LULEÅ KOMMUN
Kommunrevisionen

SLUTDOKUMENT
2024-06-11

För kännedom:
Kommunfullmäktige
Partiernas gruppledare

Kommunstyrelsen

Granskning av informationssäkerhet

KPMG har av oss Luleå kommuns revisorer fått i uppdrag att granska kommunstyrelsens ansvar för att kommunen har ett systematiskt informationssäkerhetsarbete.

Syftet med granskningen har varit att bedöma om kommunstyrelsen tillsett att ett systematiskt informationssäkerhetsarbete bedrivs.

Den samlade bedömningen utifrån granskningens syfte är att kommunstyrelsens ledning, styrning och uppföljning att tillse att det bedrivs ett systematiskt informationssäkerhetsarbete inte har varit tillfredsställande.

Kommunen har en informationssäkerhetspolicy och riktlinjer för informationssäkerhetsarbetet, men dessa saknar i stora delar reglering av ansvar, roller, mål och konkreta ramar för arbetet. Bland de få tydliga kravställningar som anges har kommunstyrelsen valt att avvakta implementering av ett ledningssystem för informationssäkerhet, vilket ses som problematiskt då ett sådant ger tydlighet och struktur åt arbetet.

Kommunstyrelsen har nyligen genomfört en organisationsförändring som berör informationssäkerhetsarbetet, och den centrala organisation som ska samordna och driva det övergripande strategiska informationssäkerhetsarbetet är under utveckling. Då granskningen genomfördes var tjänsten som informationssäkerhetssamordnare vakant.

Obeaktat informationssäkerhetssamordnarens kommande tillträde ses en risk i att organisationen inte är tillräcklig för att etablera strukturkapital, driva strategisk utveckling och tillgodose det behov av samordning och stöd som vi uppfattar finns bland nämnderna. Dessa saknar i dagsläget etablerade funktioner för det verksamhetsnära informationssäkerhetsarbetet. Det uppfattas att det finns enskilda arbetsmoment som sker med systematik, men för att tillse ett övergripande systematiskt informationssäkerhetsarbete behöver ansvar och roller formaliseras och arbetssätt likriktas inom hela kommunen. Kommunstyrelsen behöver prioritera att säkerställa en ändamålsenlig organisation för hela kommunens informationssäkerhetsarbete.

Vidare anses att kommunstyrelsen behöver anta ett mer riskbaserat förhållningssätt. Styrelsen har inte genomfört någon samlad riskbedömning ur ett informationssäkerhetsperspektiv, informationssäkerhetsarbetet följs heller inte upp på ett strukturerat sätt. Genom detta menas att kommunstyrelsen inte i tillräcklig utsträckning informerat sig om de hot och risker som kommunens informationstillgångar exponeras för. I förlängningen innebär det att styrelsen inte har tillräcklig insikt för att kunna göra nödvändiga prioriteringar och vägval i syfte att upprätthålla informationssäkerheten.

Utifrån resultatet av granskningen rekommenderas kommunstyrelsen att:

- Formalisera ansvar och roller för informationssäkerhetsarbetet.
- Tillse att ett ledningssystem för informationssäkerhet implementeras.
- Tillse revidering av styrande dokument, som också tar hänsyn till gällande lagar och regler, kommunens interna ansvarsfördelning samt kommunens målsättning för informationssäkerhetsarbetet.
- Verka för att tydliggöra gränsdragningen mellan kommunstyrelsen och infrastruktur- och servicenämnden på politisk nivå såväl som mot förvaltningen.
- Formalisera uppdrag och organisation för den centrala informationssäkerhetsorganisationen.
- Anpassa organisation och resurser utifrån kravställning i informationssäkerhetspolicyn.
- Fastställa mål för informationssäkerhetsarbetet.
- Säkerställa att riskanalys ur ett informationssäkerhetsperspektiv genomförs för hela kommunen.
- Tillse en inventering där de viktigaste informationstillgångarna identifieras och, vid behov, informationsklassas.
- Tillse löpande utbildning i informationssäkerhet för anställda och förtroendevalda.
- Etablera en strukturerad uppföljning av informationssäkerhetsarbetet.
- Ta initiativ till att samordna uppföljning och återrapportering av informationssäkerhetsarbetet med infrastruktur- och servicenämnden.

Vi överlämnar härmed granskningsrapporten för kännedom och yttrande. Yttrande från kommunstyrelsen önskas senast den 30 oktober 2024.

För Luleå kommuns revisorer/

Kurt Hauptmann/ordförande

Granskning av informationssäkerhet

Rapport

Luleå kommun

KPMG AB

2024-05-28

Antal sidor 22

Luleå kommun
Granskning av informationssäkerhet

2024-05-28

Innehållsförteckning

1 Sammanfattning

KPMG har av Luleå kommuns revisorer fått i uppdrag att granska kommunstyrelsens ansvar för att kommunen har ett systematiskt informationssäkerhetsarbete.

Syftet med granskningen har varit att bedöma om kommunstyrelsen tillsett att ett systematiskt informationssäkerhetsarbete bedrivs.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsens ledning, styrning och uppföljning att tillse att det bedrivs ett systematiskt informationssäkerhetsarbete inte har varit tillfredsställande.

Kommunen har en informationssäkerhetspolicy och riktlinjer för informationssäkerhetsarbetet, men dessa saknar i stora delar reglering av ansvar, roller, mål och konkreta ramar för arbetet. Bland de få tydliga kravställningar som anges har kommunstyrelsen valt att avvakta implementering av ett ledningssystem för informationssäkerhet, vilket vi ser som problematiskt då ett sådant ger tydlighet och struktur åt arbetet.

Kommunstyrelsen har nyligen genomfört en organisationsförändring som berör informationssäkerhetsarbetet, och den centrala organisation som ska samordna och driva det övergripande strategiska informationssäkerhetsarbetet är under utveckling. Då granskningen genomfördes var tjänsten som informationssäkerhetssamordnare vakant.

Obeaktat informationssäkerhetssamordnarens kommande tillträde ser vi en risk i att organisationen inte är tillräcklig för att etablera strukturkapital, driva strategisk utveckling och tillgodose det behov av samordning och stöd som vi uppfattar finns bland nämnderna. Dessa saknar i dagsläget etablerade funktioner för det verksamhetsnära informationssäkerhetsarbetet. Vi uppfattar att det finns enskilda arbetsmoment som sker med systematik, men för att tillse ett övergripande systematiskt informationssäkerhetsarbete behöver ansvar och roller formaliseras och arbetssätt likriktas inom hela kommunen. Vi anser härvid att kommunstyrelsen behöver prioritera att säkerställa en ändamålsenlig organisation för hela kommunens informationssäkerhetsarbete.

Vidare anser vi att kommunstyrelsen behöver anta ett mer riskbaserat förhållningssätt. Styrelsen har inte genomfört någon samlad riskbedömning ur ett informationssäkerhetsperspektiv, informationssäkerhetsarbetet följs heller inte upp på ett strukturerat sätt. Genom detta menar vi att kommunstyrelsen inte i tillräcklig utsträckning informerat sig om de hot och risker som kommunens informationstillgångar exponeras för. I förlängningen innebär det att styrelsen inte har tillräcklig insikt för att kunna göra nödvändiga prioriteringar och vägval i syfte att upprätthålla informationssäkerheten.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Formalisera ansvar och roller för informationssäkerhetsarbetet.

- Tillse att ett ledningssystem för informationssäkerhet implementeras.
- Tillse revidering av styrande dokument, som också tar hänsyn till gällande lagar och regler, kommunens interna ansvarsfördelning samt kommunens målsättning för informationssäkerhetsarbetet.
- Verka för att tydliggöra gränsdragningen mellan kommunstyrelsen och infrastruktur- och servicenämnden på politisk nivå såväl som mot förvaltningen.
- Formalisera uppdrag och organisation för den centrala informationssäkerhetsorganisationen.
- Anpassa organisation och resurser utifrån kravställning i informationssäkerhetspolicyn.
- Fastställa mål för informationssäkerhetsarbetet.
- Säkerställa att riskanalys ur ett informationssäkerhetsperspektiv genomförs för hela kommunen.
- Tillse en inventering där de viktigaste informationstillgångarna identifieras och, vid behov, informationsklassas.
- Tillse löpande utbildning i informationssäkerhet för anställda och förtroendevalda.
- Etablera en strukturerad uppföljning av informationssäkerhetsarbetet.
- Ta initiativ till att samordna uppföljning och återrapportering av informationssäkerhetsarbetet med infrastruktur- och servicenämnden.

2 Bakgrund

KPMG har av Luleås kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens ansvar för att kommunen har ett systematiskt informationssäkerhetsarbete. Uppdraget har ingått i revisionsplanen för år 2023.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Informationssäkerhet innebär att all skyddsvärd information ska vara tillgänglig, konfidentiell och spårbar.

Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Utvecklingen och den förändrade användningen av ny teknik innebär också att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. Den digitala utvecklingen måste följas av ett säkerhetsarbete för att säkerställa att inte de system och digitala tjänster som nyttjas för informationshantering och lagring är exponerade och tillgängliga för cyberhot och angrepp. Ett flertal offentliga organisationer har under de senaste åren utsatts för cyberattacker med stora konsekvenser som följd. Exempelvis har skyddsvärd information förlorats eller röjts till obehöriga eller den bristande hanteringen lett att organisationer drabbats av ekonomisk skada eller förtroendeskada. Inledningsvis 2024 utsattes en större leverantör av serverdrift och molntjänster för en ransomware-attack vilken fått en allvarlig påverkan på ett stort antal statliga myndigheters, kommuners och regioners tillgång till sina informationssystem.

Inom ramen för det kommunala åtagandet finns en rad samhällsviktiga och kritiska funktioner, vilka om de inte fungerar kan leda till skada för såväl enskilda individer som samhället i stort. Det är därför av största vikt att det bedrivs ett systematiskt informationssäkerhetsarbete för att undvika allvarlig påverkan på verksamheten och samhället i stort.

Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för kommunen. Det är således väsentligt att kommunen bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att informationssäkerhetsarbetet behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att bedöma om kommunstyrelsen tillsett att ett systematiskt informationssäkerhetsarbete bedrivs.

Granskningen har besvarat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?

- Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?
- Har styrelsen tillsett att det finns en tillräcklig säkerhetskultur?
- Har säkerhetsåtgärder vidtagits som ett resultat av riskbedömningar?
- Finns en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser?
- Finns en tillräcklig uppföljning och återrapportering av kommunens informationssäkerhetsarbete?

Granskningen har inriktats mot kommunstyrelsens övergripande ansvar för styrning och uppföljning av informationssäkerhet.

Avgränsningen har omfattat organisatorisk säkerhet, personalsäkerhet och teknisk säkerhet. Fysisk säkerhet har inte ingått i granskningen.

Granskningen har omfattat år 2024.

2.2 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut
- MSB:s metodstöd och rekommendationer avseende Ledningssystem för informationssäkerhet och it-säkerhetsåtgärder *(se bilaga A)*
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster där detta är tillämpbart

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier av styrande dokument såsom informationssäkerhetspolicy, riktlinjer för informationssäkerhet, it-policy, incidenthanteringsrutiner mm
- Intervjuer har genomförts med: kommunstyrelsens presidium, kommundirektör, biträdande kommundirektör, säkerhets- och beredskapschef, säkerhetsskyddschef, informationssäkerhetshandläggare, it-chef.

Samtliga intervjuade har getts möjlighet att faktakontrollera rapporten.

3 Resultat av granskningen

3.1 Styrande dokument

3.1.1 Ledningssystem för informationssäkerhet (LIS)

En kommuns eller ett bolags verksamhet kan identifieras som att det tillhandahåller samhällsviktiga tjänster och står därav under kraven i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, även kallat NIS-direktivet. I lagen ställs krav på att verksamheter som tillhandahåller samhällsviktiga tjänster ska ha ett etablerat ledningssystem för informationssäkerhet, ett så kallat LIS.

3.1.2 Styrande dokument inom informationssäkerhet

Kommunfullmäktige har antagit en informationssäkerhetspolicy[1] som gäller för kommunens samtliga verksamheter. Policyn redovisar övergripande mål för vad informationssäkerhetsarbetet ska leda till. Härigenom framgår att arbetet ska uppnå krav som ställs av nationella informationssäkerhetsstandarder och att det ska vara systematiskt och utgå från ett ledningssystem.

Dokumentet Riktlinjer informationssäkerhet för användare[2] konkretiserar informationssäkerhetspolicyn och beskriver hur medarbetare ska agera för en god informationssäkerhet

För IT-arbetet finns en IT-policy[3] som fastställer kommunens principiella förhållningssätt avseende IT-verksamheten. Kommunen har också antagit en systemförvaltarmodell som beskrivs i Riktlinjer informationssäkerhet och systemförvaltning[4]. Modellen reglerar ansvar och roller för funktioner kopplade till förvaltning av enskilda informationssystem.

Utöver systemförvaltarmodellens roller och de grupperingar som utpekas i Riktlinjer informationssäkerhet för användare saknar de styrande dokumenten kravställning av ansvar och roller för informationssäkerhet. I intervjuer framhålls det vara en brist som lett till att det inom nämnderna saknas etablerade strukturer för det verksamhetsnära informationssäkerhetsarbetet.

Vidare konstaterar intervjuade att de styrande dokumenten är inaktuella. Det finns även en uppfattning att dokumenten inte heller efterlevs.

Vi kan också konstatera att kommunen inte implementerat något ledningssystem för informationssäkerhet. I intervju konstateras att målsättningen är att ha ett sådant. Dock ses utmaningar med att skapa ett ledningssystem som å ena sidan är tillräckligt omfattande för att ge struktur åt hela informationssäkerhetsområdet, men å andra sidan inte är för komplext så att verksamheterna ändå inte mäktar att använda det.

[1] Daterad 2015-04-13
[2] Daterad 2015-10-01
[3] IT-policy, daterad 2016-09-14
[4] Daterad 2012-11-29

3.1.3 Bedömning

Vi bedömer att det delvis finns styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas.

Genom informationssäkerhetspolicyn och it-policyn har kommunen antagit en grund för informationssäkerhetsarbetet. Vi ser också att det finns anvisningar för det dagliga arbetet som kan fungera som stöd för den enskilda medarbetaren. Däremot saknar vi riktlinjer för hur det beslutade syftet med informationssäkerhetsarbetet ska uppnås.

Ett systematiskt informationssäkerhetsarbete förutsätter tydliga roller för både det strategiska och det operativa arbetet. Därvid anser vi att kommunstyrelsen behöver tillse att ansvar på samtliga organisatoriska nivåer, från kommunstyrelse till verksamhetsnivå, fastställs och formaliseras.

Vidare konstaterar vi att flera kravställningar i de styrande dokumenten inte efterlevs. Tillsammans med det faktum att samtliga styrande dokument är daterade bedömer vi att kommunstyrelsen behöver säkerställa att revideringen av dokument genomförs och anpassas till gällande lagar och föreskrifter samt går i linje med kommunstyrelsens ambitionsnivå för informationssäkerhetsarbetet.

3.2 Roller och ansvar

3.2.1 Ansvarsfördelning informationssäkerhet

I kommunens nämndreglemente[5] regleras kommunstyrelsens ansvar att leda och samordna informationssäkerheten inom kommunen. Som verksamhetsområde tillhör informationssäkerhet säkerhet och beredskap som ligger inom kommunstyrelseförvaltningen. Kontoret tillskapades vid årsskiftet 2023/2024. Innan dess var informationssäkerhetsenheten direkt underställd kommundirektör.

Inrättandet av säkerhet och beredskap beskrivs som en strategisk förändring för att samla och skapa samordningsvinster mellan olika säkerhetsområden. Funktionerna inom informationssäkerhet har till uppdrag att stötta och rådge verksamheterna i informationssäkerhetsarbete och dataskydd. Utöver säkerhets- och beredskapschef, som har ett övergripande ansvar för säkerhets och beredskap, fanns vid tid för granskning en informationssäkerhetshandläggare. Handläggarens arbetsuppgift är att stötta verksamheterna i det operativa informationssäkerhetsarbetet. Vidare har en informationssäkerhetssamordnare rekryterats och tillträder under hösten 2024. Hos de intervjuade framgår en avsikt att bredda den verksamhet som arbetar med informationssäkerhet då samordning av informationssäkerhetsarbetet tidigare åvilat enskilda funktioner. Till följd av det anses arbetet ha varit personbundet och inte tillräckligt resurssatt för att både stötta verksamheterna och driva den strategiska utvecklingen.

På verksamhetsnivå utförs i nuläget punktvist arbete, enligt de intervjuade. Formaliserade funktioner för såväl operativa arbetsuppgifter som för utövande av verksamhetsnära informationssäkerhetsansvar saknas. Den centrala

[5] Luleå kommuns nämndreglemente, reviderat 2023-05-22

stödorganisationen har därför fått ta ett större operativt ansvar än vad som avsetts, vilket skett på bekostnad av den övergripande samordningen.

Inom kommunledningen uttrycks en medvetenhet om att informationssäkerhetsarbetet inte är tillräckligt systematiskt på verksamhetsnivå. De intervjuade anser att nämnderna behöver ha egen kompetens för och driva det verksamhetsnära informationssäkerhetsarbetet, samtidigt som det ses utmanande att ålägga verksamheterna ytterligare arbetsuppgifter. Den kommande informationssäkerhetssamordnaren, som tillträder under hösten 2024, uppges få en avgörande roll i att etablera arbetsstrukturer på verksamhetsnivå.

Enligt Riktlinjer informationssäkerhet för användare ska ett informationssäkerhetsråd inrättas, som bland annat ska bevaka kommunens efterlevnad till styrande dokument och lagstiftning samt återrapportera till kommundirektörens ledningsgrupp. En annan gruppering ska besluta om åtgärder till följd av inrapporterade informationssäkerhetsincidenter. Även detta ska rapporteras till ledningsgruppen.

Genom intervjuer kan vi konstatera att ingen av de grupperingar som nämns i riktlinjen har tillskapats. I samtliga fall motiveras det med att verksamheterna har svårt att frigöra tid och resurser till informationssäkerhetsarbete. I stället för att inrätta två specifika grupperingar med smalt ansvarsområde vill kommunledningen hitta samordningsvinster genom att etablera bredare nätverk där säkerhetsfrågor av olika slag diskuteras.

3.2.2 Ansvarsfördelning it-säkerhet

Enligt kommunens nämndreglemente ansvarar kommunstyrelsen för ledning och samordning av it-säkerhet medan infrastruktur- och servicenämnden ansvarar för drift, support och underhåll av it-infrastrukturen. Uppdelningen skedde vid årsskiftet 2023/2024 då kommunens serviceverksamheter samlades inom nämnden.

Strategisk utveckling och leverans av it-drift är områden som kräver initierad specialistkompetens. Att separera dessa förutsätter att fackkompetens finns hos både beställare och utförare, och att förhållandet de två är mellan är tydligt definierat.

Gränsdragningen mellan kommunstyrelsens respektive nämndens ansvarsområde, där de två konstateras ha fått ett beställar- och utförararförhållande, framförs vara under utarbetning och inte helt tydliggjord. Det samma gäller förvaltningsstrukturen där kontoret it och digitaliserings ledningsgrupp, som går in i båda organisationerna, svarar mot två olika nämnder och två olika förvaltningsledningar.

Då granskningen genomfördes pågick dels en verksamhetsanalys inom it- och digitaliseringskontoret, dels en övergripande organisationsutvärdering i syfte att inventera dylika frågeställningar. Analyserna framförs vara av vikt för det fortsatta utvecklingsarbetet.

Kommunstyrelsens ansvar konkretiseras ytterligare i kommunens it-strategi[6] där det framgår att styrelsen ska vara beslutande i större it-investeringar, medan kommundirektörens ledningsgrupp ska vara beslutande i kommunövergripande it-

[6] It-strategi för Luleå kommun 2017-2019, reviderad 2016-08-29, giltig till och med 2019-12-31

frågor och it-projekt som ryms inom tilldelad ram. Strategin fastställer även it- och digitaliseringskontorets ansvar för drift och utveckling av kommunens it-miljö samt för att vidta åtgärder som leder till förbättrad informationssäkerhet inom hela kommunen. It- och digitaliseringskontoret ska också bereda större it-investeringar och strategiska it-frågor för beslut i kommunstyrelsen.

Kontoret interna organisering utgörs av drift- och serviceenheten som ansvarar för driften av kommunens samlade it-miljö, en enhet för strategisk utveckling och styrning samt en central ledningsstab. Enheterna leds av respektive enhetschef medan en it-chef ansvarar för hela avdelningen.

Inom enheten för strategisk utveckling och styrning finns en it-säkerhetssamordnare. Vid tid för granskning pågick rekrytering av en it-säkerhetssamordnare samt en teknisk it-säkerhetsspecialist.

Som vi tidigare i rapporten beskrivit har kommunen fastställt en systemförvaltarmodell. Både it-strategin och Riktlinjer för roller och ansvar inom informationssäkerhet och systemförvaltning reglerar ansvar och uppgifter av it-teknisk karaktär för funktioner inom systemförvaltarmodellen.

3.2.3 Bedömning

Vår bedömning är att kommunstyrelsen inte säkerställt en ändamålsenlig organisation för informationssäkerhetsarbetet.

Vi konstaterar att kommunen befinner sig i en utvecklingsfas där struktur och organisation för informationssäkerhetsarbetet är under förändring. Då granskningen genomfördes var rollen som informationssäkerhetssamordnare vakant, vilket innebär att strategiskt utvecklingsansvar för verksamhetsområdet inte uppbärs i nuläget. Givet behovet av utveckling av strukturkapital, det vill säga dokumentöversyn, implementering av ledningssystem och stöd till nämndernas informationssäkerhetsarbete, ser vi en risk att nuvarande organisation och resurser inte är tillräckliga i förhållande till den kravställning som anges av informationssäkerhetspolicyn.

En grundbult i ett systematiskt informationssäkerhetsarbete är central samordning. Av den anledningen anser vi att kommunstyrelsen behöver formalisera uppdrag och organisation för den centrala informationssäkerhetsorganisationen. Vi bedömer även att kommunstyrelsen behöver tillse att organisation och resurser i hela kommunen anpassas utifrån de krav som ställs i informationssäkerhetspolicyn. Att det verksamhetsnära arbetet drivs av respektive nämnd är en förutsättning för att etablera ett systematiskt informationssäkerhetsarbete i hela kommunorganisationen.

Gällande it- och digitaliseringskontoret bedömer vi att kommunstyrelsen behöver följa resultatet av den pågående verksamhetsanalysen samt, vid behov, förtydliga gränsdragning i förhållande till infrastruktur- och servicenämnden. Befintliga styrande dokument behöver också ses över så att innehåll korrelerar med den genomförda organisationsförändringen.

Vidare noterar vi att IT-strategi, IT-policy och nämndreglementet är daterade och i behov av revidering. Vi anser att revideringen bör göras med hänsyn till de förändrade

ansvarsförhållandena kommunstyrelsen och infrastruktur- och servicenämnden emellan. Vi bedömer även att kommunstyrelsen behöver verka för att gränsdragningen tydliggörs i den löpande verksamheten, på politisk nivå såväl som mot förvaltningen.

3.3 Mål och handlingsplaner

Kommunstyrelsen har inte antagit några mål för informationssäkerhetsarbetet. De intervjuade framför att arbetet i nuläget inriktas mot att etablera en sammanhållen organisatorisk bas för informationssäkerhet och återimplementering av klassningsmodell. Framtagande av mål uppges bli aktuellt i ett senare skede.

Enligt vissa intervjuade kan de övergripande viljeyttringarna i informationssäkerhetspolicyn tolkas som målsättningar för informationssäkerhetsarbetet, dock framförs att dessa inte varit styrande i arbetet.

3.3.1 Bedömning

Vi bedömer att kommunstyrelsen saknar beslutade informationssäkerhetsmål och tillhörande handlingsplaner.

Enligt vår mening är fastställda mål och handlingsplaner är ett effektivt sätt att styra och systematisera informationssäkerhetsarbetet. Tydliga mål ställda på både kort och lång sikt ger stöd i att prioritera och vägleda arbetet i enlighet med kommunstyrelsens ambition. Det ger också strukturerade möjligheter att följa upp och utvärdera genomfört arbete, samt identifiera behov av nödvändiga förbättringar.

3.4 Riskhantering och säkerhetsåtgärder

3.4.1 Riskbedömning och informationsklassning

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, framgår att leverantör av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Utifrån detta har MSB rekommendationer avseende säkerhetsåtgärder i syfte att öka skyddet mot angrepp eller minimera eventuell skada. Rekommendationerna omfattar bland annat säkerhetsuppdateringar, säkerhetskopiering samt förmågan att upptäcka säkerhetshändelser.

Enligt Riktlinjen informationssäkerhet för användare ska informationsklassning ligga till grund för hur informationstillgångar ska skyddas. Riktlinjen innehåller ingen modell för informationsklassning eller riskbedömning, men anger att klassning ska bedömas utifrån tre nivåer och genomföras av systemägare och systemförvaltare.

3.4.2 Vidtagna IT-säkerhetsåtgärder

Enligt de intervjuade har det inte genomförts någon kommunövergripande riskanalys ur ett informationssäkerhetsperspektiv.

Vi får uppfattningen att det finns en systematik i att genomföra informationsklassningar och riskbedömningar i samband med upphandling av nya system, då enligt klassningsmodellen KLASSA[7]. Det finns ingen tydlig bild över i vilken utsträckning som klassningar av befintliga system har genomförts, detta har inte heller dokumenterats. De intervjuade konstaterar emellertid att tidigare arbete inte haft tillräcklig systematik för att säkerställa att informationsklassningar genomförts utifrån vilka informationstillgångar som är mest prioriterade.

It-säkerhetsmässigt framförs att delar från klassning och riskbedömning ligger till grund för it-säkerhetsåtgärder som implementeras. Vi har erhållit ett antal handlingsplaner där resultat från informationsklassning och behov av it-säkerhetsåtgärder framgår, vilket styrker det som uppges i intervju.

Av säkerhetsskäl väljer vi att inte redovisa befintliga it-säkerhetsåtgärder i detalj, men baserat på intervjuer och dokumentation är vår bedömning att väsentliga it-säkerhetsåtgärder implementeras utifrån viss systematik. Nuvarande arbetssätt ger även förutsättningar för att tillse att säkerhetsåtgärder är aktuella genom regelbundna tester som kontoret it och digitalisering utför.

Kontoret genomför även månatliga sårbarhetsscanningar i syfte att detektera svagheter i it-säkerhetsskyddet. Inom ramen för granskningen har vi tagit del av dokumentation från ett sådant scanningstillfälle. Enligt muntliga uppgifter har resultatet av sårbarhetsscanningarna förbättrats över tid då identifierade svagheter legat till grund för förbättringar av it-säkerhetsskyddet. Därtill uppges att it- och digitaliseringskontoret genomför cykliska penetrationstester. Detta gjordes senast 2020 och ska göras på nytt under 2024.

3.4.3 Bedömning

Vår bedömning är att it-säkerhetsåtgärder delvis vidtagits som ett resultat av riskbedömningar.

Vi baserar vår bedömning på att det finns behov av att genomföra riskbedömningar i högre utsträckning på flera nivåer. Bland annat saknas i nuläget en kommunövergripande riskanalys för informationssäkerhetsrisker som kommunen skulle kunna drabbas av och vilka konsekvenser detta skulle innebära. Därtill behöver systematiken för genomförande av informationsklassningar och riskanalyser för informationstillgångar stärkas. I nuläget finns system som inte klassats vilket kan riskera att säkerhetsåtgärder inte vidtagits som det finns behov av.

[7] Ett informationsklassningsverktyg för offentliga organisationer framtaget av Sveriges kommuner och regioner.

3.5 Kritiska IT-säkerhetshändelser

Enligt flera intervjuade har ekonomiska resurser för it-säkerhet riktats mot att bygga ett skydd mot yttre hot och störningar. Då granskningen genomfördes pågick upphandling av en extern övervakningstjänst som monitorerar kommunens it-miljö och kan sätta in åtgärder vid cyberhot och attacker dygnet runt. Tjänsten ska också ge en bättre helhetsbild över pågående it-säkerhetshändelser då övervakning i nuläget utgår från enskilda delar av infrastrukturen. I nuläget framförs att kommunen har förmåga att upptäcka både organisatoriska och tekniska it-säkerhetshändelser.

Internt finns incidentberedskap i form av två team från it- och digitaliseringskontoret som rullar på schemalagd jour utanför kontorstid. Teamen är kopplade till kommunens övergripande beredskapsfunktion, varvid beredskapen även innefattar fysiska larm från till exempel serverhallen. Därtill finns på kommunövergripande nivå tjänsteperson i beredskap som är tillgänglig dygnet runt.

It- och digitaliseringskontorets incidenthantering följer ITIL:s incidenthanteringsprocess[8], vilken konkretiseras av en handbok och flera förtydligande dokument, som vi tagit del av. Processen kravställer även ett uppföljningsansvar, vilket enligt muntliga uppgifter sker enligt rutinen.

Utöver ITIL-processen regleras incidenthanteringen för vissa system av avtalade överenskommelser om servicenivåer, så kallad SLA[9]. Dessa kan likställas vid avtal som upprättas för enskilda it-system där tillgänglighet och driftleverans fastställs. Detta gäller främst system som används inom socialförvaltningen, för vilket vi delgivits dokumenterade avtal.

3.5.1 Bedömning

Vi bedömer att det delvis finns en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser.

Den externa tjänst som kommunen avser upphandla för dygnet runt-övervakning är, enligt vår mening, en viktig förstärkning av incidenthanteringsförmågan. Tjänsten ger både förbättrade tekniska förutsättningar att detektera intrångsförsök och hot samt reducerar responstider för avbrott som sker utanför kontorstid.

Vidare bedömer vi att kommunen genom att följa ITIL:s incidenthantering har en tydlig och strukturerad incidenthanteringsprocess, som också omfattar uppföljning av incidenter.

3.6 Säkerhetskultur

Av metodstödet för informationssäkerhet från Myndigheten för samhällsskydd och beredskap framgår att utbildning och medvetenhet bidrar till ett riskbaserat

[8] Ett it-ramverk med standardiserade incidenthanteringsprocesser.
[9] SLA står för “service level agreement” (överenskommen servicenivå).

förhållningssätt som är grundläggande för ett ändamålsenligt informationssäkerhetsarbete.

Vår bild utifrån intervjuer är att medvetenheten om cyberhot ökat inom kommunen, men att kunskap om informationssäkerheten är mer begränsad. Nyanställda genomgår MSB:s grundutbildning i informationssäkerhet[10]. Ytterligare utbildning tillhandahålls inte.

3.6.1 Bedömning

Vår bedömning är att kommunstyrelsen inte tillsett en tillräcklig säkerhetskultur.

Det är positivt att samtliga nyanställda genomgår utbildningen från MSB. Vi anser emellertid att kommunstyrelsen behöver tillse mer frekventa och återkommande utbildningar för samtliga anställda och förtroendevalda. Att kunskap och medvetenhet om informationssäkerhetsrisker hålls aktuellt är enligt vår mening grunden i ett säkert användarbeteende.

3.7 Uppföljning och återrapportering

Av 6 kap. 6 § Kommunallagen (2017:725) framgår att nämnderna inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten. De ska även se till att den interna kontrollen är tillräcklig och att verksamheten beskrivs på ett i övergripande tillfredställande sätt.

Vidare framgår av MSB:s metodstöd att för att ledningen på en strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i kommunen behöver det ske en kommunövergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning. Resultatet från ledningens genomgång ska dokumenteras och bevaras.

3.7.1 Uppföljning i praktiken

I Luleå kommun följs informationssäkerhet inte upp formaliserat av vare sig kommunstyrelsen eller kommunledningen. Kommunstyrelsen får vid behov situationsbaserad uppföljning i dialogform av kommundirektören, som också avrapporterar informationssäkerhetsarbetet en gång om året enligt samma tillvägagångssätt. Både de förtroendevalda och tjänstepersoner som intervjuats för granskningen anser att sådana dialoger är effektivare än skriftliga rapporter motsvarande ”ledningens genomgång”.

På kommunledningsnivå finns ”arenor” – forum där kommunens förvaltningschefer och vissa centrala ledningsfunktioner diskuterar övergripande strategisk utveckling inom dessa olika områden. Säkerhet, därigenom informationssäkerhet, tillhör ”arena

[10] Myndigheten för samhällsskydd och beredskap har tagit fram Disa – digital informationssäkerhetsutbildning för alla.

utveckling”. Områdena inom arenan följs i nuläget upp i dialogform. Mer strukturerade former för uppföljning framförs vara aktuella först i ett senare skede då samordningen av informationssäkerhetsarbetet etablerats tydligare.

3.7.2 Bedömning

Vår bedömning är att det inte finns en tillräcklig uppföljning eller återrapportering av informationssäkerhetsarbetet.

Vi anser att dokumenterad uppföljning säkerställer underlag för kunskap och information, vilket stärker kommunstyrelsens förutsättningar att vara informerad om informationssäkerhetsrisker och cyberhot som kommunen är utsatt för. Vi ser det som nödvändigt för att kunna fatta nödvändiga och välavvägda beslut samt säkerställa att kommunen når beslutade mål för arbetet.

Till följd av att kommunstyrelsen och infrastruktur- och servicenämnden ansvarar för olika aspekter av informationssäkerhetsarbetet anser vi att kommunstyrelsen behöver ta initiativ till att samordna uppföljnings- och återrapporteringsansvar konstellationerna emellan.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelsen tillsett att ett systematiskt informationssäkerhetsarbete bedrivs.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsens ledning, styrning och uppföljning att tillse att det bedrivs ett systematiskt informationssäkerhetsarbete inte har varit tillfredsställande.

Revisionsfråga	Bedömning: Delvis	Rekommendationer
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?	Informationssäkerhetspolicyn och it-policyn ger en grund för informationssäkerhetsarbetet. Anvisningar för det dagliga arbetet är stöd för den enskilda medarbetaren. Riktlinjer för hur det beslutade syftet med informationssäkerhets-arbetet ska uppnås, saknas dock. Ansvar på samtliga organisatoriska nivåer, från kommunstyrelse till verksamhetsnivå, behöver fastställas och formaliseras. Flera kravställningar i de styrande dokumenten efterlevs inte. Samtliga styrande dokument är daterade. Dokumenten behöver revideras och anpassas till gällande lagar och föreskrifter samt gå i linje med kommunstyrelsens ambitionsnivå för informationssäkerhetsarbetet.	- Formalisera ansvar och roller för informationssäkerhetsarbetet - Tillse att ett ledningssystem för informationssäkerhet implementeras - Tillse revidering av styrande dokument, som också tar hänsyn till gällande lagar och regler, kommunens interna ansvarsfördelning samt kommunens målsättning för informationssäkerhetsarbetet .
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Finns en ändamålsenlig organisation för informations-säkerhetsarbetet?	Givet behovet av utveckling av strukturkapital ser vi en risk att nuvarande organisation och resurser inte är tillräckliga i förhållande till kravställningen i informationssäkerhetspolicyn. Kommunstyrelsen behöver tillse att organisation och resurser i hela kommunen anpassas utifrån de krav som ställs i informationssäkerhets-policyn. Gällande it- och digitaliseringskontoret behöver kommunstyrelsen följa resultatet av den pågående verksamhetsanalysen samt, vid behov, förtydliga gränsdragning i förhållande till infrastruktur- och servicenämnden.	- Verka för att tydliggöra gränsdragningen mellan kommunstyrelsen och infrastruktur- och servicenämnden på politisk nivå såväl som mot förvaltningen - Formalisera uppdrag och organisation för den centrala informationssäkerhets-funktionen - Anpassa organisation och resurser utifrån kravställning

		i informations-säkerhetspolicyn
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?	Tydliga mål ställda på både kort och lång sikt ger stöd i att prioritera och vägleda arbetet i enlighet med kommunstyrelsens ambition. Det ger också strukturerade möjligheter att följa upp och utvärdera genomfört arbete, samt identifiera behov av nödvändiga förbättringar.	- Fastställa mål för informationssäkerhetsarbetet
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Har säkerhetsåtgärder vidtagits som ett resultat av riskbedömningar?	Det finns behov av att genomföra riskbedömningar i högre utsträckning på flera nivåer. Bland annat saknas i nuläget en kommunövergripande riskanalys för informationssäkerhetsrisker. Därtill behöver systematiken för genomförande av informationsklassningar och riskanalyser för informationstillgångar stärkas.	- Säkerställa att riskanalys ur ett informationssäkerhets-perspektiv genomförs för hela kommunen - Tillse en inventering där de viktigaste informations-tillgångarna identifieras och, vid behov, informations-klassas
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Finns en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhets-händelser?	Den externa tjänst som kommunen avser upphandla för dygnet runt-övervakning är en viktig förstärkning av incidenthanteringsförmågan. Genom att följa ITIL:s incidenthantering har kommunen en tydlig och strukturerad incidenthanteringsprocess, som också omfattar uppföljning av incidenter.	- Tillse att incidenthanteringsrutinerna testas
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Har styrelsen tillsett att det finns en tillräcklig säkerhetskultur?	Det är positivt att samtliga nyanställda genomgår utbildningen från MSB. Kommunstyrelsen behöver tillse mer frekventa och återkommande utbildningar för samtliga anställda och förtroendevalda.	- Tillse löpande utbildning i informationssäkerhet för anställda och förtroendevalda
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Finns en tillräcklig uppföljning och återrapportering av kommunens informationssäkerhetsarbete?	Dokumenterad uppföljning säkerställer underlag för kunskap och information, vilket stärker kommunstyrelsens förutsättningar att vara informerad om informationssäkerhetsrisker och cyberhot som kommunen är utsatt för.	- Etablera en strukturerad uppföljning av informationssäkerhetsarbetet - Ta initiativ till att samordna uppföljning och återrapportering av

	Till följd av att kommunstyrelsen och infrastruktur- och servicenämnden ansvarar för olika aspekter av informationssäkerhetsarbetet behöver kommunstyrelsen ta initiativ till att samordna uppföljnings- och återrapporteringsansvar konstellationerna emellan.	informationssäkerhetsarbetet med infrastruktur- och servicenämnden

Datum som ovan
KPMG AB

Jenny Thörn
Specialist och verksamhetsrevisor

Sofie Ernerudh
Verksamhetsrevisor

Micaela Hedin
Certifierad kommunal yrkesrevisor
och kundansvarig

5 Bilaga A

Som revisionskriterium i granskningen utgår vi från MSB:s metodstöd och rekommendationer för ett systematiskt informationssäkerhetsarbete och säkerhetsåtgärder med fokus på nedanstående områden.

Standard och krav

Metodstödet bygger på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien och då främst på SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 om ledningssystem för informationssäkerhet.

Ledningssystem för informationssäkerhet

Ett ledningssystem för informationssäkerhet (ofta förkortat LIS) är den del av ledningssystemet som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, som planering och uppföljning. Det innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och kontroller samt ser över styrdokumenten med jämna mellanrum.

Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare om vilka krav som ställs i arbetet. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer.

Ansvar och organisation

Metodstödet beskriver hur ansvaret för arbetet med informationssäkerhet bör fördelas i organisationen samt tydliggör betydelsen av ledningens förståelse och engagemang i informationssäkerhetsarbetet för att det ska lyckas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, chefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten. Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Utbildning och kommunikation

MSB:s metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet. Utbildning och kommunikation ökar också acceptansen av och förståelsen för de säkerhetsåtgärder som implementeras.

Riskanalys och informationsklassning

Genom en riskanalys ska verksamheten identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen. Riskanalyser kan göras verksamhetsövergripande, för en process eller för ett enskilt objekt. Risker och potentiella händelser som kan leda till negativa konsekvenser beskrivs och bedöms sedan avseende sannolikheten att de inträffar samt potentiella konsekvenser.

Metodstödet anger vidare att informationsklassning är en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet. Skyddsnivåerna beskriver säkerhetsåtgärder som informationens värde kräver. Identifierat behov av säkerhetsåtgärder utgör ett viktigt underlag vid exempelvis kravställning av tjänster, som interna och externa it-tjänster. De identifierade behoven av säkerhetsåtgärder bör dokumenteras i en åtgärdsplan. It-säkerhetsåtgärder rent tekniskt kan vara en del men klassningen kan även ha identifierat behov av kompletterande risk- och konsekvensanalyser, förbättrade rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Skyddsåtgärder

Informationstillgångar består av information och resurser som används för att hantera information. Själva informationen är den primära tillgången som ska klassas. Resurser som används för att hantera informationen, till exempel it-system och fysiska tillgångar, samt rutiner i verksamheten ska sedan utformas enligt skyddsnivåer som matchar klassningens resultat. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

I MSB:s föreskrift för säkerhetsåtgärder i informationssystem framgår att systemägaren behöver ha en dialog med berörda informationsägare inom organisationens olika verksamheter för att införa de säkerhetsåtgärder som ger rätt nivå av skydd för informationssystemet. Behovet av säkerhetsåtgärder identifieras utifrån de informationsklassningar och riskbedömningar som informationsägaren har genomfört, samt systemägarens egna riskbedömningar för informationssystemet.

MSB:s metodstöd beskriver att övervakning anger status för ett system, en process eller en aktivitet. Övervakning sker ofta kontinuerligt genom exempelvis att loggar i ett it-system övervakas och avvikelser automatiskt rapporteras. Övervakning och mätning görs för att bedöma om implementerade säkerhetsåtgärder har avsedd verkan och fungerar tillfredsställande.

Uppföljning och förbättringsarbete

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i organisationen behöver det ske en övergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning.

Resultatet från ledningens genomgång ska dokumenteras och bevaras.

Interna styrdokument

Enligt MSB bör ledningen se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan ledningen ge vägledning till chefer och övriga medarbetare över de krav och förhållningssätt som gäller i informationssäkerhetsarbetet.

I riktlinjer är det vanligt att det förs in bestämmelser om till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet
- incidenthantering
- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning

Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.