ÖSTERSUNDS KOMMUN

REVISIONSRAPPORT

UPPFÖLJANDE GRANSKNING AV IT-SÄKERHET

Ansvarig: Ulf Rubensson
Certifierad kommunal revisor

Innehållsförteckning

1 SAMMANFATTNING

På Östersunds kommuns revisorers uppdrag har regionens revisionskontor gjort en uppföljande granskning av kommunens IT-säkerhet. I granskningen har följande framkommit:

Den systemförvaltningsmodell som valts uppges inte vara helt förankrad inom kommunen. I nuläget har ett stort ansvar för IT-systemen lagts ut på systemägare och systemförvaltare hos resp. nämnd/förvaltning som använder systemen. Vi har dock fått intrycket att det i hög utsträckning saknas effektiv intern kontroll avseende om förvaltningen av systemen lever upp till ställda krav. Detta grundar vi på följande iakttagelser/bedömningar:

- Systemägarnas/systemförvaltarnas roller och ansvar är otydliga och behöver kommuniceras tydligare samt följas upp
- Det är oklart om risk- och konsekvensanalyser gjorts i samband med upphandlingar av IT-system. Detta bör säkerställas.
- Kontinuitetsplaner saknas i stor utsträckning.
- Det finns indikationer om att systemförvaltningsplaner saknas.
- En ny systemförvaltningsmodell har beslutats, men det finns en tröghet i införandet. Ökad information om och åtgärder för att införa den behöver vidtas. Ett tydligare stöd från kommunledningen skulle kunna bidra till ett snabbare införande.
- Många av kommunens system har inte bedömts avseende om de är verksamhetskritiska eller inte. Verksamhetskritiska system bör prioriteras med avseende på informationsklassning och skyddsåtgärder. Vi rekommenderar att analysen av om systemen är verksamhetskritiska får hög prioritet.
- Arbetet med informationsklassning har legat nere under lång tid och har nyligen återupptagits. Det gör att de flesta av kommunens system saknar en aktuell informationsklassning. Klassningen syftar till att ge svar på skyddsbehov och att välja rätt åtgärder för att skydda informationen. Vi rekommenderar arbetet med informationsklassning får fortsatt hög prioritet.
- För att möjliggöra en intern kontroll av hur systemen förvaltas behövs information om hur förvaltningen sker. I dagsläget finns ingen samlad sådan information.

  Vi rekommenderar att en genomgång görs av vad som kan anses vara viktig information ur ett kontrollperspektiv och att den kanaliseras till en kommunövergripande controllerfunktion.

Sammantaget bedömer vi att kommunens ledningssystem behöver utvecklas vad avser informations- och IT-säkerheten. Vi har noterat att kommunledningen själv har identifierat brister i processen för informationssäkerhet och har tillsatt en informationssäkerhetsansvarig, vilket vi ser som positivt.

Det är viktigt att informations- och IT-säkerheten integreras med organisationens styrning av planering och uppföljning. Det innebär till exempel att ledningen löpande informerar sig om säkerhetsarbetet, genomför kontroller samt ser över styrdokumenten med jämna mellanrum. Nuvarande policy och rutiner för IT-säkerheten är daterade 2004.

- Det är angeläget att det påbörjade arbetet med en ny informationssäkerhetspolicy slutförs.

IT-enheten har valt att arbeta enligt standarderna ISO/IEC 27001 och 27002 i sitt säkerhetsarbete. Arbete med att utveckla ledningssystemet i enlighet med vald standard

och att säkra systemen har påbörjats, men är fortfarande i uppstartsfas. Plan för etablerandet av standarderna saknas.

- Vi rekommenderar att en plan för etablerandet av standarden tas fram.

Nämndernas och styrelsernas internkontrollplaner innehåller få IT-relaterade kontroller, men de som finns följs upp.

- I kommunstyrelsens internkontrollplan för 2017 fanns ett riskområde som rör loggkontroller. Av uppföljningen framgår inte att risken har åtgärdats, men problemet finns inte med i internkontrollplan för 2018.
  Kommunstyrelsen bör bevaka att tillräckliga åtgärder vidtagits.

2 INLEDNING/BAKGRUND

Kommunens revisorer har tidigare genomfört granskningar av IT-säkerheten. Mot bakgrund av tidigare gjorda iakttagelser och erhållna svar har revisorerna, i sin risk- och väsentlighetsanalys, bedömt det angeläget att genomföra en uppföljande granskning av IT-säkerheten.

3 SYFTE, REVISIONSFRÅGA OCH AVGRÄNSNING

Syfte

Det övergripande kontrollmålet är att genomföra en uppföljning av tidigare genomförda granskningar inom IT-säkerhetsområdet.

Revisionsfrågor

- Har hot-, risk- och sårbarhetsanalyser inom IT-området genomförts?
- Har plan för tillgänglighetsanalys och informationsklassning enligt
- ISO/IEC 27001 tagits fram och har arbetet påbörjats?
- Har verksamhetskritiska IT-system analyserats med avseende på tillgänglighet och informationsklassning?
- Sker en årlig uppdatering av ansvarsroller?
- Görs årliga genomgångar av behörigheter?
- Har risk- och konsekvensanalyser gjorts i samband med ev. upphandlingar av IT-system?
- Finns risk och konsekvensanalyser med i den årliga systemförvaltningsplanen (om den innehåller förändringar/kompletteringar av befintliga system)?
- Har kontroller kopplade till IT säkerhet följts upp i den årliga internkontrollplanen i nämnderna?

Avgränsning

Granskningen är i huvudsak avgränsad till kommunstyrelsen. För övriga nämnder är omfattningen begränsad till de system resp. nämnd förvaltar och uppföljningen av IT-säkerheten i respektive nämnds internkontrollplan.

4 REVISIONSKRITERIER

Revisionskriterierna utgår huvudsakligen ifrån de svar kommunens revisorer erhållit i tidigare granskningar samt kommunens egna interna regler.

5 METOD

Granskningen har utförts genom dokumentstudier och intervjuer. Substansgranskning har utförts för att i erforderlig omfattning verifiera gjorda utsagor samt att system och rutiner fungerar på avsett sätt. Intervjuer har skett med fyra systemförvaltare inom Östersunds kommun.

6 ANSVARIGA FÖR IT-SÄKERHETEN

Kommunstyrelsen har det yttersta ansvaret för IT-säkerheten. Nämnderna har ansvaret för IT-säkerheten inom sina verksamhetsområden. Förvaltningscheferna ska organisera IT-säkerhetsarbetet inom sina förvaltningar samt ansvara för ledning och kontroll. Verksamhetsansvariga, på alla nivåer, är ansvariga för säkerheten inom sina områden och ska själva avsätta de resurser som krävs för att policy och rutiner följs.[1]

7 RESULTAT AV GRANSKNINGEN

7.1 HAR HOT-, RISK- OCH SÅRBARHETSANALYSER INOM IT-OMRÅDET GENOMFÖRTS?

Ansvaret för att genomföra hot-, risk- och sårbarhetsanalyser inom IT-området ligger hos resp. systemägare.

IT-enheten har gjort risk- och sårbarhetsanalys för sin verksamhet, men tror inte att det görs i strukturerad form hos kommunens enheter, med undantag för enheten Vatten inom teknisk förvaltning och Sociala förvaltningen.

IT-enheten saknar informationskanal som ger någon helhetsbild i detta avseende.

Ett grundproblem uppges vara att den systemförvaltningsmodell som valts inte är helt förankrad inom kommunen. Ett arbete med att ta fram en ny informationssäkerhetspolicy har pågått, men man avvaktar med slutförande till dess den nya tjänsten som informationssäkerhetsansvarig tillträds i oktober. Aktuell informationssäkerhetspolicy är daterad 2004-08-21.

Bedömning:

Det finns en indikation om att risk- och sårbarhetsanalyser inte utförs i tillräcklig omfattning. Vi rekommenderar att en översyn görs.

Det är angeläget att arbetet med informationssäkerhetspolicyn slutförs.

[1] Kommunens IT-säkerhetspolicy (2004-08-27)

7.2 HAR PLAN FÖR TILLGÄNGLIGHETSANALYS OCH INFORMATIONSKLASSNING ENLIGT ISO/IEC 27001 TAGITS FRAM OCH HAR ARBETET PÅBÖRJATS?

Informationssäkerhet

Ansvaret för informationssäkerheten ligger inom Kommunledningsförvaltningen och IT-säkerhet är en viktig och väsentlig del i kommunens informationssäkerhet.

I kommunfullmäktiges internkontrollplan för 2017 angavs att processen för arbetet med informationssäkerhet saknas och att åtgärden är att inrätta en tjänst med inriktning på informationssäkerhet. En informationssäkerhetsansvarig har anställts och tillträder i oktober 2018. IT-enheten uppger att man avvaktar med större åtgärder till dess den informationssäkerhetsansvarige har tillträtt tjänsten.

IT-säkerhet

En IT-säkerhetsansvarig finns på IT-enheten.

För närvarande upplever IT-enheten att det tillämpas många olika modeller för IT-säkerheten inom kommunen.

IT-enheten har valt standarderna ISO/IEC 27001 och 27002 som grund för sitt säkerhetsarbete. Arbete med att utveckla ledningssystemet i enlighet med vald standard och att säkra systemen påbörjats, men plan för etablerandet av standarderna saknas.

IT-enheten uppger att, när den informationssäkerhetsansvarige finns på plats, ska man fortsätta det arbete som påbörjats med att se över informations- resp. IT-säkerheten.

Standarden ISO/IEC 27001 fastställer krav som en organisation behöver uppfylla när det gäller ledningssystem för informationssäkerhet och innehåller även krav för bedömning och behandling av informationssäkerhetsrisker.

Till denna standard finns det även kopplat en standard benämnd ISO/IEC 27002 som kompletterar nyss nämnda standard och innehåller riktlinjer och beskrivningar över vilka säkerhetsåtgärder ledningssystemet generellt ska innehålla. ISO/IEC 27002 har fokus på säkerhetsåtgärder men omfattar även frågor om styrning av informationssäkerhet såsom regelverk för informationssäkerhet (policy), organisation och efterlevnad. IT-enheten beskriver standarden som mycket omfattande. Enligt IT-enheten innehåller den bl. a. 114 specifika säkerhetsåtgärder. Någon genomgång och prioritering av dessa säkerhetsåtgärder är inte gjord.

IT-enheten uppger att det finns vissa säkerhetsåtgärder i ISO/IEC 27002 som berör alla system och det är bl. a spårbarhet och segmentering av datanätverk, och att de arbetar med dessa krav. Vidare uppger man att på grund av nya säkerhetsskyddslagen har man prioriterat att arbeta med enheten Vatten inom teknisk förvaltning och dess system. I nya säkerhetsskyddslagen pekas område vatten ut som ett särskilt viktigt område.

För närvarande saknas övergripande plan för hur arbetet med ovan nämnda standarder ska etableras.

Bedömning:

Arbetet med att etablera standarden enligt ISO/IEC 27001 och 27002 har påbörjats, men är ännu i uppstartsfas.

Vi rekommenderar att en plan för etablerandet av standarden tas fram.

7.3 HAR VERKSAMHETSKRITISKA IT-SYSTEM ANALYSERATS MED AVSEENDE PÅ TILLGÄNGLIGHET OCH INFORMATIONSKLASSNING?

Systemtillgänglighet

Kommunen har, enligt uppgift, ca 200 system.

IT-enheten uppger att en genomgång har gjorts för nästan alla system tillsammans med respektive systemförvaltare. Utifrån det har en värdering gjorts över vilka system som är kritiska för verksamheten.

Vi har tagit del av två listor som innehåller förteckningar över IT-system och om de har bedömts vara verksamhetskritiska utifrån ett tillgänglighetsperspektiv. Listorna innehåller delvis överlappande uppgifter om samma system. Sammantaget innehåller listorna uppgifter om 188 system, varav det för 20 system fanns uppgift om att de bedömts vara verksamhetskritiska och 39 att de inte var det. För 129 system saknar vi uppgift i detta avseende.

IT-enheten uppger att ambitionen är att det även ska finnas kontinuitetsplaner[2] för varje IT-system. IT-enhetens bedömning är att det för närvarande saknas dokumenterade kontinuitetsplaner i mycket hög grad.

Vi har inte kunnat finna några diarieförda kontinuitetsplaner och det finns, vad vi erfarit, inget kommungemensamt sidoordnat register över sådana.

Systemförvaltningsmodeller

En systemförvaltningsmodell benämnd RACI[3] är framtagen och beslutad. Men IT-enheten uppger att den inte är förankrad för alla kommunens system och att det finns vissa svårigheter att få gehör för säkerhetsarbetet.

RACI-modellen tillämpas inte ännu för alla system. Den är, enligt uppgift, något man strävar efter att ska gälla på sikt. För de system där modellen tillämpas, uppger IT-enheten, att man har en ambition att gå igenom behörighetsrollerna årligen. Det är oklart hur roller och behörigheter förvaltas i övriga system.

Systemförvaltningsplaner

IT-enheten har inga befogenheter att styra systemägarnas åtgärder. För att försöka påverka säkerhetsarbetet i positiv riktning har IT-enheten tagit fram en mall för att förenkla arbetet med att göra systemförvaltningsplaner. Responsen från systemägarna uppges ha varit svag, trots att mallen har förankrats i Strategiska IT-beredningsrådet och Kommunledningsgruppen.

IT-enheten saknar information om i vilken utsträckning det finns systemförvaltningsplaner hos systemägarna. IT-enheten uppger att de har ett behov av att känna till om det finns systemförvaltningsplaner. Det finns dock ingen sådan informationskanal.

Inga systemförvaltningsplaner finns diarieförda och det finns, vad vi erfarit, inget kommungemensamt sidoordnat register över sådana.

---

[2] Kontinuitetsplan – En plan som beskriver hur verksamheten skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod, helst utan avbrott.

[3] RACI är en matris där man sätter ansvar för olika aktiviteter. RACI är akronym för **R**esponsible (Huvudansvarig), **A**ccountable (Utförare), **C**onsult (Konsulteras) och **I**nform (Informeras), som representerar hur varje aktivitet kopplas till olika individer.

Vid intervju med fyra systemförvaltare framkom att RACI var infört för ett av systemen, Tre system saknade någon namngiven modell. Av de som saknade modell har man i ett fall börjat titta på RACI och i ett annat fall är ett införande snart klart. I ett fall fanns ingen dokumenterad systemförvaltningsmodell.

Behörighetshantering

Central behörighetshantering är automatiserad och styrs via personalsystemet när personal börjar och avslutar sin anställning. Systemspecifika behörigheter beställs av chefer via e-tjänst.

En grundsäkerhet finns via en koppling mellan anställningsuppgift och behörighet att komma in i kommunens IT-system. Dock finns det en risk för att personer som byter befattning inom kommunen skulle kunna behålla behörigheter från den gamla befattningen om den inte avslutas.

Informationsklassning

I ett beslut i Finansutskottet 2005, bestämdes att en metod som kallas för "Basnivå för IT-Säkerhet" (BITS) skulle utgöra en gemensam metod för IT-säkerhetsarbete i Östersunds kommun. *(Dnr 262-2005)*. Återstående punkter i systemsäkerhetsplanen[4] för infrastrukturen skulle bevakas genom internkontrollen.

Arbetet med klassning av informationen syftar till att ge svar på vilken information som finns och vilket skyddsbehov den har. Informationsklassning kan hjälpa verksamheten att välja rätt åtgärder för att skydda informationen. Ansvaret för att åtgärder vidtas ligger i huvudsak på systemägarna.

I dagsläget har klassning av informationen med stöd av BITS upphört. Det har under de senaste fem åren inte gjorts några informationsklassningar med BITS. Det har pågått ett arbete med att ta fram en ny informationssäkerhetspolicy, som ännu inte är beslutad. I förslaget finns det med ett förslag om övergång till modellen ISO 27001.

Man har valt att använda SKL:s system "KLASSA" för att klassificera systemen. I första hand för de verksamhetskritiska systemen.

KLASSA är framtaget för kommunal verksamhet med krav som hämtats från f.d. Kris och beredskapsmyndighetens BITS samt krav som har koppling till ISO 27000-serien

I det nu upptagna arbetet med informationsklassning uppges de verksamhetskritiska systemen ha prioriterats. Vi har fått uppgift om att 10 av 188 system har informationsklassats. Tre av dessa finns med i den förteckningen över system som bedömts vara verksamhetskritiska ur ett tillgänglighetsperspektiv.

IT-enheten har inte någon samlad bild av hur förhållandet ser ut mellan prioriterade åtgärder och resurser för åtgärder vad avser de system som klassats.

Vi har intervjuat fyra slumpvis valda systemförvaltare som har verksamhetskritiska system. Ett av systemen har genomgått en informationsklassning som kan anses vara aktuell. Tre har inte klassats varav det i ett fall framkom att systemet var viktigt, men tveksamt vad gäller om det är verksamhetskritiskt.

---

[4] En systemsäkerhetsplan brukar beskriva den säkerhetsmålsättning som gäller för aktuellt IT-system och i denna klarläggs vilka säkerhetskrav som ska ställas utifrån aspekterna sekretess, riktighet och tillgänglighet.

Bedömning:

Systemtillgänglighet

Kontinuitetsplaner saknas i stor utsträckning. Åtgärder bör vidtas.

Systemförvaltningsmodell
Ökad information om vald systemförvaltningsmodell och åtgärder för att införa den behöver vidtas.

Mot bakgrund av uppgifterna om svårigheterna att få gehör för beslutad systemförvaltningsmodell vill vi framhålla att ett tydligt stöd av kommunledningen kan bidra till att säkerhetsarbetet får önskade effekter.

Det förefaller finnas anledning att överväga om systemägarnas/systemförvaltarnas roller och ansvar behöver förtydligas, kommuniceras tydligare och följas upp.

Informationsklassning
Det är positivt att informationsklassningen återupptagits.

Mot bakgrund av att arbetet med informationsklassning legat nere under lång tid har huvuddelen av kommunens system inte en aktuell informationsklassning. Vi bedömer detta som ett eftersatt område som bör få fortsatt hög prioritet i arbetet med att uppnå/upprätthålla en tillräcklig informations- och IT-säkerhetsnivå.

Det saknas uppgift för en stor del av kommunens IT-system med avseende på om de är verksamhetskritiska eller inte och om de således bör prioriteras med avseende på genomförande av informationsklassning och skyddsåtgärder. Av denna anledning bör även analysen av om systemen är verksamhetskritiska få hög prioritet.

7.4 SKER EN ÅRLIG UPPDATERING AV ANSVARSROLLER? GÖRS ÅRLIGA GENOMGÅNGAR AV BEHÖRIGHETER?

I den granskning som gjordes 2017 erhölls upplysning om att behörigheter gås igenom minst en gång per år och samkörs med lönesystemet. IT-enheten gör en sådan djupare årlig genomgång av de centrala behörigheterna.

I vår granskning har vi dock inte fått uppgifter om att några årliga mer omfattande kontroller sker hos systemförvaltarna.

Vid intervjuer med fyra systemförvaltare uppgav samtliga att de har en löpande bevakning av ansvarsroller och vilka som tilldelats behörigheter i systemen. Kontrollerna bygger till stor del på personkännedom. Kontrollerna förefaller dock sakna struktur vad avse frekvens och dokumentation.

Bedömning:

En löpande bevakning av behörighetsroller och tilldelning av behörigheter måste alltid ske och det är positivt att så även verkar vara fallet.

Vi rekommenderar att systemägare och systemförvaltare informeras tydligare om vad som åligger dem i arbetet med kontroll av behörigheter till olika system och att arbetet blir mer strukturerat för att säkerställa att kontrollerna görs.

7.5 HAR RISK- OCH KONSEKVENSANALYSER GJORTS I SAMBAND MED EV. UPPHANDLINGAR AV IT-SYSTEM?

I diariet fann vi sju upphandlingar under perioden 2017-2018 där det skulle ha kunnat varit tänkbart att risk- och väsentlighetsanalys skulle ha gjorts inför upphandlingen. Vi fann dock inga diarieförda uppgifter om att några sådana skulle ha gjorts under samma tidsperiod.

IT-enheten uppger att de i stor utsträckning saknar information om att risk- ock konsekvensanalyser har skett i samband med upphandlingar av IT-system. Ansvaret för detta görs ligger på systemägarna, men IT-enheten uppger att om det skett borde de kontaktats och därmed ha kunskap om det. Av de system som upphandlats under 2017 och 2018 har IT-enheten kännedom om en risk- och konsekvensanalys som ska ha skett inför anskaffandet av ett system benämnt "Nya kommunoffice".

IT-enheten upplever ett behov av att klara ut roller med mera som har inverkan på IT-säkerheten och har för avsikt att försöka träffa nämnder och styrelser för att informera om ansvarsförhållandena.

Bedömning:

Det är oklart om risk- och konsekvensanalyser gjorts i samband med upphandlingar av IT-system. Detta bör säkerställas.

7.6 FINNS RISK- OCH KONSEKVENSANALYSER MED I DEN ÅRLIGA SYSTEMFÖRVALTNINGSPLANEN (OM DEN INNEHÅLLER FÖRÄNDRINGAR/KOMPLETTERINGAR AV BEFINTLIGA SYSTEM)?

Det finns ingen gemensam systemförvaltningsplan över alla system inom kommunen. Respektive systemägare/systemförvaltare ansvarar för att det finns en systemförvaltningsplan för specifika system inom respektive verksamhet.

I vår stickprovsgranskning av fyra system saknade samtliga systemförvaltningsplaner. I tre fall kände man till vad en systemförvaltningsplan är. I ett fall uppgavs en plan vara på gång, men ännu inte riktigt klar. I ett fall uppgavs att risk- och konsekvensanalyser gjorts inför en större förändring.

Vi har inte kunnat finna några diarieförda risk- och konsekvensanalyser och det finns, vad vi erfarit, inget kommungemensamt sidoordnat register över sådana.

Vår bild är att systemförvaltningsplaner i saknas i inte obetydlig omfattning, vilket också är den bild som finns hos IT-enheten.

Bedömning:

Revisionsfrågan har inte gått att besvara. Vi har dock en indikation om att systemförvaltningsplaner saknas och om det är så finns inte heller risk- och konsekvensanalyser med i dessa.

Om indikationen stämmer innebär detta att det kan finnas ett behov av att informationsinsatser bör ske avseende t.ex. vad systemförvaltningsplaner är, hur de ska hanteras, vilka som omfattas av kravet att de ska finnas och intern kontroll över att de faktiskt finns. Vi rekommenderar därför att en undersökning görs av det verkliga förhållandet.

7.7 HAR KONTROLLER KOPPLADE TILL IT SÄKERHET FÖLJTS UPP I DEN ÅRLIGA INTERNKONTROLLPLANEN I NÄMNDERNA?

I fem internkontrollplaner för 2017 har vi funnit inslag av IT-relaterade kontroller (*kontroller kopplade till personuppgiftslag/GDPR inräknade*). I lika många styrelser/nämnder har vi inte funnit motsvarande kontroller. Nedan återges vad vi funnit i internkontrollplanerna 2017 och vad som återrapporterats till resp. nämnd.

Kommunfullmäktige:

- **Informationssäkerhet**: Process för informationssäkerhetsarbetet saknas.
  - *Uppföljning: "En ny tjänst som informationssäkerhetsansvarig inrättas 2018."*

Kommunstyrelsen:

- **Logghantering**: Risk att det inte finns systematisk och dokumenterad rutin för uppföljning av loggar.
  - *Uppföljning: "Centralt har kommunen inget sätt att analysera loggar utan där måste man titta på det enskilda systemet vid t ex en incident, vilket är en brist. Under hösten har IT-enheten genomfört informationsklassning av vissa system och där ingår ett avsnitt som belyser spårbarhet och loggning".*
- **Personuppgiftshantering**: Risk att personuppgifter hanteras i strid med lagstiftning.
  - *Uppföljning: "Ett omfattande arbete har påbörjats med anledning av ny lagstiftning, GDPR. Arbetet fortsätter 2018".*

Socialnämnden:

- **Behörigheter:** Om behörighet ej överensstämmer med typ av tjänst kan klienters rättssäkerhet åsidosättas.
  - *Uppföljning: "Avvikelse åtgärdad".*
- **Sekretess**: Sekretess i verksamhetssystem
  - *Uppföljning: "Enhetschef gör slumpvisa kontroller. Att det är rätt behörighet till sekretessärenden kontrolleras regelbundet av systemförvaltningen".*
- **IT-säkerhetsregler:** Risk att reglerna kring kommunens IT-säkerhet ej följs.
  - *Uppföljning: "En skrift lämnas till varje nyanställd som gås igenom vid genomgång av systemförvaltare".*

Utförarstyrelsen, serviceförvaltning:

- **Personuppgiftshantering**: Bristfällig personuppgiftshantering
  - *Uppföljning: "Kontroll visar att en genomgång har genomförts under hösten. I samband med inventeringen har uppgifter flyttats över till ett nytt system, Draftit förteckning, för att förbättra förutsättningarna att framgent identifiera ev. brister. Överföringen kommer att slutföras under kvartal 1 2018. Utbildningar har under året genomförts för Löner, Kundcenter, IT-enheten, och samtliga webbuppdaterare. Inom Serviceförvaltningen har samtliga anställda med chefsansvar samt all administrativ personal fått inbjudan till en obligatorisk webbaserad utbildning om GDPR. Utöver det har viss personal vid andra enheter informerats om den nya Dataskyddsförordningen som kommer att ersätta Personuppgiftslagen från 25 maj 2018".*

Kultur- och fritidsnämnden:

- **Personuppgiftshantering:** Kontroll att förvaltningen känner till sitt ansvar och att arbetsuppgifter har fördelats ut.
  - *Uppföljning: "Arbetsuppgifter har fördelats ut och flertalet känner till sitt ansvar".*

Inga IT-relaterade kontroller i internkontrollplan för 2018:

Barn- och utbildningsnämnd, Gemensamma nämnden för upphandling, Vård- och omsorgsnämnden, Utförarstyrelsen Serviceförvaltningen.

Ingen internkontrollplan funnen:
Valnämnden, Överförmyndarnämnden.

Bedömning:

Överlag ger återrapporteringen intryck av att åtgärder vidtagits. Men Kommunstyrelsens problem med logghantering ser, av återredovisningen, inte ut att ha lösts under 2017. När vi studerar Kommunstyrelsens internkontrollplan för 2018 finns problemet kring logghantering inte längre med. Om problemet inte lösts kan det vara lämpligt att Kommunstyrelsen bevakar att tillräckliga åtgärder vidtagits.

IT-enheten och systemförvaltare bör i högre grad involveras i riskanalysarbetet och framtagandet av internkontrollplaner

För informations- och IT-säkerhetsområdet finns det anledning att överväga kontrollmoment som är kommunövergripande i internkontrollplanerna. *T ex att alla använder eller strävar mot att använda RACI som systemförvaltningsmodell, att alla system genomgått informationsklassning, att kontinuitetsplaner finns.*

8 KVALITETSSÄKRING

Berörda uppgiftslämnare har faktagranskat lämnade uppgifter som finns med i revisionsrapporten. Svar från intervjuade systemförvaltare har avstämts vid intervjutillfällena.

Projektledare svarar för kvalitetssäkring gentemot uppgiftslämnare och av de insamlade uppgifter som används i analysen. Projektledaren har det primära ansvaret för att den analys och de bedömningar och förslag som förs fram är tillräckligt underbyggda.

Ansvarig för kvalitetssäkring har det övergripande ansvaret för att kontrollera om granskningen har en tillräcklig yrkesmässig och metodisk kvalitet samt att det finns en överensstämmelse mellan revisionsfrågorna/kontrollmålen, metoder, fakta, slutsatser/bedömningar och framförda förslag.

9 ANSVARIGA FÖR GRANSKNINGENS GENOMFÖRANDE

Projektledare:

Ulf Rubensson
Certifierad kommunal revisor

Kvalitetssäkring:

Leif Gabrielsson
Revisionsdirektör

10 SAMMANFATTANDE SVAR PÅ REVISIONSFRÅGORNA:

Revisionsfrågor:	**Sammanfattande svar**
Har hot-, risk- och sårbarhetsanalyser inom IT-området genomförts?	Oklart om det görs i tillräcklig omfattning
Har plan för tillgänglighetsanalys och informationsklassning enligt ISO/IEC 27001 tagits fram och har arbetet påbörjats?	Plan för arbetet saknas. Arbete har påbörjats, men är ännu i uppstartsfas.
Har verksamhetskritiska IT-system analyserats med avseende på tillgänglighet och informationsklassning?	Arbete har gjorts för att bedöma om systemen är verksamhetskritiska. Det saknas dock uppgift om detta för många system. Informationsklassning av IT-systemen är allvarligt eftersatt.
Sker en årlig uppdatering av ansvarsroller? Görs årliga genomgångar av behörigheter?	Ja, centralt hos IT-enheten, men troligen inte på systemnivå. Arbetet med behörighetskontroll till olika system är inte strukturerad och formaliserad.
Har risk- och konsekvensanalyser gjorts i samband med ev. upphandlingar av IT-system?	I något fall.
Finns risk och konsekvensanalyser med i den årliga systemförvaltningsplanen (om den innehåller förändringar/kompletteringar av befintliga system)?	I vårt stickprov saknade de intervjuade systemförvaltningsplaner. Det fanns även okunskap om vad detta är.
Har kontroller kopplade till IT säkerhet följts upp i den årliga internkontrollplanen i nämnderna?	Ja, vad avser 2017. I ett fall (KS) ser en brist ut att kvarstå men finns inte med i följande plan (2018).