Granskning av informationssäkerhet

Jokkmokks kommun

December 2023

Pär Koyanagi-Gustafsson, projektledare

Carl Nisser, projektmedarbetare

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Jokkmokks kommun genomfört en granskning inom området informationssäkerhet. Granskningen tar utgångspunkt från kommunallagens revisionskapitel.

Nedan redovisas resultatet av genomförd granskning. För fullständiga bedömningar, se respektive revisionsfråga i rapporten.

Revisionsfrågor	Bedömning	
1. Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning? Fokus på följande områden: aktualitet, heltäckande samt förankring inom organisationen.	Nej	
2. Finns i tillräcklig grad styrande riktlinjer för informationssäkerhet och är dessa väl implementerade i verksamheten?	Nej	
3. Bedriver verksamhetsorganisationen ett aktivt arbete med informationssäkerhet? Fokus på riskanalys, aktiviteter/åtgärder samt rapportering?	Nej	
4. Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?	Nej	

Utifrån genomförd granskning är vår samlade bedömning att kommunens arbete med informationssäkerhet inte bedrivs med tillräcklig intern kontroll.

För att utveckla granskningsområdet bör följande rekommendationer prioriteras:

- Att kommunstyrelsen ser till att det upprättas interna styrdokument för kommunens arbete med informationssäkerhet, däribland en informationssäkerhetspolicy som beslutas av kommunfullmäktige.
- Att kommunstyrelsen säkerställer att det finns en tydlig ansvarsfördelning för arbetet med informationssäkerhet. Detta gäller såväl inom den politiska organisationen (kommunstyrelse och nämnder) som på verksamhetsnivå.
- Att kommunstyrelsen säkerställer att kommunens arbete inom området sker på ett systematiskt sätt. Styrelsen bör här pröva om kommunen ska införa ett särskilt ledningssystem för informationssäkerhet.
- Att kommunstyrelsen utvecklar sin uppsikt inom området informationssäkerhet. Detta kan exempelvis ske genom att området inkluderas i årshjul för uppföljning/rapportering till styrelsen.

Innehållsförteckning

Inledning

Bakgrund

Kommuner och regioner har ett av det svenska samhällets mest komplexa uppdrag. Detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde.

Med dagens snabba digitalisering blir informationssäkerhet allt viktigare. Det övergripande syftet med informationssäkerhet är att säkerställa att information för medarbetare, medborgare och andra intressenter hanteras med utgångspunkt i tillgänglighet, riktighet och konfidentialitet. Klassning av informationstillgångar är viktigt för att säkerställa att den skyddsvärda informationen verkligen får det skydd som krävs.

Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering. Förtroendet för en organisation tar lång tid att bygga upp, men kan snabbt raseras av en enskild säkerhetsincident.

Revisorerna har i riskanalysen för 2023 bedömt att det finns skäl att genomföra granskning inom området. Revisionsobjekt i denna granskning är kommunstyrelsen och nämnder.

Syfte och revisionsfrågor

Revisorernas uppdrag regleras i kommunallagen kapitel 12. Syftet med granskningen är att bedöma om kommunens arbete med informationssäkerhet bedrivs med tillräcklig intern kontroll. Följande revisionsfrågor ska besvaras i granskningen:

1. Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning? Fokus på följande områden: aktualitet, heltäckande samt förankring inom organisationen.
2. Finns i tillräcklig grad styrande riktlinjer för informationssäkerhet och är dessa väl implementerade i verksamheten?
3. Bedriver verksamhetsorganisationen ett aktivt arbete med informationssäkerhet? Fokus på riskanalys, aktiviteter/åtgärder samt rapportering?
4. Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar. Följande revisionskriterier används i granskningen:

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster §11-14
- Kommunallagen 6:1, 6:6, 6:13
- Styrdokument inom kommunen som är relevanta för granskningen, främst policy, riktlinjer och rutiner gällande informationssäkerhet.

Avgränsning

I tid avgränsas granskningen i första hand till år 2023. Övrig avgränsning, se avsnitt “Syfte och revisionsfrågor”.

Metod

Granskningen har skett genom analys av för granskningen relevant dokumentation samt kompletterande intervjuer med företrädare för IT-funktionen, socialförvaltningen samt skolförvaltningen.

Revisionell bedömning av respektive revisionsfråga sker utifrån en tregradig skala: ja/uppfyllt (grön); delvis uppfyllt (gul); nej/ej uppfyllt (röd).

De intervjuade har beretts möjlighet att sakgranska rapporten.

Granskningsresultat

Organisation och ansvarsfördelning

Revisionsfråga 1: Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning? Fokus på följande områden: aktualitet, heltäckande samt förankring inom organisationen.

Iakttagelser

Av kommunallagen framgår att kommunal verksamhet ska kännetecknas av god intern kontroll. En del i den interna kontrollen är att tydliggöra ansvar och roller inom en organisation. Detta gäller inom såväl den politiska organisationen som verksamhetsorganisationen. En otydlig ansvarsfördelning riskerar försvåra möjligheten att utkräva ansvar av organisationen.

Politisk nivå

Av kommunallagen 6:1 framgår att kommunstyrelsen ansvarar för att leda och samordna förvaltningen av kommunens angelägenheter. Kommunstyrelsen kan därmed sägas ha ett lednings- och samordningsansvar för kommunens arbete med informationssäkerhet.

Granskningen kan inte finna att kommunstyrelsen - i styrdokument - preciserat vilket ansvar facknämnderna har inom området informationssäkerhet. Ansvarsfördelningen kan exempelvis regleras i en informationssäkerhetspolicy och/eller i reglemente för kommunstyrelse och nämnder.

Verksamhetsnivå

Granskningen kan inte finna att kommunstyrelsen preciserat hur ansvars- och rollfördelningen ser ut inom verksamhetsorganisationen. Inom kommunstyrelsens förvaltningsorganisationen återfinns bland annat IT-funktionen. Funktionen sköter drift och underhåll av kommunens IT-plattform.

IT-funktionen har tagit fram ett styrdokument benämnt “Säkerhetspolicy Användare 2022”. I detta dokument definieras ett antal roller med ansvarsområden inom ramen för arbetet med IT-system:

- Systemägare
- Operativt ansvarig
- IT-ansvarig (IT-chef)
- Systemadministratören (IT-tekniker)
- Användaren
- IT-säkerhetsledning
- Styrgrupper

Granskning av styrdokumentet visar att respektive roll är kortfattat beskriven.

I granskningen framkommer att förvaltningarnas kännedom om styrdokumentet och dess medföljande roller är låg, vilket medför att framtagen rollstruktur inte efterlevs.

I övrigt noteras att det inom verksamhetsorganisationen inte preciserats med vem/vilka inom organisationen som är informationssäkerhetsansvarig respektive dataskyddsombud.

Vår sammanfattande bild är att det inom verksamheten saknas en heltäckande roll- och ansvarsbeskrivning som beskriver hur organisationen ska arbeta, exempelvis vad förvaltningarna förväntas göra inom ramen för informationssäkerhet.

Bedömning

Revisionsfråga 1: Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning? Fokus på följande områden: aktualitet, heltäckande samt förankring inom organisationen.

Nej

Bedömningen baseras på följande:

- Kommunstyrelsens ansvar för informationssäkerhet regleras i kommunallagen. I övrigt har det inte preciserats vilket eventuellt ansvar som vilar på facknämnderna.
- Det saknas en heltäckande beskrivning hur ansvar och roller för informationssäkerhet fördelas inom verksamhetsorganisationen. Förekommande styrdokument är i låg grad kända inom förvaltningarna.

För att utveckla granskningsområdet föreslås att kommunstyrelsen tydliggör organisation och ansvarsfördelning avseende informationssäkerhet. Detta gäller på såväl politisk nivå som på verksamhetsnivå. På verksamhetsnivå finns ett behov att bland annat utse en informationssäkerhetssamordnare.

Styrdokument

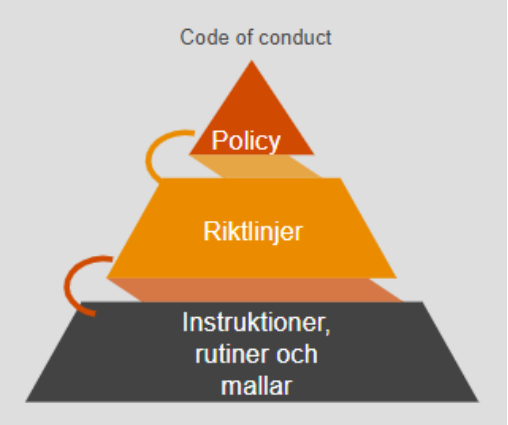
Revisionsfråga 2: Finns i tillräcklig grad styrande riktlinjer för informationssäkerhet och är dessa väl implementerade i verksamheten?

Iakttagelser

Av kommunallagen framgår att kommunal verksamhet ska styras genom mål, riktlinjer och planer. Mål och riktlinjer ska beslutas av den politiska organisationen.

I *Myndigheten för samhällsskydd och beredskaps* (MSB) uppdrag ingår att lämna råd och stöd till organisationer hur de ska arbeta med informationssäkerhet. I MSB:s vägledning beskrivs vikten av att ta fram styrdokument. Styrdokumenten kan utgöras av policy, riktlinjer, planer och instruktioner.

Nedan presenteras en figur på hur en dokumentationshierarki kan se ut:



Figur 1. Dokumentationshierarki

Granskningen visar att varken kommunfullmäktige eller kommunstyrelsen fastställt styrdokument som specifikt rör området informationssäkerhet. Vi noterar att det på verksamhetsnivå påbörjats ett arbete att ta fram en informationssäkerhetspolicy. Tanken är att policyn ska beslutas av kommunfullmäktige.

Utöver styrdokument som beslutas på politisk nivå bör det även upprättas dokumenterade instruktioner och rutiner på verksamhetsnivå. Följande styrdokument har noterats i granskningen:

1. Riktlinjer Lagring 2022
2. Säkerhetspolicy Användare 2022

I *styrdokument 1* beskrivs hur anställda inom organisationen ska lagra dokumentation baserat på en informationsklassning utifrån ett GDPR-perspektiv. Anvisningen inkluderar en modell för hur information ska hanteras utifrån vilka personuppgifter dokumentet innehåller. Anvisningen beskriver de informationstyper samt en klassificeringsmodell (nivå 1, nivå 2, nivå 3) som beskriver kraven för lagring baserat på vilken informationstyp det handlar om. Klassificeringsmodellen utgår från ett GDPR-perspektiv, eftersom konsekvenser beskrivna i modellen utgår från att information når obehöriga. En brist med denna modell är att den saknar informationssäkerhetsaspekterna Riktighet och Tillgänglighet. Dessa aspekter återfinns inte heller i någon annan klassningsmatris.

I *styrdokument 2* definieras ett antal roller med ansvarsområden inom ramen för arbetet med IT-system vilket är att likna vid ett embryo till en systemförvaltarmodell.

Vår granskning indikerar att granskade styrdokument i låg grad är kända inom kommunens förvaltningar.

Den sammantagna bild som framträder i granskningen är att det även på verksamhetsnivå saknas en tillfredsställande dokumentationsstruktur för området informationssäkerhet.

Avsaknad av styrdokument inom Jokkmokks kommun riskerar medföra att information inte hanteras i enlighet med dess skyddsvärde utifrån konfidentialitet, integritet eller tillgänglighet.

Bedömning

Finns i tillräcklig grad styrande riktlinjer för informationssäkerhet och är dessa väl implementerade i verksamheten?

Nej

Bedömningen baseras på följande:

- Granskningen visar att det på såväl politisk nivå som verksamhetsnivå saknas styrdokument för området informationssäkerhet.
- Granskningen indikerar att de styrdokument som upprättats av kommunens IT-funktion som rör säkerhet samt GDPR i låg grad är implementerade i verksamheten.

För att utveckla granskningsområdet föreslås att kommunstyrelsen - tillsammans med IT-funktionen - tar fram en grund med styrande dokumentation för informationssäkerhet. När dessa finns på plats är det av vikt att öka medvetenheten gällande styrdokument och sprida kunskaper om deras innehåll hos kommunens personal.

Systematiskt arbetssätt

Revisionsfråga 3: Bedriver verksamhetsorganisationen ett aktivt arbete med informationssäkerhet? Fokus på riskanalys, aktiviteter/åtgärder samt rapportering.

Iakttagelser

Myndigheten för samhällsskydd och beredskap (MSB) betonar vikten av att svenska myndigheter och organisationer bedriver ett systematiskt arbete med informationssäkerhet. Ett systematiskt arbetssätt kännetecknas vanligtvis av följande moment:

1. Inventering och bedömning av risker
2. Mål och aktivitetsplaner
3. Uppföljning
4. Utvärdering

Enligt lag 2018:1174 vilar det på aktörer som tillhandahåller samhällsviktiga tjänster att bedriva ett systematiskt arbete med informationssäkerhet. Till samhällsviktiga tjänster räknas bland annat digital infrastruktur, hälso- och sjukvård samt leverans och distribution av dricksvatten. För kommunmedborgarna inom Jokkmokk ansvarar kommunen för ett flertal av dessa tjänster.

En metod att säkerställa ett systematiskt arbetssätt är att införa ett ledningssystem för informationssäkerhet. Granskningen visar att kommunen saknar ett sådant ledningssystem.

Några av de mest centrala aktiviteter som bör göras inom ramen för ett aktivt informationssäkerhetsarbete är informationsklassificering och riskanalyser. Som berörts i revisionsfråga 2 finns det en dokumenterad rutin för hur informationsklassificering ska göras utifrån ett GDPR-perspektiv, som dock inte tycks efterlevas i praktiken.

Granskningen visar att det saknas en rutin för att identifiera och analysera informationssäkerhetsrisker som är relaterade till hanteringen av information i den egna verksamheten i syfte att ta fram skyddsåtgärder. Därmed saknas en samlad formaliserad bild över kommunens informationssäkerhetsrisker.

Granskningen påvisar brister i fråga om kontinuitetsplanering. Ingen central kravställan görs gentemot verksamheterna att kontinuitetsplaner skall tas fram för att kunna bemöta oplanerade avbrott i IT-miljön. Förvaltningarna själva har ändå delvis arbetat fram sådana planer vilket är positivt. Socialförvaltningen har exempelvis en kontinuitetsplan framtagen för hemtjänsten om systemet som inkluderar patientjournaler skulle få driftstopp som heter *"Krisplan för hantering av patientjournal vid cyberattack eller långvarigt driftstopp"*. Enligt intervju återfinns personuppgifter gällande brukare förberedda på USB-stickor, samt reservlaptops, vilket dock inte finns beskrivet i framtagen kontinuitetsplan.

Granskningen visar att det inte reglerats vem/vilka i organisationen som ansvarar för uppföljning och utvärdering av kommunens arbete med informationssäkerhet.

Vi kan inte finna att det inom organisationen genomförs tydliga kontroller att mäta verksamheternas arbete med informationssäkerhet. Enligt genomförda intervjuer sker det inom verksamheten ingen heltäckande uppföljning/utvärdering inom området.

Bedömning

Bedriver verksamhetsorganisationen ett aktivt arbete med informationssäkerhet? Fokus på riskanalys, aktiviteter/åtgärder samt rapportering.

Nej

Bedömningen baseras på följande:

- Arbetet med riskanalys, aktiviteter/åtgärder samt rapportering sker inte på ett systematiskt sätt.
- Kommunens arbete inom området motsvarar inte de krav som anges i lag 2018:1174 om samhällsviktiga tjänster.

För att utveckla området föreslås att det tas fram styrdokument som säkerställer ett systematiskt arbetssätt. Bland annat finns ett behov att formalisera en process för analys av informationssäkerhetsrelaterade risker. Kommunstyrelsen bör även pröva om det ska skapas ett särskilt ledningssystem för informationssäkerhet.

Kommunstyrelsens uppsikt

Revisionsfråga 4: Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?

Iakttagelser

Enligt kommunallagen har kommunstyrelsen ett ansvar att utöva uppsikt över kommunens samtliga angelägenheter. Uppsikten ska bland annat innefatta området informationssäkerhet. Som tidigare nämnts har kommunen en lagstadgad skyldighet att bedriva ett systematiskt arbete med informationssäkerhet.

Granskningen kan inte finna att kommunstyrelsen preciserat formerna för hur den ska utöva uppsikt inom området informationssäkerhet.

En genomgång av kommunstyrelsens sammanträdesprotokoll för kalenderår 2023 visar att kommunstyrelsen inte fått någon heltäckande uppföljning/utvärdering av kommunens arbete med informationssäkerhet.

Granskningen kan inte finna att området informationssäkerhet inkluderats i kommunstyrelsens arbete med intern kontroll, exempelvis uppföljning av arbetsmoment för informationssäkerhet i de styrdokument som finns (läs: *Säkerhetspolicy Användare 2022* och *Riktlinjer Lagring 2022*).

Bedömning

Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?

Nej

Bedömning baseras på följande:

- Kommunstyrelsen har inte reglerat formerna för hur den ska utöva uppsikt inom området informationssäkerhet.
- Kommunstyrelsen kan inte verifiera att den genomfört heltäckande uppföljning/utvärdering inom området under år 2023.

För framtiden föreslås att kommunstyrelsen utvecklar sin uppsikt inom området. Rapporteringen bör fokusera på måluppfyllelse samt verkställighet av beslutade planer.

Avslutning

Sammanfattande revisionell bedömning

Nedan presenteras revisionell bedömning för respektive granskningsområde:

Granskningsområde	Bedömning	
1.Organisation och ansvar	**Nej**	
2. Styrdokument	**Nej**	
3. Systematiskt arbetssätt	**Nej**	
4. Kommunstyrelsens uppsikt	**Nej**	

Utifrån genomförd granskning är vår samlade bedömning att kommunens arbete med informationssäkerhet inte bedrivs med tillräcklig intern kontroll.

Rekommendationer

För att utveckla verksamheten bör följande rekommendationer prioriteras:

- Att kommunstyrelsen ser till att det upprättas interna styrdokument för kommunens arbete med informationssäkerhet, däribland en informationssäkerhetspolicy som beslutas av kommunfullmäktige.
- Att kommunstyrelsen säkerställer att det finns en tydlig ansvarsfördelning för arbetet med informationssäkerhet. Detta gäller såväl inom den politiska organisationen (kommunstyrelse och nämnder) som på verksamhetsnivå.
- Att kommunstyrelsen säkerställer att kommunens arbete inom området sker på ett systematiskt sätt. Styrelsen bör här pröva om kommunen ska införa ett särskilt ledningssystem för informationssäkerhet.
- Att kommunstyrelsen utvecklar sin uppsikt inom området informationssäkerhet. Detta kan exempelvis ske genom att området inkluderas i årshjul för uppföljning/rapportering till styrelsen.

2023-12-12

Pär Koyanagi-Gustafsson ***Bo Rehnberg***

Projektledare *Uppdragsledare*

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av förtroendevalda revisorer i Jokkmokks kommun enligt de villkor och under de förutsättningar som framgår av projektplan från 2023-06-27. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.