Granskning av arbetet med informationssäkerhet

Rapport

Håbo kommun

KPMG AB

2024-01-22

Antal sidor 14

Håbo kommun
Granskning av arbetet med informationssäkerhet

2024-01-22

Innehållsförteckning

1 Sammanfattning

KPMG har av Håbo kommuns förtroendevalda revisorer fått i uppdrag att genomföra en översiktlig granskning av kommunens informationssäkerhetsarbete.

Syftet med granskningen har varit att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsens och nämndernas informationssäkerhetsarbete inte är systematiskt eller ändamålsenligt.

Då granskningen genomfördes pågick ett omfattande utvecklingsarbete inom hela kommunen, vilket också inriktas mot arbetet med informationssäkerhet. Vi konstaterar att en organisatorisk grund för arbetet lagts, och att det pågår ett arbete för att upprätta och etablera väsentliga styrdokument inom området. Däremot saknas flera operativa processer och systematik i både det operativa och långsiktiga arbetet.

Kommunledningen uttrycker en medvetenhet om betydelsen av ett ändamålsenligt informationssäkerhetsarbete där strategisk utveckling och samordning sker centralt och där nämnderna är drivande i det operativa arbetet. Vår uppfattning är att nämnderna behöver stöd för att etablera former för informationssäkerhetsarbetet, varför vi anser att kommunstyrelsen behöver prioritera det initialt. Med ett systematiskt informationssäkerhetsarbete ges möjlighet att identifiera ändamålsenliga it-säkerhetsåtgärder som skyddar kommunens informationstillgångar. I nuläget baseras implementerade it-säkerhetsåtgärder inte på säkerhetsbehov som identifierats genom riskanalyser och informationsklassningar, vilket enligt vår bedömning riskerar att exponera kommunen för cyberhot och intrång.

I det följande redovisas våra bedömningar och rekommendationer kopplat till revisionsfrågorna.

Revisionsfråga	Bedömning: Delvis	Rekommendationer
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas	I nuläget finns en informationssäkerhetspolicy som ger principiell grund för styrningen. Vi ser dock behov av att denna kompletteras med riktlinjer och rutiner som kan konkretisera hur arbetet ska bedrivas. Kommunstyrelsen behöver därtill säkerställa att det finns tillräckliga personella resurser som är anpassade efter det arbete som ska genomföras.	- Prioritera framtagandet av styrande dokument - I styrande dokument tydliggöra ansvar och roller för nyckelfunktioner inom informationssäkerhetsarbetet - Utvärdera nuvarande personella resurser är tillräckliga för att genomföra ett systematiskt informationssäkerhetsarbete.

Revisionsfråga	Bedömning: Nej	Rekommendationer
Finns ett systematiskt arbete med riskanalyser och informationsklassning och vidtas säkerhetsåtgärder som ett resultat av dessa underlag?	Momenten är väsentliga för att kunna vidta ändamålsenliga it-säkerhetsåtgärder. Kommunstyrelsen behöver tillse att stöd för informationsklassning och riskbedömning ges till berörda funktioner.	- Säkerställa att en kommunövergripande riskanalys genomförs - Etablera en modell för informationsklassning - Tillse stöd och utbildning i informationsklassning och riskbedömning
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?	Det finns behov av utbildningsinsatser som innefattar informationssäkerhet samt cybersäkerhet, och att dessa ges till både anställda och förtroendevalda.	- Säkerställa att utbildning inom informationssäkerhet ges till anställda och förtroendevalda
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i IT-miljön?	Övervakningen ger möjlighet att upptäcka hot om intrång och andra säkerhetsincidenter. Nuvarande funktioner och bemanning bör dock utvärderas i förhållande till risker samt de behov av tillgänglighet som finns i verksamheterna.	- Säkerställa att nuvarande övervakning, både personellt och tekniskt är tillräckligt mot bakgrund av behov samt nuvarande risker
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Finns etablerade incidenthanteringsrutiner och inkluderar dessa uppföljning av inträffade incidenter?	Incidenter hanteras enligt viss struktur. Den behöver formaliseras i en incidenthanteringsrutin med tydliga eskaleringsvägar för incidenter. Innebörden av och anmälningsförfarande för informationssäkerhetsincidenter behöver förtydligas.	- Upprätta en incidenthanteringsrutin med tydliga eskaleringsvägar - Tillse att utbildning inom informationssäkerhet omfattar informationssäkerhetsincidenter
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Finns en etablerad uppföljning av informationssäkerhetsarbetet och rapporteras denna till styrelsen med regelbundenhet?	Uppföljning kravställs i styrande dokument men har endast i begränsad omfattning genomförts. Bristande uppföljning begränsar kommunstyrelsens förmåga att fatta välavvägda beslut.	- Säkerställa att uppföljning genomförs i enlighet med informationssäkerhetspolicyn - Säkerställa att beslutade mål följs upp regelbundet för att säkerställa att arbetet genomförs så att målen kan nås

2 Bakgrund

KPMG har av Håbo kommuns förtroendevalda revisorer fått i uppdrag att genomföra en översiktlig granskning av kommunens informationssäkerhetsarbete. Uppdraget ingår 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 anpassat och balanserat säkerhetsarbete för att säkerställa att de system och digitala tjänster som nyttjas för informationshantering och lagring inte är exponerade och tillgängliga för cyberhot och angrepp. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer.

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 har en tillräcklig intern styrning och kontroll av sitt IT-säkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

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

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt och ändamålsenligt informationssäkerhetsarbete

Granskningen har omfattat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning och vidtas säkerhetsåtgärder som ett resultat av dessa underlag?
- Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?
- Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i IT-miljön?
- Finns etablerade incidenthanteringsrutiner och inkluderar dessa uppföljning av inträffade incidenter?

— Finns en etablerad uppföljning av informationssäkerhetsarbetet och rapporteras denna till styrelsen med regelbundenhet?

Granskningen har omfattat kommunstyrelsens övergripande ansvar för informationssäkerhet samt uppsikt över nämndernas arbete.

Granskningen har omfattat både administrativ säkerhet och tekniska säkerhetsåtgärder.

Granskningen har avgränsats till revisionsfrågorna.

2.2 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen 6 kap § 6
- Tillämpbara interna regelverk och policyer.

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier omfattandes informationssäkerhetspolicy samt riktlinje för informationssäkerhet, reglementen och rutin för informationsklassificering.
- Intervjuer har genomförts med:

  Kommunstyrelsens presidium

  Kommundirektör

  Säkerhetschef

  It-chef

  Informationssäkerhetssamordnare inom kommunstyrelsen

Samtliga intervjuade har faktakontrollerat rapporten.

3 Resultat av granskningen

3.1 Styrning och organisation av informationssäkerhetsarbetet

3.1.1 Styrande dokument

Kommunfullmäktige har antagit en informationssäkerhetspolicy[1] som gäller för hela kommunen. Policyn utgör principiellt ramverk för Håbo kommuns informationssäkerhetsarbete och redovisar roller, ansvar och mål ur ett övergripande perspektiv. Bland annat framgår att informationssäkerhetsarbetet ska följa ISO-standardserien SS ISO/IEC 27000, och att ett ledningssystem ska implementeras som grund för ett systematiskt informationssäkerhetsarbete.

För att konkretisera arbetet finns en riktlinje för informationssäkerhet[2] från 2014. I intervju konstateras att riktlinjen är daterad och inte ligger i linje med aktuella arbetssätt. Då granskningen genomfördes pågick arbete med att ta fram en ny riktlinje vars innehåll ska överensstämma med kommunens mål och organisatoriska former för informationssäkerhetsarbetet. Ytterligare rutiner uppges därtill vara under framtagande.

3.1.2 Ansvar och roller

Av kommunstyrelsens reglemente[3] framgår att styrelsen ska bedriva, utveckla, samordna och följa upp frågor som rör riskhantering, säkerhet, sårbarhet och beredskap inom hela den kommunala verksamheten samt utvecklingen av informations- och it-system. I det sistnämnda ingår att samordna kommunens informationssäkerhetsarbete och tillse strategisk ledning och drift av it-verksamhet och it-system.

I informationssäkerhetspolicyn definieras att kommunstyrelsen har det yttersta ansvaret för informationssäkerhetsarbetet, och för att tillse att det bedrivs i enlighet med policyn. Det ankommer också på styrelsen att tillse resurser så att övriga verksamheter kan bedriva ett systematiskt och kontinuerligt informationssäkerhetsarbete. Nämnderna och bolagsstyrelser ska å sin sida vidta nödvändiga åtgärder för att upprätthålla en ändamålsenlig informationshantering och följsamhet till styrande dokument

Vidare anges att kommundirektör har det övergripande operativa ansvaret för informationssäkerhet, liksom att det delegerade verksamhetsansvaret tillika innebär ansvar för informationssäkerhet. Förvaltningschefer och verksamhetsansvariga har även att ombesörja former för respektive verksamhets arbete, samt att utse informationssägare inom respektive verksamhet.

Kommunen har en säkerhetschef som enligt intervjuer är ansvarig för informationssäkerhetsarbetet. Hösten 2023 anställdes en informationssäkerhetssamordnare som har till uppgift att samordna arbetet. Båda dessa tillhör kommunstyrelseförvaltningens kansli.

[1] Beslutad 2023-12-11
[2] Riktlinjer för informationssäkerhet i Håbo kommun, daterad 2014-04-30
[3] Daterad 2021-12-13

Inom kommunstyrelseförvaltningen finns också digitaliserings- och it-enheten, som leds av en it-chef. Enheten består av en driftenhet och en supportenhet, men saknar utpekade funktioner för it-säkerhetsarbetet, vilket utförs av medarbetare inom driftsorganisationen.

Utöver det linjebaserade ansvaret för informationssäkerhet som åligger förvaltningschefer har varje förvaltning utsett en samordnande funktion för informationssäkerhetsarbetet. Vi har i granskningen tagit del av ett kommuninternt underlag från hösten 2023 där förvaltningarna beskriver aktuell status för informationssäkerhetsarbetet. Utifrån detta kan vi konstatera att förvaltningarna inte bedriver ett systematiskt informationssäkerhetsarbete, och att det finns behov av stöd för att etablerat ett sådant.

Vår bild är att kommunens informationssäkerhetsarbete är i en initial utvecklingsfas. Vid tid för granskningen hade kommundirektör tillträtt relativt nyligen och initierat ett antal processer i syfte att utveckla strukturer för styrning och ledning samt organisering. Detta har enligt uppgift även inkluderat organisering och styrning av informationssäkerhetsarbetet. Bland annat genom att etablera en organisationsstruktur samt upprättande och beslut informationssäkerhetspolicyn. Arbetets fortsatta inriktning beskrivs vara att ta fram ytterligare styrande dokument samt att stötta förvaltningarna i deras arbete med att etablera ett mer systematiskt informationssäkerhetsarbete inom respektive verksamhet.

3.1.3 Bedömning

Vår bedömning är att det delvis finns styrande dokument som tydliggör ansvar, krav och former för informationssäkerhetsarbetet.

Vi bedömer att informationssäkerhetspolicyn ger en principiell grund för styrningen av informationssäkerhetsarbetet. Samt att de mål som kommunen antagit genom policyn ger uttryck för en viljeinriktning mot att systematisera informationssäkerhetsarbetet, vilket också bekräftas i de intervjuer vi genomfört. Vi anser att kommunstyrelsen behöver prioritera framtagandet av riktlinjer då policyn inte är tillräcklig för att konkretisera det arbete som behöver genomföras utifrån policyns ambitioner och krav. I riktlinjerna ser vi behov av att rollen informationssäkerhetssamordnare ytterligare beskrivs så att uppdrag och uppgifter tydliggörs då detta är en nyckelroll i informationssäkerhetsarbetet.

För att arbetet ska nå upp till den systematik som beslutats för kommunens informationssäkerhet är det därtill väsentligt att kommunstyrelsen säkerställer att det finns personella resurser för att genomföra de aktiviteter som krävs för att arbetet ska vara systematiskt och riskbaserat. Vi konstaterar dels att nämnderna har behov av stöd för att arbetet ska vara systematiskt och vi konstaterar även att nuvarande organisation för it-säkerhetsarbetet kan behöva utvärderas i förhållande till de säkerhetsnivåer som kommunen fastställt för sitt arbete samt i förhållande till aktuella hot och risker.

3.2 Informationssäkerhetsarbetet i praktiken

3.2.1 Riskbedömning och informationsklassning

Ett mål för informationssäkerhetsarbetet är att det som minst ska omfatta risk- och sårbarhetsanalys och informationsklassningar, enligt vad som anges av informationssäkerhetspolicyn.

Muntliga uppgifter gör gällande att den riktlinje för informationssäkerhet som kommunen avser upprätta ska innehålla anvisningar för riskbedömning och informationsklassning. I nuläget saknas en etablerad modell för dessa aktiviteter. Som stöd innan riktlinjen tas fram har en provisorisk rutin för informationsklassificering[4] tillskapats. I rutinen redovisas en klassningsmodell som baseras på omfattningen av de konsekvenser som kan uppstå om inte informationssäkerheten upprätthålls.

Rutinen anger även att informationsklassning ska genomföras inför upphandling av ett system. För att betona vikten av att så sker avser kommunen ta fram en särskild rutin som tydliggör detta.

Vi har genom intervjuer och de nulägesbeskrivning av informationssäkerhetsarbetet vi tagit del av gjort iakttagelsen att riskbedömningar och informationsklassningar genomförts sporadiskt. Enligt uppgifter från kommunen har endast en mindre del av kommunens informationstillgångar inventerats under de två senaste åren. Det har inte heller genomförts någon riskanalys för den kommungemensamma it-miljön. Bland förvaltningarna uppges detta i stor utsträckning bero på avsaknad av kunskap och stöd för att genomföra momenten.

3.2.2 Etablerade it-säkerhetsåtgärder

Av informationssäkerhetspolicyn framgår att insikter från risk- och sårbarhetsanalyser ska generera ändamålsenliga säkerhetsåtgärder i syfte att skydda informationstillgångar. Vidare ska it-säkerhetsarbetet uppfylla legala och regulatoriska krav, och efterlevnaden ska säkerställas via omvärldsbevakning. Ett mål för arbetet är att oväntade händelser i it-systemen ska minimeras och förebyggas.

De intervjuade framför att det inom kommunen finns samhällsviktig verksamhet varför implementerade it-säkerhetsåtgärder har utvärderats i förhållande till krav som ställs i NIS-direktivet[5]. It-enheten har även genomfört ett penetrationstest av del av it-miljön och vidtagit ett antal säkerhetsåtgärder för att möta sårbarheter.

Likaledes konstaterar de intervjuade att it-säkerhetsskyddet skulle behöva utvärderas mer regelbundet, både för att tillse att implementerade säkerhetsåtgärder är aktuella och för att få en kontinuerlig uppfattning om aktuell hotbild. Att så inte sker i nuläget uppges bero på att it-enheten saknar dedikerade funktioner för it-säkerhetsarbetet, vilket fått till följd att säkerhetsarbetet utgår från omvärldsspaningar och för området gällande rekommendationer.

[4] 2023-10-26
[5] Ramverk för krav på säkerhet i nätverk och informationssystem som avser utförare av samhällsviktiga tjänster. Källa: msb.se.

3.2.3 Bedömning

Vår bedömning är att kommunen saknar ett systematiskt arbete med riskanalyser och informationsklassning.

Momenten kravställs i informationssäkerhetspolicyn, och är, enligt vår mening, väsentliga för att it-enheten ska kunna identifiera och vidta ändamålsenliga säkerhetsåtgärder i syfte att skydda både enskilda system och it-infrastrukturen. I nuläget utgår etablerade it-säkerhetsåtgärder inte från skyddsvärdet på befintliga informationstillgångar, vilket riskerar att exponera kommunen för cybersäkerhetsrisker.

Vi bedömer därigenom att kommunstyrelsen behöver säkerställa att den kommande riktlinjen för informationssäkerhet innehåller anvisningar om riskbedömning och informationsklassning samt att momenten genomförs både för den gemensamma it-miljön och för de system som respektive verksamhet ansvarar för.

Utifrån det stödbehov som förvaltningarna uttryckt anser vi att kommunstyrelsen behöver tillse att stöd för informationsklassning och riskbedömning ges, samt att det innefattar utbildning för berörda funktioner.

3.3 Säkerhetskultur

Informationssäkerhetspolicyn innehåller två mål med bäring på en god säkerhetskultur:

- att samtliga anställda ska ges möjlighet till grundläggande utbildning inom informationssäkerhet
- att ett systematiskt informationssäkerhetsarbete ska generera en god säkerhetskultur som är anpassad till varje verksamhets förutsättningar och behov

Enligt policyn är det upp till förvaltningschef och verksamhetsansvariga att tillse att anställda har tillräcklig kunskap för det specifika verksamhetsområdet.

Enligt uppgift från intervjuade har ingen utbildning inom informationssäkerhet genomförts. Vi uppfattar att det finns en medvetenhet om att kommunen behöver etablera en säkerhetskultur, och att meningen är att förvaltningarnas interna informationssäkerhetssamordnare ska samordna information och utbildning inom respektive förvaltning på sikt. Utbildning påtalas vara angeläget inte minst till förtroendevalda där det bland vissa intervjuade finns en uppfattning att kunskapsbristen är extra tydlig.

3.3.1 Bedömning

Vi bedömer att styrelse och nämnder inte tillsett en tillräcklig säkerhetskultur.

Vi anser att det finns behov av utbildningsinsatser som innefattar informationssäkerhet samt cybersäkerhet, och att dessa ges till både anställda och förtroendevalda. Utbildning kan bidra till att höja kunskapsnivån samt medvetenheten avseende hot och risker som kan påverka kommunens verksamheter, vilket i sin tur kan minska risken för att incidenter inträffar.

3.4 Incident- och krishantering

3.4.1 Övervakning och loggning

Kommunen har avtal med extern part avseende tjänst för övervakning av nätverk och de klienter och brandväggar som är anslutna till nätverken. Vid försök till intrång eller andra angrepp går larm till it-enheten.

Vid tid för granskning var övervakningen på väg att utökas från att ske under kontorstid till dygnet runt. Utöver det uttrycks behov av en integrerad övervakning där komponenter som ligger inom segmenterade nätverk ingår i den totala övervakningen, vilket konstateras ge en bättre helhetsbild över avvikande mönster och händelser.

3.4.2 Incidenthantering

Ett mål, enligt informationssäkerhetspolicyn, är att kommunen ska ha en incidenthanteringsrutin.

Rutinen fanns inte upprättad då granskningen genomfördes. Kommunen har däremot en e-tjänst via intranätet för anmälan av olika typer av säkerhetsincidenter. De anmälningar som görs tas emot av säkerhets- och beredskapsenheten och hanteras sedan av säkerhetschef.

Anmälningarna redovisas sedan i kommunens säkerhetsforum där representanter för olika delar av säkerhetsarbetet ingår, exempelvis it-säkerhet och fysisk säkerhet i fastigheter ingår. Antalet anmälda informationssäkerhetsincidenter konstateras vara lågt, delvis till följd av att kommunens till del har en kultur att inte anmäla händelser.

3.4.3 Bedömning

Vår bedömning är att kommunen delvis har etablerat en ändamålsenlig övervakning av it-miljön men att det för närvarande saknas incidenthanteringsrutiner.

Övervakningen ger möjlighet att upptäcka hot om intrång och andra säkerhetsincidenter. Vi konstaterar att det för närvarande finns en e-tjänst för att anmäla incidenter men saknas en dokumenterad rutin för hur incidenter ska hanteras i kommunen. Vår bedömning är att rutinen bör inkludera eskaleringsvägar i händelse av allvarliga incidenter för att säkerställa att relevanta funktioner involveras och informeras.

De incidenter som anmäls inkluderas i en strukturerad uppföljning. Att antalet anmälda incidenter är lågt kan, enligt vår mening, tyda på att kunskapen om informationssäkerhet och dylika incidenter är begränsad. Vår bedömning är därför att kommunstyrelsen behöver säkerställa att utbildning inom informationssäkerhet även innehåller information om vad som är incidenter och hur dessa behöver hanteras.

3.5 Uppföljning

3.5.1 Rutiner för uppföljning

I informationssäkerhetspolicyn redovisas de tolv mål som kommunen antagit för arbetet. Två av målen avser uppföljning, där uppföljning mot kommunstyrelse och kommunledning ska genomföras minst en gång per år. Därtill ska kommunens verksamheter upprätta en årlig verksamhetsplan där informationssäkerhetsarbetet ska vara mätbart och följas upp.

Då granskningen genomfördes följdes informations- och it-säkerhetsarbetet upp inom kommunledningen, men inte mot kommunstyrelsen. Ambitionen på sikt uppges vara att uppföljning mot kommunstyrelsen ska ske i enlighet med informationssäkerhetspolicyn, och i form av en samlad redogörelse för arbetet.

För den uppföljning som kravställts på verksamhetsnivå framförs att det vid tid för granskning pågick arbete med att ta fram kontrollpunkter och ett årshjul för informationssäkerhetsarbetet. Uppföljning av informationssäkerhetsarbetet är tänkt att vara en integrerad del i ordinarie verksamhetsuppföljning, vilket avser uppföljning i bland annat delårsrapport och årsredovisning.

3.5.2 Bedömning

Vår bedömning är att kommunen saknar en etablerad uppföljning av informationssäkerhetsarbetet.

I informationssäkerhetspolicyn har uppföljning kravställts men detta har endast delvis gjorts i enlighet med denna. Vi anser att de mål som kommunen antagit genom informationssäkerhetspolicyn ger tydliga förutsättningar att följa upp arbetet.

Det är, enligt vår bedömning, angeläget inte minst utifrån att det systematiska informationssäkerhetsarbetet är i en etableringsfas, att kommunstyrelsen, tillser en kontroll över utvecklingen för att säkerställa att arbetet etableras så att det finns förutsättningar att nå de beslutade målen.

Mot bakgrund av det förhöjda säkerhetsläget med ökad risk för cyberhot och intrång är det viktigt att kommunstyrelsen och nämnderna är informerade om aktuella hot och risker samt kommunens nuvarande förmåga att skydda sig mot dessa. Detta så att sårbarheter kan identifieras och åtgärder för att stärka informations- och it-säkerheten beslutas.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsens och nämndernas informationssäkerhetsarbete inte är systematiskt eller ändamålsenligt.

Då granskningen genomfördes pågick ett omfattande utvecklingsarbete inom hela kommunen, vilket också inriktas mot arbetet med informationssäkerhet. Vi konstaterar att en organisatorisk grund för arbetet lagts, och att det pågår ett arbete för att upprätta och etablera väsentliga styrdokument inom området. Däremot saknas flera operativa processer och systematik i både det operativa och långsiktiga arbetet.

Kommunledningen uttrycker en medvetenhet om betydelsen av ett ändamålsenligt informationssäkerhetsarbete där strategisk utveckling och samordning sker centralt och där nämnderna är drivande i det operativa arbetet. Vår uppfattning är att nämnderna behöver stöd för att etablera former för informationssäkerhetsarbetet, varför vi anser att kommunstyrelsen behöver prioritera det initialt. Med ett systematiskt informationssäkerhetsarbete ges möjlighet att identifiera ändamålsenliga it-säkerhetsåtgärder som skyddar kommunens informationstillgångar. I nuläget baseras implementerade it-säkerhetsåtgärder inte på konstaterade säkerhetsbehov, vilket enligt vår bedömning riskerar att exponera kommunen för cyberhot och intrång.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Prioritera framtagandet av styrande dokument
- I styrande dokument tydliggöra ansvar och roller för nyckelfunktioner inom informationssäkerhetsarbetet
- Utvärdera nuvarande personella resurser är tillräckliga för att genomföra ett systematiskt informationssäkerhetsarbete
- Säkerställa att en kommunövergripande riskanalys genomförs
- Etablera en modell för informationsklassning
- Tillse stöd och utbildning i informationsklassning och riskbedömning
- Säkerställa att utbildning inom informationssäkerhet ges till anställda och förtroendevalda
- Säkerställa att nuvarande övervakning, både personellt och tekniskt är tillräckligt mot bakgrund av behov samt nuvarande risker
- Upprätta en incidenthanteringsrutin med tydliga eskaleringsvägar
- Tillse att utbildning inom informationssäkerhet omfattar informationssäkerhetsincidenter
- Säkerställa att uppföljning genomförs i enlighet med informationssäkerhetspolicyn

— Säkerställa att beslutade mål följs upp regelbundet för att säkerställa att arbetet genomförs så att målen kan nås

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Sofie Ernerudh
Verksamhetsrevisor

Micaela Hedin
Kundansvarig och certifierad revisor