www.pwc.se

Revisionsrapport

IT- och informations-säkerhet

Kalix kommun

Robert Bergman
Revisionskonsult

December 2017

pwc

Innehåll

Sammanfattning

På uppdrag av de förtroendevalda revisorerna har PwC granskat kommunens informationssäkerhetsarbete. Granskningen syftar till att bedöma om *kommunstyrelsen* har säkerställt att informationssäkerhetsarbetet bedrivs på ett ändamålsenligt sätt och med tillräcklig intern kontroll. För att bedöma granskningens syfte har följande kontrollmål formulerats:

Ändamålsenlighet

- Styrning i form av planer och riktlinjer finns
- Riskbedömningar finns - kommunicerade till politisk- och förvaltningsledning
- Roller och ansvar avseende informationssäkerhetsarbetet är tydliga

Intern kontroll

- Rutiner för rapportering av incidenter och problem är tillfredställande
- Rutiner för backup/säkerhetskopiering och behörigheter är tillfredställande
- Användare har tillräcklig kunskap för en effektiv och säker användning av IT
- Uppföljning, utvärdering och analys är tillräcklig
- Kommunstyrelsen erhåller regelbunden och tillräcklig rapportering inom området

Utifrån genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen inte har säkerställt att informationssäkerhetsarbetet bedrivs på ett ändamålsenligt sätt. Den interna kontrollen bedöms vara bristande för granskningsområdet

I syfte att utveckla verksamheten lämnas följande rekommendationer:

- Kommunstyrelsen säkerställer att styrning i form av planer och riktlinjer upprättas för arbetet med informationssäkerhet. Styrningen kan med fördel omfatta mål, ansvar och roller samt hur uppföljning och utvärdering ska ske
- Kommunstyrelsen utvecklar arbetet med att bedöma risker avseende hur information hanteras samt att resultatet av riskbedömningarna kommuniceras till både politisk ledning och förvaltningsledning
- Kommunstyrelsen säkerställer att verksamheternas behov, i form av utbildning, systemstöd, etc följs upp och utvärderas på ett systematiskt sätt så att lämpliga åtgärder kan vidtas, exempelvis i form av utbildningsinsatser.

1. Inledning

1.1. Bakgrund

Kommunens förtroendevalda revisorer har utifrån risk- och väsentlighet bedömt det angeläget att granska kommunens arbete med informationssäkerhet.

Kommuner är i dag alltmer beroende av sina informationssystem för att kunna leverera nyttigheter till medborgarna på ett effektivt och säkert sätt. Detta ställer krav på ett väl fungerande informationssäkerhetsarbete som säkerställer att rätt information når rätt person. En förutsättning för detta är att styrningen av informationssäkerhetsarbetet är tydlig, att risker i kommunens IT-miljö är kända och kommunicerade samt att det finns fungerande rutiner för att fånga upp och analysera incidenter och problem i syfte att kunna vidta åtgärder.

I en nyligen publicerad undersökning får kommuner generellt sett ett lågt betyg när det gäller IT-säkerhet. Vidare har Myndigheten för säkerhet och beredskap, MSB, 2015 gjort motsvarande bedömning.

1.2. Syfte och Revisionsfråga

Granskningen syftar till att bedöma om *kommunstyrelsen* har säkerställt att informationssäkerhetsarbetet bedrivs på ett ändamålsenligt sätt och med tillräcklig intern kontroll. Bedömning av granskningens syfte ska baseras på följande kontrollmål:

Ändamålsenlighet

- Styrning i form av planer och riktlinjer finns
- Riskbedömningar finns - kommunicerad till politisk- och förvaltningsledning.
- Roller och ansvar avseende informationssäkerhetsarbetet är tydliga

Intern kontroll

- Rutiner för rapportering av incidenter och problem är tillfredställande
- Rutiner för backup/säkerhetskopiering och behörigheter är tillfredställande
- Användare har tillräcklig kunskap för en effektiv och säker användning av IT
- Uppföljning, utvärdering och analys är tillräcklig
- Kommunstyrelsen erhåller regelbunden och tillräcklig rapportering inom området

Granskningens revisionskriterier utgörs av kommunallagens kap 6 samt kommuninterna styrdokument relevanta för området.

1.3. Metod och avgränsning

Genomgång av styrdokument som är upprättade för granskningsområdet. Vidare har intervjuer med kommundirektör, stabschef, driftsansvarig för IT samt systemförvaltare/administratörer inom bl.a. ekonomi, löner och kansli.

Följande bedömningsskala har används vid bedömning av syfte samt kontrollmål.

Inte/ Otillräcklig	I begränsad utsträckning/ Bristande	Till övervägande del	Ja

2. Iakttagelser och bedömningar

2.1. Ändamålsenlighet

2.1.1. Iakttagelser – Styrning

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

Politisk nivå

Granskningen visar att det saknas kommunövergripande styrning, i form av planer eller policys, som reglerar hur informationssäkerhetsarbetet ska bedrivas och vilket syfte som ska uppnås. Vidare kan vi konstatera att det även saknas riktlinjer för hur e-post och mobiltelefoner får användas. Detta kan medföra att användarna exempelvis använder kommunens e-post för avisering av privata paket, vilket medför en risk att skadlig kod som figurerar tar sig in i kommunens system med negativa konsekvenser som följd.

Förvaltningsnivå

På förvaltningsnivå kan vi konstatera att det helt saknas dokumenterade rutiner och riktlinjer för att säkerställa att den information som lagras hanteras på ett säkert sätt. Exempel på sådana riktlinjer kan vara informationssäkerhetsinstruktioner, användarinstruktioner för e-post eller mobiltelefoni. Detta bekräftas i intervju med stabschef på kommunkansliet. Vi konstatera dock att det har påbörjats ett arbete enligt SKL:s verktyg KLASSA[1] samt att frågan har lyfts på ledningsnivå i syfte att skapa medvetenhet om att arbetet med att säkerställa en god informationssäkerhet är eftersatt.

Inom ramen för vår granskning har vi intervjuat systemadministratörer för bl.a. ekonomisystemet, lönesystem, diarium samt system kopplade till socialförvaltningens schemaläggning. Av dessa intervjuer framgår att det generella arbetssättet för att säkerställa att information inte kommer obehörig tillhanda är i första hand att konsultera med närmaste chef, exempelvis vid begäran av utlämning av handlingar. Det finns även etablerade arbetssätt, exempelvis att lönespecifikationer m.m. inte skickas till annan adress än folkbokföringsadressen.

[1] Metod/verktyg för att kartlägga system och information. Utifrån resultatet ska riktlinjer och handlingsplaner upprättas.

2.1.2. Bedömning

Styrning i form av planer och riktlinjer saknas. Bedömningen baseras på följande:

- Övergripande styrning i form av policys eller planer har inte upprättats och fastställts på politisk nivå.
- Rutiner och riktlinjer på verksamhetsnivå har inte upprättats.

2.1.3. Iakttagelser – Riskbedömningar

En viktig del i informationssäkerhetsarbetet är att kartlägga den information som lagras i organisationens olika system samt bedöma hur kritisk informationen är samt vilka risker som finns för att, exempelvis obehöriga får del av informationen. Exempel på risker som kan äventyra att information hanteras på ett säkert sätt kan dels vara kopplad till den tekniska utrustningen men också användarnas kunskap och medvetenhet.

Vår granskning visar att det inte har skett någon kartläggning över den information som finns lagrad inom kommunens olika verksamheter. Vi kan vidare konstatera att det inom verksamheterna inte sker några analyser kring vilka risker som finns kopplat till hantering och lagring av information.

Att klassificera lagrad information utifrån krav på sekretess, riktighet och tillgänglighet är en grundläggande del i arbetet med informationssäkerhet. Detta ger möjlighet att exempelvis basera vilka system som ska prioriteras vid större avbrott. Granskningen visar att kommunens verksamheter inte klassificerar information som finns lagrad i kommunens olika system. Av intervju framgår att IT-enheten har prioriterat vilka system som är mest kritiska. Granskningen har dock inte kunnat styrka att denna prioritering är baserad på verksamheternas behov. Vidare framgår av intervjuer med systemförvaltare/ systemadministratörer att det har påbörjats ett arbete utifrån den nya dataskydds-förordningen GDPR liksom att inventera vilka typer av dokument som saknas. Som nämnts i avsnitt 2.1.1 används SKL:s verktyg KLASSA för detta samt för att få en översikt hur verksamhetssystem förvaltas utifrån ett informationssäkerhetsperspektiv.

Av intervju med driftsansvarig och stabschef för kommunkansliet framgår att tester i syfte att kunna analysera sårbarheter på kommunens IT-miljö har genomförts genom externa s.k. PEN-tester. Resultatet av testerna ger en bild över hur väl kommunens IT-miljö klarar att stå emot försök att ta sig in i kommunens miljö utifrån. Resultatet gav goda resultat vilket indikerar att de åtgärder som vidtas för att obehöriga ska kunna ta sig in i kommunens IT-miljö är tillfredställande. Däremot har det inte skett några kontroller av program/system som används för lagring av information.

Utifrån genomförda intervjuer kan vi konstatera att identifierade risker i kommunens IT-miljö och arbete med att uppnå en god informationssäkerhet i låg utsträckning kommuniceras till kommunens ledning. Intervjuer indikerar att medvetenheten hos den politiska ledningen, såväl som i förvaltningsledningen, är i allmänhet låg.

2.1.4. Bedömning

Riskbedömningar finns i begränsad utsträckning. Bedömningen baseras på följande:

- Arbete för att systematiskt kartlägga och analysera risker kopplat till kommunens informationssäkerhet saknas.
- Riskbedömningar av system inom verksamheterna saknas.
- Kännedom på enhetsnivå finns gällande risker i kommunens IT-miljö.
- Identifierade risker har inte kommunicerats till den politiska ledningen eller till förvaltningsledningen.

2.1.5. Iakttagelser – Ansvar och roller

Politisk nivå

Kommunstyrelsens uppdrag regleras bl.a. i kommunstyrelsens reglemente. I reglementet framgår inte om styrelsen är ansvarig för kommunens informationssäkerhet. Däremot kan vi utläsa att kommunstyrelsen bl.a. är arkivmyndighet för sina verksamheter samt ansvarar för personregister som styrelsen och dess verksamheter förfogar över. Kommunstyrelsen har i övrigt ett ansvar för att kommunens organisation bedrivs på ett effektivt sätt.

Granskningen visar att roller och ansvar för kommunens informationssäkerhetsarbete inte har reglerats i exempelvis riktlinjer, planer eller förvaltningsmodell. Exempelvis finns inte reglerat vad som ingår i att vara systemförvaltare eller motsvarande. Granskningen har heller inte kunnat styrka, i dokument, roll- och ansvarsfördelningen mellan förvaltningarna och IT-enheten. Av intervju med kanslichef och IT-chef framgår att IT-enheten ansvarar för kommunens infrastruktur, d.v.s. datorer, switchar, servrar och nätverk medan förvaltningarna ska ansvara för respektive verksamhetssystem.

Utifrån intervjuer med tjänstepersoner som är systemförvaltare, systemadministratörer eller motsvarande kan vi konstatera att ansvarsfördelningen mellan IT-enheten och systemförvaltare/administratörer överlag upplevs vara tydligt. Även IT-enhetens ansvar gentemot förvaltningarna upplevs vara tydligt. Det som däremot upplevs otydligt, och som vi kunnat konstatera inte har reglerats i riktlinjer eller liknande, är vad som ingår i systemförvaltarnas roller och ansvar. Trots detta upplever de flesta systemförvaltare som intervjuats i denna granskning att det är att tydligt vad som förväntas av en systemförvaltare/systemadministratör.

Utifrån genomförda intervjuer kan vi konstatera att i rollen som systemförvaltare ingår bl.a. att ge behörigheter, utbilda personal i system, bevaka uppdateringar samt ha kontakt med systemleverantör och IT-enheten.

En undersökning, som Myndigheten för samhällsskydd och beredskap (MSB) har genomfört under år 2015 visade, att ca 60 % av 190 svarande kommuner hade utsett ansvariga för ledning och samordning av informationssäkerhetsarbetet. Utifrån genomförda intervjuer kan vi konstatera att det inte finns någon utsedd informationssäkerhetssamordnare. I dagsläget finns ett PUL-ombud som kommer att bli dataskyddsombud när den nya dataskyddsförordningen träder i kraft.

2.1.6. Bedömning

Roller och ansvar avseende informationssäkerhetsarbetet är inte tydliga. Bedömningen baseras på följande:

- Övergripande styrning som fastställer det politiska ansvaret för kommunens informationssäkerhetsarbete saknas.
- Informationssäkerhetssamordnare har inte utsetts. Därmed saknas en viktig funktion för att övervaka och samordna kommunens övergripande informationssäkerhetsarbete.
- Styrning som reglerar ansvar och roller i verksamheten avseende informationssäkerhet saknas.

2.2. Intern kontroll

En förutsättning för att uppnå en god intern kontroll i informationssäkerhetsarbetet är att det finns väl utvecklade rutiner för att hantera exempelvis incidenter och problem, men även att det är tydligt hur lagrad information ska bevaras på ett säkert sätt. Det är också viktigt att det finns en systematisk uppföljning, utvärdering och analys av arbetet samt att det sker en regelbunden kommunikation med ansvariga inom såväl förvaltningsledningen som den politiska ledningen.

2.2.1. Iakttagelser – Rutiner för incidenter och problem

Granskningen visar att det saknas en dokumenterad beskrivning hur användare ska hantera uppkomna problem/incidenter. Inom kommunen finns en servicedesk-funktion som kan hantera generella problem som inte i första hand är kopplade till ett visst system. Detta kan vara allt från lösenordshantering till serveråtkomst. Av intervjuer med systemförvaltare/systemadministratörer framgår dock att det är i första hand till systemleverantör eller IT-tekniker som användarna vänder sig.

Servicedesk har ett ärendehanteringssystem där lösningar på incidenter/problem dokumenteras. Användaren får även feedback hur incident/problem har lösts, exempelvis att programvara har uppdaterats. Av intervjuer med driftsansvarig för IT framgår att ärenden som inte hanteras via servicedesk, exempelvis i de fall användare kontaktar IT-tekniker direkt, dokumenteras i låg utsträckning.

2.2.2. Bedömning

Rutiner för rapportering av incidenter är i begränsad utsträckning tillräcklig. Bedömningen baseras på följande:

- IT-enheten har ärendehanteringssystem som ger förutsättningar att dokumentera ärenden och lösningar.
- Tydliga dokumenterade riktlinjer saknas.
- Intervjuer indikerar att användarna ofta vänder sig direkt till IT-tekniker, därmed uteblir dokumentation och möjlighet till att spåra återkommande incidenter/ problem. Detta åsidosätter även servicedesk/IT-enhetens möjlighet att prioritera ärenden utifrån väsentlighet.

2.2.3. Iakttagelser – Rutiner för back-up/säkerhetskopiering

Granskningen visar att det saknas någon form av överenskommelse mellan IT-enheten och övrig verksamhet gällande säkerhetskopiering och back-up av filer. IT-enheten har rutiner för att säkerhetskopiera och ta back-up för att kunna återskapa eventuellt förlorad information. Däremot saknar IT-enheten kännedom om detta är tillräcklig utifrån verksamheternas behov.

2.2.4. Bedömning

Rutiner för back-up och säkerhetskopiering är i begränsad utsträckning tillräcklig. Bedömningen baseras på följande:

- Back-up och säkerhetskopiering sker regelbundet men är inte baserad på verksamheternas behov.
- Det saknas överenskommelse mellan IT-enheten och verksamheterna som bl.a. reglerar vilken information som ska gå att återskapa samt hur långt tillbaka i tid.

2.2.5. Iakttagelser – Användarnas kunskap

Av intervjuer framgår att det saknas en samlad bild över användarnas kunskapsnivåer när det gäller hur information ska hanteras på ett korrekt och säkert sätt. Det saknas även en samlad bild över användarnas kunskaper när det gäller att använda verksamhetssystem och andra IT-baserade verktyg. Av intervjuer som skett med tjänstepersoner framgår att det inte finns någon strukturerad grundutbildning för nya användare, att nya användare förväntas veta hur man ska göra/bete sig i kommunens system och miljöer samt att mycket ansvar ligger på kollegor att utbilda och/eller föra kunskap vidare.

Överlag upplever de intervjuade att kunskapsnivån, när det dels gäller informations-säkerhet men även användning av system och utrustning, är låg. Exempelvis saknas förståelse för vissa grundläggande åtgärder som kan hindra obehöriga att få tillträde till information/system, exempelvis att byta till säkra lösenord eller inte använda varandras inloggningar.

2.2.6. Bedömning

Användarna har i begränsad utsträckning tillräcklig kunskap för en effektiv och säker användning av IT. Bedömningen baseras på följande:

- En samlad bild över användarnas kunskapsnivåer saknas i dagsläget, dock indikerar intervjuer att kunskapsnivån när det gäller informationssäkerhet är låg.
- Det saknas en strukturerad grundutbildning för nya användare.
- Kunskapsöverföringen sker i hög grad mellan kollegor.

2.2.7. Iakttagelser – Uppföljning, utvärdering och analys

Granskningen visar att det inte sker någon systematisk uppföljning av kommunens informationssäkerhet. Området har identifierats som ett utvecklingsområde och verksamheterna har, som nämnts i tidigare avsnitt, inlett ett kartläggningsarbete enligt SKL:s verktyg KLASSA. Vidare kan vi konstatera, utifrån intervju med driftsansvarig för IT, att IT-enheten har genomförts sårbarhetstester i syfte att se vilka system som är öppna för intrång och behöver uppdateras för att hindra obehöriga från att få tillgång till kommunens IT-miljö.

Av intervju med chef för kommunkansliet och driftsansvarig för IT framgår att information om att personal har avslutat sin anställning inte når IT-enheten. Detta medför en risk att obehöriga har/får tillgång till kommunens system och IT-miljö. Mot denna bakgrund gör IT-enheten kontroller varannan månad över de användare som varit inaktiva eller inte loggat in till kommunens system. Dessa användare görs inaktiva och raderas sedan efter 6 månader. IT-enheten ser ett behov av rutiner där användarnas behörigheter stäms av, på ett automatiserat sätt, mot uppgifter i kommunens lönesystem.

2.2.8. Bedömning

Uppföljning, utvärdering och analys är i begränsad utsträckning tillräcklig. Bedömningen baseras på följande:

- Det sker ingen systematisk uppföljning, utvärdering och analys av informationssäkerheten inom verksamheterna. I sammanhanget noteras dock att ett kartläggningsarbete har inletts i syfte att upprätta styrning och stödjande dokument, vilket ses som positivt.
- IT-enheten gör vissa uppföljningar för att säkerställa att obehöriga inte har tillgång till kommunens system.

2.2.9. Iakttagelser – Rapportering till kommunstyrelsen

I kommunstyrelsens reglemente regleras vad som ingår i kommunstyrelsens styrfunktion. Enligt reglementet ska kommunstyrelsen följa upp och utvärdera kommunens organisation, och därvid vidta eller föreslå åtgärder för att ha en så effektiv organisation som möjligt

En viktig del i att bedriva ett bra informationssäkerhetsarbete är att risker och incidenter rapporteras till beslutsfattare som sedan, med hjälp av väl belysta och allsidiga underlag, kan fatta beslut om ändamålsenliga åtgärder. För att säkerställa detta bör det finnas tydliga rutiner för rapportering.

Granskningen visar att det är främst kostnader kopplade till kommunens IT som rapporteras till kommunstyrelsens arbetsutskott vid begäran. Av intervjuer med chef för kommunkansliet sker ingen återrapportering till utskott eller styrelse om hur kommunens arbete med informationssäkerhet fungerar.

2.2.10. Bedömning

Rapportering till kommunstyrelsen bedöms inte vara tillräcklig. Bedömningen baseras på följande:

- Återrapportering avseende IT sker inte systematiskt och avser främst ekonomi/kostnader.
- Ingen systematisk återrapportering sker hur kommunens informationssäkerhetsarbete bedrivs.

3. Bedömningar

3.1. Bedömningar mot kontrollmål

I tabellen nedan redovisas en sammanfattning av kontrollmålens bedömningar enligt bedömningsskala. Bedömningarna ligger till grund för vår sammanfattande bedömning om *kommunstyrelsen* har säkerställt att informationssäkerhetsarbetet bedrivs på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Inte/ Otillräcklig	I begränsad utsträckning/ Bristande	Till övervägande del	Ja

Kontrollmål	Kommentar
Ändamålsenlighet	***Inte***
Styrning i form av planer och riktlinjer finns	Nej
Riskbedömningar finns - kommunicerad till politisk-och förvaltningsledning.	I begränsad utsträckning tillräcklig
Roller och ansvar avseende informationssäkerhetsarbetet är tydliga	Nej
Intern kontroll	***Bristande***
Rutiner för rapportering av incidenter och problem är tillfredställande	I begränsad utsträckning tillräcklig
Rutiner för backup/säkerhetskopiering och behörigheter är tillfredställande	I begränsad utsträckning tillräcklig
Användare har tillräcklig kunskap för en effektiv och säker användning av IT	I begränsad utsträckning tillräcklig
Uppföljning, utvärdering och analys är tillräcklig	I begränsad utsträckning tillräcklig
Kommunstyrelsen erhåller regelbunden och tillräcklig rapportering inom området	Inte tillräcklig

Utifrån genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen inte har säkerställt att informationssäkerhetsarbetet bedrivs på ett ändamålsenligt sätt. Den interna kontrollen bedöms vara bristande för granskningsområdet.

I syfte att utveckla verksamheten lämnas följande rekommendationer:

- Kommunstyrelsen säkerställer att styrning i form av planer och riktlinjer upprättas för arbetet med informationssäkerhet. Styrningen kan med fördel omfatta mål, ansvar och roller samt hur uppföljning och utvärdering ska ske
- Kommunstyrelsen utvecklar arbetet med att bedöma risker avseende hur information hanteras samt att resultatet av riskbedömningarna kommuniceras till både politisk ledning och förvaltningsledning
- Kommunstyrelsen säkerställer att verksamheternas behov, i form av utbildning, systemstöd etc, följs upp och utvärderas på ett systematiskt sätt så att lämpliga åtgärder kan vidtas, exempelvis i form av utbildningsinsatser.