Kramfors kommun

Datum
2023-09-20

**Revisionen**

Till:
Kommunstyrelsen
Bildningsnämnden
Produktionsnämnden
Välfärdsnämnden

För kännedom:
Kommunfullmäktiges presidium

# Revisionsrapport ”Uppföljande granskning av informationssäkerhet”

KPMG har på uppdrag av kommunens revisorer genomfört en uppföljande granskning av informationssäkerhet.

Revisionen ser allvarligt på att åtgärder i enlighet med tidigare rekommendationer inte har vidtagits och uppmanar därför kommunstyrelse och nämnder att skyndsamt vidta åtgärder.

Revisionen önskar att kommunstyrelsen och ovanstående nämnder lämnar synpunkter på de slutsatser som finns redovisade i rapporten senast den 22 december 2023. Av svaret bör det framgå vilka eventuella åtgärder som ska vidtas och när de beräknas vara genomförda.

Med vänliga hälsningar

Bertil Böhlin
Ordförande

Postadress
Kramfors kommun
Revisionen
872 80 Kramfors

E-post
kramfors.kommun@kramfors.se

Hemsida
www.kramfors.se

Besöksadress
Torggatan 2

Telefon
0612-800 00

Fax
0612-157 57

Organisationsnr
212000-2429

# Uppföljande granskning av informationssäkerhet

Rapport
Kramfors kommun

KPMG AB

2023-09-20

Antal sidor 15

**Kramfors kommun**
Uppföljande granskning av informationssäkerhet

2023-09-20

# Innehållsförteckning

# 1 Sammanfattning

KPMG har av Kramfors kommuns revisorer fått i uppdrag att följa upp resultatet av tidigare genomförda granskning av informationssäkerhet från 2021. Uppdraget ingår i revisionsplanen för år 2023.

Vår sammanfattande bedömning är att kommunstyrelsen och de nämnder som ingick i den tidigare granskningen inte i tillräcklig omfattning hörsammat de rekommendationer som lämnades vid granskningen av informationssäkerhet från år 2021.

Vi konstaterar att samtliga rekommendationer som lämnades vid den tidigare granskningen kvarstår helt eller delvis, vilket vi betraktar som mycket allvarligt utifrån de informationssäkerhetsrisker som kommunen därvid exponeras för. Flera av de tidigare rekommendationerna avsåg grundläggande aktiviteter för att kommunen ska bedriva ett systematiskt arbete med informationssäkerhet. Att dessa inte hörsammats utsätter kommunen både för ekonomiska risker och risk för förtroendeskada om det skulle visa sig att nuvarande skyddsnivåer inte är tillräckliga för att skydda kommunens informationstillgångar.

Vid den uppföljande granskningens genomförande pågick en organisationsförändring med syfte att stärka arbetet inom säkerhet och beredskap, däribland informationssäkerhet. I intervjuer beskrivs den nya organisationen som en förutsättning för att kommunen ska kunna arbeta vidare med åtgärder inom informationssäkerhet, bland annat de rekommendationer som den tidigare granskningen identifierat. Mot bakgrund av detta ser vi det som väsentligt att kommunstyrelsen följer utvecklingsarbetet och att tillkommande resurser får i uppdrag att påbörja ett förbättringsarbete i enlighet med de rekommendationer och andra åtgärder som kommunen bedömer som nödvändiga för att etablera ett systematiskt och riskbaserat informationssäkerhetsarbete.

Mot bakgrund av genomförd uppföljning konstaterar vi att samtliga rekommendationer kvarstår. Vi rekommenderar därför kommunstyrelsen och att prioritera nedanstående:

- Göra en översyn av styrande dokument så att dessa utgör en sammanhållen helhet för styrningen av kommunens informationssäkerhetsarbete.
- Säkerställa att informationsägarna är medvetna om sitt ansvar och vidtar de åtgärder och aktiviteter som krävs för ett systematiskt informationssäkerhetsarbete för den information de ansvarar för.
- Upprätta en årlig handlingsplan med prioriterade åtgärder och aktiviteter för att utveckla informationssäkerhetsarbetet.
- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- Säkerställa att rutiner och regler finns för behörighetshantering på kommunövergripande nivå.
- Säkerställa att nya och befintliga medarbetare får del av utbildning och information om informationssäkerhet så att en tillräcklig medvetenhet och kunskap finns över enskildas hantering och för att upptäcka incidenter.
- Besluta om kommunövergripande rutin för hantering av informationssäkerhetsincidenter och säkerställa att inträffade incidenter dokumenteras på övergripande nivå samt analyseras och följs upp som en del i det systematiska förbättringsarbetet.
- Säkerställa att uppföljning av beslutad handlingsplan och kommunens informationssäkerhetsarbete sker genom att etablera en årlig rapportering i form av ledningens genomgång till kommunstyrelsen.

Mot bakgrund av genomförd uppföljning tillkommer följande rekommendation till kommunstyrelsen:

- Säkerställa att den planerade organisationsförstärkningen påbörjar ett strukturerat förbättringsarbete inom informationssäkerhet. Exempelvis genom att inkludera informationssäkerhetsrisker i arbetet med internkontroll och löpande följa upp att arbetet leder till önskat resultat.

Mot bakgrund av genomförd uppföljning konstaterar vi att samtliga rekommendationer kvarstår. Vi rekommenderar därför nämnderna att prioritera nedanstående:

- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- Säkerställa att nya och befintliga medarbetare får del av utbildning och information om informationssäkerhet så att en tillräcklig medvetenhet och kunskap finns över enskildas hantering och för att upptäcka incidenter.

Mot bakgrund av genomförd uppföljning rekommenderar vi produktionsnämnden att prioritera:

- Om möjligt utveckla rutiner genom en mer automatiserad process som kvalitetssäkrar hantering, uppföljning samt kontroll av tilldelade behörigheter.

# 2 Bakgrund

## 2.1 Syfte

Det övergripande syftet har varit att bedöma om kommunstyrelse och nämnder har vidtagit åtgärder i enlighet med lämnade rekommendationer för att etablera ett systematiskt och riskbaserat informationssäkerhetsarbete.

De svar vi efterfrågat i uppföljningen har varit:

- Har åtgärder utifrån lämnade rekommendationer vidtagits?
- Har uppföljning av vidtagna åtgärder genomförts?
- Har kommunstyrelsen utifrån den ökade hotbild för cyberhot och attacker som funnits under 2022 och 2023 efterfrågat riskanalys eller presentation över kommunens förmåga att skydda information och upprätthålla verksamhet vid säkerhetshändelser inom IT?

## 2.2 Avgränsning

Uppföljningen avser avlämnad revisionsrapport för granskning av informationssäkerheten från 2021.

## 2.3 Revisionskriterier

Vi har utifrån genomförd granskning efterfrågat svar på åtgärder som vidtagits med anledning av granskningen. Vidare har vi utifrån resultatet begärt att få ta del av revisionsbevis i form av styrdokument, planer och rutiner för att verifiera uppgifter.

## 2.4 Ansvarig styrelse

Granskningen avser kommunstyrelsen och de nämnder som var inkluderade i granskningen 2021.

## 2.5 Metoder

Granskningen har genomförts intervjuer med kommunchef, digitaliseringschef samt representanter från välfärdsförvaltningen. Då inga tillkommande underlag och styrdokument etablerats sedan den tidigare granskningen har ingen dokumentgranskning genomförts.

Samtliga intervjuade har getts möjlighet att faktakontrollera rapporten.

# 3 Resultat av den uppföljande granskningen

## 3.1 Granskning av informationssäkerhet från år 2021

Syftet med granskningen var att granska kommunstyrelsens och samtliga nämnders rutiner för informationssäkerhetsarbetet.

Den sammanfattande bedömning utifrån granskningens syfte var att kommunstyrelsen och nämnderna inte hade säkerställt ett ändamålsenligt och systematiskt arbete med kommunens informationssäkerhet.

## 3.2 Uppföljning år 2023

I nedanstående stycken presenteras granskningens rekommendationer från 2021 samt de åtgärder som intervjupersoner beskriver ha vidtagits sedan dess. Efter beskrivna åtgärder gör vi en bedömning om styrelse och nämnder har vidtagit tillräckliga åtgärder.

I samband med uppföljningsgranskningen beskrev intervjupersoner att det vid tid för granskningen pågick en större organisationsförändring inom Kramfors kommun. Kommunstyrelsen uppdrog under 2022 till kommundirektör att göra en översyn av kommunledningsförvaltningen. Som del i uppdraget har en samordningsfunktion för säkerhet och beredskap tillskapats. Intervjuade uppger att informationssäkerhet ska ingå som ett av flera fokusområden som funktionen ska hantera. Funktionen består av tre personer, men exakta arbetsformer var inte fastställda då den uppföljande granskningen genomfördes. De organisatoriska förändringarna uppges kräva en revidering av reglementet, vilket tros vara genomfört vid årsskiftet 2023/2024.

### 3.2.1 Rekommendation

- Göra en översyn av styrande dokument så att dessa utgör en sammanhållen helhet för styrningen av kommunens informationssäkerhetsarbete.

#### Åtgärd

Vid den tidigare granskningen bedömdes befintliga styrande dokument tydliggöra ansvar och krav för informationssäkerhetsarbetet. Dokumenten var däremot inte implementerade eller tillräckligt kända med följden att det ansvar som de styrande dokumenten beskrev inte efterlevdes.

Enligt intervjupersoner har ett arbete påbörjats med att se över och revidera flera styrdokument. Som exempel nämns *Riktlinjer för informationssäkerhet* och *Tjänsteföreskrift för informationssäkerhet*. Revidering pågår men har inte slutförts. Arbetet beskrivs ha påbörjats för något år sedan, men fått pausats till följd av att tidigare informationssäkerhetssamordnare avslutat sin tjänst och ersättaren ännu inte tillträtt.

#### Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen kvarstår. Vår bedömning är att arbetet behöver prioriteras då adekvata styrdokument ger principiella grunder för informationssäkerhetsarbetet och behövs för att tydliggöra ansvar och vilka aktiviteter som måste genomföras inom respektive verksamhet för att arbetet ska ske på ett systematiskt sätt.

### 3.2.2 Rekommendation

- Säkerställa att informationsägarna är medvetna om sitt ansvar och vidtar de åtgärder och aktiviteter som krävs för ett systematiskt informationssäkerhetsarbete för den information de ansvarar för.

#### Åtgärd

Genom den tidigare granskningen framkom att kommunen i stor utsträckning saknade resurser och funktioner för att bedriva ett systematiskt informationssäkerhetsarbete. Granskningen underströk vikten av att säkerställa informationsägarnas ansvarsägande och att åtgärder för att skydda information vidtogs utifrån behov.

Av intervjuer i den uppföljande granskningen framgår att inget systematiskt arbete genomförts för att öka medvetenheten om ansvar hos informationsägare. På förvaltningsnivå förekommer enskilda initiativ där aktiviteter genomförs, men generellt i kommunen sker inget aktivt arbete med detta. Överlag beskriver intervjuade det har saknats engagemang och kunskap informationssäkerhet vilket resulterat i att arbetet inte kommit igång.

Orsaker som lyfts är både ointresse och begränsad tillgång till personella resurser där arbetet i stor del är personberoende och sårbart.

#### Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte har hörsammats.

### 3.2.3 Rekommendation

- Upprätta en årlig handlingsplan med prioriterade åtgärder och aktiviteter för att utveckla informationssäkerhetsarbetet.

#### Åtgärd

Den tidigare granskningen visade att kommunen saknade en beslutad handlingsplan där kommunstyrelsen prioriterat samt tids- och resurssatt åtgärder för att upprätthålla informationssäkerheten i kommunen.

Någon handlingsplan finns inte heller vid den uppföljande granskningen. Relaterat till den organisationsförändring som vi beskrev i rapportavsnitt *3.2 Uppföljning år 2023* uppges att vissa funktioner, som IT-chef och digitaliseringsansvarig, kommer få ett tydligare ansvar för säkerhetsfrågor kopplat till respektive ansvarsområde. Det framförs även att enheten kommer ha större personella resurser att lägga på informationssäkerhet än vad som tidigare funnits.

#### Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte hörsammats. Med den nya organisationsförändringen bedömer vi att förutsättningar för ett ändamålsenligt informationssäkerhetsarbete förbättrats. Vi anser att en handlingsplan är en grundbult i ett systematiskt arbete med informationssäkerhet varför vi bedömer det angeläget att det pågående riskarbetet utmynnar i en dylik plan med de mest prioriterade åtgärderna för att möta risker och sårbarheter.

### 3.2.4 Rekommendation

- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.

#### Åtgärd

En iakttagelse vid den tidigare granskningen var att kommunen saknade beslutad modell för informationsklassning. Arbetet med informationsklassning var då i en uppstartsfas varvid endast en liten del av kommunens samlade informationsmängd genomgått informationsklassning.

I uppföljande intervjuer framförs att det fortfarande saknas en kommungemensam struktur för informationsklassning. Enligt uppgift har att ett arbete påbörjats med att ta fram en klassningsmodell som bygger på sortering av information utifrån känslighet och som ska beslutas politiskt. Samtidigt lyfts att arbetet är komplext då det involverar personal på övergripande nivå såväl som på verksamhetsnivå.

Likaledes beskrivs att det finns ambitioner om att genomföra en prioritering av system, men att personella resurser begränsat arbetets framdrift.

På operativ nivå tar vi del av arbetssätt som tillämpas i, vad som benämns som, brist på en kommungemensam klassningsmodell. Ett av dessa arbetssätt är ”Ordnat införande” som används vid införandet av nya system. Arbetssättet liknas vid en slags checklista där ett antal förutsättningar ska vara uppfyllda före avtalsskrivande, som att systemet ska vara klassat, att analyser av nödvändiga integrationer ska ha genomförts och att systemförvaltarplan ska finnas. Syftet framställs vara att stärka kontrollen av nya system genom att beakta alla aspekter av införandet innan beslutet om att köpa systemet väl tas.

I fråga om informationsklassning är välfärdsförvaltningen den förvaltning som hanterar störst volym klassad information. Intervjuade förvaltningsrepresentanter upplever att stort ansvar för informationsklassning åvilar varje enskild förvaltning i avsaknad av en gemensam modell för informationsklassning.

## Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen hörsammats i viss utsträckning. Vår bedömning är att det framför allt är enskilda förvaltningar som hittat arbetsformer och metoder för klassning samt att det främst genomförs som en del i upphandling av nya system.

### 3.2.5 Rekommendation

- Säkerställa att rutiner och regler finns för behörighetshantering på kommunövergripande nivå. Rutiner bör om möjligt utvecklas genom en mer automatiserad process som kvalitetssäkrar hantering, uppföljning samt kontroll av tilldelade behörigheter.

#### Åtgärd

Utifrån iakttagelser vid den tidigare granskningen bedömdes hanteringen kring behörigheter vara personberoende och den manuella hanteringen vid tiden innebära viss risk. Förändringar kunde bli fördröjda eller riskerades inte uppmärksammas i tillräckligt hög grad. Vidare visade granskningen att styrande dokument avseende åtkomsthantering saknades, vilket av intervjuade ansågs skapa en osäker process som riskerade leda till att obehöriga personer kunde få åtkomst till information.

Det framkommer vid den uppföljande granskningen att behörigheter tidigare godkändes mer godtyckligt medan förfarandet numera uppges bygga på systematik och struktur. På kommunens intranät lanserades i början på 2023 en e-tjänst för ansökningar från personal som önskar systembehörighet utöver de standardbehörigheter som respektive anställningskategori medger. Ansökan når sedan närmaste chef för beslut samt till systemförvaltare för verkställande. Syftet uppges vara att säkerställa spårbarhet kring vem som delger och delges behörigheter.

Vidare framförs att IT-avdelningen, digitaliseringsenheten och HR-avdelningen tillsammans initierat en översyn av hela anställningsprocessen utifrån ett systemperspektiv. Arbetet syftar till att försöka automatisera och säkerställa adekvat kontohantering vid nyanställningar, byte av anställning samt avslut av anställning. Utgångspunkt för arbetet beskrivs vara de rekommendationer som Integritetsmyndigheten ger (tidigare Datainspektionen).

#### Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen delvis hörsammats. Det är dock väsentligt att översynen av anställningsprocessen slutförs och ligger till grund för en strukturerad behörighetshantering som stöds av dokumenterade rutiner.

### 3.2.6 Rekommendation

- Säkerställa att nya och befintliga medarbetare får del av utbildning och information om informationssäkerhet så att en tillräcklig medvetenhet och kunskap finns över enskildas hantering och för att upptäcka incidenter.

#### Åtgärd

Enligt vad som framkom vid den tidigare granskningen hade utbildning och information avseende informationssäkerhet inte erbjudits i tillräcklig omfattning för att uppnå en grundläggande kunskapsnivå inom området. Detta bedömdes kunna leda till en säkerhetsrisk då oaktsamhet hos enskilda kan utsätta IT-miljön och kommunens informationstillgångar för sårbarheter.

I likhet med vad som uppgavs vid den tidigare granskningen erbjuder kommunen fortfarande så kallade Nano-utbildningar (kortare digitala utbildningssessioner som sänds ut via e-post) inom informationssäkerhet. Utbildningen genomfördes senast under hösten 2022 och avses repeteras under hösten 2023. Något korrekt statistikunderlag för att följa upp deltagarantalet från 2022 finns inte, men uppfattningen är att deltagandet var högt.

Därtill framgår att diskussioner pågår mellan HR-avdelningen och digitaliseringsenheten kring hur utbildningen kan bli en del av den formella introduktionen för nya medarbetare.

På verksamhetsnivå uppges utbildningen fylla ett visst behov för framför allt administrativa tjänstepersoner, men intervjuade verksamhetsföreträdare anser den inte tillräckligt verksamhetsnära för att vara fullt ut relevant inom hela organisationen. Som komplettering till den kommunövergripande utbildningen har välfärdsförvaltningen satt ihop eget, verksamhetsanpassat utbildningsmaterial, som samtliga medarbetare tagit del av. Resultatet från utbildningarna beskrivs sedan ha sammanställts per enhet och använts som underlag till mer gruppanpassade utbildningar.

#### Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen delvis hörsammats.

### 3.2.7 Rekommendation

- Besluta om kommunövergripande rutin för hantering av informationssäkerhetsincidenter och säkerställa att inträffade incidenter dokumenteras på övergripande nivå samt analyseras och följs upp som en del i det systematiska förbättringsarbetet.

#### Åtgärd

Enligt dokument som delgavs vid den tidigare granskningen fanns rutiner för incidenthantering. Via iakttagelser framkom emellertid att rutinen inte efterlevdes samt att det förelåg en stor risk att incidenter inte rapporterades. Detta på grund av att systemet för incidentanmälningar ansågs svårhanterat samt att det uppfattades råda en kultur där incidenter betraktades som bestraffningar snarare än grund för förbättringar.

Den uppföljande granskningen visar att samma rutin för incidenthantering som fanns vid den tidigare granskningen ännu används.

#### Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte hörsammats.

### 3.2.8 Rekommendation

- Säkerställa att uppföljning av beslutad handlingsplan och kommunens informationssäkerhetsarbete sker genom att etablera en årlig rapportering i form av ledningens genomgång till kommunstyrelsen.

#### Åtgärd

Av den föregående granskningen framkom att det inte skedde någon systematisk uppföljning enligt vad som stipulerades av kommunens interna riktlinjer. Enligt dessa ska kommunstyrelsen en gång om året informera sig om informationssäkerhetsarbetet i förvaltningarna. Utifrån uppföljningen ska kommunstyrelsen besluta om åtgärder för att förbättra informationssäkerheten samt tilldelning av resurser, enligt vad som angavs av riktlinjen.

I de intervjuer som gjorts inom ramen för den uppföljande granskningen förmedlas ingen kännedom om uppföljning eller åtgärder som beslutats till följd av detta. Generellt uppfattas informationssäkerhetsarbetet inom kommunen sakna struktur och gemensamma former. Det förs fram att kommunen anlitat ett externt dataskyddsombud på konsultbasis, vilken varit ett bra stöd i det dagliga arbetet med personuppgiftsfrågor.

Däremot har strategiska frågor på kommunövergripande nivå inte hanterats, där helhetssyn och systematik avseende informationssäkerhetsfrågor uppges saknas och därigenom påverkar informationssäkerheten på ett negativt sätt.

#### Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte hörsammats.

### 3.2.9 Tillkommande frågeställning i uppföljande granskning

- Har kommunstyrelsen utifrån den ökade hotbild för cyberhot och attacker som funnits under 2022 och 2023 efterfrågat riskanalys eller presentation över kommunens förmåga att skydda information och upprätthålla verksamhet vid säkerhetshändelser inom IT?

#### Åtgärd

Intervjuade har inte kännedom om kommunstyrelsen efterfrågat information om hot eller risker för kommunen, exempelvis om de skulle drabbas av en cyberattack. Den generella medvetenheten kring informationssäkerhetsfrågor påtalas ha höjts efter bland annat IT-attacken mot Kalix kommun. I samband med händelsen etablerades bland annat en krisgrupp för kontinuitet men som nu har avslutats.

Det operativa arbetet beskrivs främst rapporteras till produktionsnämnden. Detta görs av funktioner som inte varit inkluderade i granskningen (it-driftspersonal). Vi har av protokollsgenomläsning kunnat ta del av att kommunstyrelsen hanterat fråga om samhällsviktiga system, dock är protokollet maskerat med hänvisning till sekretess.

Vidare anges av intervjuade att den nya säkerhets- och beredskapsenheten genomfört en risk- och sårbarhetsanalys där informationssäkerhet pekats ut som ett av 13 prioriterade områden. I intervju konstateras att det finns en medvetenhet om att kommunens arbete med informationssäkerhet inte är tillräckligt. Som exempel relaterar intervjupersoner till de risker och rekommendationer som den tidigare granskningen identifierade.

Intervjuade lyfter att it-infrastrukturella säkerhetsåtgärder vidtagits utifrån aktuella hot och risker. Bland annat för kommunens servrar samt nya rutiner för backup på känslig information. Detta har finansierats genom beredskapspengar som kommunen erhållit samt inom it-avdelningens investeringsbudget.

#### Bedömning

Vi bedömer att kommunstyrelsen till viss del har bedömt informationssäkerhetsrisker som del i övergripande risk- och sårbarhetsanalys. Kommunen har därtill vidtagit ett antal tekniska säkerhetsåtgärder som följd av externa hot och risker. Vi vill dock påtala att det utan ett systematiskt informationssäkerhetsarbete med informationsklassning för information och informationstillgångar inte kan säkerställas att det finns ett tillräckligt skydd. Vi anser att kommunstyrelsen bör utvärdera nuvarande resurser och kompetens i linjen samt inom it-avdelningen så det finns tillräckliga förutsättningar att genomföra informationssäkerhetsarbetet i förhållande till behov och risker.

## 3.3 Samlad bedömning och rekommendationer

Vår sammanfattande bedömning är att kommunstyrelsen och de nämnder som ingick i den tidigare granskningen inte i tillräcklig omfattning hörsammat de rekommendationer som lämnades vid granskningen av informationssäkerhet från år 2021.

Vi konstaterar att samtliga rekommendationer som lämnades vid den tidigare granskningen kvarstår helt eller delvis, vilket vi betraktar som mycket allvarligt utifrån de informationssäkerhetsrisker som kommunen därvid exponeras för. Flera av de tidigare rekommendationerna avsåg grundläggande aktiviteter för att kommunen ska bedriva ett systematiskt arbete med informationssäkerhet. Att dessa inte hörsammats utsätter kommunen både för ekonomiska risker och risk för förtroendeskada om det skulle visa sig att nuvarande skyddsnivåer inte är tillräckliga för att skydda kommunens informationstillgångar.

Det förekommer enskilda initiativ inom informationssäkerhetsarbete på förvaltningsnivå men även de som har ett pågående arbete saknar styrning och gemensamma arbetsformer och metoder. Detta befäster ytterligare vikten av styrande och stödjande dokument med kommungemensamma principer som kan sätta former för ett sammanhållet informationssäkerhetsarbete.

Mot bakgrund av genomförd uppföljning konstaterar vi att samtliga rekommendationer kvarstår. Vi rekommenderar därför kommunstyrelsen och att prioritera nedanstående:

- Göra en översyn av styrande dokument så att dessa utgör en sammanhållen helhet för styrningen av kommunens informationssäkerhetsarbete.
- Säkerställa att informationsägarna är medvetna om sitt ansvar och vidtar de åtgärder och aktiviteter som krävs för ett systematiskt informationssäkerhetsarbete för den information de ansvarar för.
- Upprätta en årlig handlingsplan med prioriterade åtgärder och aktiviteter för att utveckla informationssäkerhetsarbetet.
- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- Säkerställa att rutiner och regler finns för behörighetshantering på kommunövergripande nivå.

- Säkerställa att nya och befintliga medarbetare får del av utbildning och information om informationssäkerhet så att en tillräcklig medvetenhet och kunskap finns över enskildas hantering och för att upptäcka incidenter.
- Besluta om kommunövergripande rutin för hantering av informationssäkerhetsincidenter och säkerställa att inträffade incidenter dokumenteras på övergripande nivå samt analyseras och följs upp som en del i det systematiska förbättringsarbetet.
- Säkerställa att uppföljning av beslutad handlingsplan och kommunens informationssäkerhetsarbete sker genom att etablera en årlig rapportering i form av ledningens genomgång till kommunstyrelsen.

Mot bakgrund av genomförd uppföljning tillkommer följande rekommendation till kommunstyrelsen:

- Säkerställa att den planerade organisationsförstärkningen påbörjar ett strukturerat förbättringsarbete inom informationssäkerhet. Exempelvis genom att inkludera informationssäkerhetsrisker i arbetet med internkontroll och löpande följa upp att arbetet leder till önskat resultat.

Mot bakgrund av genomförd uppföljning konstaterar vi att samtliga rekommendationer kvarstår. Vi rekommenderar därför nämnderna att prioritera nedanstående:

- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- Säkerställa att nya och befintliga medarbetare får del av utbildning och information om informationssäkerhet så att en tillräcklig medvetenhet och kunskap finns över enskildas hantering och för att upptäcka incidenter.

Mot bakgrund av genomförd uppföljning rekommenderar vi produktionsnämnden att prioritera:

- Om möjligt utveckla rutiner genom en mer automatiserad process som kvalitetssäkrar hantering, uppföljning samt kontroll av tilldelade behörigheter.

**Kramfors kommun**
Uppföljande granskning av informationssäkerhet

2023-09-20

2023-09-20

KPMG AB

Sofie Ernerudh
*Kommunal revisor*

Jenny Thörn
*Kommunal revisor*

Lena Medin
*Certifierad kommunal revisor*
*Kundansvarig*