Nyköping

Revisorerna, 2023-2026

Revisionsskrivelse

Kommunstyrelsen
Barn- och ungdomsnämnden
Socialnämnden
Vård- och omsorgsnämnden

Kommunfullmäktige, för kännedom

Granskning av Informationssäkerheten

KPMG har av Nyköpings kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens och utvalda nämnders rutiner för informationssäkerhetsarbetet. Granskningen ingår i revisionsplanen för år 2023.

Syftet med granskningen har varit att bedöma om kommunstyrelsen, socialnämnden, barn- och ungdomsnämnden samt vård- och omsorgsnämnden bedriver ett systematiskt informationssäkerhetsarbete.

Mot bakgrund av vår granskning bedömer vi att kommunstyrelsen, socialnämnden, barn- och ungdomsnämnden samt vård- och omsorgsnämnden i stora delar bedriver ett systematiskt informationssäkerhetsarbete.

Vi bedömer att det finns aktuella styrande dokument för informationssäkerhetsarbetet som tydliggör ansvar, krav och hur arbetet ska bedrivas. Vi bedömer att den organisation som framgår av styrande dokument är ändamålsenlig. Styrning och organisering av informationssäkerhetsarbetet behöver dock förankras ytterligare mot bakgrund av att styrande dokument nyligen har antagits och den reglering som beslutats ännu inte fått fäste fullt ut i samtliga verksamheter.

Verksamheterna genomför riskanalyser och informationsklassning på ett strukturerat sätt och det har i huvudsak genomförts för de informationstillgångar som verksamheten ansvarar för. Vi vill dock påtala att samtliga verksamheter behöver säkerställa att de behov av skyddsåtgärder som analys och klassning identifierar etableras så att tillgångarna skyddas med tillräckliga åtgärder samt att dessa regelbundet följs upp.

Kommunen har etablerat incidenthanteringsrutiner för informationssäkerhetsincidenter med tillhörande eskaleringsvägar. Kommunen genomför i nuläget utbildningar inom informationssäkerhetsområdet vilka följs upp systematiskt.

Vi konstaterar att den etablerade strukturen för uppföljning av arbetet efterlevs. Vi anser dock att det bör övervägas om kommunstyrelsen bör inkluderas vid beslut om förbättringsåtgärder inom informationssäkerhet.

Vi rekommenderar kommunstyrelsen att:

- Tillse att styrande dokument på informationssäkerhetsområdet förankras i kommunens verksamheter för att säkerställa att dessa efterlevs
- Säkerställa att informationsklassningar och riskanalyser genomförs för de egna informationstillgångarna och att åtgärder följs upp
- Säkerställa att kommunövergripande utbildningar inom informationssäkerhet genomförs och följs upp

Vi rekommenderar barn- och ungdomsnämnden, socialnämnden samt vård- och omsorgsnämnden att:

- Tillse att styrande dokument på informationssäkerhetsområdet efterlevs
- Säkerställa att informationsklassningar och riskanalyser genomförs för de egna informationstillgångarna och att åtgärder följs upp
- Utred behov av särskilda utbildningsinsatser inom nämndernas egna verksamhetsområden utifrån den informationshantering som sker

Granskningen översänds härmed till kommunstyrelsen, barn- och ungdomsnämnden, socialnämnden samt vård- och omsorgsnämnden för yttrande **senast 2023-09-30**. Rapporten skickas även till kommunfullmäktige för kännedom.

För Nyköpings kommuns revisorer

Göran Silfverling,
ordförande

Christer Gustafsson,
vice ordförande

Granskning av informationssäkerhet

Rapport

Nyköpings kommun

KPMG AB

2023-05-31

Antal sidor 17

Innehållsförteckning

1 Sammanfattning

KPMG har av Nyköpings kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens och utvalda nämnders rutiner för informationssäkerhetsarbetet. Granskningen ingår i revisionsplanen för år 2023.

Syftet med granskningen har varit att bedöma om kommunstyrelsen, socialnämnden, barn- och ungdomsnämnden samt vård- och omsorgsnämnden bedriver ett systematiskt informationssäkerhetsarbete.

Mot bakgrund av vår granskning bedömer vi att kommunstyrelsen, socialnämnden, barn- och ungdomsnämnden samt vård- och omsorgsnämnden i stora delar bedriver ett systematiskt informationssäkerhetsarbete.

Vi bedömer att det finns aktuella styrande dokument för informationssäkerhetsarbetet som tydliggör ansvar, krav och hur arbetet ska bedrivas. Vi bedömer att den organisation som framgår av styrande dokument är ändamålsenlig. Styrning och organisering av informationssäkerhetsarbetet behöver dock förankras ytterligare mot bakgrund av att styrande dokument nyligen har antagits och den reglering som beslutats ännu inte fått fäste fullt ut i samtliga verksamheter.

Verksamheterna genomför riskanalyser och informationsklassning på ett strukturerat sätt och det har i huvudsak genomförts för de informationstillgångar som verksamheten ansvarar för. Vi vill dock påtala att samtliga verksamheter behöver säkerställa att de behov av skyddsåtgärder som analys och klassning identifierar etableras så att tillgångarna skyddas med tillräckliga åtgärder samt att dessa regelbundet följs upp.

Kommunen har etablerat incidenthanteringsrutiner för informationssäkerhetsincidenter med tillhörande eskaleringsvägar. Kommunen genomför i nuläget utbildningar inom informationssäkerhetsområdet vilka följs upp systematiskt.

Vi konstaterar att den etablerade strukturen för uppföljning av arbetet efterlevs. Vi anser dock att det bör övervägas om kommunstyrelsen bör inkluderas vid beslut om förbättringsåtgärder inom informationssäkerhet.

Vi rekommenderar kommunstyrelsen att:

- Tillse att styrande dokument på informationssäkerhetsområdet förankras i kommunens verksamheter för att säkerställa att dessa efterlevs
- Säkerställa att informationsklassningar och riskanalyser genomförs för de egna informationstillgångarna och att åtgärder följs upp
- Säkerställa att kommunövergripande utbildningar inom informationssäkerhet genomförs och följs upp

Vi rekommenderar barn- och ungdomsnämnden, socialnämnden samt vård- och omsorgsnämnden att:

- Tillse att styrande dokument på informationssäkerhetsområdet efterlevs
- Säkerställa att informationsklassningar och riskanalyser genomförs för de egna informationstillgångarna och att åtgärder följs upp
- Utred behov av särskilda utbildningsinsatser inom nämndernas egna verksamhetsområden utifrån den informationshantering som sker

2 Bakgrund

KPMG har av Nyköpings kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens och utvalda nämnders rutiner för 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. 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 informationssäkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

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

2.1 Syfte och revisionsfrågor

Granskningen syftar till att bedöma om kommunstyrelsen, socialnämnden, barn- och ungdomsnämnden samt vård- och omsorgsnämnden bedriver ett systematiskt informationssäkerhetsarbete.

Granskningen avser att besvara följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
- Har riskanalyser och informationsklassning genomförts för de informationstillgångar som verksamheten ansvarar för?
    - Har säkerhetsåtgärder vidtagits som ett resultat av dessa?
    - Har säkerhetsåtgärderna följts upp?
- Finns etablerade incidenthanteringsrutiner för informationssäkerhetsincidenter?
    - Finns tillräcklig kunskap och medvetenhet hos medarbetare för att identifiera och anmäla incidenter?
    - Inkluderar rutiner eskaleringsvägar och krav på hur incidenter ska dokumenteras och följas upp?
- Finns en etablerad uppföljning av informationssäkerhetsarbetet och rapporteras denna till styrelse och nämnder så att beslut om förbättringsåtgärder kan beslutas?

2.2 Revisionskriterier

Granskningen har utgått från nedanstående revisionskriterier:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policyer och beslut
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet

2.3 Ansvarig nämnd/styrelse

Granskningen har avsett kommunstyrelsen, socialnämnden, barn- och ungdomsnämnden samt vård- och omsorgsnämnden och omfattar styrningen av informationssäkerhetsarbetet.

2.4 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer/avstämningar med berörda tjänstepersoner.

Följande underlag har granskats:

- Program för effektiv organisation
- Riktlinjer för informationssäkerhet
- Riktlinjer för informationssäkerhet för medarbetare
- Interna rutiner
- Genomförda informationsklassningar och riskanalyser

Följande funktioner har intervjuats:

- Kommundirektör
- Divisionschef social omsorg
- Enhetschef division utbildning
- Medarbetare inom it-funktionen
- Informationssäkerhetssamordnare

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 policyer 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 hållas informerad om informationssäkerhetsarbetets status och därmed kunna besluta om åtgärder utifrån föreslagna förbättringsområden är uppföljning av vikt. Informationssäkerhetssamordnaren bör presentera det samlade informationssäkerhetsarbetet årligen.

3.2 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 policyer och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.

4 Resultat

4.1 Styrning och organisering av informationssäkerhetsarbetet

4.1.1 Styrdokument

Vi har i granskningen tagit del av styrande dokument inom informationssäkerhet som beskrivs översiktligt i detta avsnitt. Riktlinjerna var vid tiden för granskningen nyligen antagna och en förankringsprocess pågick för att etablera dessa i organisationen.

4.1.1.1 Program för effektiv organisation

Vi har tagit del av Nyköpings kommuns Program för effektiv organisation.[1] Programmet beskriver bland annat systematiskt informationssäkerhetsarbete i kommunen. Det anges att kommunens informationssäkerhetsarbete ska omfatta all kommunens verksamhet, exklusive bolagen. Information ska skyddas utifrån principerna om tillgänglighet, riktighet och konfidentialitet. Ansvaret för informationssäkerheten beskrivs följa det delegerade verksamhetsansvaret och ingår således i linjeansvaret.

Kommundirektören beskrivs vara övergripande ansvarig för att informationssäkerhetsarbetet bedrivs i enlighet med kommunens övergripande mål och inriktning. Den politiska viljeriktningen är att kommunen ska bedriva ett systematiskt, riskbaserat och hållbart informationssäkerhetsarbete utifrån etablerade standarder. Det anges vidare att informationssäkerhetskultur i form av säkerhetsmedvetenhet ska prioriteras, att information ska skyddas i proportion till skyddsvärde samt att upphandling ska ske där hänsyn tas till informationssäkerhet.

4.1.1.2 Riktlinjer för informationssäkerhet

Vi har tagit del av kommunens riktlinjer för informationssäkerhet.[2] Riktlinjerna anger övergripande styrningen av informationssäkerhetsarbetet i kommunen. Riktlinjerna för informationssäkerhet är uppdelade i två dokument, där en del vänder sig till chefer och personal som arbetar med informations- och IT-säkerhet och den andra delen vänder sig till samtliga medarbetare (beskrivs nedan i avsnitt 4.1.1.3).

Riktlinjerna avser informationssäkerhet för all information som hanteras i kommunen, analog såväl som digital. Riktlinjerna gäller alla medarbetare och förtroendevalda. Riktlinjerna beskriver vidare personalsäkerhet, hantering av informationstillgångar, åtkomst till informationstillgångar, kommunikationssäkerhet, leverantörsrelationer anskaffning och underhåll av system, kontinuitetshantering samt teknisk och fysisk säkerhet i större detalj.

[1] KF, 2022-02-08 §§ framgår ej.
[2] Antagen av kommundirektör 2023-02-04.

4.1.1.3 *Riktlinjer för informationssäkerhet för medarbetare*

Vi har tagit del av riktlinjer för informationssäkerhet för medarbetare.[3] Riktlinjerna vänder sig till samtliga medarbetare och förtroendevalda i kommunen och även externa utförare såsom konsulter som har tillgång till kommunens information. Riktlinjerna utgår från Digital informationssäkerhetsutbildning för alla (DISA), vilken är framtagen av Myndigheten för samhällsskydd och beredskap (MSB). Riktlinjen ska läsas av medarbetare i samband med att de genomför DISA och på så sätt erhålla kunskap om informationssäkerhet.

Riktlinjerna beskriver vidare lösenordshantering, säkerhetskopiering, hantering av molntjänster och e-post, bedrägeririsker och skadlig kod. Därtill beskrivs olika typer av informationssäkerhetsincidenter samt innehåller en hänvisning till kommunens rutin för rapport av säkerhetsincidenter (se 4.2.3).

4.1.2 Organisation och ansvarsfördelning

Riktlinjerna för informationssäkerhet anger informationssäkerhetsarbetets organisation genom att beskriva roll- och ansvarsfördelningen. Utgångspunkten i ansvarsfördelningen av informationssäkerhetsarbetet är att det följer det ordinarie verksamhetsansvaret. Detta innebär att den som är ansvarig för en viss verksamhet, såsom en division, enhet, process eller projekt således är ansvarig att skydda information som hanteras inom verksamheten.

Kommunstyrelsen är ytterst ansvarig för kommunens informationssäkerhet och kommundirektören ansvarar för att informationssäkerhetsarbetet bedrivs enligt kommunens övergripande mål och inriktning. Vidare beskrivs roller såsom personuppgiftsansvarig, personuppgiftskoordinator dataskyddsombud, IT-säkerhetssamordnare, systemförvaltningssamordnare (inriktning informationssäkerhet) informationssäkerhetssamordnare och lokala informationssäkerhetssamordnare.

Det framgår exempelvis att informationssäkerhetssamordnaren är övergripande ansvarig för ledning och samordning av informationssäkerhetsarbetet i kommunen.

Enligt riktlinjerna ska lokala informationssäkerhetssamordnare finnas etablerade i respektive verksamhet. Intervjupersoner styrker att funktionen finns etablerad, men att lokal samordnare saknas inom division social omsorg.

Det framgår även av riktlinjerna att systemförvaltningssamordnare ska utgöra sakkunniga i informationssäkerhetsfrågor och stödja IT-avdelningen i deras informationssäkerhetsarbete. Systemförvaltningssamordnare ska utgöra lokal informationssäkerhetssamordnare på IT-avdelningen.

Av riktlinjerna framgår att det finns två forum för dialog om informationssäkerhetsfrågor. Dels informationssäkerhetsforum, dels forum för IT-och informationssäkerhet.

[3] Antagen av kommundirektör 2023-02-04.

Informationssäkerhetsforum finns enligt riktlinjerna för att diskutera och samordna informationssäkerhets- och personuppgiftsfrågor inom kommunen och deltagare i forumet anges vara informationssäkerhetssamordnare, dataskyddsombud, lokala informationssäkerhetssamordnare och personuppgiftskoordinatorer.

Forum för IT- och informationssäkerhet finns enligt riktlinjerna för att diskutera och samordna frågor om informations- och IT-säkerhet. De som ska ingå i forumet är IT-säkerhetssamordnare, informationssäkerhetssamordnare och systemförvaltningssamordnare (inriktning informationssäkerhet). Intervjupersoner styrker att beskrivningen av dessa fora stämmer.

Av intervjuer framgår att den organisation som etablerats upplevs skapa goda förutsättningar i arbetet men att den är förhållandevis ny. Därtill upplevs att personuppgifts- och informationssäkerhetsarbetet samordnats som positivt.

Mot bakgrund av att styrande dokument i form av riktlinjer vid tid för intervjuer var nyligen beslutade uppges av intervjuade att dessa ännu inte fått fäste fullt ut i verksamheterna.

4.1.3 Bedömning

Vi bedömer att det finns aktuella styrande dokument för informationssäkerhetsarbetet som tydliggör ansvar, krav och hur arbetet ska bedrivas. Riktlinjerna för informationssäkerhet har dock nyligen antagits och har således ännu inte fullt ut fått fäste i kommunens verksamheter.

Vi bedömer att den organisation som framgår av styrande dokument är ändamålsenlig, men att organiseringen av informationssäkerhetsarbetet i likhet med vad som i övrigt anges i styrdokumenten behöver förankras ytterligare.

4.2 Det systematiska informationssäkerhetsarbetet

4.2.1 Årshjul för informationssäkerhet

Kommunens informationssäkerhetsarbete utgår från ett årshjul.[4]

Av årshjulet framgår att informationssäkerhetssamordnaren har i uppdrag att:

- lyfta strategiska frågor till kommunledningen
- planera och samordna informationssäkerhetsarbetet övergripande
- utveckla arbetssätt och processer
- stötta verksamheterna i genomförande
- utvärdera och följa upp resultat

Årshjulet beskriver de aktiviteter inom informationssäkerhetsarbetet som ska genomföras under årets gång och när i tid samordnaren ska genomföra dessa.

4.2.2 Riskanalys och informationsklassning

Enligt MSB:s metodstöd är informationsklassning 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.

Kommunen har beslutat om gemensam modell för klassning och använder sig av SKR:s modell KLASSA. Kommunens förvaltningar har möjlighet till stöd i arbetet med klassningar och riskanalys dels av lokala informationssäkerhetssamordnare, dels av centralt placerad informationssäkerhetssamordnare.

Av intervju med division utbildning framgår att det bedrivs ett aktivt arbete med riskanalys och informationsklassning i divisionens verksamheter. De flesta större verksamhetssystemen har klassats, med undantag för ett mindre antal äldre system som enligt uppgift ska klassas framöver. Intervjupersoner uppger dock att det finns en problematik med informationsklassning och riskanalys inom divisionen. Detta mot bakgrund av att det finns ett stort antal mindre system. Rektorer har inom sina enheter själva upphandlat och implementerat digitala tjänster och verktyg. Detta uppges skapa en problematik vad gäller översikt av systemfloran och riskerar leda till eventuella risker.

Av intervju med division social omsorg framgår att det bedrivs ett aktivt arbete med riskanalys och informationsklassning i divisionens verksamheter. De intervjuade uppger att man i nuläget, likt division utbildning, klassat de flesta stora systemen, men att ett flertal mindre och äldre system återstår.

[4] Rutin framtagen av informationssäkerhetssamordnare, giltig från 2022-06-22.

Vi har tagit del av exempel på informationsklassningar och riskanalyser för divisionerna som styrker att det finns ett etablerat arbetssätt avseende riskanalys och informationsklassning för informationstillgångar som hanteras i system.

4.2.3 Bedömning

Vi bedömer att riskanalyser och informationsklassning i huvudsak har genomförts för de informationstillgångar som verksamheten ansvarar för. Det pågår ett aktivt arbete med att slutföra arbetet för samtliga system. Vi vill dock påtala att samtliga verksamheter behöver säkerställa att de behov av skyddsåtgärder som analys och klassning identifierar etableras så att tillgångarna skyddas med tillräckliga åtgärder samt att dessa regelbundet följs upp.

4.3 Incidenthantering och säkerhetsmedvetenhet

4.3.1 Säkerhetsmedvetenhet och kunskapshöjande insatser

Av intervjuer framgår att kommunen i nuläget genomför kommunövergripande utbildningar för samtliga medarbetare. Utbildningarna genomförs i syfte att höja medarbetarnas säkerhetsmedvetenhet och behandlar i huvudsak ämnen som phishing, lösenordshantering och generella risker och hot i digital miljö. Enligt uppgift följs alla obligatoriska utbildningar upp och genomförandegraden presenteras både hos kommunledningsgrupp och kommunstyrelsen. Avseende kortare utbildningar skickas en rapport ut till respektive chef där genomförandegrad presenteras. Därtill har uppföljning presenterats på bland annat intranätet. Statistik utifrån av kommunen genomförda nätfisketester presenteras också för chefer.

Av intervju framgår att användare ska ta del av utbildningar inför tilldelning av behörighet i något av kommunens verksamhetssystem. Vi har tagit del av en utbildningsplan från kommunen, av vilken det framgår att utbildningarna ska innefatta systemspecifika regler, rutiner och aspekter av informationssäkerhet.

Tips på generella utbildningar framgår av utbildningsplanen. Exempel på sådana utbildningar och information är Riktlinjer för informationssäkerhet, DISA och kurs i dataskydd samt allmän information om lösenordshantering. Hänvisning görs även till intranätet där systemspecifika utbildningar/information samt stödmaterial finns tillgängligt.

Av intervju med division utbildning framgår att riskmedvetenheten hos medarbetarna uppges vara ojämn. Intervjupersoner ser att det i nuläget finns risker relaterade till medarbetarnas varierande kunskap och medvetenhet, exempelvis avseende phishing.[5]

Intervjupersoner från division social omsorg delar denna bild och menar att det finns risker kopplat till bristande datorvana och digital mognad inom divisionens

[5] Phishing är en typ av falsk e-post som skickas till mottagaren i syfte att få denne att utlämna lösenord eller andra känsliga uppgifter som riskerar skada organisation och/eller mottagare.

verksamheter. Medarbetare inom divisionen uppges utifrån det ha olika förutsättningar att kunna identifiera informationssäkerhetsincidenter.

4.3.2 Incidenthantering

Av kommunens riktlinjer för informationssäkerhet framgår att kommunen ska ha ett gemensamt system för rapportering och hantering av säkerhetsincidenter, inklusive informationssäkerhetsincidenter. Systemet ska vara känt av samtliga medarbetare och externa utförare med tillgång till kommunens information.

Vi har tagit del av underlag i form av utdrag från kommunens intranät. Av utdraget framgår att kommunen använder ett formulär för anmälan av incidenter på intranätet. Intervjupersoner uppger att kommunens system för incidenthantering har en gemensam portal, oavsett vad för incident som avses inom informationssäkerhet. Genom systemet sorteras sedan incidenten till rätt område. För informations- och personuppgiftsincidenter finns medarbetare som bevakar incidentflödet.

Av intervjuer framgår att incidenthanteringsrutinerna är kända inom delar av kommunens verksamheter, men att intervjupersoner uppfattar att kännedomen inom särskilda verksamheter är låg. Av intervjuer framgår vidare att inträffade informationsincidenter dokumenteras för analys.

4.3.3 Bedömning

Vi bedömer att de incidenthanteringsrutiner för informationssäkerhetsincidenter som finns är tillräckliga och innehåller eskaleringsvägar. Vi bedömer att det till viss del finns en tillräcklig kunskap och medvetenhet hos medarbetare för att identifiera och anmäla incidenter. Utbildningar har genomförts i viss utsträckning i syfte att etablera en säkerhetsmedvetenhet samt för att etablera kunskap om informationsklassning och riskanalyser inom området.

4.4 Uppföljning och återrapportering

4.4.1 Ledningens genomgång

Av kommunens årshjul[6] framgår att informationssäkerhetssamordnaren årligen ska redovisa årets informationssäkerhetsarbete för kommunledningen.

Intervjupersoner bekräftar att både förvaltningsledningen och kommunstyrelsen får del av information avseende status i informationssäkerhetsarbetet. På grund av att kommunens nuvarande informationssäkerhetssamordnare nyligen tillträtt sin tjänst har föregående års informationssäkerhetsarbete ännu inte redovisats för kommunledningen. Intervjupersoner uppger att det ska göras under året.

[6] Se 3.2.1.

Av protokoll[7] framgår att informationssäkerhetsarbetet presenterats enligt vad som anges av årshjulet. I protokollet anges bland annat att 2021 års informationssäkerhetsarbete redovisats tillsammans med förslag till mål för 2022 års arbete.

4.4.2 Bedömning

Vi bedömer att kommunen har en etablerad struktur för uppföljning av informationssäkerhetsarbetet. Utifrån ovan beskrivna årshjul skapas förutsättningar för att informationssäkerhetsarbetet ska följas upp på ett strukturerat sätt, för att identifiera utvecklingsområden och dela information med kommunstyrelse och ledningsgrupp. Vi konstaterar att den etablerade strukturen för uppföljning av arbetet efterlevs. Vi anser dock att det bör övervägas om kommunstyrelsen bör inkluderas vid beslut om förbättringsåtgärder inom informationssäkerhet.

[7] KS 2022-03-14 § 57.

5 Svar på revisionsfrågor

Nedan framgår de revisionsfrågor som varit aktuella i samband med granskningen och tillhörande bedömning.

Finns aktuella styrande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas?

Vår bedömning är att det finns aktuella styrande dokument för att tydliggöra ansvar, krav och hur informationssäkerhetsarbetet ska bedrivas. Vi ser dock ett behov av att ytterligare förankra de styrande dokumenten i kommunens verksamheter.

Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?

Vår bedömning är att kommunens organisation av informationssäkerhetsarbetet är ändamålsenlig.

Har riskanalyser och informationsklassning genomförts för de informationstillgångar som verksamheten ansvarar för?

- *Har säkerhetsåtgärder vidtagits som ett resultat av dessa?*
- *Har säkerhetsåtgärderna följts upp?*

Vi bedömer att riskanalyser och informationsklassning i stor del har genomförts för de informationstillgångar som respektive verksamheter svarar för. Därtill ser vi ett aktivt arbete med slutförande av återstående klassningar. Säkerhetsåtgärder har i viss utsträckning vidtagits och följs upp och vi vill påtala vikten av att samtliga verksamheter genomför detta.

Finns etablerade incidenthanteringsrutiner för informationssäkerhetsincidenter?

- *Finns tillräcklig kunskap och medvetenhet hos medarbetare för att identifiera och anmäla incidenter?*
- *Inkluderar rutiner eskaleringsvägar och krav på hur incidenter ska dokumenteras och följas upp?*

Vi bedömer att de incidenthanteringsrutiner för informationssäkerhetsincidenter som finns är tillräckliga och innehåller eskaleringsvägar samt att det finns en tillräcklig kunskap och medvetenhet hos medarbetare för att identifiera och anmäla incidenter.

Finns en etablerad uppföljning av informationssäkerhetsarbetet och rapporteras denna till styrelse och nämnder så att beslut om förbättringsåtgärder kan beslutas?

Vi bedömer att kommunen har en etablerad struktur för uppföljning av informationssäkerhetsarbetet. Vi konstaterar att den etablerade strukturen för uppföljning av arbetet efterlevs. Vi anser dock att det bör övervägas om kommunstyrelsen bör inkluderas vid beslut om förbättringsåtgärder inom informationssäkerhet

6 Slutsats och rekommendationer

Mot bakgrund av vår granskning bedömer vi att kommunstyrelsen, socialnämnden, barn- och ungdomsnämnden samt vård- och omsorgsnämnden i stora delar bedriver ett systematiskt informationssäkerhetsarbete.

Vi bedömer att det finns aktuella styrande dokument för informationssäkerhetsarbetet som tydliggör ansvar, krav och hur arbetet ska bedrivas. Vi bedömer att den organisation som framgår av styrande dokument är ändamålsenlig. Styrning och organisering av informationssäkerhetsarbetet behöver dock förankras ytterligare mot bakgrund av att styrande dokument nyligen har antagits och den reglering som beslutats ännu inte fått fäste fullt ut i samtliga verksamheter.

Verksamheterna genomför riskanalyser och informationsklassning på ett strukturerat sätt och det har i huvudsak genomförts för de informationstillgångar som verksamheten ansvarar för. Vi vill dock påtala att samtliga verksamheter behöver säkerställa att de behov av skyddsåtgärder som analys och klassning identifierar etableras så att tillgångarna skyddas med tillräckliga åtgärder samt att dessa regelbundet följs upp.

Kommunen har etablerat incidenthanteringsrutiner för informationssäkerhetsincidenter med tillhörande eskaleringsvägar. Vi ser emellertid risker avseende bristande medvetenhet kring informationssäkerhet inom kommunen som helhet. Det är väsentligt att säkerhetsmedvetenheten i kommunen är tillräcklig. Dels så att informationssäkerhetsincidenter kan identifieras och anmälas av medarbetare, dels för att minska risken för informationssäkerhetsincidenter som beror på den mänskliga faktorn.

Vi konstaterar att den etablerade strukturen för uppföljning av arbetet efterlevs. Vi anser dock att det bör övervägas om kommunstyrelsen bör inkluderas vid beslut om förbättringsåtgärder inom informationssäkerhet.

Vi rekommenderar kommunstyrelsen att:

- Tillse att styrande dokument på informationssäkerhetsområdet förankras i kommunens verksamheter för att säkerställa att dessa efterlevs
- Säkerställa att informationsklassningar och riskanalyser genomförs för de egna informationstillgångarna och att åtgärder följs upp
- Säkerställa att kommunövergripande utbildningar inom informationssäkerhet genomförs och följs upp

Vi rekommenderar barn- och ungdomsnämnden, socialnämnden samt vård- och omsorgsnämnden att:

- Tillse att styrande dokument på informationssäkerhetsområdet efterlevs
- Säkerställa att informationsklassningar och riskanalyser genomförs för de egna informationstillgångarna och att åtgärder följs upp

— Utred behov av särskilda utbildningsinsatser inom nämndernas egna verksamhetsområden utifrån den informationshantering som sker

2023-05-31

KPMG AB

Anders Petersson

Certifierad kommunal yrkesrevisor

Jenny Thörn

Verksamhetsrevisor/Projektledare

William Andreasson

Verksamhetsrevisor