3.1 Accelerera arbetet med informationsklassning och riskanalyser



Iakttagelse

Kommungemensam IT-samordning har drivit informationsklassning som ett prioritetsområde för att öka medvetenheten hos förvaltningsobjekten och stödja dem i genomförandet av klassningarna. Dock har man kommit olika långt i olika förvaltningsobjekt och verksamheter, och det återstår fortfarande ett antal objekt och verksamheter där informationsklassning är delvis eller ej ännu genomförd.

Riskanalyser ska alltid ske i förstudiefasen enligt IT-upphandlingsmodellen för att bedöma risker för datan som kommer att behandlas i systemet. Detta bedöms av kommunen fungera väl. För befintliga system och informationen i dessa finns dock ingen kommungemensam rutin eller centralt framtagen modell för att kontinuerligt identifiera och se över risker. För att säkerställa att information hanteras på ett säkert sätt bör hot och risker relaterade till informationen kontinuerligt identifieras, analyseras och hanteras med lämpliga skyddsåtgärder.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Säkerställa fortsatt prioritering av- och genomförande av informationsklassningar i verksamheter och förvaltningsobjekt, förslagsvis av person i nämnderna som ska ansvara för att samordna och driva nämndens arbete med IT- och informationssäkerhet (se iakttagelse 4.1.2)
- Inventera kommunens verksamhetssystem och utifrån nivå av känslighet på informationen som behandlas i systemen besluta mål för vilka verksamhetssystem riskanalys och informationsklassning skall genomföras
- Införa en modell för uppföljning av att riskanalys och informationsklassning har genomförts för beslutade system

4.3.2 Tydliggör riktlinjer för uppföljning och övervakning av externa leverantörer

Organisationer förlitar sig mer och mer på tredjepartsleverantörer av IT-lösningar för att effektivisera och uppnå större verksamhetsnytta och Umeå kommun är inget undantag. Detta ökade beroende av externa leverantörer introducerar nya risker.

Iakttagelse

Kommunen har i avtalsmallar lämpliga skrivningar som ställer krav på leverantören avseende informationssäkerhet och dataskydd. Dock sker ingen standardiserad uppföljning av att leverantörer följer avtalade villkor. Det är systemförvaltarnas ansvar att vid behov följa upp på driftsnivåer samt hantering av incidenter med respektive IT-leverantör. Det saknas dock riktlinjer och metodstöd relaterat till IT- och informationssäkerhet, som bör följas upp. Detta leder till att uppföljningar inte genomförs eller håller olika nivå, samt ökar risken för påverkan av incidenter som är bortom kommunens kontroll.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Införa en process för att löpande granska tredjepartsleverantörer av IT-lösningar med tydliga riktlinjer och krav på innehåll samt deltagande av sakkunniga vid dessa tillfällen.
- Definiera vilken funktion eller vilka personer som är ansvariga för att säkerställa att granskning av tredjepartsleverantörer sker enligt punkten ovan.

5. Svar på revisionsfrågor

Granskningen har syftat till att på uppdrag av revisorerna genomföra en övergripande genomgång av kommunens IT- och informationssäkerhet. Granskningen har utgått från tre revisionsfrågor, vilka besvaras nedan.

Kan styrningen av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?

Styrningen av informationssäkerhetsarbetet i Umeå kommun bedöms vara **delvis ändamålsenligt**. Umeå kommun har etablerat ett grundläggande ramverk i form av systemförvaltningsmodell, policy, riktlinjer och instruktioner för informationssäkerhetsarbetet. Det har dock noterats att den övergripande styrningen av arbetet med informationssäkerhet i vissa hänseenden saknar tydlighet avseende ansvar, mandat och uppföljning för att säkerställa ändamålsenligt arbete med informationssäkerhet i alla kommunens verksamheter. Kommunens mål och vision med sitt informationssäkerhetsarbete samt hur man ska uppnå en god kommungemensam nivå av säkerhet är inte tydliggjort. Vidare har brister noterats i kontinuitetsplanering, behörighet- och åtkomsthantering samt informationsklassning och riskanalyser.

Är arbetet med att följa upp att beslut och styrningsdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?

Arbetet med uppföljning av efterlevnad av beslut och styrningsdokument relaterat till informationssäkerhet bedöms vara **delvis ändamålsenligt**. Svaret grundar sig i att Umeå kommun inte har upprättat en ansvarsfördelning rörande uppföljning av arbetet och inte tillsett ändamålsenliga processer för att uppföljning av nämndernas och förvaltningarnas arbete med informationssäkerhet implementerats och genomförs. Detta inkluderar exempelvis uppföljning av externa leverantörsavtal avseende informationssäkerhet och kontroll för borttag av användares behörigheter. Kommunen saknar en ansvarig funktion eller roll för samordning och koordinering mellan intressenter och aktiva förvaltningar inom IT- och informationssäkerhetsarbetet vilket blir synligt i avsaknaden av övergripande informationsklassning och kontinuitetsplan samt brister den i övergripande riskanalysen.

Är Umeå kommuns incidenthanteringsprocess ändamålsenlig?

Umeå kommun bedöms ha en **delvis ändamålsenlig** incidenthanteringsprocess. Kommunens incidentprocess är utformad enligt god praxis och är väl fungerande. Visst utrymme för förbättring finns, till exempel när det gäller att följa upp incidenter med leverantörer. Den huvudsakliga förbättringspunkten är dock att det saknas en rutin för att granska efterlevnaden av incidenthanteringsprocessen. I dagsläget är det osäkert om man fångar upp flertalet av de IT- och informationssäkerhetsrelaterade incidenterna ute i verksamheterna.

6. Slutsats

Digitaliseringen skapar inte bara affärsmöjligheter utan möjliggör fler sätt att attackera verksamheters information och system. De senaste åren har antalet cyberattacker ökat kraftigt, och bakom dem finns inte bara kriminella och hackare utan även statsstödda aktörer som har stor uthållighet och substantiella resurser. Genom att påskynda åtgärder för att öka säkerheten inom kritisk infrastruktur, höjs hela samhällets robusthet mot yttre störningar. IT och informationssäkerhet med stödjande lagstiftning i form av GDPR, Säkerhetsskyddslagen och NIS-direktivet är sätt att göra detta.

Granskningen syftar till att bedöma om Umeå kommun tillsett ändamålsenligt arbete med IT- och informationssäkerhet.

Utifrån granskningens syfte och grunderna för ansvarsprövning bedömer vi att Umeå kommun delvis tillsett ett ändamålsenligt arbete med IT- och informationssäkerhet. Kommunen har ett grundläggande informationssäkerhetsramverk i form av styrande dokument, roller och ansvar men brister i att inkorporera IT- och informationssäkerhet i verksamhetens dagliga arbete samt övrigt säkerhetsarbete, men vi rekommenderar att Umeå kommun överväger att införa ett ledningssystem för informationssäkerhet (LIS), förtydligar roller och ansvar, samt utvecklar en tydlig strategi. I kommunens operationella arbete bör fokus vara på att etablera processer och dokumentationsstöd för samordning, uppföljning och utbildning som säkerställer en ändamålsenlig säkerhetsnivå runtom i kommunen. Detta gäller en förbättrad process med tydligare ansvarsfördelning för granskning av behörigheter, fler utförda informationsklassningar och riskanalyser, samt att implementera en kommungemensam kontinuitetsplan.

Bilaga 1: Källförteckning

Intervjuade roller:

- IT-driftchef
- Informationssäkerhetssamordnare
- Samordnare för systemförvaltningsmodell

Dokumentation:

- Informationssäkerhetspolicy för Umeå kommun
- Riktlinjer för informationssäkerhet – användare
- Riktlinjer för informationssäkerhet – verksamhet
- IT-strategi
- E-post regler
- Filer och loggning av internettrafik
- Informationshantering O365 mejl och OneDrive
- Instruktion för informationsklassificering
- Riskanalys Datahallarna Interna & Externa resurser
- Kontinuitetsplan för strömavbrott datahallarna
- Förvaltningsarkitektur Umeå kommun
- Systemförvaltning i Umeå kommun
- Ansvar och roller för ägande och förvaltande av informationssystem
- Årshjul grundmall förvaltningsobjekt
- Printbilder med information om systemförvaltning och förvaltningsledarforum
- Nanoutbildning i informationssäkerhet
- ITupphandlingsmodellen_ver5
- ITU_4_1_Checklista
- Årsberättelse informationssäkerhet