Granskning av informationssäkerhet

Högsby kommun

December 2022

Markus Månsson

Martin Lundin

pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Högsby kommun genomfört en granskning av kommunens arbete med informationssäkerhet. Granskningens syfte är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhets-arbete och om detta sker med tillräcklig intern kontroll.

Utifrån genomförd granskning är vår samlade bedömning att Högsby kommuns kommunstyrelse **inte helt** säkerställer ett ändamålsenligt informationssäkerhetsarbete och att det inte sker med tillräcklig intern kontroll.

Nedan delges bedömning för respektive revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten eller det avslutande avsnittet "Sammanfattande bedömningar utifrån revisionsfrågor".

Revisionsfrågor	Bedömning
Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?	Delvis
Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?	Delvis
Finns ett ledningssystem för informationssäkerhet implementerat?	Delvis
Arbetar informationssäkerhetsorganisationen aktivt med efterlevnad av informationssäkerheten?	Nej
Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet?	Nej

Rekommendationer

Vi rekommenderar kommunstyrelsen följande:

- Intensifiera arbetet med att förtydliga och förankra roller och ansvar inom informationssäkerhet i kommunens verksamheter.
- Öka medvetenheten kring de styrande dokumenten för informationssäkerhet och förankra dess innehåll för att stärka efterlevnaden.
- Säkerställ att tillämpningsanvisningen som beskriver roller- och ansvar för informationssäkerhet färdigställs, förankras och beslutas.

- Säkerställ att kommunens informationstillgångar identifieras, klassificeras samt skyddas på ett ändamålsenligt sätt.
- Säkerställ att analys av informationssäkerhetsrisker genomförs systematiskt i kommunens verksamheter.
- Etablera övergripande mål för informationssäkerhet. Målen bör följas upp på regelbunden basis och åtgärdsplaner för att hantera avvikelser bör upprättas.
- Etablera styrande principer för hur informationssäkerhetsincidenter ska hanteras.
- Säkerställ att kontinuitetsplaner för att upprätthålla verksamheten vid olika typer av avbrott etableras. Återställningsplaner för kritiska system bör också etableras.
- Stärk förmågan att ställa krav på leverantörer ur ett informationssäkerhetsperspektiv.
- Etablera en process för att följa upp efterlevnad av de styrande dokumenten för informationssäkerhet på regelbunden basis.
- Säkerställ att medarbetare erbjuds utbildning inom informationssäkerhet. Utbildningarna bör innehålla grundläggande delar samt delar som är anpassade utifrån roll. Att utbildningarna genomförs bör även följas upp på årlig basis.
- Överväg att utforma avsnitt 7 i riktlinjerna för informationssäkerhet till ett eget dokument då denna information berör alla medarbetare. Detta för att underlätta för medarbetare att ta till sig informationen. Informationen i detta avsnitt bör därefter kommuniceras till kommunens medarbetare.
- Säkerställ att kommunens forum/råd för informationssäkerhet etableras för att på så sätt stärka samordningen, etablera gemensamma arbetssätt och sprida goda exempel relaterat till arbetet med informationssäkerhet inom kommunen.

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 leder till ett försämrat förtroende för tjänster och bakomliggande aktörer. Förtroendet för en organisation tar lång tid att bygga upp, men kan snabbt raseras av en enskild informationssäkerhetsincident.

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

Information är värdefull och behöver många gånger skyddas. 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.

Utmaningar gällande informationssäkerhet har även resulterat i NIS-direktivet, som i korthet innebär krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga- och vissa digitala tjänster, både för privata och offentliga aktörer. Ett nytt förslag på det direktivet, NIS 2, inkluderar bland annat hårdare säkerhetskrav samt ett sanktionssystem.

Revisorerna har i sin riskanalys för 2022 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att finns en god informationssäkerhet inom kommunen och har därför gett PwC ett uppdrag att granska området.

Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll. För att bedöma detta har nedan revisionsfrågor undersökts.

Revisionsfrågor:

- Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?
- Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?
- Finns ett ledningssystem för informationssäkerhet implementerat?
- Arbetar informationssäkerhetsorganisationen aktivt med efterlevnad av informationssäkerheten?

- Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet?

Revisionskriterier

- Kommunallagen
- IT-styrdokument
- Informationssäkerhetsdokumentation

Avgränsning

I tid avgränsas granskningen till år 2022 samt till granskningens revisionsfrågor. Bedömningen har baserats på den inkomna dokumentationen och de intervjuer som genomförts inom ramen för granskningen.

Metod

Granskningen genomförs med hjälp av intervjuer av identifierade nyckelpersoner i kommunen, samt inläsning och genomgång av tillgänglig dokumentation för området. En lista med granskade dokument finns på sidan 13.

Intervju har genomförts med följande:

- Kommunchef
- Informationssäkerhetsstrateg
- Socialchef
- Systemförvaltare Socialförvaltningen

Granskningen har genomförts mellan september och november 2022 av Markus Månsson och Martin Lundin (PwC) och kvalitetssäkrats av Caroline Liljebjörn (uppdragsledare) på PwC samt faktakontrollerats av företrädare i Högsby kommun.

Granskningsresultat

Revisionsfråga 1: Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?

Iakttagelser

I granskningen framkommer att det finns en antagen informationssäkerhetspolicy inom Högsby kommun. I policyn anges att grundprincipen avseende ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret, vilket betyder att den som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten i den verksamheten. I policyn finns även ett avsnitt som beskriver organisation, ansvar och roller ur ett bredare perspektiv. Exempelvis anges ansvaret för kommunfullmäktige, kommunstyrelse, kommunchef, informationssäkerhetsstrateg, chefer och informationsägare.

Inom kommunen finns också dokumentet *riktlinjer för informationssäkerhet* antagen. Dokumentet beskriver vad som ska göras för att uppfylla ledningens viljeyttring (som anges i informationssäkerhetspolicyn). I riktlinjerna finns en utförligare beskrivning av roller och ansvar både inom den politiska ledningen, i verksamheten samt övriga roller.

Som beskrivs ovan har förvaltningarna och verksamhetsansvariga ett stort ansvar för att bedriva ett systematiskt informationssäkerhetsarbete utifrån framtagna riktlinjer för informationssäkerhet. Ansvaret för att driva arbetet med informationssäkerhet på en övergripande nivå bedöms som tydligt där kommunens informationssäkerhetsstrateg ansvarar för att leda, samordna och utveckla det strategiska informationssäkerhetsarbetet. Däremot framkommer det utifrån intervjuer, både centralt och med representanter från socialförvaltningen, att ansvar och roller inte är tillräckligt väl förankrade ute i kommunens förvaltningar och verksamheter.

För att stärka roll- och ansvarsfördelningen har ett förslag på en *tillämpningsanvisning* för informationssäkerhet arbetats fram. Dokumentet syftar till att tydliggöra vem som ansvarar för vad gällande riktlinjerna för informationssäkerhet. Tillämpningsansvisningen är under tiden för granskningen under arbete och ska diskuteras, anpassas samt förankras inom organisationen. Därefter ska den godkännas av kommunchefen.

Bedömning

Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?

Vår bedömning är att revisionsfrågan är **delvis uppfylld**. Bedömningen baseras på följande:

- Organisation, roll- och ansvarsfördelning finns angivet i kommunens antagna informationssäkerhetspolicy samt riktlinjer för informationssäkerhet.
- Roll- och ansvarsfördelningen bedöms inte vara tillräckligt förankrad och etablerad i kommunens verksamheter.

Revisionsfråga 2: Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?

Iakttagelser

I Högsby kommun finns övergripande styrdokument som utgör grunden för kommunens informationssäkerhetsarbete. Styrdokumenten är utformade utifrån en dokumentationshierarki där informationssäkerhetspolicyn är högst upp i hierarkin. Informationssäkerhetspolicyn är ett strategiskt dokument som redovisar kommunfullmäktiges övergripande mål och viljeinriktning för informationssäkerhetsarbetet i Högsby kommun samt hur ansvaret i dessa frågor är fördelade. Informationssäkerhetspolicyn är antagen av Kommunfullmäktige 2022-02-07 och har en giltighetstid fram till 2024.

Policyn understöds av dokumentet *Riktlinjer för informationssäkerhet* som beskriver hur policyn ska upprätthållas på taktisk nivå. Riktlinjerna för informationssäkerhet är antagen av kommunstyrelsen 2022-01-18 med giltighetstid till 2024. Dokumentet innehåller bland annat riktlinjer för riskbedömning och riskhantering, åtkomst till information, driftsäkerhet, kommunikations- och nätverkssäkerhet. Styrande principer avseende hantering av informationssäkerhetsincidenter finns däremot ej dokumenterade.

Utöver policyn och riktlinjerna för informationssäkerhet finns stödjande dokument för att genomföra riskanalyser och informationsklassning. En riskanalys avseende informationssäkerhet har genomförts på övergripande nivå i kommunen under 2021 och ska revideras årligen.

Under intervju beskrivs det att dokumenten inte efterlevs på ett tillräckligt bra sätt i kommunens verksamheter. Representanter från socialförvaltningen anger att ledande personer i förvaltningen har tagit del av de styrande dokumenten för informationssäkerhet. Däremot har moment som beskrivs i de styrande dokumenten inte etablerats eller utförts i någon vidare omfattning. Det som har etablerats inom socialförvaltningen är främst kontinuitetsplaner för att hantera störningar i verksamheten samt vissa stödjande rutiner - exempelvis rutiner för att hantera uppgifter om personer med skyddad identitet. Däremot finns det en avsaknad av exempelvis identifierade och klassade informationstillgångar, genomförda riskanalyser och handlingsplaner för informationssäkerhet. Medarbetare har inte heller tagit del av de regler som gäller för användning av Högsby kommuns IT-system och arbetsredskap som datorer, e-post, telefoner och sociala medier.

På en generell nivå för kommunens verksamheter beskrivs det även att det fortsatt behöver dokumenteras och implementeras rutiner avseende hantering av behörigheter i system, återställningsplaner av kritiska system, fysiska skydd av kommunens verksamheter samt kontinuitetsplaner. Det beskrivs även att kommunens arbete med att ställa krav på leverantörer (exempelvis IT-leverantörer) ur ett informationssäkerhetsperspektiv behöver stärkas.

Att de styrande dokumenten inte är implementerade i verksamheterna i nödvändig utsträckning beskrivs bland annat bero på att roll- och ansvarsfördelningen avseende informationssäkerhet inte är tillräckligt tydlig. Vidare beskrivs det att informationssäkerhet upplevs som ett komplext område och att kompetensen hos medarbetare behöver höjas för att de styrande dokumenten ska kunna implementeras på ett ändamålsenligt sätt.

Av granskningen framgår det även att kommunen inte genomför systematiska kontroller att dokumentationen rörande informationssäkerhet efterlevs i verksamheterna.

Bedömning

Vår bedömning är att revisionsfrågan är **delvis uppfylld**. Bedömningen baseras på följande:

- Informationssäkerhetspolicy samt riktlinjer för informationssäkerhet med styrande principer för informationssäkerhet finns antagna.
- Dokumenten anses inte vara väl implementerade i verksamheten.
- Uppföljning av att de styrande dokumenten efterlevs i kommunen genomförs ej.

Revisionsfråga 3: Finns ett ledningssystem för informationssäkerhet implementerat?

Iakttagelser

Ett ledningssystem för informationssäkerhet (LIS) är ett stöd för hur informationssäkerhetsarbetet styrs i en organisation. I Högsby kommuns informationssäkerhetspolicy anges det att arbetet med informationssäkerhet inom Högsby kommun ska ske systematiskt och bygga på etablerad standard (ISO 27000).

Ett ledningssystem för informationssäkerhet kan vara utformat på flera sätt men vanligtvis är styrande dokument, informationssäkerhetsmål samt identifiering av informationstillgångar och informationssäkerhetsrisker, centrala delar i planeringen av arbetet med informationssäkerhet. För att ett ledningssystem för informationssäkerhet (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.

Styrande dokument och informationssäkerhetsmål: Övergripande styrande dokument i form av informationssäkerhetspolicy samt riktlinjer för informationssäkerhet är etablerade och antagna i kommunen. Dessa dokument utgör en bra grund i ett ledningssystem för informationssäkerhet. Vissa utvecklingsområden avseende de styrande dokumenten återstår dock, exempelvis saknas styrande principer för hur informationssäkerhetsincidenter ska hanteras. Det saknas även definierade informationssäkerhetsmål som löpande följs upp.

Informationstillgångar, klassning av information och riskhantering: I granskningen noteras att kommunens informationstillgångar inte har identifierats eller klassats i någon större skala. Detta medför också att adekvata skyddsåtgärder inte har upprättats. Däremot har arbetet med informationsklassning påbörjats, där information i ett system har identifierats och klassats. Det noteras också att det finns en samsyn om att arbetet med att identifiera informationstillgångar och att klassa information behöver fortgå och stärkas.

Informationssäkerhetsrisker har identifierats på en övergripande nivå i kommunen, men under intervju beskrivs det att analyser av informationssäkerhetsrisker inte har utförts på ett ändamålsenligt sätt i kommunens verksamheter. Inom socialförvaltningen har en analys av informationssäkerhetsrisker ej genomförts.

Efterlevnad i verksamheten: Vilket beskrevs i revisionsfråga 2 efterlevs inte de styrande dokumenten på ett ändamålsenligt sätt i kommunens verksamheter. Det återstår ett större arbete med att förankra och implementera de styrande dokumenten i kommunen. Det återstår även ett arbete med att etablera och implementera verksamhetsspecifika rutiner inom ett flertal områden i verksamheterna. Ledningssystemet anses därför inte vara en integrerad del av organisationens processer.

Uppföljning: Intern revision för att följa upp att de styrande dokumenten efterlevs genomförs inte i dagsläget, varken på övergripande nivå i kommunen eller inom Socialförvaltningen.

Bedömning

Vår bedömning är att revisionsfrågan är **delvis uppfylld**. Bedömningen baseras på följande:

- Övergripande styrande dokument för informationssäkerhet finns etablerade och antagna.
- Informationssäkerhetsmål har ej definierats.
- Informationstillgångar har ej identifierats och klassats i någon större skala. Ett systematiskt arbete med hantering av informationstillgångar finns ej på plats.
- Riskanalyser har ej genomförts i någon större omfattning. Inom Socialförvaltningen har analys av informationssäkerhetsrisker ej genomförts.
- Uppföljning utförs inte om de styrande dokumenten efterlevs.

Revisionsfråga 4: Arbetar informationssäkerhetsorganisationen aktivt med efterlevnad av informationssäkerheten?

Iakttagelser

Enligt kommunens informationssäkerhetspolicy ska arbetet med informationssäkerhet följas upp regelbundet. Detta för att bevaka att beslutade åtgärder har genomförts, att årliga mål har uppfyllts, att regler efterlevs samt att policydokument och säkerhetsplaner revideras vid behov. I riktlinjerna för informationssäkerhet anges att kommunstyrelsen

har det övergripande ansvaret för uppföljning av informationssäkerheten. Det anges även att det åligger varje nämnd att vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll samt att varje förvaltning ska granska sin informationssäkerhet. Förvaltningarna ska sedan baserat på genomförda granskningar och identifierade avvikelser säkerställa att skyddsåtgärder vidtas, anpassas och kompletteras.

Av granskningen framgår det att intern revision, gällande uppföljning av att de styrande dokumenten efterlevs, i dagsläget inte genomförs. Intern revision genomförs varken på övergripande nivå i kommunen eller inom socialförvaltningen. Anledningen beskrivs vara att det fortfarande pågår ett gediget arbete med att implementera och förankra de styrande dokumenten och dess innehåll i organisationen. Vilka principer som ska följas, vilka kontinuerliga moment som ska utföras samt hur roll- och ansvarsfördelning ska ske i praktiken behöver också förankras och implementeras på ett bättre sätt.

Vidare framgår det i informationssäkerhetspolicyn att kommunens informationssäkerhetsstrateg minst två gånger årligen ska rapportera läge och status gällande informationssäkerhet till kommunchefen och kommunstyrelsen. Av granskningen framgår att informationssäkerhetsstrategen genomför månatliga avstämningar med kommunchefen för att gå igenom status för området. Rapportering till kommunstyrelsen sker en gång om året.

Bedömning

Vår bedömning är att revisionsfrågan **inte är uppfylld**. Bedömningen baseras på följande:

- Intern revision avseende informationssäkerhet genomförs ej.

Revisionsfråga 5: Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet?

Iakttagelser

I kommunens riktlinjer för informationssäkerhet beskrivs det att samtliga anställda inom kommunen ska få den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter och för att säkerställa målen för informationssäkerhet. Av granskningen framgår att det inte finns en etablerad process i kommunen för att utbilda medarbetare inom informationssäkerhet på regelbunden basis. Ett utredande arbete har påbörjats för att få utbildningar på plats, exempelvis genom så kallade nanolearnings (även benämnt som mikroutbildningar), men frågeställning har ännu inte klarlagts. Det framgår även att kommunledningen inte har genomfört någon dedikerad utbildning inom området informationssäkerhet.

Under intervju beskrivs det att medarbetarnas medvetenhet avseende informationssäkerhet har stärkts under de senaste åren. Men många medarbetare i organisationen skulle behöva få mer kunskap. Att erbjuda utbildningar inom

informationssäkerhet på årlig basis till alla anställda beskrivs i granskningen som en högaktuell fråga.

I riktlinjerna för informationssäkerhet finns ett avsnitt som beskriver hur anställda får använda datorer, internetuppkoppling, telefoner, e-post och andra arbetsredskap för att upprätthålla en god informationssäkerhet. Avsnittet innehåller styrande principer som är relevanta för alla medarbetare att ta del av. Av granskningen framgår att informationen i detta avsnitt inte förmedlats till medarbetare på ett ändamålsenligt sätt. Information likt detta har tidigare tillgängliggjorts för nyanställda, men förmedlas inte längre.

Inom kommunen pågår ett arbete med att etablera ett gemensamt råd/forum för informationssäkerhet. Utöver informationssäkerhetsstrategen ska rådet bestå av representanter från respektive förvaltning och kommunalt bolag. Rådets uppgift ska vara att främja, stödja, samordna och följa upp Högsby kommuns informationssäkerhetsarbete på en övergripande nivå. Rådet ska också främja erfarenhets- och kunskapsutbyte samt bevaka vilket stöd som verksamheterna behöver avseende arbetet med informationssäkerhet.

Bedömning

Vår bedömning är att revisionsfrågan **inte är uppfylld**. Bedömningen baseras på följande:

- Det finns inte en etablerad process för att utbilda medarbetare i informationssäkerhet på regelbunden basis.
- Informationssäkerhetsrådet finns ännu ej etablerat (däremot pågår ett arbete med att få det på plats).

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Högsby kommun genomfört en granskning av kommunens arbete med informationssäkerhet. Granskningens syfte är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhets-arbete och om detta sker med tillräcklig intern kontroll.

Utifrån genomförd granskning är vår samlade bedömning att Högsby kommuns kommunstyrelse **inte helt** säkerställer ett ändamålsenligt informationssäkerhetsarbete och att det inte sker med tillräcklig intern kontroll.

Rekommendationer

Vi rekommenderar kommunstyrelsen följande:

- Intensifiera arbetet med att förtydliga och förankra roller och ansvar inom informationssäkerhet i kommunens verksamheter.
- Öka medvetenheten kring de styrande dokumenten för informationssäkerhet och förankra dess innehåll för att stärka efterlevnaden.
- Säkerställ att tillämpningsanvisningen som beskriver roller- och ansvar för informationssäkerhet färdigställs, förankras och beslutas.
- Säkerställ att kommunens informationstillgångar identifieras, klassificeras samt skyddas på ett ändamålsenligt sätt.
- Säkerställ att analys av informationssäkerhetsrisker genomförs systematiskt i kommunens verksamheter.
- Etablera övergripande mål för informationssäkerhet. Målen bör följas upp på regelbunden basis och åtgärdsplaner för att hantera avvikelser bör upprättas.
- Etablera styrande principer för hur informationssäkerhetsincidenter ska hanteras.
- Säkerställ att kontinuitetsplaner för att upprätthålla verksamheten vid olika typer av avbrott etableras. Återställningsplaner för kritiska system bör också etableras.
- Stärk förmågan att ställa krav på leverantörer ur ett informationssäkerhetsperspektiv.
- Etablera en process för att följa upp efterlevnad av de styrande dokumenten för informationssäkerhet på regelbunden basis.
- Säkerställ att medarbetare erbjuds utbildning inom informationssäkerhet. Utbildningarna bör innehålla grundläggande delar samt delar som är anpassade utifrån roll. Att utbildningarna genomförs bör även följas upp på årlig basis.
- Överväg att utforma avsnitt 7 i riktlinjerna för informationssäkerhet till ett eget dokument då denna information berör alla medarbetare. Detta för att underlätta för medarbetare att ta till sig informationen. Informationen i detta avsnitt bör därefter kommuniceras till kommunens medarbetare.
- Säkerställ att kommunens forum/råd för informationssäkerhet etableras för att på så sätt stärka samordningen, etablera gemensamma arbetssätt och sprida goda exempel relaterat till arbetet med informationssäkerhet inom kommunen.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning	
1. Finns en informations-säkerhetsorganisation med tydlig roll- och ansvars-fördelning?	**Delvis** Organisation, roll- och ansvarsfördelning finns angivet i kommunens antagna informationssäkerhetspolicy samt riktlinjer för informationssäkerhet. Roll- och ansvarsfördelningen bedöms inte vara tillräckligt förankrad och etablerad i kommunens verksamheter.	
2. Finns styrande informationssäkerhets-dokumentation och är dessa väl implementerade i verksamheten?	**Delvis** Styrande dokument för informationssäkerhet finns antagna. Dokumenten anses dock inte vara väl implementerade i verksamheten. Uppföljning av att de styrande dokumenten efterlevs i kommunen genomförs ej.	
3. Finns ett ledningssystem för informationssäkerhet implementerat?	**Delvis** Övergripande styrdokument finns antagna och utgör en bra grund i ett ledningssystem. Däremot är inte de styrande dokumenten tillräckligt väl implementerade och arbetet med informationssäkerhet bedöms inte ske systematiskt.	
4. Arbetar informationssäkerhets-organisationen aktivt med efterlevnad av informationssäkerheten?	**Nej** Intern revision avseende informationssäkerhet genomförs ej.	
5. Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhets-området?	**Nej** Det finns inte en etablerad process för att utbilda medarbetare i informationssäkerhet på regelbunden basis. Informationssäkerhetsrådet finns ännu ej etablerat.	

Bilaga: Dokumentgranskning

Dokument	Beslutad	Reviderad
Analysverktyg GAP - Högsby kommun	-	-
Beslutsunderlag - Riskanalys	-	-
Informationsklassningsmodell - Högsby kommun 2022	-	-
Informationssäkerhetspolicy - Högsby kommun	2022-02-07	2021-12-16
Riktlinjer för informationssäkerhet - Högsby kommun	2022-01-18	-
Riskanalys - Högsby kommun 2021-09-09	-	-

2022-12-21

Caroline Liljebjörn

Uppdragsledare

Markus Månsson

Projektledare

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Högsby kommun förtroendevalda revisorer enligt de villkor och under de förutsättningar som framgår av projektplan från 2022-04-13. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.