Bollebygds kommun

Granskning av informationssäkerhet

April 2023

Uppdragsledare: Marie Lindblad, marie.lindblad@pwc.com
Projektledare: Charlotte Arnell, charlotte.arnell@pwc.com
Projektmedlem: Markus Månsson, markus.maansson@pwc.com

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Bollebygds kommun genomfört en granskning av kommunens styrning av informationssäkerhetsarbetet. Granskningens syfte är att bedöma om kommunstyrelsen säkerställer att styrningen av informationssäkerhetsarbetet är ändamålsenlig och om detta sker med tillräcklig intern kontroll.

Utifrån genomförd granskning är vår samlade bedömning att kommunstyrelsen **inte helt** säkerställer en ändamålsenlig styrning och att tillräcklig uppföljning och intern kontroll **ej sker**.

Granskningen har utgått från fyra revisionsfrågor. Nedan anges bedömning för respektive revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten samt det avslutande avsnittet “Samlad bedömning”.

Revisionsfrågor	**Bedömning**
Finns ändamålsenlig styrande informationssäkerhetsdokumentation?	**Delvis** 
Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?	**Delvis** 
Sker uppföljningen av informationssäkerhetsarbetet på ett ändamålsenligt sätt?	**Nej** 
Finns ett ändamålsenligt ledningssystem för informationssäkerhet?	**Nej** 

Rekommendationer

Efter genomförd granskning rekommenderar vi kommunstyrelsen att vidta åtgärder för att stärka kommunens ledning, styrning och uppföljning av informationssäkerhetsarbetet. Nedan redovisas konkretiserade rekommendationer:

- De nu gällande dokumenten policy och riktlinje för informationssäkerhet och dataskydd bör kompletteras och i vissa delar konkretiseras för att bli ändamålsenliga. Detta exempelvis för områden som kontinuitetsplanering, behörighetshantering, informationsklassning, riskhantering och incidenthantering. De styrande dokumenten bör sedan implementeras och förankras i verksamheterna.
- Tydliggör roller och ansvar (inkl. mandat) för arbetet med informationssäkerhet. Detta bör finnas dokumenterat på en övergripande nivå i antingen policyn eller riktlinjen för informationssäkerhet och dataskydd, och sedan konkretiseras i underliggande dokument (exempelvis i en instruktion).
- Säkerställ att arbetet med att identifiera och klassa information fortskrider samt färdigställs. Adekvata säkerhetsåtgärder i linje med genomförd informationsklassning bör även identifieras och implementeras.
- Säkerställ att riskanalyser avseende informationssäkerhet genomförs och att skyddsåtgärder vidtas för att skydda information, verksamhet, IT-system, processer och motsvarande.
- Riskanalyserna och informationsklassningarna bör i större utsträckning vara styrande för det operativa IT-arbetet, både i den centrala förvaltningen och i övriga verksamheter. Exempel på sådan styrning kan vara checklistor för hur införskaffandet av ett nytt IT-verktyg ska gå till eller fastslagna beslutsprocesser för olika former av förändringar kopplat till IT-miljö och IT-verktyg.
- Fortsätt arbetet med att etablera och färdigställa kontinuitetsplaner för kritiska delar av verksamheten. Återställningsplaner för kritiska system bör etableras samt testas på regelbunden basis.
- Säkerställ att en systematisk uppföljning av arbetet med informationssäkerhet upprättas och genomförs på regelbunden basis. Uppföljningen behöver vara förankrad både i tjänstemannaorganiationen, och formaliserad genom exempelvis återrapportering till kommunstyrelse.

1

Inledning

Inledning

Bakgrund

Kommuner har ett av det svenska samhällets mest komplexa uppdrag, detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. Brister i hantering av information inom dessa verksamheter kan leda till försämrat förtroende för både den enskilda aktören men även samhället i stort. I de flesta fall är även verksamheterna mer eller mindre beroende av information, oftast i digital form, för att kunna klara sitt uppdrag. Informationen som en kommun ansvarar för är dessutom en tillgång med ett betydande ekonomiskt värde. Det innebär att det finns starka ekonomiska och strategiska skäl att säkerställa ett ändamålsenligt skydd för informationen.

Det övergripande syftet med informationssäkerhet är att säkerställa att information för medarbetare, medborgare och andra intressenter hanteras så att tillgänglighet, riktighet, konfidentialitet och spårbarhet kan säkerställas. Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering, vilket i sin tur skapar förtroende både internt och externt samt är en förutsättning för att organisationen ska kunna leverera ett fullgott skydd.

Revisorerna har utifrån sin riskanalys beslutat att granska informationssäkerhetsarbetet.

Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelsen säkerställer att styrningen av informationssäkerhetsarbetet är ändamålsenlig och om detta sker med tillräcklig intern kontroll.

Granskningen besvaras med följande revisionsfrågor:

Revisionsfrågor:

1. Finns ändamålsenlig styrande informationssäkerhetsdokumentation?
2. Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?
3. Sker uppföljningen av informationssäkerhetsarbetet på ett ändamålsenligt sätt?
4. Finns ett ändamålsenligt ledningssystem för informationssäkerhet?

Revisionskriterier

- Kommunallagen
- Offentlighet- och sekretesslagen och annan relevant sekretesslagstiftning
- Den allmänna dataskyddsförordningen (GDPR) och annan relevant dataskyddslagstiftning
- NIS-direktivet med tillhörande relevant lagstiftning
- Övriga föreskrifter, allmänna råd och standarder avseende informationssäkerhet från ex. Myndigheten för samhällsskydd och beredskap samt Integritetsskyddsmyndigheten

Metod

Granskningen sker genom studier av styrdokument, beslut och beslutsunderlag samt ett mindre antal samtal/intervjuer med nyckelpersoner. De funktioner som intervjuats inom ramen för granskningen är följande:

- Informationssäkerhetssamordnare
- IT-samordnare
- Kommundirektör

De intervjuade har getts möjlighet att faktagranska denna rapport.

2

Granskningsresultat

Revisionsfråga 1: Finns ändamålsenlig styrande informationssäkerhetsdokumentation?

Iaktagelser

Av granskningen framgår att en policy för informationssäkerhet och dataskydd för Bollebygds kommun finns etablerad och antagen av kommunfullmäktige. Dokumentet antogs i maj 2022 och innehåller kommunens viljeinriktning och övergripande principer gällande informationssäkerhetsarbetet och personuppgiftshanteringen i kommunen.

Utöver policyn har kommunen även antagit en riktlinje för informationssäkerhet, en digitaliseringsstrategi (där informationssäkerhet är med som ett perspektiv) samt en rutin för hantering av personuppgiftsincidenter. Riktlinjen innehåller exempelvis styrande principer avseende informationsklassning samt mål för arbetet med informationssäkerhet. Både policy, riktlinje och rutinen är relativt övergripande, även avseende konkreta, operativa frågor. Rutinen innehåller bland annat följande skrivning “Informationssäkerhetsansvarig och ansvarig chef för den verksamhet där incidenten skett tar ansvar i frågan och minimerar skadan” men det framgår inte hur eller vilken funktion som faktiskt ansvarar för att utreda och ta beslut om anmälan av incidenten.

Det saknas styrande principer och dokument för flera områden, såsom behörighetshantering, incidenthantering, riskhantering och kontinuitetshantering. Detta är viktiga områden att få på plats för att uppnå ett ändamålsenligt arbete med informationssäkerhet. Vid intervjuerna framgår att det finns en medvetenhet om detta, och att kommunen arbetar stegvis för att etablera fler styrande dokument.

I policy för informationssäkerhet anges att förvaltningarna har till ansvar att arbeta fram egna rutiner för arbetet med informationssäkerhet. Under intervju framgår att rutiner ännu inte har etablerats inom förvaltningarna, men att detta arbete nyligen har påbörjats.

Bedömning

Delvis

Bedömningen baseras på att:

- Informationssäkerhetspolicy och riktlinje för informationssäkerhet finns antagna.
- Ändamålsenliga riktlinjer och instruktioner avseende exempelvis behörighetshantering, incidenthantering, klassning av information, kontinuitetshantering och riskhantering saknas.
- Det finns en avsaknad av ändamålsenliga instruktioner och rutiner relaterat till informationssäkerhet på förvaltningarna.
- De existerande styrande dokumenten är i vissa delar alltför otydliga för att utgöra effektiva styrande dokument. Åtminstone så länge de inte kompletteras av tydliga och konkreta instruktioner och beskrivningar för det operativa arbetet.

Avsaknaden av ändamålsenliga riktlinjer och instruktioner på en operativ nivå medför risk att det blir otydligt vad som ska göras för att uppfylla viljeyttringen i kommunens informationssäkerhetspolicy. Detta medför i sin tur risk för att det uppstår brister i kommunens operativa arbete med informationssäkerhet.

Revisionsfråga 2: Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?

Iaktagelser

I kommunens policy för informationssäkerhet beskrivs fördelning av roller och ansvar i arbetet med informationssäkerhet på en övergripande nivå. Ansvaret anges för kommunfullmäktige, kommunstyrelsen och för nämnder/förvaltningar. Kommunen har en informationssäkerhetssamordnare utsedd i kommunen som har en central roll i att driva arbetet med informationssäkerhet. Beskrivning av ansvaret för denna roll saknas dock i de styrande dokumenten.

I policyn anges att nämnder med förvaltning ansvarar för informationsägarskapet inom ramen för sina verksamheter och att informationsägaren har det yttersta ansvaret för sin information. Under intervjuer framgår att det finns ett behov av att tydliggöra ansvaret för informationsägare i kommunen, vilket är roller som innehas av förvaltningscheferna. Det finns även ett behov av att stärka förvaltningarnas ägarskap avseende arbetet med informationssäkerhet.

Under intervjuer framgår att det finns en otydlighet avseende vem som har det övergripande ansvaret för att styra, bedriva och utveckla arbetet med IT-säkerhet på tjänstemannanivå. Kommunen saknar även en modell för systemförvaltning, även om det finns utsedda systemägare. Ansvaret för systemägare ur ett informationssäkerhetsperspektivet saknas dock i policyn för informationssäkerhet.

Bedömning

Delvis

Bedömningen baseras på att:

- En övergripande beskrivning av roller och ansvar finns i policyn för informationssäkerhet.
- Det finns en informationssäkerhetssamordnare utsedd på kommunövergripande nivå.
- Beskrivning av ansvar saknas för exempelvis kommundirektör, informationssäkerhetssamordnare och systemägare.
- Det saknas tydlighet avseende vad “informationsägarskap” konkret innebär, och vilka aktiviteter och åtgärder som förväntas av informationsägaren.
- Det finns en viss otydlighet avseende vem som har det övergripande ansvaret för att styra, bedriva och utveckla arbetet med IT-säkerhet på tjänstemannanivå.
- Kommunstyrelsens delegationsordning saknar delegation avseende IT-förvaltning, incidenter och andra frågor relaterade till informationssäkerhet, både på operativ och strategisk nivå.

Revisionsfråga 3: Sker uppföljningen av informationssäkerhetsarbetet på ett ändamålsenligt sätt?

Iaktagelser

I kommunens policy för informationssäkerhet och dataskydd anges att efterlevnaden av informationssäkerhetspolicyn och riktlinjer för informationssäkerhet regelbundet ska följas upp. Även i riktlinjerna för informationssäkerhet anges målsättningen att informationssäkerheten som en del av den ordinarie verksamhetsredovisningen ska följas upp på central nivå och inom respektive nämnd. Vidare anges det i policyn att Informationssäkerhetssamordnare en gång per år ska rapportera läge och status gällande informationssäkerhet till kommunstyrelsen.

Under intervju framgår att uppföljning av verksamheternas arbete med informationssäkerhet inte följs upp, varken på central nivå eller inom respektive nämnd/förvaltning. Det framgår även att informationssäkerhetssamordnaren ännu inte har rapporterat läge och status avseende informationssäkerhet till kommunstyrelsen.

Kommunens informationssäkerhetssamordnare har regelbundna avstämningar och möten med kommundirektören för att stämma av arbetet med informationssäkerhet. Det framgår också av intervju att informationssäkerhetssamordnaren rapporterar till kommunens ledningsgrupp var sjätte vecka, exempelvis kring rapporterade incidenter.

I kommunstyrelsens internkontrollplan för 2022 ingår kontroll av röjande av känsliga personuppgifter eller sekretessuppgifter. I delårsrapporten per augusti 2022 framgår att inga incidenter har rapporterats under 2022, men att det sannolikt inte beror på att det i realiteten inte skett några incidenter utan snarare på okunskap bland kommunens medarbetare och brist på en tydlig rutin för rapportering.

Bedömning

Nej

Bedömningen baseras på att:

- Uppföljning av verksamheternas arbete med informationssäkerhet genomförs ej. Detta medför risk för att kommunens policy och riktlinje för informationssäkerhet inte efterlevs och att kommunens arbete med informationssäkerhet inte är ändamålsenligt.
- Informationssäkerhetssamordnaren har vid tidpunkten för denna granskning inte rapporterat läge och status avseende informationssäkerhet till kommunstyrelsen, så som anges i policyn..
- Det är positivt att en kontrollpunkt kopplat till informationssäkerhet finns med i internkontrollplanen. I uppföljningen konstateras inga brister, men också att detta sannolikt inte stämmer med den verkliga situationen. Det är sannolikt en korrekt iakttagelse, men det innebär också att åtgärder behöver vidtas för få vetskap om den reella statusen avseende incidenter. I annat fall är det tveksamt om kommunstyrelse har erforderlig kontroll över verksamheten och utifrån det kan ta beslut om nödvändiga åtgärder.
- Utifrån bristen på uppföljning, både inom kommunstyrelsens egna verksamhet men även i relation till övriga nämnders verksamhet, bedömer vi det som tveksamt om kommunstyrelsen lever upp till den uppsiktsplikt och överblick som stadgas i kommunallagen.

Revisionsfråga 4: Finns ett ändamålsenligt ledningssystem för informationssäkerhet?

Iaktagelser

Ett ledningssystem för informationssäkerhet (LIS) är ett stöd för hur informationssäkerhetsarbetet styrs och systematiskt bedrivs i en organisation. Ett LIS kan vara utformat på flera sätt, men vanligtvis är styrande dokument, informationssäkerhetsmål samt arbete med informationsklassning och informationssäkerhetsrisker, centrala delar i styrningen av arbetet med informationssäkerhet. För att ett LIS (exempelvis i linje med ISO 27001) ska anses vara implementerat är det viktigt att ledningssystemet är en integrerad del av organisationens processer och övergripande ledningsstruktur. Det är också viktigt att arbetet med informationssäkerhet följs upp och att ständiga förbättringar genomförs systematiskt.

Enligt kommunens policy för informationssäkerhet ska arbetet med informationssäkerhet ske med ISO 27000 som grund. Under intervjuer framgår att ett ledningssystem för informationssäkerhet inte finns implementerat, även om vissa delar är påbörjade.

Utifrån iakttagelserna i revisionsfråga 1-3 noterar vi att informationssäkerhetsarbetet inte är en del av kommunens övergripande styrningsprocesser, ett systematiskt förbättrings- och aktualitetsarbete är inte påbörjat och det sker ännu i princip ingen uppföljning.

Bedömning

Nej

Bedömningen baseras på att:

- Den samlade bedömningen av revisionsfrågorna 1-3.
- Styrande dokumentation finns endast på övergripande nivå och efterlevnaden behöver stärkas i kommunens verksamheter.
- Arbetet med informationsklassning har påbörjats, men sker inte systematiskt eller på ett etablerat sätt. Riskanalyser har ej genomförts.
- Övergripande informationssäkerhetsmål finns angivet i riktlinjerna för informationssäkerhet. Ett systematiskt arbete med att följa upp målen finns dock inte på plats.
- Uppföljning av verksamheternas arbete med informationssäkerhet genomförs ej och rapportering till kommunstyrelsen sker ej systematiskt. Avstämning mellan informationssäkerhetssamordnaren och kommundirektör och ledningsgrupp sker dock kontinuerligt.

3

Samlad bedömning

Samlad bedömning

Granskningens syfte är att bedöma om kommunstyrelsen säkerställer att styrningen av informationssäkerhetsarbetet är ändamålsenlig och om detta sker med tillräcklig intern kontroll. Utifrån genomförd granskning är vår samlade bedömning att kommunstyrelsen **delvis** säkerställer en ändamålsenlig styrning men att tillräcklig uppföljning och intern kontroll **inte sker**.

Vi noterar att arbetet med att etablera ett systematiskt arbetssätt och ett LIS är påbörjat. Vid intervjuerna noteras även en berömvärd insikt om brister avseende informationssäkerhetsarbetet och om angelägenheten av ett väl fungerande sådant arbete. Dock behöver de insikterna i högre grad konkretiseras i specifik styrning och uppföljning av området för att styrningen ska bli ändamålsenlig.

Revisionsfrågor	Bedömning	
1. Finns ändamålsenlig styrande informationssäkerhetsdokumentation?	**Delvis** - Informationssäkerhetspolicy och riktlinje för informationssäkerhet finns antagna. Ändamålsenliga riktlinjer avseende behörighetshantering, incidenthantering, riskhantering och kontinuitetshantering saknas. Det saknas även instruktioner och rutiner relaterat till informationssäkerhet på förvaltningarna. Detta innebär att det finns viss styrande dokumentation på övergripande nivå, men dokumenterad styrning på operativ nivå saknas. Styrningen på operativ nivå är nödvändig för att informationshanteringen ska kunna ske på ett tillräckligt säkert sätt, och därför utgör avsaknaden av densamma en betydande brist.	
2. Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?	**Delvis** - En övergripande beskrivning av roller och ansvar finns i policyn för informationssäkerhet. Beskrivning av ansvar saknas för exempelvis kommundirektör, informationssäkerhetssamordnare och systemägare. Det är också otydligt vad de olika ansvaren och rollerna konkret innebär. Sammantaget innebär detta en risk för att nödvändiga aktiviteter och åtgärder inte genomförs alls eller fördröjs.	
3. Sker uppföljningen av informationssäkerhetsarbetet på ett ändamålsenligt sätt?	**Nej** - Uppföljning av verksamheternas arbete med informationssäkerhet genomförs i princip inte. Informationsäkerhetssamordnaren har vid denna granskning inte rapporterat läge och status avseende informationssäkerhet till kommunstyrelsen. Utifrån bristen på uppföljning, både inom kommunstyrelsens egna verksamhet men även i relation till övriga nämnders verksamhet, bedömer vi det som tveksamt om kommunstyrelsen lever upp till den uppsiktsplikt och överblick som stadgas i kommunallagen.	
4. Finns ett ändamålsenligt ledningssystem för informationssäkerhet?	**Nej** - Styrande dokumentation finns endast på övergripande nivå och efterlevnaden behöver stärkas i kommunens verksamheter. Arbetet med informationsklassning har påbörjats, men har ej färdigställts. Riskanalyser har ej genomförts. Systematisk uppföljning av arbetet med informationssäkerhet sker ej på ett ändamålsenligt sätt.	

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Bollebygds kommun enligt de villkor och under de förutsättningar som framgår av projektplan från den 21 oktober 2022. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.

2023-04-21

Marie Lindblad	**Charlotte Arnell**
Uppdragsledare	Projektledare

4

Bilagor

Granskad dokumentation

Dokument	Beslutad
Policy för informationssäkerhet och dataskydd	2022-05-05, KF § 49
Riktlinjer för informationssäkerhet och dataskydd	2022-06-14, KS § 139
Beslutad rutin vid personuppgiftsincident	2022-10-11, fastställd av kommundirektör
Digitaliseringsstrategi	2018-06-14, KF § 65
Delårsrapport augusti 2022, kommunstyrelsen	2022-09-27, KS § 192
Verksamhetsplan och budget 2022 för kommunstyrelsen	2022-01-25 KS § 15
Handlingsplan för informationssäkerhet och dataskydd i Bollebygds kommun	Endast utkast, ej beslutat