Granskning av IT-säkerhet

Uppföljning av kommunens informationssäkerhetsarbete

Huddinge Kommun – 28 November 2022

Innehåll

Sammanfattning

Vi har av Huddinge kommuns revisorer fått i uppdrag att granska om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2022. Syftet med granskningen har varit att bedöma om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll för sin IT-säkerhet och i samband med granskningen följa upp om de rekommendationer som lämnades i granskningen för 2020 är åtgärdade.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen inte har säkerställt att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerheten. Ett flertal av de rekommendationer som lämnades i tidigare granskning har inte åtgärdats. Vi bedömer att flertalet av dessa även i vissa delar påverkar förutsättningarna för en god IT-säkerhet.

I avsaknad av beskrivningar av ansvarsförhållanden inom informationssäkerhet avseende den tekniska säkerheten går det i nuläget inte att bedöma om organisationen är ändamålsenlig. Vi noterar att roller är otydliga och ansvar behöver tydliggöras på olika nivåer avseende informationssäkerhetsarbetet, inklusive den tekniska säkerheten. De nu gällande styrdokumenten saknar hierarkisk ordning och utgör inte en sammanhållen helhet. De är i delar föråldrade och därigenom saknas angivelser till nya lagar, exempelvis GDPR och NIS-direktivet, som hör till informationssäkerhetsarbetet.

Säkerhetsåtgärder vidtas till viss del som ett resultat av informationsklassningar och systemsäkerhetsanalyser. Kopplingen mellan åtgärder och verksamheternas bedömningar av informationens skyddsvärde kan emellertid stärkas. Modellen för informationsklassning är därtill att betrakta som föråldrad. Inom IT-avdelningen sker viss verksamhetsnära uppföljning av de tekniska säkerhetsåtgärder som är vidtagna. Uppföljning av IT-säkerhetsarbetet på en övergripande nivå, tillika rapportering till kommunstyrelsen är emellertid att betrakta som otillräcklig.

Kommunens IT-avdelning har vissa tekniska verktyg som möjliggör övervakning för att ha en förmåga att upptäcka hot om intrång eller andra incidenter. Det finns en medvetenhet om försök till intrång och kommunen har med hjälp av övervakningsverktyg och övriga säkerhetsåtgärder kunnat stå emot intrångsförsök utan att det hittills har lett till allvarlig konsekvens för verksamheten. Det finns en etablerad organisation och rutiner för att hantera incidenter inom IT-avdelningen men vi uppfattar att det finns behov av att tydliggöra incidenthantering generellt i kommunens verksamheter. Kontinuitetsplaner som kan utgöra stöd vid allvarligare störningar finns till viss del i kommunens verksamheter, de planer som finns har dock endast testats i begränsad omfattning.

Efter den senare tidens uppmärksammade attacker mot kommuner runt om i Sverige har information efterfrågats av kommunstyrelsen och kommunledningen. Vi kan dock konstatera att den information som rapporterats inte har lett till beslut om särskilda åtgärder för verksamheten att verkställa.

Rekommendationer

Utifrån uppföljning av tidigare genomförd granskning av informationssäkerhet kvarstår följande rekommendationer till kommunstyrelsen:

— Implementera en informationssäkerhetspolicy.

— Implementera en obligatorisk utbildning om informationssäkerhet med kontinuerliga och regelbundna uppföljningsutbildningar.

— Implementera en systematisk och regelbunden rapportering och uppföljning av informationssäkerhetsarbetet till kommunledningen och kommunstyrelsen.

— Säkerställa att alla verksamheter har tillgång och kännedom om de styrdokument som gäller för verksamheten, samt vilka ansvarsförhållanden som gäller.

— Säkerställa att informationssäkerhetsorganisationen har en tillräcklig omfattning för att möta kommunens behov.

— Ser över möjligheten att implementera nya rutiner för att säkerställa att anställda har rätt behörigheter.

— Implementera en rutin för rapportering av informationssäkerhetsincidenter i ett avvikelserapporteringssystem.

Utifrån vår bedömning och slutsats i den fördjupade granskningen av IT-säkerhet rekommenderar vi kommunstyrelsen att:

— Revidera riktlinjer för informationssäkerhet avseende ansvar för den tekniska säkerheten.

— Se över vilka ytterligare instruktioner och anvisningar som det finns behov av för att etablera en styrning av informations-säkerhetsarbetet.

— Fastställa en ny och uppdaterad modell för riskanalys och informationsklassning.

— Stärka verksamheternas roll i bedömningen av informations skyddsvärde.

— Tillse att de beslut om riskreducerande åtgärder i internkontrollen verkställs och att uppföljning sker av att åtgärder lett till minimerad risk.

— Att genomföra penetrationstester av IT-miljön.

— Fastställa kommunövergripande incidenthanteringsrutiner som tillämpas av alla verksamheter. Samt tillse att nämnder upprättar kompletterande incidenthanteringsrutiner utifrån verksamhetsspecifika krav och lagar.

— Utvärdera befintliga kontinuitetsplaner samt införa tester av de planer som finns för att säkerställa att underlag skulle fungera vid särskilda händelser.

Inledning

KPMG har av Huddinge kommuns revisorer fått i uppdrag att granska om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerhet.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och en stor del av informationen hanteras i IT-system vilket ställer höga krav på att dessa är tillgängliga och säkra. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Brister i hanteringen kan leda till både ekonomisk skada och förtroendeskada för organisationen. Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd.

I tidigare genomförd granskning från 2020 bedömdes att kommunstyrelsen inte hade ett ändamålsenligt och systematiskt arbetssätt avseende informationssäkerhet. De brister som identifierades var bland annat en otydlighet kring roller och ansvarsfördelning inom kommunstyrelsens förvaltning samt i förhållande till övriga förvaltningar. Verksamheterna som har det övergripande ansvaret för riskhantering saknade vid tiden kompetens vilket resulterade i att identifierade sårbarheter, trots att risker identifierats och dokumenterats i den interna kontrollen, hanterades dessa inte så att de inte skulle inträffa på nytt. Verksamheterna saknade stöd och resurser för att bedriva detta arbete på ett tillfredställande sätt. Granskningen resulterade i ett antal rekommendationer.

Utifrån granskningens resultat rekommenderades kommunstyrelsen att:

- Implementera en informationssäkerhetspolicy.
- Implementera en obligatorisk utbildning om informationssäkerhet med kontinuerliga och regelbundna uppföljningsutbildningar.
- Implementera en systematisk och regelbunden rapportering och uppföljning av informationssäkerhetsarbetet till kommunledningen och kommunstyrelsen.
- Säkerställa att alla verksamheter har tillgång och kännedom om de styrdokument som gäller för verksamheten, samt vilka ansvarsförhållanden som gäller.
- Säkerställa att informationssäkerhetsorganisationen har en tillräcklig omfattning för att möta kommunens behov.
- Ser över möjligheten att implementera nya rutiner för att säkerställa att anställda har rätt behörigheter.
- Implementera en rutin för rapportering av informationssäkerhetsincidenter i ett avvikelserapporteringssystem.
- Säkerställa att det finns en ändamålsenlig organisation för rapportering av incidenter enligt NIS-direktivet.

Med anledning av den väsentligt ökade hotbilden gällande IT-säkerhet och intrång drar kommunens revisorer slutsatsen i sin riskanalys, att kommunens rutiner avseende IT-säkerheten behöver granskas och tidigare rekommendationer behöver följas upp.

Syfte, revisionsfrågor och avgränsning

Granskningen syftar till att bedöma om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll för sin IT-säkerhet och i samband med granskningen följa upp om de rekommendationer som lämnades i granskningen för 2020 är åtgärdade.

Granskningen ska besvara följande revisionsfrågor:

- Finns det i nuläget en ändamålsenlig organisation för IT–säkerhetsarbetet?
- Finns beslutade och aktuella styrdokument i form av policys och riktlinjer för informationssäkerhet där IT-säkerhet ingår och säkerställs det att dessa följs?
- Vidtas tillräckliga tekniska säkerhetsåtgärder som ett resultat av verksamheternas informationsklassningar och riskanalyser?
- Finns en tillräcklig kontroll för att upptäcka eventuella hot om intrång eller andra incidenter i IT-system?
- Finns det en tillräcklig uppföljning av att de säkerhetsåtgärder som är vidtagna fungerar ändamålsenligt?
- Finns ändamålsenliga rutiner och etablerade arbetssätt för att hantera och dokumentera allvarliga IT-incidenter?
- Har kommunstyrelsen efter den senare tidens uppmärksammade attacker mot kommuner gjort någon analys av kommunens nuläge och förutsättningar att stå emot eventuella intrångsförsök eller störningar i IT-miljön? Har åtgärder vidtagits?
- Finns dokumenterade kontinuitetsplaner avseende IT-drift vid allvarligare störningar och avbrott? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?

Granskningen omfattar kommunstyrelsens ansvar för IT.

Revisionskriterier

Vi har bedömt kommunens arbete utifrån följande kriterier:

- Tillämpbara interna regelverk, policys och beslut
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

Metod

Granskningen har genomförts genom:

— Intervjuer med berörda tjänstemän däribland: Informationssäkerhetssamordnare, IT-säkerhetsansvarig, IT-arkitekt, Kommundirektör, Framtidsdirektör digitaliseringsavdelningen och Dataskyddsombud

— Dokumentstudier av tillgängliggjord dokumentation

Kvalitetssäkring av granskningen och revisionsrapporten har skett i enlighet med KPMGs gällande rutiner. Rapporten är faktakontrollerad av samtliga intervjuade innan presentation.

Uppföljning

Rekommendation	Åtgärdat?	Iakttagelse
Implementera en informationssäkerhetspolicy.	**Nej**	Att en policy ska tas upprättas framgår av 2022 års verksamhetsplan, detta har emellertid inte gjorts. Intervjuade menar att det beror på att de styrande dokumentens utformning hör samman med etableringen av ett ledningssystem för informationssäkerhet, LIS. En beställning utav ett etableringsprojekt har genomförts för uppstart av ett LIS men har ännu inte implementerats.
Implementera en obligatorisk utbildning om informations-säkerhet med kontinuerliga och regelbundna uppföljnings-utbildningar.	**Nej**	Utbildningar ska enligt intervjuade genomföras när styrdokument reviderats och ett LIS är etablerat.
Implementera en systematisk och regelbunden rapportering och uppföljning av informationssäkerhetsarbetet till kommunledningen och kommunstyrelsen.	**Delvis**	Rapportering till KS och kommunledningen har gjorts men sker inte med regelbundenhet. Rapportering görs till chef för trygghet och säkerhet, vilken inte är en del av ledningsgruppen.
Säkerställa att alla verksamheter har tillgång till och kännedom om de styrdokument som gäller för verksamheten, samt vilka ansvarsförhållanden som gäller.	**Nej**	Kännedomen om styrdokumenten framhålls fortsatt vara överlag dålig ute i verksamheterna. Framförallt sett till roller och ansvar.
Säkerställa att informationssäkerhetsorganisationen har en tillräcklig omfattning för att möta kommunens behov.	**Delvis**	Resursernas uppges tillräckliga sett till nuvarande ambitionsnivå. Om ett LIS ska etableras krävs utökade resurser.
Ser över möjligheten att implementera nya rutiner för att säkerställa att anställda har rätt behörigheter.	**Nej**	Rutiner finns på plats sedan tidigare, men uppföljning och kontroll av behörigheter framhålls som delvis bristande.
Implementera en rutin för rapportering av informationssäkerhetsincidenter i ett avvikelserapporteringssystem.	**Nej**	Riktlinje för behandling av personuppgifter tillika rutin för anmälan personuppgiftsincident finns. Anmälan görs till Dataskyddsinspektionen. Andra incidenter anmäls till help-desk men dokumenterad rutin/riktlinje saknas. Därtill saknas avvikelserapporteringssystem för att rapportera om incidenter.
Säkerställa att det finns en ändamålsenlig organisation för rapportering av incidenter enligt NIS-direktivet.	**Ja**	Instruktion för anmälan av NIS-incident finns framtagen och hanteringen framstår som tydlig.

Uppföljning (fortsättning)

IT-säkerheten som underställt informationssäkerheten

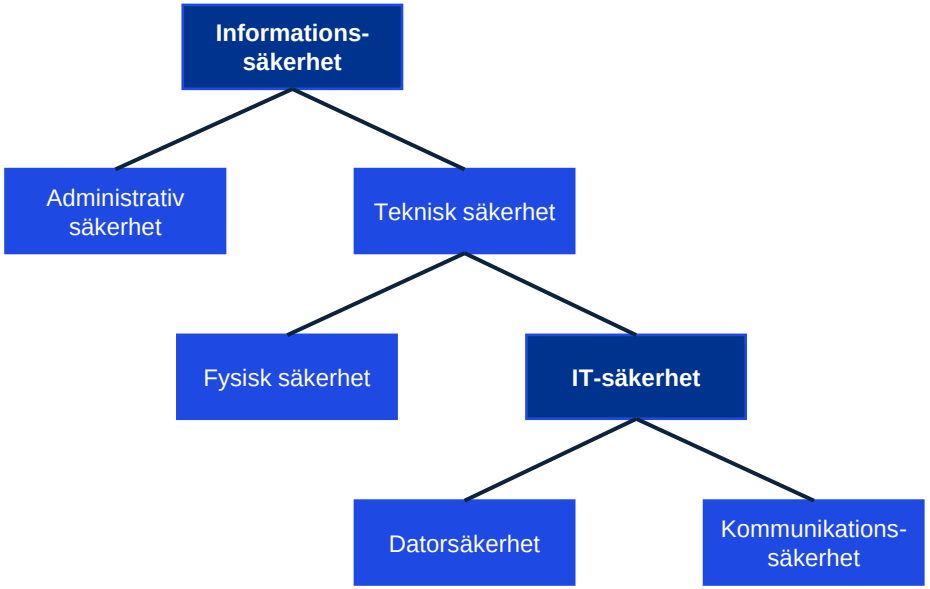
Illustrationen till höger ämnar beskriva olika informationsrelaterade begrepp/funktionernas relation till varandra. Funktionerna längre ner i ledet är att betrakta som underställda de ovan.

I praktiken innebär detta att samtliga funktioner, inklusive IT-säkerheten, kräver en ändamålsenlig informationssäkerhet för att kunna betraktas som fullt ut fungerande.

Överlag visar uppföljningen på att förhållandevis få utav de rekommendationer som lämnades i KPMG:s granskning 2020 har åtgärdats. Endast **tre av åtta** rekommendationer har helt eller delvis åtgärdats. Syftet med dessa rekommendationer var att möjliggöra för en mer ändamålsenlig informationssäkerhet i Huddinge kommun. Då dessa inte har åtgärdats kan informationssäkerheten fortfarande inte betraktas som fullt ut ändamålsenlig och flertalet rekommendationer kvarstår att åtgärda.

Det finns därför en risk att de brister som kvarstår för informationssäkerheten också innebär att IT-säkerheten försvagas.

I nästkommande avsnitt redogör KPMG för resultatet av granskning av IT-säkerheten. Viktigt att ha i åtanke är att, trots en potentiellt välfungerande IT-säkerhet avseende tekniska säkerhetsåtgärder så kan fel hantering av information och IT-användande innebära risker för IT-säkerheten.



Resultat av granskningen

Organisation - Iakttagelser

➢ **Finns det i nuläget en ändamålsenlig organisation för IT–säkerhetsarbetet?**

I vår dokumentgranskning noterar vi att ansvar för informationssäkerhet och IT-säkerhet inte är dokumenterat mer än att det är ett verksamhetsansvar. Exempelvis saknas roll- och uppdragsbeskrivning för informationssäkerhetssamordnare och IT-säkerhetsansvarig vilka är nyckelfunktioner i arbetet. Våra iakttagelser av organisationen baseras därigenom på intervjuuppgifter då styrande dokument saknar beskrivningar.

Informationssäkerhetssamordnare och dataskyddsombud tillhör trygghets- och säkerhetssektionen inom kommunstyrelsens förvaltning.

IT-säkerhetsarbetet i Huddinge kommun är organiserat inom digitaliseringsavdelningen, som är en del av kommunstyrelsens förvaltning. Avdelningen består av runt 55 personer.

Ansvaret för arbetet med IT-säkerhet, ligger enligt intervjuade, i huvudsak på IT-säkerhetsansvarig och en IT-arkitekt. Utöver de funktionerna innehar även teknikerna inom digitaliseringsavdelningen visst ansvar för IT-säkerhet inom sina tjänsteområden.

En systemsäkerhetsanalys (SSA) ska initieras av systemägaren (men kan delegeras). Under SSA:n deltager bl.a. Informationssäkerhets-samordnaren, som håller i själva arbetet, samt IT-säkerhetsansvarig och IT-arkitekt.

IT-säkerhetsansvarig har, inom sitt ansvar att övervaka sårbarheter i kommunens IT-miljö. Enligt intervjuade finns IT-säkerhetsansvarig tillgänglig som stöd till förvaltningarna när behov av IT-säkerhetskompetens finns.

Samverkan mellan informationssäkerhetssamordnare, dataskyddsombud och IT-säkerhetsansvarig uppges vara välfungerande och samordnaren samt ombud sitter tillsammans med IT-säkerhetsansvarig och IT-arkitekt i en gemensam ”teknisk säkerhetsgrupp”, ett forum där gemensamma frågor diskuteras.

Det finns ett informationssäkerhetsforum etablerat i kommunen. Forumet är frivilligt men riktar sig till samtliga förvaltningar. Syftet är att diskutera frågor gällande informationssäkerhet, inklusive personuppgifter och krav i NIS-direktivet. Möten sker enligt uppgift en gång varje kvartal.

Kommunen jobbar utifrån PM3-modellen där objektsförvaltare/ledare finns ute i verksamheterna som ansvarar för uppdatering av system och är de som för dialog med systemleverantörer. Roller och ansvar kring uppdraget som objektsförvaltare ute i organisationerna framhålls av intervjuade emellertid som otydligt.

Resultat av granskningen

Organisation – Bedömning

➢ **Finns det i nuläget en ändamålsenlig organisation för IT–säkerhetsarbetet?**

Vår bedömning

Det saknas dokumenterade beskrivningar hur IT-säkerhetsansvaret är fördelat och vilket uppdrag IT-avdelningen och utpekade funktioner inom avdelningen har att förhålla sig till.

Det framgår av styrande dokument att IT-säkerhet är ett verksamhetsansvar, vi anser att det är en felaktig beskrivning. Den administrativa säkerheten inom informationssäkerhet är ett verksamhetsansvar och det vilar på ansvariga att göra riskbedömningar och informationsklassning i syfte att identifiera behov av IT-säkerhet. Den tekniska säkerheten inom informationssäkerhet är dock ett ansvar som åligger intern eller extern funktion för IT-drift och säkerhet, exempelvis IT-avdelningen. Detta då ordinarie verksamhetsansvariga inte kan förväntas ha specialistkunskap inom IT för att kunna ta ansvar för IT-säkerheten.

I avsaknad av beskrivningar av ansvarsförhållanden går det inte att bedöma om organisationen är ändamålsenlig. Vi noterar dock att roller är otydliga och ansvar behöver tydliggöras på olika nivåer avseende informationssäkerhetsarbetet, inklusive den tekniska säkerheten.

Resultat av granskningen

Styrdokument - Iakttagelser

- **Finns beslutade och aktuella styrdokument i form av policys och riktlinjer för informationssäkerhet där IT-säkerhet ingår och säkerställs det att dessa följs?**

Utöver styrning genom kommunens vision, budget och förvaltningens verksamhetsplan finns ett övergripande styrdokument för styrning av informationssäkerhetsarbetet i kommunen i form av *Riktlinje för informationssäkerhet,* beslutat av Kommunfullmäktige 2019-12-09. Riktlinjen anger målet att skydda verksamheterna mot avbrott eller felaktigheter i informationsflödet och minimera risken för att informationen används så att den skadar kommunen, dess invånare eller tredje man. Riktlinjerna ställer bland annat krav på informationsklassning, riskanalyser, krav om säkerhetsåtgärder samt incident- och kontinuitetsplanering. Det saknas i dokumentet en tydliggjord styrning av den tekniska säkerheten i form av IT-säkerhet.

Vi har i granskningen tagit del av *Riktlinje för IT-säkerhet*, dokumentet har dock inte antagits och är därmed inte gällande. Anledningen uppges vara att dokumentet *Riktlinje för användning av Internet, e-post och mobila enheter,* vilken antagits av kommunfullmäktige 2015-01-12, bedömdes krocka med den nya riktlinjen. Vi noterar att båda dessa dokument avser att tydliggöra regler och anvisningar för IT-användare. Således skulle styrning av IT-avdelningens arbete och kravnivåer för IT-säkerhet inte varit tydliggjorda utifrån formuleringar i något av dessa dokument.

En rekommendation i KPMG:s granskning av informationssäkerhet från 2020 var att en informationssäkerhetspolicy skulle fastställas samt att det fanns behov av ytterligare rutiner för att tydliggöra styrning inom vissa områden, bland annat avseende behörigheter och incidenthantering.

I kommunstyrelsens verksamhetsplan för 2022 framgår att ett ledningssystem för informationssäkerhet (LIS) ska inrättas och en informationssäkerhetspolicy ska beslutas under året. Detta som riskreducerande åtgärder som bedömts nödvändiga i den interna kontrollen. Detta har emellertid inte gjorts vid tiden för granskningen. I granskningen framkommer att kommunledningen upplever att behovet av ett LIS inte klargjorts på ett tydligt och begripligt sätt och därför har inget formellt beslut fattats i frågan. Kommunikationen mellan ledning och funktioner inom informationssäkerhet och IT framhålls som ett utvecklingsområde så att komplexa frågor beskrivs på ett mer pedagogiskt sätt, för en ökad förståelse. Utan detta upplevs det svårt att fatta beslut om nödvändiga åtgärder och resurser för informationssäkerhetsarbetet.

Rekommendation om att inrätta rutiner för behörighetshantering och incidenthantering har verkställts. Ytterligare styrande dokument som delgivits i granskningen är riktlinjer och rutiner för dataskyddsarbetet (GDPR), digitaliseringsstrategi, programmet för trygghet och säkerhet (vilken har utgått sedan 2021) och riktlinjer för säkerhetsskydd.

Resultat av granskningen

Styrdokument- Bedömning

- **Finns beslutade och aktuella styrdokument i form av policys och riktlinjer för informationssäkerhet där IT-säkerhet ingår och säkerställs det att dessa följs?**

Vår bedömning

Vår bedömning är att det till viss del finns beslutade och aktuella styrdokument i form av en riktlinje samt kompletterande rutiner. Vår bedömning är dock att nuvarande dokument behöver revideras och kompletteras för att etablera en styrning av informationssäkerhetsarbetet inklusive IT-säkerheten. De nu gällande styrdokumenten saknar hierarkisk ordning och utgör inte en sammanhållen helhet. De är i delar föråldrade och därigenom saknas angivelser till nya lagar, exempelvis GDPR och NIS-direktivet, som hör till informationssäkerhetsarbetet.

Därtill saknas i stora delar dokumentation av ansvarsbeskrivningar för nyckelroller vid etableringen av ett systematiskt informationssäkerhetsarbete. Kommunstyrelsen har i sin interna kontroll bedömt behov av att etablera ett ledningssystem för informationssäkerhet och att fastställa en informationssäkerhetspolicy. Vi anser att kommunstyrelsen brustit i sin interna kontroll då arbetet med riskreducerande åtgärder inte formellt verkställts och inga beslut om uppdrag eller åtgärder för att påbörja arbetet gjorts.

Informationssäkerhetsarbetet bör utgå från en övergripande policy som kommunfullmäktige fastställer. Övriga styrdokument bör beslutas av kommunstyrelsen gällande den kommunövergripande styrningen. Vid behov bör dessa kompletteras med nämndspecifika anvisningar utifrån verksamheternas olika krav på följsamhet till lagar och föreskrifter.

Resultat av granskningen

Tekniska säkerhetsåtgärder - lakttagelser

- **Vidtas tillräckliga tekniska säkerhetsåtgärder som ett resultat av verksamheternas informationsklassningar och riskanalyser?**

Riktlinje för informationssäkerhet reglerar krav att riskanalyser och informationsklassning ska genomföras. Enligt riktlinjen ska risk- och sårbarhetsanalyser genomförs årligen för verksamhetskritiska system. Därtill ska riskanalyser göras vid anskaffning av nya system eller väsentliga förändringar av befintliga system. Samtliga verksamhetskritiska informationstillgångar ska klassificeras utifrån funktion och betydelse för verksamheten. Vidare framgår att systemägaren utifrån resultat i klassningar och riskanalyser ska ställa krav på säkerhetsåtgärder. Dessa ska dokumenteras i systemförvaltningsplaner och följas upp.

En modell för informationsklassning finns beskriven i riktlinjerna för informationssäkerhet. Tillhörande bilaga ”Informationsklassificerings-modell för informationstillgångar” (senast reviderad 2014-04-09) beskriver detaljerat hur bedömningar ska göras av informations-tillgångarna. Med undantag för formuleringar om att anställda ska ha ”rätt behörighet” framkommer inte vilka åtgärder som ska vidtas som ett resultat av informationsklassningar. Hur det praktiska arbetet ser ut har inte heller framgått av genomförda intervjuer.

Systemsäkerhetsanalyser tas fram av verksamheterna men är till stor del beroende av verksamheternas kunskap inom området. Enligt intervjuade för granskningen är medvetenheten hos verksamheterna vad gäller vilken information deras system innehåller och vad som behöver skyddas väldigt låg. Kravställning och bedömningar över vilka system som är verksamhetskritiska (utifrån vilken information systemet hanterar) och som därigenom bedöms vara i behov utav stärkt skydd, behöver därför till stor del göras av IT.

I de fall då system är att betrakta som i behov av extra skydd uppger intervjuade att multifaktorsauktorisering är en säkerhetsåtgärd som vidtagits.

Resultat av granskningen

Tekniska säkerhetsåtgärder - Bedömning

- **Vidtas tillräckliga tekniska säkerhetsåtgärder som ett resultat av verksamheternas informationsklassningar och riskanalyser?**

Vår bedömning

Vår bedömning är att det till viss del vidtas säkerhetsåtgärder som ett resultat av informationsklassningar. Verksamheternas roll i bedömningen av informations skyddsvärde behöver emellertid stärkas då verksamhetsinsyn krävs för en fullt ut tillfredsställande informationsklassningar. Det bristfälliga underlaget medför att det inte i nuläget inte går att fullt ut bedöma om åtgärderna är tillräckliga för att skydda informationen. Vi anser dessutom att det är en brist då arbetet inte sker i enlighet med beslutade riktlinjer.

Den modell för informationsklassning som är beslutad är föråldrad och tar därigenom inte hänsyn till att klassningar som genomförs nu behöver beakta ett antal ytterligare aspekter vid analyser, exempelvis tillkommande lagar och regler som införts sedan 2014.

Resultat av granskningen

Kontroll för hot om intrång - Iakttagelser

- **Finns en tillräcklig kontroll för att upptäcka eventuella hot om intrång eller andra incidenter i IT-system?**

Intervjuade uppger att mängden kritiska intrång eller försök till intrång varit få och att det finns en stor medvetenhet kring hot och risker. Övervakning utav delar av IT-miljön sker genom köp av extern tjänst (SIEM - Security information management) med automatiska varningar till kommunen vid säkerhetshändelser eller avvikelser som fångas av tjänsten. Analys av övervakningen har tidigare varit ett ansvar hos IT-säkerhetsansvarig, men ligger idag i objektet ”Säkerhet och Lokaler”. Den externa tjänsten fungerar dock endast för de system som kommunen har valt att integrera mot tjänsten. Intervjuade uppger att förhållandevis få system idag är kopplade. Det finns enligt intervjuade ett lågt intresse från verksamheterna att inrätta detta, främst utifrån rädsla att hanteringen ska skapa mer jobb och ta tid i anspråk.

Behov har identifierats av IT-avdelningen att etablera en organisation för övervakning och kontroll, ett så kallat SOC, Security Operations Center. Genom en sådan förstärks arbetet dels av nya tekniska verktyg för övervakning, larm och rapportering av händelser i IT-miljön, dels i form av en förstärkt organisation och bemanning med dygnet runt-beredskap vilket saknas i nuläget.

Resultat av granskningen

Kontroll för hot om intrång - Bedömning

- **Finns en tillräcklig kontroll för att upptäcka eventuella hot om intrång eller andra incidenter i IT-system?**

Vår bedömning

Vår bedömning är att kommunen till viss del har infört tekniska verktyg som möjliggör övervakning för att ha en förmåga att upptäcka hot om intrång eller andra incidenter. Det finns en medvetenhet om försök till intrång och kommunen har med hjälp av övervakningsverktyg och övriga säkerhetsåtgärder kunnat stå emot intrångsförsök utan att det blivit någon allvarlig konsekvens för verksamheten.

Det finns till viss del en organisation för att upptäcka eventuella hot om intrång, dock endast under kontorstid. Genom etablering av en SOC skulle denna förmåga kunna stärkas i kommunen både tekniskt och organisatoriskt. Detta bör dock utvärderas så att beslutsunderlag tydligt beskriver nytta, kostnad och hur arbetet inom SOC ska bedrivas.

Resultat av granskningen

Uppföljning av säkerhetsåtgärder - lakttagelser

➢ **Finns det en tillräcklig uppföljning av att de säkerhetsåtgärder som är vidtagna fungerar ändamålsenligt?**

Enligt intervjuade finns ingen etablerad och regelbunden uppföljning av IT-säkerheten förutom den som genomförs i den interna kontrollen. Det har inte heller tydliggjorts några krav om uppföljning eller hur den ska genomföras och rapporteras.

Inom IT-avdelningens verksamhetsansvar görs en löpande uppföljning av säkerhetsåtgärder för att identifiera sårbarheter som är i behov av åtgärder. Som vi tidigare nämnt har IT-säkerhetsansvarig en regelbunden övervakning av kommunens IT-system och miljö för att identifiera svagheter vilket är en form av uppföljning. Därtill finns ett önskemål från IT-organisationen om att utvärdera de skyddsfunktioner som är implementerade genom penetrationstester.

Intervjuade beskriver att det finns vissa brister inom bland annat uppföljning av behörigheter, där avvikelser med felaktiga behörigheter noterats för olika system. Det finns därtill brister i nuvarande förmåga till spårbarhet vid säkerhetshändelser där intervjuade uppger att det är svårt att få en överblick över vad som skett och hur stor påverkan händelsen fått.

I kommunstyrelsens verksamhetsplan 2022 där plan för internkontroll ingår, framgår två identifierade risker för informationssäkerhet, vilka vi har beskrivit tidigare i rapporten.

Därtill finns två identifierade risker inom IT-drift.

- Risk för exponering för eventuella cyberattacker och intrångsförsök på grund av ökad cyberbrottslighet.
- Risk att bryta mot lagstiftning genom användning av icke-europiska molntjänster.

En riskreducerande åtgärd för risken om cyberattacker är att stärka kommunens skydd mot phisingmail. Avseende risk kring molntjänster framgår att kommunen ska upprätta ett underlag med kommunens ställningstagande i frågan.

Uppföljning av intern kontroll görs enligt verksamhetsplan i delårsrapport och verksamhetsberättelse. I delårsrapport per 2022-08-31 nämns uppföljning av intern kontroll, saknas dock beskrivning av dessa kontroller och åtgärder med undantag för beskrivning nedan.

”De avvikelser som har rapporterats nämns inte innebära några väsentliga risker. Delar av kommunstyrelsens planerade arbete med intern kontroll är dock försenat och förskjuts i tid. På kommunstyrelsen beror detta på att åtgärderna i vissa fall är mer omfattande än beräknat och att arbete med det pågående omställningsarbetet har behövt prioriterats”.

Vi kan därigenom inte utläsa om de åtgärder som beslutats avseende IT-drift och informationssäkerhet har åtgärdats och risker reducerats.

Resultat av granskningen

Uppföljning av säkerhetsåtgärder - Bedömning

- **Finns det en tillräcklig uppföljning av att de säkerhetsåtgärder som är vidtagna fungerar ändamålsenligt?**

Vår bedömning

Vår bedömning är att det inom IT-avdelningen sker viss verksamhetsnära uppföljning av de tekniska säkerhetsåtgärder som är vidtagna. I huvudsak genom att IT-miljön regelbundet övervakas för att identifiera sårbarheter. Det finns ambitioner inom IT-organisationen om att genomföra penetrationstester av IT-miljön. Sådana bör med fördel genomföras i syfte att säkerställa kommunens IT-säkerhet.

Vår bedömning är att det inte finns en tillräcklig uppföljning av IT-säkerhetsarbetet på en övergripande nivå, det har inte heller etablerats rapporteringsvägar så att kommunstyrelsen erhåller en löpande information om säkerhetsläget.

Vi noterar att det i tidigare granskning av informationssäkerhet (se sidan 5) samt i denna granskning finns indikationer på att beslutade riskreducerande åtgärder i den interna kontrollen inte genomförs. Vi bedömer att det är en brist och att den interna kontrollen bör stärkas.

Resultat av granskningen

Rutiner och arbetssätt vid IT-incidenter - lakttagelser

➢ **Finns ändamålsenliga rutiner och etablerade arbetssätt för att hantera och dokumentera allvarliga IT-incidenter?**

I kommunens riktlinje för informationssäkerhet framgår att informationsincidenter ska rapporteras, utvärderas och åtgärdas för att uppfylla det övergripande målet med informationssäkerhet. Det finns inga kompletterande anvisningar för hantering av informationssäkerhetsincidenter i kommunen.

För personuppgift och NIS-direktivet finns dock framtagna rutiner och instruktioner. Rutin för personuppgiftsincident finns, som beskriver processen för hantering och anmälan till tillsynsmyndighet. Instruktion för anmälan av NIS-incident är ett stöd för kommunens samhällsviktiga verksamheter. Instruktionen beskriver hantering tillsammans med tidsangivelser att förhålla sig till för rapportering till tillsynsmyndighet.

Intervjuade framhåller att process för hur anmälan och hantering av incidenter saknar tydlig struktur. I intervjuer beskrivs hur hanteringen vanligen utförs men samtidigt anges att det på grund av otydlighet i ansvar och hur frågan ska eskaleras har inneburit att information vid tillfällen har cirkulerat mellan chefer, objektsägare med flera under längre tid utan egentlig åtgärd.

IT-avdelningen har etablerat en ”major incident process”. Det innebär att IT-avdelningen har en utsedd incident manager vilken har ansvar för samordningen av incidenter och hanteringen sker i enlighet med en fastlagd rutin.

När externa leverantörer driftar system åt kommunen kravställs i samband med upphandling att support ska finnas 24 timmar om dygnet, varje dag. Som en säkerhetsåtgärd säkerhetskopieras även data vid extern drift på lokala servrar, i det fall något skulle inträffa som innebär att kommunen inte har tillgång till sin data.

Resultat av granskningen

Rutiner och arbetssätt vid IT-incidenter - Bedömning

- **Finns ändamålsenliga rutiner och etablerade arbetssätt för att hantera och dokumentera allvarliga IT-incidenter?**

Vår bedömning

Vår bedömning är att kommunen saknar ändamålsenliga rutiner för sin övergripande incidenthantering så att det är känt hur incidenter kan upptäckas och hur de ska hanteras. Risken vid bristande rutiner är dels att incidenter inte upptäcks i tillräckligt hög grad, dels att agerandet vid inträffade incidenter inte sker tillräckligt skyndsamt. Det kan resultera i både ekonomisk skada och förtroendeskada för kommunen.

Vår bedömning är att IT-avdelningen har etablerat arbetssätt och rutiner för att hantera IT-incidenter. Informations- och systemägare i kommunen bör dock utvärdera vilka behov av tillgänglighet och beredskap de har för de system som driftas lokalt, på samma sätt som att krav ställs på externa leverantörer.

Resultat av granskningen

Nulägesanalyser och åtgärder - lakttagelser

- **Har kommunstyrelsen efter den senare tidens uppmärksammade attacker mot kommuner gjort någon analys av kommunens nuläge och förutsättningar att stå emot eventuella intrångsförsök eller störningar i IT-miljön? Har åtgärder vidtagits?**

Enligt kommundirektör har ett antal informationsinsatser genomförts till kommunstyrelsen med information om hur väl förberedd kommunen är vid en potentiell IT-säkerhetsrelaterad händelse. Exempelvis ombads IT-säkerhetsansvarig, i samband med att kriget i Ukraina bröt ut, att upprätta ett underlag för att beskriva kommunens IT-säkerhet.

Överlag upplevs intresset ha ökat från ledningsgruppen inom dessa frågor. Ett ökat intresse har även noterats av intervjupersoner från de förtroendevalda men det har inte gått att härleda att nya beslut om åtgärder fattats som ett resultat av de informationsinsatser som gjorts. Samtidigt har under granskningen framkommit att befintlig IT-miljö upplevs vara välfungerande och säker.

Vi noterar att det i kommunstyrelsens investeringsbudget för 2022 framgår att det ska göras nyinvesteringar, vilka beräknas uppgå till 4,8 miljoner kronor för posterna Utbyggnad och utökning av IT-infrastruktur samt Säkerhet och övervakning av system. Av uppföljning i delårsrapporter under 2022 går inte att utläsa i hur hög grad dessa investeringar genomförts.

Behovet av utbildningsinsatser för anställda och förtroendevalda i kommunen inom IT/informationssäkerhet lyfts fram av intervjuade, då sådana insatser inte genomförts under en längre period.

Resultat av granskningen

Nulägesanalyser och åtgärder - Bedömning

- **Har kommunstyrelsen efter den senare tidens uppmärksammade attacker mot kommuner gjort någon analys av kommunens nuläge och förutsättningar att stå emot eventuella intrångsförsök eller störningar i IT-miljön? Har åtgärder vidtagits?**

Vår bedömning

Vår bedömning är att kommunstyrelsens har efterfrågat information om kommunens nuläge inom IT-säkerhet utifrån det förändrade säkerhetsläget och en ökad hotbild för exempelvis cyberhot. Detta har utifrån de uppgifter vi tagit del av inte resulterat i några konkreta åtgärder. Mot bakgrund av att IT-miljön, av ansvariga, bedöms vara säker kan vi inte göra någon bedömning om åtgärder borde ha vidtagits utifrån den rapportering som gjorts. Det finns planer om investeringar för att stärka IT-säkerheten. Vi kan dock inte fastställa utifrån genomförd uppföljning i delårsrapport om detta verkställts under 2022.

Mot bakgrund av de brister som tidigare identifierats i granskning av kommunens informationssäkerhet, utan att åtgärder vidtagits från kommunstyrelsen, är vår bedömning att kommunstyrelsens agerande endast delvis är tillräckligt.

Resultat av granskningen

Kontinuitetsplan - Iakttagelser

- **Finns dokumenterade kontinuitetsplaner avseende IT-drift vid allvarligare störningar och avbrott? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?**

I Riktlinje för informationssäkerhet kravställs att samtliga verksamheter ska ha en kontinuitetsplan. I kommunens instruktion för genomförande av SSA (systemsäkerhetsanalys) framgår att analysen är en metod, bestående utav tre delar. Dessa är informationssäkerhetsklassning, risk- och sårbarhetsanalys, samt kontinuitetskrav. En SSA ska, enligt instruktionerna, genomföras inför anskaffning av nya system, i samband med väsentliga förändringar samt årligen för verksamhets-kritiska system och var tredje år för system som inte bedöms vara verksamhetskritiska. En sådan systemsäkerhetsanalys har enligt uppgift nyligen genomförts på ett av kommunens redan existerande system system för att testa och bedöma hur systemet påverkats om IT-miljön gått ner. Arbetet med SSA:er bedöms av intervjuade vara välfungerande, men huruvida de genomförs i den regelbundenhet som instruktionerna beskriver var man inte helt säker på.

En genomlysning av vilka system och komponenter som finns i kommunens IT-miljö har genomförts av IT-avdelningen. Detta inkluderade framtagande av en uppstartsordning (med prioriteringar) av system. Det har dokumenterats vilka system som är verksamhetskritiska samt de som används inom samhällsviktig verksamhet.

.I genomlysningen av kommunens system och komponenter dokumenterades även beskrivning av roller vid eventuell kris. Dokumentationen framhålls av intervjuade vara omfattande, men ändå i vissa delar sakna väsentligt innehåll.

En skrivbordsövning har genomförts av IT-avdelningen för att testa prioriteringslistan för att se om beslutad uppstartsordning skulle fungera. Detta gjordes emellertid bara med representanter från IT.

Kontinuitetsplaner finns enligt intervjuade både inom IT och andra delar av kommunens verksamheter. Planerna uppges dock inte ha testats. Det framhålls därför finnas en risk att de olika kontinuitets-planerna inte är kompatibla mellan verksamhetsområden om en större incident skulle inträffa. Intervjuade menar att det finns behov av en översyn av kontinuitetsplanerna för att säkerställa att de är aktuella och uppdaterade.

.

.

Resultat av granskningen

Kontinuitetsplan - Bedömning

- **Finns dokumenterade kontinuitetsplaner avseende IT-drift vid allvarligare störningar och avbrott? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?**

Vår bedömning

Vår bedömning är att kontinuitetsplaner för IT-drift finns i vissa delar som kan nyttjas som stöd vid allvarligare störning. De planer som finns har dock endast testats i begränsad omfattning. Utan att planer testas regelbundet utifrån olika scenarier så finns en risk att de inte fungerar tillräckligt väl i kris eller vid en särskild händelse.

Vi ser det därtill som väsentligt att det sker en större samordning av kontinuitetsplanering och hantering där verksamheterna, IT och kommunens säkerhetsfunktioner behöver stämma av planer och bedömningar. Detta så att det finns en samsyn samt för att säkerställa att de underlag som verksamhet och IT ska agera utifrån är tillförlitliga.

Slutsats

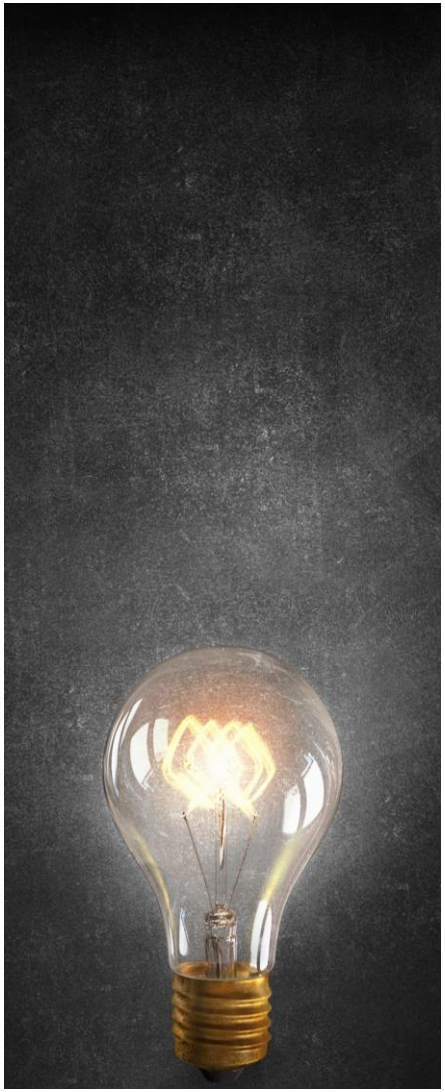
Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen inte har säkerställt att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerheten. Bland annat har ett flertal av de rekommendationer som lämnades i tidigare granskning inte åtgärdats. Vi bedömer att flertalet av dessa även i vissa delar påverkar förutsättningarna för en god IT-säkerhet.

I nuläget saknas en tillräcklig styrning av IT-säkerhet då de styrande dokument som är antagna är i behov kompletteringar för att tydliggöra ansvar inom informationssäkerhetsarbetet, särskilt avseende den tekniska säkerheten. I avsaknad av beskrivningar av ansvarsförhållanden kan vi inte bedöma om organisationen är ändamålsenlig. Vi noterar dock att roller är otydliga och ansvar behöver tydliggöras på olika nivåer.

Modell för informationsklassning finns men är att betrakta som föråldrad. Säkerhetsåtgärder vidtas till viss del som ett resultat av informationsklassningar och systemsäkerhetsanalyser. Kopplingen mellan åtgärder och verksamheternas bedömningar av informationens skyddsvärde kan emellertid stärkas. Kommunens IT-avdelning har vissa tekniska verktyg som möjliggör övervakning för att ha en förmåga att upptäcka hot om intrång eller andra incidenter. Det finns därtill etablerade rutiner för viss verksamhetsnära uppföljning av tekniska säkerhetsåtgärder.

Incidenthanteringsrutiner finns till viss del, främst över IT-avdelningens hantering. Vi ser därför behov av att tydliggöra rutiner så att det finns gemensamma rutiner som används av samtliga verksamheter. Kontinuitetsplaner som kan utgöra stöd vid allvarligare störningar finns till viss del i kommunens verksamheter, de planer som finns har dock endast testats i begränsad omfattning.

Efter den senare tidens uppmärksammade attacker mot kommuner runt om i Sverige har information efterfrågats av kommunstyrelsen och kommunledningen. Vi kan dock konstatera att den information som rapporterats inte har lett till beslut om särskilda åtgärder för verksamheten att verkställa. I övrigt saknas för närvarande en samlad uppföljning av det informationssäkerhetsarbete (inkl. teknisk säkerhet i form av IT-säkerhet) som genomförs i kommunen. Det medför att någon sådan rapportering inte i nuläget genomförs till kommunstyrelsen. Utifrån kommunstyrelsens övergripande ansvar för säkerheten i kommunen anser vi att det är en brist. Utan ett sådant underlag kan inte kommunstyrelsen ha en tillräcklig kontroll och fatta beslut om prioriterade åtgärder för att stärka kommunens informations- och IT-säkerhet.



Rekommendationer

Utifrån uppföljning av tidigare genomförd granskning av informationssäkerhet kvarstår följande rekommendationer till kommunstyrelsen:

— Implementera en informationssäkerhetspolicy.

— Implementera en obligatorisk utbildning om informationssäkerhet med kontinuerliga och regelbundna uppföljningsutbildningar.

— Implementera en systematisk och regelbunden rapportering och uppföljning av informationssäkerhetsarbetet till kommunledningen och kommunstyrelsen.

— Säkerställa att alla verksamheter har tillgång och kännedom om de styrdokument som gäller för verksamheten, samt vilka ansvarsförhållanden som gäller.

— Säkerställa att informationssäkerhetsorganisationen har en tillräcklig omfattning för att möta kommunens behov.

— Ser över möjligheten att implementera nya rutiner för att säkerställa att anställda har rätt behörigheter.

— Implementera en rutin för rapportering av informationssäkerhetsincidenter i ett avvikelserapporteringssystem.

Utifrån vår bedömning och slutsats i den fördjupade granskningen av IT-säkerhet rekommenderar vi kommunstyrelsen att:

— Revidera riktlinjer för informationssäkerhet avseende ansvar för den tekniska säkerheten.

— Se över vilka ytterligare instruktioner och anvisningar som det finns behov av för att etablera en styrning av informations-säkerhetsarbetet.

— Fastställa en ny och uppdaterad modell för riskanalys och informationsklassning.

— Stärka verksamheternas roll i bedömningen av informations skyddsvärde.

— Tillse att de beslut om riskreducerande åtgärder i internkontrollen verkställs och att uppföljning sker av att åtgärder lett till minimerad risk.

— Att genomföra penetrationstester av IT-miljön.

— Fastställa kommunövergripande incidenthanteringsrutiner som tillämpas av alla verksamheter. Samt tillse att nämnder upprättar kompletterande incidenthanteringsrutiner utifrån verksamhetsspecifika krav och lagar.

— Utvärdera befintliga kontinuitetsplaner samt införa tester av de planer som finns för att säkerställa att underlag skulle fungera vid särskilda händelser.

Datum som ovan

KPMG

Viktor Tagesson *Jenny Thörn*

Viktor Tagesson
Verksamhetsrevisor

Jenny Thörn
Verksamhetsrevisor

Micaela Hedin

Kundansvarig

Detta dokument har upprättats enbart för i dokumentet angiven uppdragsgivare och är baserat på det särskilda uppdrag som är avtalat mellan KPMG AB och uppdragsgivaren. KPMG AB tar inte ansvar för om andra än uppdragsgivaren använder dokumentet och informationen i dokumentet. Informationen i dokumentet kan bara garanteras vara aktuell vid tidpunkten för publicerandet av detta dokument. Huruvida detta dokument ska anses vara allmän handling hos mottagaren regleras i offentlighets- och sekretesslagen samt i tryckfrihetsförordningen.

Jenny Thörn

Viktor Tagesson

kpmg.com/socialmedia

Document Classification: KPMG Public