Timrå kommun
Kommunstyrelsen
Barn- och utbildningsnämnden
Kultur- och tekniknämnden
Miljö- och byggnadsnämnden
Socialnämnden

För kännedom: Kommunfullmäktiges presidium

2023-06-13

Revisionsrapport ”Granskning av informations- och IT-säkerhet”

KPMG har på uppdrag av kommunens revisorer genomfört en granskning av kommunens arbete för att upprätthålla en god informations- och IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Revisionen önskar att kommunstyrelsen och berörda nämnder lämnar synpunkter på de slutsatser som finns redovisade i rapporten senast den 29 september 2023. Av svaret bör det framgå vilka eventuella åtgärder som ska vidtas och när de beräknas vara genomförda.

Svaret skickas till Lena Medin, KPMG (mailadress lena.medin@kpmg.se) för vidarebefordran till revisorerna.

För Timrå kommuns revisorer

Keijo Ojala
Ordförande

Inger Nyhman
Vice ordförande

Granskning av informations- och it-säkerhet

Rapport

Timrå kommun

KPMG AB

2023-06-13

Antal sidor: 21

Timrå kommun
Granskning av informations- och it-säkerhet

2023-06-13

Innehållsförteckning

Timrå kommun
Granskning av informations- och it-säkerhet

2023-06-13

1 Sammanfattning

KPMG har av Timrå kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunens arbete för att upprätthålla en god informations- och it-säkerhet.

Utifrån genomförd granskning bedömer vi att kommunstyrelsen, barn- och utbildningsnämnden, kultur- och tekniknämnden samt miljö- och byggnadsnämnden inte bedriver ett systematiskt informationssäkerhetsarbete i enlighet med Myndigheten för samhällsskydd och beredskaps (MSB:s) rekommendationer[1] och beslutade styrdokument. Vi bedömer att det inom socialnämndens verksamheter till viss del har genomförts aktiviteter inom informationssäkerhet men konstaterar dock att arbetet inte sker med en tillräcklig systematik i enlighet med MSB:s rekommendationer och beslutade styrdokument.

Det finns en etablerad organisation för arbetet med informationssäkerhet som utgår från linjeansvaret. Därtill finns i viss utsträckning utsedda funktioner, bland annat informationssäkerhetssamordnare, it-samordnare och systemförvaltare som stöd i arbetet. Flertalet intervjupersoner lyfter dock att resurserna för informationssäkerhetsarbetet upplevs otillräckliga och att det till viss del saknas kompetens inom förvaltningarna för att bedriva ett systematiskt informationssäkerhetsarbete. Vad gäller den tekniska säkerheten så har kommunen avtal med en extern driftsleverantör där även it-säkerhetsarbetet ingår.

De styrande dokument som beslutats tydliggör ansvar samt krav på aktiviteter för hur informationssäkerhetsarbetet ska bedrivas. Dock konstaterar vi att dokumenten inte i tillräcklig grad är förankrade i kommunens verksamheter. Det operativa informationssäkerhetsarbete som genomförs i kommunen är därigenom inte systematiskt och de krav på aktiviteter som ställs i styrande dokument genomförs endast till viss del. Vi konstaterar bland annat att informationsklassningar och riskanalyser vid tidpunkten för vår granskning endast genomförs i mindre utsträckning och att arbetet inte är systematiskt. De klassningar som gjorts har inkluderat färre aspekter i analysen än vedertagna metoder innehåller. Detta kan riskera att leda till att de skyddsbehov som behöver bedömas i klassningen inte beaktats tillräckligt så att åtgärder kan vidtas. Det är positivt att kommunen har gjort en prioritering av sina mest kritiska system. Emellertid ser vi att nämnderna brustit vid genomförande av informationsklassningar enligt de krav som anges i styrande dokument.

Genom det avtal som kommunen har med extern driftsleverantör kan vi konstatera att leverantören presenterat underlag som beskriver det säkerhetsarbete som de tillhandahåller till kommunen. Vi kan konstatera att organisation och säkerhetsarbetet är i enlighet med den standard som kommunen beslutat om som gällande. Löpande uppföljningar sker med leverantören där risker och behov diskuteras. Vi bedömer dock att dessa moment i högre grad kan formaliserar och dokumenteras så att det finns en spårbarhet över de säkerhetsåtgärder som leverantören och kommunen ser behov av att implementera. Vi ser därtill behov av att förvaltningarna efter genomförda informationsklassningar och riskanalyser bör omsätta resultatet av dessa till krav om

[1] Dessa redovisas i avsnitt 3.

tekniska säkerhetsåtgärder så att skyddsvärd information skyddas med relevanta åtgärder.

Kommunen har genomfört utbildningsinsatser för att etablera en säkerhetsmedvetenhet i organisationen, dock har deltagandet minskat på senare tid. Tester som genomförts över medvetenheten har inte varit tillfredsställande och påvisat brister som skulle kunna leda till att incidenter sker. Vi bedömer att det finns tydligt beskrivna incidenthanteringsrutiner i kommunens vägledningar, men noterar samtidigt att dessa inte tycks vara fullt ut förankrade i kommunens verksamheter.

Vi bedömer att kommunstyrelse och nämnder har en bristande uppföljning av informationssäkerhetsarbetet då uppföljning och rapportering i nuläget endast sker utifrån dataskyddsarbetet. Det är av vikt att kommunstyrelsen och nämnderna tillser en tillräcklig uppföljning och rapportering av informationssäkerhetsarbetet, för att få kännedom om hot och risker samt eventuella brister så att förutsättningar finns för att besluta om adekvata åtgärder.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi kommunstyrelsen, i deras övergripande ansvar för informationssäkerhet, att:

- Säkerställa att de beslutade styrdokumenten förankras i samtliga verksamheter, se avsnitt 4.1
- Tillse att resurserna för informations- och it-säkerhetsarbetet står i proportion till organisationens behov och samtida risker och hot.
- Beakta informationssäkerhetsrisker i risk- och väsentlighetsanalys.
- Tillse att den uppföljning som sker tillsammans med den externa leverantören för it-drift sker på ett strukturerat sätt och att väsentliga risker och behov av åtgärder dokumenteras.
- Tillse en tillräcklig uppföljning och regelbunden rapportering av informationssäkerhetsarbetet

Utifrån våra iakttagelser och vår bedömning rekommenderar vi kommunstyrelsen och de granskade nämnderna att:

- Etablera ett informationssäkerhetsarbete i enlighet med styrande dokument
- Tillse att obligatoriska utbildningar inom informationssäkerhet genomförs
- Tillse att riskanalys och informationsklassningar genomförs i de egna verksamheterna och att dessa prioriteras utifrån skyddsvärde för den information som hanteras i systemen.

2 Bakgrund

KPMG har av Timrå kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunens arbete för att upprätthålla en god informations- och it-säkerhet. 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 inte de system och digitala tjänster som nyttjas för informationshantering och lagring 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 informations- och it-säkerhet behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningen har syftat till att bedöma om kommunstyrelsen, barn och utbildningsnämnden, socialnämnden, kultur- och tekniknämnden samt miljö- och byggnadsnämnden bedriver ett systematiskt informationssäkerhetsarbete.

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?
- Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?
- Har kommunen etablerat tekniska skyddsåtgärder som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?
- Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön?
- Finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp tillsammans med tydliggjorda eskaleringsvägar?
- Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?
- Finns en etablerad uppföljning av informations- och it-säkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?

2.2 Revisionskriterier

Vi har i granskningen utgått från följande kriterier:

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

2.3 Ansvarig nämnd/styrelse

Granskningen har avsett kommunstyrelsen, barn- och utbildningsnämnden, socialnämnden, kultur- och tekniknämnden samt miljö- och byggnadsnämnden.

Granskningen har omfattat kommunstyrelsens övergripande ansvar för informationssäkerhet och it-säkerhet samt nämndernas verksamhetsansvar för de informationstillgångar som hanteras inom respektive nämnd.

2.4 Metod

Granskningen har genomförts genom dokumentstudier av följande dokument:

- Program för arbetet med Trygghet och säkerhet i Timrå kommun 2020–2023
- Informationssäkerhetspolicy
- It-strategi
- Vägledande råd och bestämmelser för användare av it-system (m.fl.)

Intervjuer har genomförts med följande funktioner:

- Tillförordnad kommundirektör
- Informationssäkerhetssamordnare
- Driftsansvarig it
- Förvaltningschef Barn- och utbildningsförvaltningen
- Förvaltningschef Socialförvaltningen
- Förvaltningschef Kultur och teknikförvaltningen
- Tillförordnad förvaltningschef Miljö- och byggnadsförvaltningen
- Systemförvaltare
- GDPR-samordnare
- Nämndssekreterare

3 Inledning

3.1 Metodstöd för systematiskt informationssäkerhetsarbete och säkerhetsåtgärder

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 ska kunna fatta beslut om förbättring inom informationssäkerhetsarbetet är det av vikt att denne hålls informerad. För att ledningen löpande ska hållas informerad rekommenderas åtminstone en årlig genomgång av informationssäkerhetssamordnaren. Under genomgången diskuteras det gångna årets informationssäkerhetsarbete och väsentliga iakttagelser avseende eventuella förbättringsområden lyfts.

Styrning av det interna arbetet

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.

4 Resultat av granskningen

4.1 Styrning och organisering av informationssäkerhetsarbetet

4.1.1 Program för arbetet med Trygghet och säkerhet i Timrå kommun 2020-2023

Vi har tagit del av Program för arbetet med Trygghet och säkerhet i Timrå kommun.[2] Av programmet framgår att informationssäkerhet ingår i kommunens övergripande arbete med trygghet och säkerhet. Programmet anger att informationssäkerhet ska genomsyra all den verksamhet som kommunen bedriver. Programmet beskriver att informationssäkerhetspolicy och It-strategi i kommunen (beskrivs i nedanstående avsnitt) är de huvudsakliga styrdokumenten för informationssäkerhetsarbetet.

4.1.2 Informationssäkerhetspolicy för Timrå kommun

Vi har tagit del av kommunens informationssäkerhetspolicy.[3] Informationssäkerhetspolicyn är det huvudsakliga styrdokumentet för kommunens informationssäkerhetsarbete och fastslår att standarden ISO/IEC 27002 är utgångspunkt för arbetet.

De mål som anges i informationssäkerhetspolicyn är följande:

- All personal har kunskap om gällande informationssäkerhetsregler
- Informationsförsörjningen är säker och effektiv samt bidrar till ökat skydd och stöd
- Krishanteringsförmågan upprätthålls
- Alla investeringar i form av information och teknisk utrustning har tillräckligt skydd
- Det finns tillgång till en säker infrastruktur för extern och intern kommunikation
- Hotbilden mot varje enskilt informationssystem av vikt för verksamheten analyseras fortlöpande; systemägare ansvarar för att analysera och arbeta förebyggande för att motverka

Informationssäkerhetspolicyn ställer ett antal generella krav på kommunens informationssäkerhetsarbete. Bland annat framgår att prioriteringar av åtgärder ska göras för de system som är kritiska för att verksamhet ska kunna bedrivas. Därtill ska system vara identifierade och förtecknade, där systemägar- och förvaltningsansvar framgår. Informationssäkerhetspolicyn anger att det finns en informationssäkerhetshandbok, vilken ska innehålla riktlinjer och anvisningar. En sådan informationssäkerhetshandbok har inte presenterats i granskningen.

[2] KF, 2019-11-25 § 192.
[3] KS 2017-05-02 § 135, senast rev. KS 2020-11-10 § 359.

4.1.3 IT-strategi för Timrå kommun

Vi har tagit del av kommunens IT-strategi. Strategin syftar till att åstadkomma en förflyttning av fokus från informationsteknologi till verksamheternas behov och visa på hur en ökad integration av elektroniska tjänster kan utveckla kommunal verksamhet.

IT-strategin utgör grunden för kommunens IT-arbete som helhet och ska tydliggöra kommunens förhållningssätt och ambitionsnivå. Frågor som bedöms vara inom IT-området i förvaltningarnas strategiska arbete ska behandlas i kommunens IT-råd (se avsnitt 4.1.5).

Av IT-strategin framgår ett antal mål. Målen avser bland annat medborgarservice, effektivisering samt säkerhet och kvalitet.

4.1.4 Vägledande råd och bestämmelser

Kommunens övergripande styrdokument för arbetet kompletteras med praktiska anvisningar kallade Vägledande råd och bestämmelser (VROB). I detta avsnitt presenteras dessa i korthet.

Vägledande råd och bestämmelser – Förvaltning & Drift av it inom Timrå kommun

Vägledningen[4] beskriver och systemförvaltningen i kommunen och definierar för arbetet centrala begrepp. Vägledningen beskriver även systemförvaltningsorganisationen, inklusive roll- och ansvarsfördelningen i detalj. Det framgår information kring säkerhet inom ramen för systemförvaltningen.

Vägledande råd och bestämmelser för användare av it-system i Timrå kommun

Vägledningen[5] beskriver bland annat vilka krav som ställs på medarbetare. Vägledningen anger även övergripande information om bland annat informationssäkerhet, kommunens informationssäkerhetsarbete och hur medarbetare ska agera vid misstanke om incident.

Vägledande råd och bestämmelser för distansarbete

Vägledningen[6] innehåller kort information kring distansarbete och tillhörande risker. Bilagt är ett avtal för distansarbete som ska skrivas under av berörd medarbetare.

Vägledande råd och bestämmelser – Dataskydd inom Timrå kommun

Vägledningen[7] beskriver kommunens dataskyddsarbete. Information om organisation och ansvar, personuppgiftshantering, incidenthantering, webbpublicering samt upphandling och installation av nya system framgår.

[4] KS, 2016-12-06 § 292. Senast rev. 2020-11-10 § 362.
[5] KS, 2016-12-06 § 291. Senast rev. KS 2020-11-10 § 360
[6] KS, 2018-12-04 § 352.
[7] KS, 2018-06-12 § 192

4.1.5 Organisation och ansvarsfördelning

Av kommunens informationssäkerhetspolicy framgår roll- och ansvarsfördelningen för informationssäkerhetsarbetet. Kommunstyrelsen är övergripande ansvarig för informationssäkerheten i kommunen. Kommunchefen är operativt ansvarig för informationssäkerhetsarbetet och dennes ledningsgrupp är gemensamt ansvariga för den övergripande planeringen och genomförandet av informationssäkerhetsarbetet. Enligt policyn är informationssäkerhetssamordnare direkt underställd kommunchef vilken även är den som utser funktionen. För närvarande är it-samordnare på it-enheten utsedd att ha funktionen informationssäkerhetssamordnare. Uppdraget utgör 10% av dennes tjänst. Samordnaren ansvarar operativt för den kommunövergripande samordningen av arbetet. I intervjuer beskrivs att den arbetstid som funktionen har att tillgå främst har funnits förutsättningar att se över styrande dokument samt till viss del informationsklassningsarbetet i förvaltningarna.

Kommunens it-strategi anger att förvaltningschefer har rollen som systemägare och informationsägare. En detaljerad roll- och ansvarsfördelning för kommunens systemförvaltning framgår av *Vägledande råd och bestämmelser för förvaltning och drift*. Ansvaret för kommunens system fördelas mellan systemägare och systemförvaltare. Systemförvaltarna utses av respektive systemägare och ansvarar för användningen av systemet, inklusive informationssäkerhet. Förvaltningarna har olika bemanning av systemförvaltarrollen, där socialförvaltningen har två heltidstjänster för systemförvaltare och de andra förvaltningarna endast har systemförvaltare på delad tjänst.

Kommunens it-enhet som leds av chefen för verksamhetsstöd, enheten består av it-driftansvarig, it-samordnare (tillika informationssäkerhetssamordnare) samt två tekniker Det finns även två medarbetare som arbetar mer dedikerat med verksamhetsutveckling med hjälp av digitalisering. Kommunens it-drift ligger på extern leverantör, vilken också tillhandahåller den it-tekniska säkerheten. It-driftsansvarig och it-samordnare deltar främst i den uppföljning och dialog som sker med den externa leverantören.

4.1.6 Bedömning

Vi bedömer att kommunstyrelsen tillsett att det finns styrande dokument och att dessa tydliggör ansvar samt krav på aktiviteter för hur informationssäkerhetsarbetet ska bedrivas. Vi bedömer att kommunstyrelsen etablerat en organisation som utgår från linjeansvaret samt därtill kompletterande funktioner som ska bidra i arbetet med informationssäkerhet, bland annat systemförvaltare och it-samordnare.

Kommunen har i enlighet med MSB utsett en samordningsfunktion. Vi bedömer att det finns risk med nuvarande tjänstgöringsgrad för funktionen att förutsättningarna inte är tillräckliga för samordnaren att klara sina uppgifter i enlighet med beskrivning av funktionen. Bland annat finns risk att förvaltningarna har större behov av stöd i sina processer än vad som kan levereras som kan få följder att väsentliga aktiviteter inte genomförs fullt ut i förhållande till krav och behov. Vi ser även att det finns risk för bristande förutsättningar i uppföljningsarbetet där kommunen kan missa att fånga viktiga förbättringsåtgärder för sitt informationssäkerhetsarbete.

4.2 Informationssäkerhetsarbetet

4.2.1 Informationsklassning och riskanalyser

Informationssäkerhetspolicyn anger att information ska klassas utifrån den funktion och betydelse för verksamheten som den har och de konsekvenser som skulle medföras om informationen skulle bli otillgänglig eller hanteras felaktigt. Kommunen ska enligt underlagen klassa information utifrån principerna om sekretess, riktighet och tillgänglighet. Informationssäkerhetspolicyn ställer krav på att en verksamhets- samt riskanalys ska genomföras för samtliga prioriterade system.

Av intervjuer framgår att riskanalyser genomförs i viss utsträckning inom kommunens verksamheter. It-enheten genomför riskanalyser för den egna verksamheten men även tillsammans med extern leverantör av it-drift.

Intervjupersoner uppger att kommunens informationssäkerhetssamordnare utgör det huvudsakliga stödet vid informationsklassningar tillsammans med vissa systemförvaltare. Kommunen har haft som ambition att implementera KLASSA[8] i sitt arbete med informationsklassning och riskanalys. Emellertid uppger intervjupersoner att kommunen valt att arbeta efter en förenklad version av KLASSA, då verktyget som helhet har bedömts vara för omfattande och tidskrävande för att användas i kommunens verksamheter.

Av intervjuer och underlag vi tagit del av i form av genomförda klassningar framgår att klassningar genomförs i viss utsträckning. Vi har tagit del av informationsklassning för de tio prioriterade systemen som kommunen identifierat. Vad gäller resterande system har klassningar i huvudsak inte genomförts.

Om ett tröskelvärde överstigs vid informationsklassning, det vill säga att informationen har ett förhöjt skyddsvärde, ska riskanalys och konsekvensbedömning genomföras. It-enheten bistår förvaltningarna med stöd i riskanalysarbetet vid behov. Intervjupersoner uppger exempelvis att it-enheten har samarbetat med socialförvaltningen vid införande av ett nytt verksamhetssystem.

Det framgår av intervjuer att kompetens för att genomföra klassningar enligt KLASSA behöver utvecklas inom kommunens verksamheter så att dessa kan ske mer självständigt inom respektive verksamhet.

Utöver detta kan vi se att informations- och it-säkerhet ingår som noterade risker i internkontrollplan 2023 för kultur- och tekniknämnden. Därutöver har vi noterat att informations- och/eller it-säkerhet saknas i övriga nämnders riskanalyser och därmed även i internkontrollplaner.

[8] KLASSA är ett verktyg för informationsklassificering och riskanalys som tillhandahålls av Sveriges kommuner och regioner (SKR).

Som en del av kommunens informationsklassningsprocess ingår handlingsplaner där åtgärder utifrån identifierade risker/fastställt skyddsvärde på information ska dokumenteras och vidtas. Mot bakgrund av att processen för informationsklassning och riskanalys i nuläget endast genomförs i viss utsträckning så innebär det att åtgärdsplaner endast upprättas mot den mer begränsade analysen och klassningen av skyddsvärde.

4.2.2 Säkerhethetskultur

Av kommunens vägledande råd och bestämmelser avseende förvaltning och it-drift framgår att systemägare ansvarar för medarbetarnas säkerhetsmedvetenhet. Systemägare ska exempelvis tillse att de egna medarbetarna erhåller information och utbildning om de bestämmelser (VROB) de omfattas av. Systemägare ska också säkerställa att medarbetare har tillräckliga kunskaper om säkerhetsregler innan de beviljas åtkomst till it-system. Ansvar för att påtala behov av utbildning åligger emellertid medarbetare.

Kommunens vägledande råd och bestämmelser för användare av it-system beskriver aktuellt ansvar för systemanvändare. Av vägledningen framgår att användare måste känna till det egna ansvaret och de allmänna säkerhetsbestämmelserna avseende informationssäkerhetsarbetet; hur medarbetare ska agera vid olika typer av it-incidenter samt hur medarbetare får använda kommunens e-post och internet.

Vägledningen beskriver även behörighet, lösenordshantering samt övergripande information kring exempelvis informationsklassning, offentlighet och sekretess samt dataskyddsförordningen. Därtill framgår information kring distansarbete.

Kommunen har genom it-enheten, genomfört obligatoriska övergripande utbildningar. Utbildningarna har i huvudsak berört grundläggande informations- och it-säkerhet, där information om till exempel nätfiske, lösenordshantering och användning av webben framgått. Utbildningarna har följts upp, deltagande har undersökts och tester i form av ”nätfiskemejl” som skickats ut av it-enheten har genomförts.

Intervjupersoner uppger att deltagandenivån successivt försämrats över tid, från en initial deltagarfrekvens om ca. 90% till ca. 30% och att resultaten av nätfisketester inte varit tillfredsställande. Dessa resultat har återkopplats till respektive förvaltningschef. I nuläget samverkar kommunens it-enhet med extern driftsleverantör avseende utbildning till kommunens anställda för att utveckla utbildningsinsatserna.

4.2.3 Bedömning

Vi bedömer att det i styrande dokument är tydliggjort krav på riskanalyser och informationsklassning. Vi konstaterar dock att informationsklassningar och riskanalyser vid tid för granskningen endast genomförs i mindre utsträckning och att arbetet inte är systematiskt. De klassningar som gjorts har inkluderat färre aspekter i analysen än vedertagna metoder innehåller. Detta kan riskera att leda till att de skyddsbehov som behöver bedömas i klassningen inte beaktats tillräckligt så att åtgärder kan vidtas.

Vi ser det som positivt att en prioritering har gjorts för kommunens viktigaste system. Vi bedömer dock samtliga nämnder brustit i att göra informationsklassning och riskanalyser i enlighet med krav i styrande dokument då endast den mindre omfattande

klassningen gjorts. Det är därtill av betydelse att även övriga system inom respektive nämnd klassas då sårbarheter i enskilda system kan riskera att påverka den totala säkerheten i kommunens it-miljö.

För att frigöra tid för informationssäkerhetssamordnaren ser vi att det är av vikt att utbildningar i informationsklassning genomförs så att förvaltningarna i högre grad självständigt kan genomföra arbetet med klassningar och riskanalyser. Detta kan bidra till att samordnarens tid kan nyttjas mer effektivt för råd och stöd vid mer komplexa frågeställningar och inte i själva genomförandet.

Vi bedömer att styrelse och nämnder inte fullt ut har tillsett att det finns en tillräcklig säkerhetskultur. Det är positivt att utbildning har erbjudits men det behöver säkerställas genom uppföljning att dessa genomförs i högre grad över tid för att nå den effekt som förväntas. Då den mänskliga faktorn ofta är orsak till informationssäkerhetsincidenter är det väsentligt att medarbetare är medvetna om risker och kan agera på ett säkert sätt för att minimera risken att dessa sker.

4.3 IT-säkerhet

Som vi har beskrivit i avsnittet om organisation så har kommunen sin it-drift hos en extern leverantör. Internt i kommunen finns funktioner i form av en it-samordnare samt en it-driftsansvarig som har regelbunden dialog med leverantören. I dialogen berörs enligt intervjuade informations- och it-säkerhetsfrågor.

Av underlag som vi tagit del av gällande den externa leverantören finns beskrivningar av dennes informationssäkerhetsarbete. Underlagen styrker att leverantörens arbete sker i enlighet med den etablerade standarden för informationssäkerhet, ISO/IEC 27000.

4.3.1 Riskanalys och omvärldsbevakning

Vi har tagit del av underlag som kommunen erhållit från leverantören som styrker att riskanalys och omvärldsbevakning genomförs på regelbunden basis som en del i det avtal och uppdrag som kommunen gett till leverantören. Leverantören genomför även riskanalys tillsammans med företrädare för kommunen från it-enheten vid gemensamma möten.

Riskanalysen utgår från hot-och sårbarhetsanalys, inträffade incidenter och avgränsas till de informationstillgångar som berörs av analysen.

4.3.2 Implementerade skyddsåtgärder

Befintliga skyddsåtgärder tillhandahålls av leverantören i form av bland annat antivirus, brandväggar och lösenordssystem. Rutiner finns för automatiserade säkerhetsuppdateringar av it-komponenter. Leverantören informerar löpande kommunen i de fall de identifierar sårbarheter och får därefter godkännande om relevanta åtgärder. Intervjupersoner uppger att befintlig hantering upplevs som välfungerande.

Av intervjuer framgår att specifika krav om säkerhetsåtgärder utöver det som avtalats inte ställs till leverantören. Det saknas enligt uppgift rutiner för att omsätta resultat från

informationsklassning och riskanalyser till krav om tekniska skyddsåtgärder hos den externa driftsleverantören eller andra systemleverantörer förutom vid införande av nya system där detta är en del i upphandlingsprocessen.

Av kommunens vägledningar och bestämmelser för förvaltning och drift av it framgår information kring loggning och spårbarhet. Det anges att målet är att det i samtliga it-system ska finnas en säkerhetslogg som registrerar användaridentitet, uppgift om inloggning och utloggning samt datum och klockslag för aktiviteter. Det underlag från leverantören vi tagit del av tyder på att säkerhetshändelser samlas i logg för analys och att övervakning av miljön sker löpande.

Enligt ovan nämnda VROB ska systemägares övriga säkerhetskrav på säkerhets- och transaktionsloggar framgå av de säkerhetsplaner som ska finnas upprättade av respektive systemägare. Vid tidpunkten för granskningen har vi inte erhållit underlag eller uppgifter som tyder på att sådana krav har kommunicerats mellan systemägare och leverantör.

Sårbarhetsskanning eller penetrationstest för att utvärdera implementerade skyddsåtgärder ingår inte i det avtal kommunen har med leverantören. Intervjupersoner uppger att kommunen har ett annat ramavtal på området, men inte sett behov av att avropa sådana tjänster de senaste åren. Intervjupersoner påtalar att kommunen genomfört tester motsvarande sårbarhetsskanning eller penetrationstest senast under 2020. Utifrån resultatet har åtgärder enligt uppgift vidtagits.

4.3.3 Reserv- och återgångsrutiner

Kommunens vägledningar och bestämmelser för förvaltning och drift av it beskriver krav på säkerhetskopiering och lagring. Det framgår att systemägarnas krav på säkerhetskopiering och lagring för de egna systemen ska framgå av riskanalyser upprättade av respektive systemägare. Av vägledningarna framgår vidare att backup ska tas regelbundet och att redundans ska vara etablerat genom servrar som åtskilts geografiskt.

Av den information vi fått i granskningen saknas dokumenterade riskanalyser som påvisar behov av säkerhetskopiering. Både backup- och återläsning hanteras av extern leverantör och av det underlag vi tagit del av som beskriver leverantörens leverans framgår att backup- och återläsning genomförs regelbundet.

4.3.4 Bedömning

Vår bedömning är att kommunstyrelsen i huvudsak har säkerställt att det finns en tillräcklig it-säkerhet i kommunen, främst genom tidigare beslut att lägga ut kommunens it-drift hos extern leverantör. Genom det avtal som kommunen har med extern driftsleverantör kan vi konstatera att leverantören presenterat underlag som beskriver det säkerhetsarbete som de tillhandahåller till kommunen, vilka är i enlighet med den standard som kommunen beslutat om som gällande. Genom det avtal som kommunen har med leverantören noterar vi bland annat att:

- Det finns krav om ett antal it-säkerhetsåtgärder för att skydda kommunens information och system i relation till aktuella hot och risker.
- Tekniska implementationer har etablerats för att upptäcka hot om intrång eller andra säkerhetsincidenter.
- Det finns dokumenterade reserv- och återgångsrutiner som upprättats av den externa leverantören som inkluderar rutiner för back-up och återläsning.

Löpande uppföljningar sker med leverantören där risker och behov diskuteras. Vi bedömer dock att dessa moment i högre grad kan struktureras och dokumenteras så att det finns en spårbarhet över de säkerhetsåtgärder som leverantören och kommunen ser behov av att implementera. Utvärdering och test av skydd har inte genomförts sedan 2020. Mot bakgrund av att hotbild och risker eskalerat sedan dess kan det finnas risk att nya sårbarheter uppstått som inte har utvärderats.

Vi konstaterar I att nämnderna brustit i efterlevnad av beslutade styrdokument. Dels avseende att det i nuläget saknas etablerade rutiner där tekniska säkerhetsåtgärder vidtas som ett resultat av verksamheternas informationsklassningar och riskanalyser. Systemägarna har inte heller genom dokumenterade riskanalyser bedömt specifika behov av säkerhetskopiering för de verksamhetssystem som nyttjas inom respektive förvaltning. Vi ser därigenom att det finns en risk att verksamhetskritisk information kan ha för lågt ställda krav avseende säkerhetskopiering och att det finns en risk att information förloras vid en allvarligare störning eller incident.

4.4 Incidenthantering

Av kommunens vägledningar och bestämmelser för förvaltning och drift av it framgår att it-säkerhetssamordnaren ska sammanställa och rapportera incidenter till kommunledningen. Intervjupersoner styrker att informationsincidenter rapporteras till kommunledning. I dokumentet beskrivs olika typer av incidenter som ska rapporteras, exempelvis intrång, brott mot lagstiftning samt incidenter som riskerar att orsaka större avbrott och störningar. Även driftsleverantören omnämns ha ett ansvar där kritiska händelser, som virus och skadlig kod i it-miljö ska rapporteras.

Vägledningarna beskriver också den aktuella arbetsprocessen vid inträffad incident. Processen utgår från en genomgång av loggar samt analys av oväntade händelser i systemen görs. Därefter ska data säkras och källa till incident spåras. Vägledningen beskriver även att förebyggande åtgärder för att motverka att liknande incident inträffar ska föreslås.

Arbetet ska enligt vägledningen genomföras av utsedd medarbetare på kommunens it-enhet. Intervjupersoner upplever dock svårigheter att upprätthålla beskriven arbetsgång på grund av personalbrist och att processen i stora delar är beroende av kapacitet hos den externa leverantören.

Av intervjuer framgår att kommunens incidenthanteringsrutin är inte är tillräckligt förankrad bland medarbetarna. De intervjuade menar att indikationer på detta är att systemförvaltare i förvaltningarna ibland felaktigt kontaktas vid misstanke om incident.

4.4.1 Bedömning

Vi bedömer att det finns tydligt beskrivna incidenthanteringsrutiner i kommunens vägledningar, men noterar samtidigt att dessa inte tycks vara fullt ut förankrade i kommunens verksamheter.

Vi bedömer att det till viss del finns tydliggjorda eskaleringsvägar. Hanteringen är dock beroende av den externa leverantörens förmåga och resurser för att upptäcka och hantera incidenter. I vissa fall sker dock incidenter som ett resultat av användares hantering och behöver därför upptäckas och hanteras internt i kommunen. Vi ser därför att det är av vikt att de utbildningar som erbjuds genomförs regelbundet samt att rutiner tydliggörs så att incidenter anmäls i tid och till rätt funktion. Detta då en skyndsam hantering vid allvarliga incidenter krävs för att minimera skada eller konsekvens för verksamheterna.

4.5 Uppföljning och återrapportering

4.5.1 Uppföljning

Intervjupersoner lyfter att uppföljning av informationssäkerhetsarbetet inte genomförs i nuläget, främst beroende av tidsbrist hos utsedd informationssäkerhetssamordnare. Det sker därigenom inte heller någon rapportering till kommunstyrelsen eller nämnderna.

Intervjupersoner lyfter att uppföljning görs inom ramen för dataskyddsarbetet och att detta rapporteras till styrelse och nämnder.

4.5.2 Bedömning

Vi bedömer att det saknas en etablerad uppföljning av informationssäkerhetsarbetet och att det i nuläget saknas former för att återrapportera om det arbete som bedrivs. Det är av vikt att kommunstyrelsen tillser en tillräcklig rapportering av arbetet, för att få kännedom om hot och risker för informationssäkerhet samt eventuella brister i informationssäkerhetsarbetet för att ha förutsättningar att besluta om adekvata åtgärder.

5 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen, barn och utbildningsnämnden, kultur- och tekniknämnden samt miljö- och byggnadsnämnden inte bedriver ett systematiskt informationssäkerhetsarbete i enlighet med MSB:s rekommendationer och beslutade styrdokument. Vi bedömer att det inom socialnämndens verksamheter till viss del har genomförts aktiviteter inom informationssäkerhet men konstaterar dock att arbetet inte sker med en tillräcklig systematik i enlighet med MSB:s rekommendationer och beslutade styrdokument.

Det finns en etablerad organisation för arbetet som utgår från linjeansvaret. Därtill finns i viss utsträckning utsedda funktioner som stöd i arbetet. Intervjuade upplever dock att nuvarande resurser inte är tillräckliga för att bedriva ett systematiskt informationssäkerhetsarbete i enlighet med de krav som ställs.

De styrande dokument som beslutats tydliggör ansvar samt krav på aktiviteter för hur informationssäkerhetsarbetet ska bedrivas. Dock konstaterar vi att dokumenten inte i tillräcklig grad är förankrade i kommunens verksamheter. Det operativa informationssäkerhetsarbete som genomförs i kommunen är därigenom inte systematiskt och de krav på aktiviteter som ställs i styrande dokument genomförs endast till viss del. Vi konstaterar bland annat att informationsklassningar och riskanalyser vid tid för granskningen endast genomförs i mindre utsträckning och att arbetet inte är systematiskt. Vi bedömer att styrelsen och samtliga nämnder brustit i att göra informationsklassning och riskanalyser i enlighet med krav i styrande dokument då endast en mindre omfattande klassning gjorts.

Genom det avtal som kommunen har med extern driftsleverantör kan vi konstatera att leverantören presenterat underlag som beskriver det säkerhetsarbete som de tillhandahåller till kommunen. Vi kan konstatera att organisation och säkerhetsarbetet är i enlighet med den standard som kommunen beslutat om som gällande.

Vi bedömer att kommunstyrelse och nämnder har en bristande uppföljning av informationssäkerhetsarbetet då uppföljning och rapportering i nuläget endast sker utifrån dataskyddsarbetet.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi kommunstyrelsen, i deras övergripande ansvar för informationssäkerhet, att:

- Säkerställa att de beslutade styrdokumenten förankras i samtliga verksamheter
- Tillse att resurserna för informations- och it-säkerhetsarbetet står i proportion till organisationens behov och samtida risker och hot
- Beakta informationssäkerhetsrisker i risk- och väsentlighetsanalys
- Tillse att den uppföljning som sker tillsammans med den externa leverantören för it-drift sker på ett strukturerat sätt och att väsentliga risker och behov av åtgärder dokumenteras
- Tillse en tillräcklig uppföljning och regelbunden rapportering av informationssäkerhetsarbetet

Utifrån våra iakttagelser och vår bedömning rekommenderar vi kommunstyrelsen och de granskade nämnderna att:

- Etablera ett informationssäkerhetsarbete i enlighet med styrande dokument
- Tillse att obligatoriska utbildningar inom informationssäkerhet genomförs
- Tillse att riskanalys och informationsklassningar genomförs i de egna verksamheterna och att dessa prioriteras utifrån skyddsvärde för den information som hanteras i systemen

Datum som ovan

KPMG AB

William Andreasson
Kommunal revisor

Jenny Thörn
Projektledare, kommunal revisor

Lena Medin
Certifierad kommunal revisor
Kundansvarig