Till
Kommunstyrelsen

Skrivelse
2019-09-18

Granskning av IT-säkerhet och informationssäkerhet

De förtroendevalda revisorerna i Simrishamns kommun har gett EY i uppdrag att granska om kommunstyrelsen säkerställer kommunens arbete med IT-säkerhet och informationssäkerhet.

Det är den sammanfattande bedömningen av rapporten att kommunstyrelsen bör stärka den interna kontrollen avseende IT- och informationssäkerhet. Det saknas däri kontinuerliga riskanalyser inom ramen för det praktiska arbetet för kommunens IT-system och informationstillgångar. Därtill bedöms det vara en svaghet att det inom kommunen inte genomgående finns dokumenterade kontinuitetsplaner samt angivet längsta acceptabla tid som informationssystem får vara ur funktion. Likaså anses det att kommunstyrelsen bör stärka den kontinuerliga utbildningen för anställda avseende IT- och informationssäkerheten.

Vi rekommenderar kommunstyrelsen att:

- Säkerställa att informationssäkerhetspolicy färdigställs enligt plan.
- Stärka utbildningsinsatserna avseende IT- och informationssäkerheten för kommunens anställda och förtroendevalda.
- Utarbeta och dokumentera en kontinuitetsplan för kommunens informationssystem samt tydliggöra längsta acceptabla tid dessa får vara ur funktion.
- Upprätta systemsäkerhetsanalyser för kommunens samtliga informationssystem.
- Upprätta rutiner för systematiska kontroller av nyckeltaggar.
- Skapa möjlighet till krypterad kommunikation över öppna nät.

Vi revisorer anser att det råder brister i styrningen avseende IT- och informationssäkerhet vilka är nödvändiga att åtgärdas. Vi önskar yttrande över vilka åtgärder som kommunstyrelsen kommer att genomföra med bakgrund i rapportens resultat och rekommendationer senast den 18 december 2019.

Med vänlig hälsning

Revisorerna i Simrishamns kommun

Alf-Göran Andersson
Ordförande revisionen

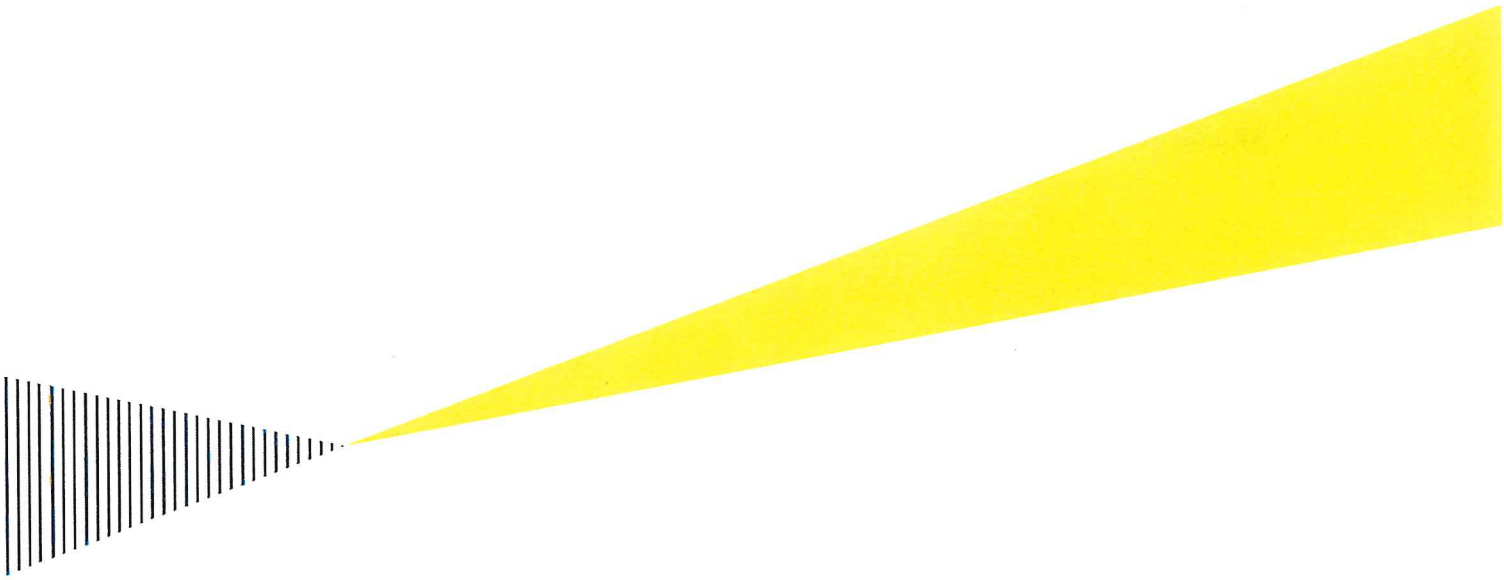
Birger Johansson
Vice ordförande

ADRESS: 272 80 Simrishamn
BESÖK: Stadshuset, Stortorget
TELEFON: 0414-81 90 00
FAX: 0414-81 97 00
E-POST: revisionen@simrishamn.se

Granskningsrapport 2019
Genomförd på uppdrag av revisorerna
Augusti 2019

Simrishamns kommun

Granskning av IT-säkerhet och informationssäkerhet



EY
Building a better working world

1. Sammanfattning

Granskningens övergripande syfte är att bedöma hur kommunstyrelsen säkerställer kommunens arbete med IT-säkerhet och informationssäkerhet. Inom ramen för granskningen har vi bedömt ett antal olika kontrollpunkter fördelade på de olika momenten kontrollmiljö, riskanalys, kontrollaktiviteter, information/kommunikation och utvärdering/uppföljning. Resultatet av granskningen visar följande fördelning.

Sammanfattande tabell, kontrollpunkter:

	Kontrollen finns och fungerar tillfredsställande.	Kontrollen finns och fungerar delvis.	Kontrollen finns ej eller fungerar ej tillfredsställande.	Ej tillämplig, kontrollen behövs ej av särskilda skäl.
Kontrollmiljö	4	2	2	0
Riskanalys	3	3	1	0
Kontrollåtgärd	20	12	5	1
Information/kom.	1	1	0	0
Uppföljning/utvärdering	2	1	5	0

Det är vår sammanfattande bedömning att kommunstyrelsen bör stärka den interna kontrollen avseende IT- och informationssäkerhet. Vi saknar däri kontinuerliga riskanalyser inom ramen för det praktiska arbetet för kommunens IT-system och informationstillgångar. Vi bedömer det vara en svaghet att det inom kommunen inte genomgående finns dokumenterade kontinuitetsplaner samt angivet längsta acceptabla tid som informationssystem får vara ur funktion. Ett stort ansvar ligger i nuläget på respektive verksamhet.

Därtill menar vi att kommunstyrelsen bör stärka den kontinuerliga utbildningen för anställda avseende IT- och informationssäkerheten. En del av det arbetet noterar vi kommer ske inom ramen för arbetsgruppen och utredarens roll som informationssäkerhetssamordnare under 2019.

Vi noterar som positivt att det av framställd RSA och bruttorisklista för den interna kontrollen vilka inkluderar områden med avseende på IT-säkerhet.

Vi rekommenderar kommunstyrelsen att:

- Säkerställa att informationssäkerhetspolicy färdigställs enligt plan.
- Stärka utbildningsinsatserna avseende IT- och informationssäkerheten för kommunens anställda och förtroendevalda.
- Utarbeta och dokumentera en kontinuitetsplan för kommunens informationssystem samt tydliggöra längsta acceptabla tid dessa får vara ur funktion.
- Upprätta systemsäkerhetsanalyser för kommunens samtliga informationssystem.
- Upprätta rutiner för systematiska kontroller av nyckeltaggar.
- Skapa möjlighet till krypterad kommunikation över öppna nät.

2.2.1. *Avgränsning*

Granskningen avser kommunstyrelsens arbete med IT-säkerhet och informationssäkerhet och baseras på information från intervjuer och dokumentstudier. Inga tester av IT-säkerheten eller informationssäkerheten har genomförts, såsom generella IT-kontroller eller applikationskontroller. Det kan finnas brister i kommunens hantering av IT som vi inte har identifierat.

2.3. Revisionskriterier

COSO-modellens ramverk för intern kontroll utgör grundkriterierna för granskningen. Vidare har granskningen genomförts mot så kallad god praxis inom informationssäkerhetsområdet genom utvalda delar av Myndigheten för samhällsskydd och beredskaps ramverk för IT- och informationssäkerhet BITS (Basnivå för IT-säkerhet), som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27001.

Dataskyddsförordningen samt styrande och stödjande dokument från Datainspektionen ligger till grund för granskningen i den del som avser dataskyddsförordningen.

Ansvarig nämnd

Granskningen avser kommunstyrelsen.

2.4. Genomförande

Granskningen har genomförts genom insamling av bakgrundsinformation samt intervjuer med representanter från kommunens IT-organisation som arbetar med IT-och informationssäkerhet. Insamlad dokumentation rör information om organisation, IT-säkerhetspolicy, riskanalyser, rapportering av kontrollaktiviteter, rutindokument mm. Samtliga intervjuade har beretts tillfälle att sakgranska rapporten. Granskningen är genomförd maj - augusti 2019.

4. Kommunens arbete avseende IT-säkerhet och informationssäkerhet

Rapporten redovisar i vilken grad kommunen uppfyller valda rekommendationer ur BITS. Resultatet är en sammanvägd bedömning, som baseras på information som lämnats vid intervjuerna samt genom erhållen dokumentation. Den sammanvägda bedömningen av svaren på kontrollerna har bedömts enligt följande alternativ:

Ja	Kontrollen finns och fungerar tillfredsställande.
Delvis	Kontrollen finns och fungerar delvis.
Nej	Kontrollen finns ej eller fungerar ej tillfredsställande.
E/T	Ej tillämplig, kontrollen behövs ej av särskilda skäl.

4.1. Kontrollmiljö

I kontrollmiljön ingår moment som kan hänföras till ledningsfrågor, organisation, riktlinjer och styrdokument samt resursfrågor. Kontrollmiljön inbegriper ofta målformuleringar eller andra krav som ställs på verksamheten, därför är bedömning av riktlinjer av särskilt intresse. Även personalens kompetens och de insatser som genomförs som vidareutbildning m.m. ingår i kontrollmiljön. Kontrollmiljön är viktig för att bedöma kommunens förmåga att leda verksamheten i riktning mot säkerhet i och i anslutning till informationssäkerhetssystemen.

IK 1 Organisation av säkerheten, policy m.m.			
1.1	Finns policy och riktlinjer för informationssäkerhet?	Det finns ingen specifik informationsäkerhetspolicy. Av kommunfullmäktige antagen IT-policy, 2016.01.27, avser ett stycke informationssäkerhet. Däri framgår att korrekt säkerhetsnivå ska sättas och att beslut kring säkerhet i system, inloggningar och behörigheter ska finnas. I samband med införandet av GDPR och NIS-direktivet beskrivs frågan rörande informationssäkerhet ha uppmärksammats i kommunen. I november 2018 har kommundirektören upprättat ett uppdragsdirektiv för det systematiska informationssäkerhetsarbetet. Av direktivet framgår att en informationssäkerhetspolicy ska arbetas fram. Socialtjänsten har arbetet fram en informationsäkerhetspolicy för sitt verksamhetsområde.	
1.2	Beskriv organisation, kompetens och behov	Organisationen för IT- och informationssäkerhet avser tre delar. 1. Det finns två arbetsgrupper som arbetar med kommunens IT-organisation. a. En samordningsgrupp (SamIT) ansvarar för det strategiska arbetet och föreslår kommunens ledningsgrupp utvecklingsmål och hur de ska följas	

1.5	Finns det en samordningsfunktion för att länka samman den operativa verksamheten för informationssäkerhet och ledningen?	Ja, en utredare med informationssäkerhetsuppdrag har en samordnande funktion enligt mottagen beskrivning på tjänstemannanivå. Säkerhetschef ansvarar för samordning gällande RSA samt ledningsplan för det operativa arbetet. Därtill deltar kommunstyrelsens ordförande och vice ordförande enligt uppgift vid koncernledningens möten vari kommundirektör utgör samordningsfunktion. Av uppdragsplanen framgår att utredare ska presentera uppdraget för kommunstyrelsen under hösten 2019. Vid intervju framkommer dock att aktiviteterna i relation till aktuell tidplan har förskjutits.	
1.6	Har ansvaret för informationssäkerheten reglerats i avtal i de fall verksamhet/drift m.m. lagts ut på en utomstående organisation?	Nej. Det framgår av personuppgiftsavtal men inte särskilt gällande ansvar för informationssäkerhet. Sedan NIS-direktivet implementerades har kommunen inte genomfört någon upphandling och kravet har inte ställts tidigare.	

4.2. Riskanalys

I riskanalysen ingår att bedöma hur kommunen arbetar med IT-säkerheten utifrån riskanalys och identifiering av olika risker. Riskanalysen bör vara utformad med vedertagna metoder om sannolikhet och konsekvenser. Riskanalysen bör också vara genomförd av medarbetare/personer som besitter tillräcklig kompetens för att identifiera och bedöma risker. Handlingsplaner bör vara kopplade till risker som har höga riskvärden.

IK 2 Riskanalys			
2.1	Genomförs riskanalyser avseende IT- och informationssäkerhet?	Delvis. Det har genomförts riskanalyser avseende IT- och informationssäkerhet för enskilda system. Riskanalyserna har då genomförts inför större förändringar. Den senaste riskanalysen genomfördes i samband med byte av telefonoperatör. Av bruttolistan inför antagande av internkontrollplan 2019 framgår ytterligare fem riskområden avseende IT varav en avser informationssäkerhet. Fyra av dessa kommer inte omfattas av kommunstyrelsens internkontroll för 2019. De fyra riskområdena som framgår av bruttolistan är: ▸ Röjda personuppgifter genom en uppföljning av rapporterade incidenter (avser informationssäkerhet) ▸ Integration mellan personal- och IT-system genom stickprov	

IK 3 Personal och säkerhet			
3.1	Får inhyrd/inlånad personal information om vilka säkerhetskrav och instruktioner som gäller? (utbildning/ introduktion/kurs m.m.)	Det genomförs inte någon särskild utbildning eller introduktion avseende säkerhetskrav. Dock får inhyrd/inlånad personal ta del av de riktlinjer som samtliga medarbetare tar del av i form av användarpolicy.	
3.2	Har systemägaren definierat vilka krav som ställs på användare som får tillgång till informationssystem och information (leta information i individuella akter m.m.)?	Ja, men dessa har inte dokumenterats. Respektive verksamhet har begränsade behörigheter baserat på behov för att fullgöra tjänsten. Exempelvis är nätverk inom socialtjänstens arbetsområde segmenterade utifrån roller och geografiskt område. Av intervju framkommer att det mot bakgrund av kommunens storlek tilldelats anpassad behörighet för att information ska vara tillgänglig oavsett frånvaro. Även om det inte är dokumenterat uppges det finnas en god styrning av behörigheterna, men det är respektive systemägares ansvar. Därtill är diariet segmenterat för respektive nämnd. Det är endast kommunens kontaktcenter som har behörighet till samtliga diarier.	
3.3	Genomförs regelbundet utbildningsinsatser inom informationssäkerhet?	Delvis. Utbildningsinsatser har genomförts i samband med lagändringar. Vid implementering av GDPR har det arrangerats utbildningar och upprättats informationsmaterial. I enlighet med uppdragsdirektiv rörande systematiskt informationssäkerhetsarbete ska utbildningsmaterial sammanställas och utbildningar genomföras. Verksamhetsansvariga ska se till att medarbetare har en tillräcklig kunskap och ett säkerhetsmedvetande. Av intervju framkommer att utbildningar inledningsvis kommer arrangeras för chefer och nyckelpersoner i organisationen. I likhet med MSB:s datorstödda informationssäkerhetsutbildning för användare (DISA) ska ansvarig utredare ta fram en informationsfilm för att nå ut till samtliga medarbetare. Syftet beskrivs vara att ta fram en enklare och kortare variant av DISA utifrån teman som lösenord, lagringsytor och mobiltelefon. Informationsfilmen beräknas distribueras under hösten 2019.	

3.11	Finns information och regler som anger att IT-utrustning m.m. inte får föras ut från organisationens lokaler utan medgivande från ansvarig chef?	Det finns inte dokumenterade rutiner, men det är tillåtet att arbeta från valfri plats på eller utanför organisationens lokaler. Medgivande från chef behövs ej.	
3.12	Finns driftdokumentation för verksamhetskritiska informationssystem? (backup, jourpärm m. kontaktpersoner)	Ja. Driftdokumentationen sparas över tid och är olika för olika system. Det sker inte någon kontroll för att säkra att en backup går att återläsa. Vid intervju framkommer att det fungerat i de fall då det behövts. Återläsning av backup framgår av kommunstyrelsens bruttolista för intern kontroll 2019, men är inte ett av de beslutade kontrollmomenten.	
3.13	Sker system-/programutveckling samt tester av modifierade system åtskilt från driftsmiljön?	Ja.	
3.14	Finns rutiner för hur utomstående leverantörers tjänster följs upp och granskas?	Nej. För de fall där det regleras framgår det av respektive avtal/upphandlingsunderlag. Härtill nämns svårigheter med personalkompetens avseende upphandling. Det anges ha diskuterats inom ramen för samverkan med övriga SÖSK-kommuner angående exempelvis eventuella utbildningsinsatser. Kommunens samordningsgrupp (SamIT) fungerar som en kontrollinstans vid nyinköp av IT-system.	
3.15	Godkänner systemägaren eller annan lämplig personal driftsättningar av förändrade informationssystem?	Ja, denna rutin är dock inte dokumenterad. Det är IT-enheten som informerar angiven systemägare att exempelvis en uppdatering är klar.	
3.16	Finns det för både servrar och klienter rutiner för skydd mot skadlig programkod?	Ja.	
3.17	Har organisationens nätverk delats upp i mindre enheter (segmentering) så att en (virus-) attack enbart drabbar en del av nätverket?	Ja.	
3.18	Genomförs säkerhetskopiering regelbundet?	Ja, säkerhetskopiering sker varje natt.	
3.19	Finns det alternativa vägar vid sidan av organisationens	Nej.	

		För en del arbetsgrupper beskrivs det vara svårt att kontrollera då samtliga personalgrupper inte har homogena tjänster/arbetsuppgifter. Därtill har exempelvis utredare behörighet att gå in enligt arkivaries behörighet för att underlätta vid exempelvis semestertider. Säkerhetschef uppger även att det uppdagats att taggar tappats bort eller kunnat användas av obehöriga.	
3.27	Öppnas låsta användarkonton endast efter säker identifiering av användaren?	Rutinen är att det ska ske en säker identifiering av användaren genom en personvalidering via BankID. Det har hänt att låsta konton öppnats utan personalvalidering då kommunens medarbetare känner varandra. Detta kan exempelvis ske då en medarbetare ringer till IT-supporten och känner igen rösten på den som ringer.	
3.28	Finns en gemensam lösenordspolicy?	Ja, policyn framgår av kommunens riktlinjer för användning av kommunens IT.	
3.29	Finns en dokumenterad brandväggspolicy där det beskrivs vilka tjänster brandväggen ska tillhandahålla?	Ja, den finns i brandväggen.	
3.30	Har organisationen ställt och dokumenterat tekniska säkerhetskrav och krav på praktisk hantering avseende användandet av mobil datorutrustning och distansarbete?	Delvis, av riktlinjer för användning av kommunens IT anges att IT-resurser ägs av kommunen och är avsedda att användas i och för kommunens uppdrag. All annan användning är otillåten. Med IT-resurser menas datorer, surfplattor, telefoner, nätverk, programvara och all annan kringutrustning som nyttjas i samband med hantering av information i digital form. Som en del av utredarens uppdrag ska en ny riktlinje färdigställas under 2019. Kontroll av efterlevnad sker på förekommen anledning, men inte regelmässigt.	
3.31	Finns det aktuell dokumentation med regler för distansarbete?	Delvis, det framgår att vid användande av distansåtkomst till kommunens IT-resurser är medarbetaren en del av kommunens nätverk, på samma sätt som om medarbetaren är fysiskt på arbetsplatsen. Samma regler är därför tillämpliga.	
Anskaffning, utveckling och underhåll av informationssystem			

5.1	Finns det en gemensam kontinuitetsplan dokumenterad för organisationen?	Nej, det finns inte gemensamma kontinuitetsplaner men det finns analoga rutiner för delar av verksamheten. Respektive verksamhet ansvarar i form av systemägare att säkerställa att det finns rutiner. Analoga rutiner finns enligt uppgift inom hälso-sjukvård, socialtjänst och skolan. Vid intervjutillfället beskrivs kommunens Va-system vara analogt. Därför finns det inte en kontinuitetsplan. Av kommunens RSA från 2015 framgår det att en identifierad risk är att serverproblem inom VA kan slå ut larmsystem för färskvattensystem och avlopp. Kontinuitetsplan för kommunens IT-tekniska områden finns inte, det finns enbart nedtecknat rörande telefoni.	
5.2	Har systemägaren eller motsvarande beslutat om den längsta acceptabla tid som informationssystemet bedöms kunna vara ur funktion innan verksamheten äventyras?	Nej. En prioritering beskrivs ske utifrån aktuell situation. Detta är dock inte dokumenterat.	
5.3	Finns det en dokumenterad avbrottsplan med återstarts- och reservrutiner för datadriften som vidtas inom ramen för den ordinarie driften?	Nej. Internt beskrivs det däremot finnas en god kännedom om hur arbetet ska genomföras.	
Efterlevnad			
5.4	Används endast programvaror i enlighet med gällande avtal och licensregler?	Ja.	
5.5	Har organisationen förtecknat och anmält personuppgifter till personuppgiftsombud?	Ja, det finns ett upprättat register som är anmält till personuppgiftsombud.	
5.6	Genomförs interna och externa penetrationstester kontinuerligt?	Nej. Ett externt penetrationstest ska dock genomföras enligt kommunstyrelsens beslut av intern kontrollplan för 2019 den 22 maj 2019, § 147. Säkerhetschef tillägger att ett penetrationstester endast speglar den kunskap som företaget besitter. Därmed skapas inte en fullständig bild av den faktiska IT-säkerheten.	
5.7	Granskar ledningspersoner regelbundet att säkerhetsrutiner, policy och normer efterlevs?	Nej.	

5. Analys avseende intern kontroll

Inom ramen för granskningen har vi bedömt ett antal olika kontrollpunkter fördelade på olika moment inom intern kontroll. Resultatet av granskningen visar följande fördelning.

Sammanfattande tabell, kontrollpunkter:

	Kontrollen finns och fungerar tillfredsställande.	Kontrollen finns och fungerar delvis.	Kontrollen finns ej eller fungerar ej tillfredsställande.	Ej tillämplig, kontrollen behövs ej av särskilda skäl.
Kontrollmiljö	4	2	2	0
Riskanalys	3	3	1	0
Kontrollåtgärd	20	12	5	1
Information/kom.	1	1	0	0
Uppföljning/utvärdering	2	1	5	0

Det är vår sammanfattande bedömning att kommunstyrelsen bör stärka den interna kontrollen avseende IT- och informationssäkerhet. Vi saknar däri kontinuerliga riskanalyser inom ramen för det praktiska arbetet för kommunens IT-system och informationstillgångar. Vi bedömer det vara en svaghet att det inom kommunen inte genomgående finns dokumenterade kontinuitetsplaner samt angivet längsta acceptabla tid som informationssystem får vara ur funktion. Ett stort ansvar ligger i nuläget på respektive verksamhet.

Därtill menar vi att kommunstyrelsen bör stärka den kontinuerliga utbildningen för anställda avseende IT- och informationssäkerheten. En del av det arbetet noterar vi kommer ske inom ramen för den tillsatta arbetsgruppen och utredarens roll som informationssäkerhetssamordnare under 2019.

Vi noterar som positivt att det av framställd RSA och bruttorisklista för den interna kontrollen vilka inkluderar områden med avseende på IT-säkerhet.

Kontrollmiljö

I kontrollmiljön ingår moment som kan hänföras till ledningsfrågor, organisation, riktlinjer och styrdokument samt resursfrågor.

Det är positivt att ett arbete pågår för att ta fram en kommungemensam informationsäkerhetspolicy samt att en arbetsgrupp tillsats för säkerhetsrelaterade frågor. Vi anser dock att detta är ett så pass viktigt styrdokument att det är bristfälligt att detta inte utarbetats tidigare. Med anledning av förseningar i arbetet ställer vid oss därtill frågande till om kommunens informationsäkerhetspolicy kommer beslutas senast i januari 2020 i enlighet med tidplanen.

Vi bedömer det vara av vikt att säkerheten framledes regleras i de avtal för verksamheter som lagts ut på en utomstående organisation/företag.

Riskanalys

Vi bedömer det vara en brist att heltäckande riskanalyser inte genomförs löpande. Det finns en risk- och väsentlighetsanalys upprättad avseende kommunens IT-säkerhet, vari endast ett riskområde avser informationssäkerhet. Kommunstyrelsen bör säkerställa att verksamhetskritiska system identifieras för en korrekt hantering, särskilt då det i vår mening inte finns en

6. Källförteckning

Intervjuade funktioner

- IT-chef
- Utredare med informationssäkerhetsuppdrag
- Säkerhetschef

Medverkande revisorer vid intervju

- Alf-Göran Andersson
- Jan Rydén

Dokument

- Kommunstyrelsens reglemente
- Avtal IT- och telefoni
- Bruttolista Intern kontroll 2019
- Informationsäkerhetspolicy och regler för verksamhetssystem, Socialtjänsten
- IT-policy
- Riktlinjer för användning av kommunens IT
- Rutin för inköp av IT- kommunikationssystem
- Samverkansavtal inom områdena säkerhet och risk
    - Överenskommelse med anledning av uppsägning
- Uppdragsplan informationssäkerhet
- Verksamhetssystem
- Ärendehandbok
- Risk- och sårbarhetsanalys för 2015, samt arbetsmaterial för 2019
- Intern kontrollplan 2019
- Bruttolista Intern kontrollplan 2019