Granskning av informationssäkerhet

Rapport

Linköpings kommun

KPMG AB

2022-02-07

Antal sidor 20

Linköpings kommun
Granskning av informationssäkerhet

2022-02-07

Innehållsförteckning

Linköpings kommun
Granskning av informationssäkerhet

2022-02-07

1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Linköpings kommun fått i uppdrag att genomföra en granskning av kommunstyrelsen och samtliga nämnders rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för 2021.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnderna till viss del har ett ändamålsenligt informationssäkerhetsarbete.

Det finns i stora delar en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågor i kommunen. Kommunstyrelsen har genom beslut av styrande dokument och uppdrag till verksamheten tydliggjort ansvarsfördelning och de aktiviteter som ingår i kommunens ledningssystem för informationssäkerhet. Den informationssäkerhetshandbok som nyligen fastställts har dock vid tiden för granskningen inte hunnit implementeras så att ansvar och krav i arbetet är etablerat fullt ut.

Kommunens förvaltningsstyrningsmodell har bidragit till att etablera en tydlig roll- och ansvarsfördelning mellan verksamhet och IT-organisation. Vi noterar dock att informationssäkerhetsarbetet i nuläget har en tydlig koppling till rutiner och arbetssätt inom LKDATA som initierar aktiviteter där informationsägarna och andra representanter från verksamheten kallas. Ansvar hos nämnderna och informationsägarna behöver etableras så att de aktiviteter som anges i styrande dokument genomförs och följs upp löpande.

Vår bedömning är att det till viss del finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet. Riskbedömning och informationsklassning görs främst inför implementering av nya system, på initiativ från LKDATA. Rutiner saknas däremot för att regelbundet ompröva de genomförda informationsklassningar och riskanalyser som gjorts för att möta nya risker och behov när systemen är i drift. Kommunstyrelsen och nämnderna har inte etablerat arbetssätt och rutiner för att systematiskt följa upp genomförda åtgärder. Det finns därigenom inte någon dokumenterad uppföljning där underlag kan ligga till grund för beslut om förbättringsåtgärder för att utveckla informationssäkerheten. Inom LKDATA finns etablerade uppföljningsprocesser för den del av informationssäkerhetsarbetet som de har ansvar för kopplat till IT-tjänster. Det saknas i nuläget former för att löpande följa upp att beslut och styrande dokument för informationssäkerhet efterlevs.

Kommunens incidenthanteringsprocess är i vissa delar och för vissa typer av incidenter i huvudsak ändamålsenlig. Detta avser främst personuppgiftsincidenter samt IT-säkerhetsincidenter där vi konstaterar att det finns etablerade rutiner för anmälan och hantering av inträffade incidenter. Det finns däremot risk att informationssäkerhetsincidenter inte upptäcks i tillräckligt hög grad. Det kan medföra att incidenter sker som inte utreds och kan utgöra grund i det löpande förbättringsarbetet.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Följa upp att implementeringen av informationssäkerhetshandboken följer projektplanen och når de milstolpar och mål som finns beslutade.
- Säkerställa att de krav och förväntningar som finns i utvecklingsarbetet tilldelas tillräckliga resurser i form av stöd och utbildning så att den ansvarsfördelning som etableras kan upprätthållas.
- Inrätta kommungemensamma incidenthanteringsrutiner och erbjuda utbildnings- och informationsinsatser så att incidenter upptäcks och hanteras.
- Säkerställa att uppföljning av efterlevnad av styrande dokument görs, exempelvis genom interna revisioner.
- Säkerställa att det arbete och de åtgärder som genomförs i syfte att stärka informationssäkerheten följs upp och löpande utvärderas.

Utifrån vår bedömning och slutsats rekommenderar vi nämnderna att:

- Säkerställa att de roller som beskrivs i styrande dokument etableras så att det finns en organisation och resurser för informationssäkerhetsarbetet.
- Inrätta rutiner för att regelbundet följa upp de riskanalyser och informationsklassningar som gjorts för att möta nya risker och behov.
- Inrätta uppföljningsrutiner för att säkerställa en tillräcklig efterlevnad av de styrande dokumenten för informationssäkerhet.

2 Bakgrund

KPMG har av Linköpings kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsen och nämndernas rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2021.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används om informationssäkerhet för information som hanteras i kommunens IT-system. Allt mer information hanteras idag med olika tekniska lösningar och aldrig förr har kommunerna hanterat sådana mängder information som görs idag. Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod. Många verksamheter inom kommunen är idag helt beroende av väl fungerande IT. För flera verksamheter handlar ett väl fungerande IT-stöd såväl om säkerhet som möjlighet till en fungerande verksamhet utan driftstörningar. Ett kritiskt område är ofta äldreomsorg där driftstörningar i journalsystem och schemaprogram kan få stora direkta konsekvenser för brukarna. Ett annat område är kommunens elevregister där stora mängder personlig information om eleverna i kommunens skolor finns samlat.

Informationssäkerhet innebär att skydda information utifrån dess krav på konfidentialitet, riktighet och tillgänglighet i alla kommunens system. För att kunna hantera detta på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget. Informationssäkerhet är inte en IT-fråga utan en fråga om att säkra och trygga driften av kommunens kärnverksamheter. 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.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att arbetet med informationssäkerheten behöver granskas.

2.1 Syfte, revisionsfråga och avgränsning

Granskningens syfte är bedöma om kommunstyrelsen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Med ändamålsenlighet menar vi att kommunen bedriver ett arbete som skyddar information så:

- att den alltid finns när vi behöver den (tillgänglighet)
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den (konfidentialitet)

Granskningen ska besvara följande revisionsfrågor:

- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i kommunen?
- Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?
- Arbetar kommunens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?
- Finns det ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet (dokumenterat och förankrat i kommunens verksamheter)?
- Är kommunens incidenthanteringsprocess ändamålsenlig?
- Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?
- Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?

Granskningen avser kommunstyrelsen och samtliga nämnder.
Granskningen avser revisionsåret 2021.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

2.3 Metod

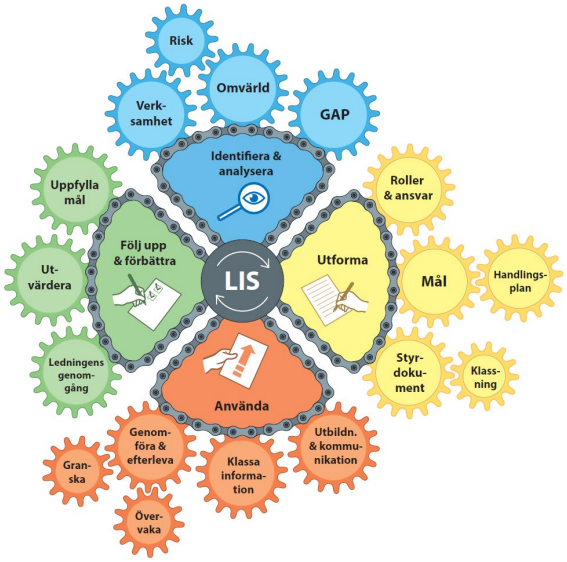
Granskningen har genomförts genom dokumentstudier (bilaga 1) och intervjuer/avstämningar med berörda tjänstemän (bilaga 2).

Granskningen har genomförts av Jenny Thörn, verksamhetsrevisor under ledning av Karin Helin Lindqvist, certifierad kommunal revisor som deltar i granskningen utifrån sin roll som kundansvarig.

2.4 Metodstöd för systematiskt informationssäkerhetsarbete

MSB har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet är baserat på den internationella standardserien för informationssäkerhet, ISO/IEC 27000 och ämnar till att förtydliga hur informationssäkerhetsarbetet kan utformas.

Metodstödet består av fyra olika metodsteg för informationssäkerhetsarbetet vilka illustreras i nedanstående figur.



2.4.1 Identifiera och analysera

Syftet med att analysera avseende informationssäkerhetsarbetet är enligt MSB att säkerställa att informationssäkerheten utformas utifrån verksamhetens rådande förutsättningar. Det ska även leda till att väsentliga informationstillgångar identifieras, vilka risker de ska skyddas mot, samt valda säkerhetsåtgärder.

2.4.2 Utforma

Enligt MSB:s metodstöd behövs följande delar för ett systematiskt informationssäkerhetsarbete:

- Organisation
- Informationssäkerhetsmål
- Styrdokument
- Klassningsmodell

- Handlingsplan
- Kontinuitetshantering för informationstillgångar

2.4.3 Använda

När verksamheten har utformat styrningen enligt avsnitt 2.4.2 ska det tillämpas. Det innebär:

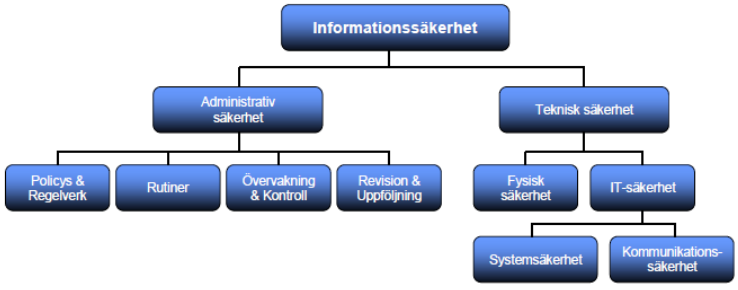
- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet
- Utbilda och kommunicera informationssäkerhetsfrågor till organisationens medarbetare. Det är ständigt pågående arbete som är nödvändigt för att skapa ett systematiskt informationssäkerhetsarbete.

2.4.4 Följa upp och förbättra

Informationssäkerhetsarbetet ska utvärderas och följas upp för att säkerställa att arbetets fortsatta lämplighet, tillräcklighet och verkan. Det kan enligt MSB ske genom övervakning, mätning och måluppföljning.

2.4.5 Roller och ansvar

Informationssäkerhetsbegreppet och dess innehåll kan översiktligt beskrivas i nedanstående skiss:



Informationssäkerhetsarbetet kan struktureras i ett Ledningssystem för informationssäkerhet, kallat LIS. I ett sådant har verksamheten tydliggjort krav som ställs genom styrande dokument och hur ansvaret är fördelat.

En central del i ett ledningssystem är, enligt MSB, ledningens uttalade stöd. Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare. Det är viktigt att alla i en organisation

känner till och förstår innehållet i policys och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete. En stor del av arbetet med att driva ett ledningssystem handlar därför om att informera medarbetare om de regler som ingår i ledningssystemet.

Den svenska och internationella standardserien SS-ISO/IEC 27000 visar på ett sådant ledningssystem där säkerhetsnivån tar sin utgångspunkt i en verksamhetsanpassad riskanalys, och där informationssäkerhetsarbetet följer en tydlig process. Tillämpning av standarderna enligt denna serie underlättar arbetet med informationssäkerhet inom organisationer och förbättrar också möjligheterna att externt bedöma säkerhet och revidera denna på ett enhetligt sätt.

Enligt MSB:s metodstöd för hur ett systematiskt informationssäkerhetsarbete ska bedrivas framgår det hur ansvaret för arbetet med informationssäkerhet bör fördelas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, verksamhetschefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten.

Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men bör generellt vara placerad nära ledningen, exempelvis i ledningsstaben. Vanliga organisatoriska placeringar, enligt MSB:s metodstöd är exempelvis:

- Säkerhet
- Kvalitet
- Juridik

I de fall rollen är placerad i en strategisk IT-funktion bör funktionen vara åtskild från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetssamordnaren både ska granska och vara kravställande gentemot IT-driften och riskerar annars att brista i opartiskhet.

3 Resultat av granskningen

3.1 Organisation

3.1.1 Styrande dokument

Kommunens informationssäkerhetsarbete tar sin utgångspunkt i en beslutad *Säkerhetspolicy*[1]. Av policyn framgår att den tillsammans med underliggande dokument syftar till att tydliggöra mål, omfattning och ansvar för säkerhetsarbetet. Policyn avser att skapa förutsättningar och vara ett stöd i kommunens säkerhetsarbete. Arbetet ska leda till att kommunens förmåga att hantera informationen utifrån legala, etiska, och verksamhetsmässiga intentioner upprätthålls. Kommunen ska i arbetet värdera information och kartlägga risker så att relevanta skyddsåtgärder vidtas.

Säkerhetspolicyn konkretiseras genom underliggande riktlinjer. En av dessa är *Riktlinje för informationssäkerhet*[2]. Det övergripande målet med riktlinjen är ”att tillse att det operativa informationssäkerhetsarbetet bedrivs i enlighet med gällande lagstiftning”.

Vidare framgår att kommunstyrelsen med stöd i riktlinjen ska kunna styra kommunens informationssäkerhetsarbete i enlighet med Myndigheten för samhällsskydd och beredskaps rekommendationer för kommuners informationssäkerhet samt de krav som anges i informationssäkerhetsstandarden ISO/IEC 27000.

Riktlinjen anger att kommundirektören har i uppdrag att upprätta och vid behov revidera tillämpningsanvisningar i form av en informationssäkerhetshandbok som ska utgöra kommunens ledningssystem för informationssäkerhet. Handboken har fastställts under hösten 2021 och för implementeringen finns en projektplan och utsedd projektledare. Projektplanen anger tidsplan med beslutspunkter och milstolpar för olika aktiviteter.

Av projektplanen framgår att kommunen inte har ett gemensamt arbetssätt för informationssäkerhet. Införande av ledningssystemet ska skapa en gemensam hantering och process för arbetet med informationssäkerhet. I projektplanen beskrivs att nulägesanalyser ska genomföras inom alla verksamheter så att åtgärdsplaner kan upprättas i syfte att nå ställda krav i ledningssystemet på sikt.

Informationssäkerhetshandboken kommer enligt intervjupersoner att vara ett viktigt underlag för ett mer systematiskt arbetssätt med informationssäkerhet. Bland annat nämns att handboken på ett tydligare sätt kan utgöra grund för intern kontroll och uppföljning av att de regler och krav som finns dokumenterade efterlevs. Detta upplevs till stor del ha saknats tidigare i arbetet.

Intervjupersoner beskriver dock att kommunen under ett antal år arbetat systematiskt med riskanalyser och informationsklassningar samt andra aktiviteter kopplade till system och IT-tjänster.

[1] Antagen av Kommunfullmäktige 2021-04-27, § 176
[2] Antagen av Kommunstyrelsen 2019-11-19, § 359, reviderad 2021-04-20, § 118

3.1.2 Roller och ansvar

I *Reglemente för Linköpings kommun*[3] framgår att kommunstyrelsen har ansvar att leda och samordna informationssäkerhetsfrågor i kommunen. I kommunstyrelsens ansvar ingår enligt *Riktlinje för informationssäkerhet* att de ska ange vad som ska skyddas, hur en verksamhet ska avgöra lämplig skyddsnivå samt hur det faktiska skyddet uppnås.

Respektive nämnd ansvarar för att säkerhetsarbetet som gäller den/de egna förvaltningen/förvaltningarna följer säkerhetspolicyn samt övriga till området gällande styrdokument. Ansvar för informationssäkerheten följer det ordinarie verksamhetsansvaret hela vägen från kommunfullmäktige till enskilda medarbetare.

Principen är att den som är formellt ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamheten. I informationssäkerhetshandboken finns ansvarsfördelning beskriven såväl inom verksamheterna som mellan respektive verksamhet och kommunens IT-organisation, LKDATA.

I intervjuer framkommer att det finns ett stort engagemang hos kommunledningen för säkerhetsfrågor där resurser tillsatts. Det har medfört att arbetet har kunnat utvecklats löpande för flera av de ansvarsområden som kommunen har och att flera funktioner nu är iblandade i informationssäkerhetsarbetet. Enligt uppgift i intervjuer pågår därtill en ett utvecklingsarbete för att ytterligare stärka kommunens säkerhetsarbete och säkerhetskultur. Resurser i förvaltningarna stärks genom utsedda säkerhetsombud. En tilläggsbudget har beslutats för att kunna genomföra utbildningsinsatser under 2022 så att säkerhetsombuden rustas med kunskap och kan vara nyckelpersoner i arbetet med informationssäkerhetshandboken, riskanalysarbete mm.

Som stöd i verksamheternas arbete finns en centralt placerad informationssäkerhets-samordnare som rapporterar till säkerhetschef. Samordnaren har inget formellt ansvar för informationssäkerhet men har i uppdrag att leda, samordna och följs upp arbetet. Enligt uppgift har kommunen haft en centralt utsedd informationssäkerhetssamordnare i närmare tio år och rollen beskrivs ha blivit mer och mer renodlad med åren. Det anges finnas ett nära samarbete mellan samordnaren och funktioner inom LKDATA.

I kommunen tillämpas en förvaltningsstyrningsmodell, pm3[4]. I modellen beskrivs mer i detalj hur samverkan och rollfördelning ser ut mellan verksamhet och IT-förvaltning. I intervjuer beskrivs modellen ha bidragit på ett bra sätt för att tydliggöra gränsdragning mellan verksamhet och IT-organisation. Objektledare verksamhet som företräder verksamheten och objektledare IT som företräder den tekniska sidan är exempel på roller i modellen. Dessa är på övergripande nivå ansvariga för IT-komponenter som ingår i pm3-arbetet, där en struktur, processer och aktiviteter finns definierade.

LKDATA har en process för hantering av informationssäkerhet relaterat till IT-tjänster inom Linköpings kommun, vilken benämns Information Security Management.

[3] Antaget av Kommunfullmäktige, 2018-03-27, § 77, reviderat senast 2020-11-24, § 248
[4] En externt utvecklad förvaltningsmodell för IT-stöd som nyttjas av många verksamheter för systemförvaltning eller verksamhetsstyrning.

Processen beskriver aktiviteter vid införande och förändring av IT-tjänster. LKDATA är certifierade i enlighet med ISO 20000-1 inom IT-tjänstehantering och genom det sker löpande externa revisioner av processer och arbetssätt där återkoppling med rekommendationer om förbättringsåtgärder ges.

I kommunen finns ett informationssäkerhetsråd som behandlar informationssäkerhets-relaterade ärenden. Informationssäkerhetsrådet består av kommunens säkerhetschef, CIO[5], IT-säkerhetssamordnare, objektägare IT, informationssäkerhetssamordnare samt chefsjurist. Det är informationssäkerhetssamordnaren som leder forumet och adjungerar övriga medlemmar (till exempel företrädare för juridik, fastigheter och digitalisering) efter behov beroende på aktuella ärendens art.

3.1.3 Bedömning

Vår bedömning är att det i huvudsak finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågor i kommunen. Kommunstyrelsen har genom beslut av styrande dokument och uppdrag till verksamheten tydliggjort ansvarsfördelning och de aktiviteter som ingår i kommunens ledningssystem för informationssäkerhet. Den informationssäkerhetshandbok som nyligen fastställts har dock vid tiden för granskningen inte hunnit implementeras så att ansvar och krav i arbetet är etablerat.

Vår bedömning är att kommunens förvaltningsstyrningsmodell har bidragit till att etablera en tydlig roll- och ansvarsfördelning mellan verksamhet och IT-organisation. Inom IT-verksamheten finns tydliggjorda rutiner i arbetet där informationsägare och andra representanter kallas för att delta i processer i informationssäkerhetsarbetet.

Vi konstaterar att den höga ambitionsnivån som beslutats för kommunens arbete behöver mötas med en strukturerad kommunikation, utbildning, stöd och resurser. Utan detta finns en risk att handboken upplevs alltför omfattande och verksamheterna därför brister i efterlevnad. Det i sin tur riskerar att leda till att kommunens informations-säkerhetsarbete inte når de intentioner och förväntningar som finns.

[5] Chief Information Officer, ofta översatt till IT-direktör eller IT-chef.

3.2 Analys av behov och risker för informationssäkerhet

Eftersom skadeverkningarna av bristande säkerhet i system även medför risker hos andra informationsägare och verksamheter behöver riskbedömning och kravställningar om åtgärder ske med samsyn och med delaktighet från olika funktioner i kommunen.

3.2.1 Riskhantering

Det finns framtagna mallar för riskanalys avseende informationstillgångar. I mallarna ingår att bedöma de fyra aspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Utifrån en riskmatris ska sedan risker värderas i förhållande till sannolikhet och konsekvens.

I intervjuer beskrivs att arbetet med riskanalyser främst sker inför utveckling, upphandling och införande av nya system. Inför nya systeminföranden säkerställer LKDATA att riskanalyser och bedömningar görs så att rätt krav kan ställas och säkerhetsåtgärder vidtas för att möta identifierade risker.

Intervjupersoner beskriver att det i nuläget saknas rutiner för att uppdatera riskanalyser med nya bedömningar när system och tjänster är i drift och verksamheten har tagit över ansvaret. Nya riskbedömningar sker inte utifrån en rutin eller regelbundenhet, utan främst när någon uppmärksammar att det finns behov.

3.2.2 Informationsklassificering

För att tydliggöra att olika typer av information har olika värde för verksamheten bör en klassning av information och system genomföras. Kommunen kan därefter skapa förutsättningar för lämpliga skyddsnivåer. Detta görs oftast med en systemöversikt där ansvar och roller är definierade och dels med stöd av någon metod för informationsklassning.

Linköpings kommun har infört en modell för informationsklassning med tillhörande instruktioner och mallar. I intervjuer beskrivs att riskanalys och klassning har genomförts under flera år och är etablerat som process i informationssäkerhetsarbetet.

I informationssäkerhetshandboken finns väl beskrivet vilka krav som ställs på informationsklassning och de bedömningar av risker som ska göras. I handboken framgår bland annat att informationsklassning innebär att information klassas i olika nivåer utifrån vad konsekvensen skulle kunna bli om informationen:

- röjs till obehörig (konfidentialitet)
- inte är korrekt eller aktuell (riktighet)
- inte finns att tillgå när den behövs (tillgänglighet)
- inte är spårbar (spårbarhet)

Klassningen ska ske i fyra nivåer av konsekvenser; lindrig, måttlig, betydande, allvarlig. Vidare framgår att realistiska värderingar bör göras för att undvika att information får onödigt högt skydd, med höga kostnader som följd, eller för lågt skydd, vilket medför för stor riskexponering.

Enligt den nyligen antagna informationssäkerhetshandboken är informationsägaren ansvarig för att informationsklassning utförs för verksamhetens information. Detta ska dokumenteras i verksamhetens informationshanteringsplan.

I intervjuer beskrivs att ett internt arbete har pågått under ett antal år för att utveckla det som tidigare benämndes dokumenthanteringsplan till att vara informationshanteringsplaner där informationssäkerhetsaspekter inkluderas. I det arbetet har informationsklassning gjorts utifrån informationstyper men intervjupersoner har inte kunnat uppskatta för hur stor del av kommunens informationstillgångar detta har gjorts.

I projektplan för implementering av ledningssystemet framgår effektmålet ”*Samtliga förvaltningar har en uppdaterad och berikad informationshanteringsplan (IHP) med informationsklassning och påbörjad informationsklassning av arbetsmaterial*”. Vi uppfattar målet som att det finns informationstillgångar som inte är klassade ännu.

Intervjupersoner beskriver väl etablerade arbetssätt för informationsklassning för de system som implementerats. Vid dessa tillfällen kallar LKDATA berörda till ett antal workshops för att göra riskbedömning och informationssäkerhetsklassning. I workshops närvarar dels LKDATA med teknisk expertis, dels representanter från verksamheten i form av objektledare och slutanvändare. Vid behov deltar även ytterligare funktioner, exempelvis dataskyddsombud eller juridisk kompetens.

Beroende på vilken typ av system som ska klassas närvarar olika antal personer och funktioner. Intervjupersoner bekräftar betydelsen av att ha en stor representation från verksamheten, då de är experter på vilka informationstillgångar som avses att hanteras i systemet.

I intervjuer beskrivs att dokumentation sker i avsedda mallar för klassning och riskanalys och förvaras i gemensamma mappar/samarbetsytor som verksamhet och LKDATA har tillgång till. Underlagen ligger till grund för kravställningar till leverantörer men även behov av åtgärder internt som identifierats för att möta risker. Vi har i granskningen tagit del av exempel på genomförda klassningar och den dokumentation som utgör underlag för dessa. Intervjupersoner uppskattar att ca 70-80 % av informationstillgångarna som hanteras i system är informationsklassade och att samtliga verksamhetskritiska system ingår i dessa.

I intervjuer beskrivs vidare att personuppgiftshantering är en väsentlig del i arbetet med riskanalys och klassning. Konsekvensbedömningar utifrån dataskyddsförordningen upprättas i de fall personuppgifter är en del av informationstillgångarna som hanteras.

I intervjuer beskrivs att det saknas rutiner för att löpande uppdatera informations-klassningar efter det att system är i drift.

3.2.3 Medvetenhet och förståelse

En viktig del i ett systematiskt informations- och IT-säkerhetsarbete är att det finns en tillräcklig medvetenhet hos de som har tillgång till kommunens information. I kommunen är detta bland annat förtroendevalda, medarbetare, elever och externa konsulter.

I intervjuer framkommer att medvetenheten har ökat i hög grad i kommunen av flera anledningar. Dels anges det ökade fokuset generellt i samhället för dessa frågor ha spelat roll, dels utvecklingsarbete som genomförts internt i kommunen. Bland annat anges implementering av Google Workspace där information och utbildningsinsatser genomförts för att säkerställa informationshanteringen, främst avseende personuppgifter.

Därtill anges att flera av kommunens verksamheter har stor erfarenhet av att hantera känslig information, dels inom vård- och omsorg, dels inom skolverksamheten.

I projektplanen för implementering av ledningssystemet för informationssäkerhet finns utbildningsinsatser som milstolpar. Under hösten 2021 ska utbildningar erbjudas till olika målgrupper i kommunen. Aktiviteten är även ett av effektmålen i projektet och ska mätas genom statistik från e-utbildningar och ett kunskapstest. Av planen framgår att det är ett ansvar inom projektet att säkerställa att det finns krav och rutiner för att alla genomför utbildningarna i respektive förvaltning. Därtill ska rutiner tas fram så att utbildningar ingår i introduktion för nyanställda samt vidareutbildning för de funktioner som bedöms behöva fördjupade kunskaper.

En av intervjupersonerna har vid tiden för intervjun genomgått sin utbildning och upplevde att utbildningen var lätt att förstå och ta till sig. Vidare sågs det som en god insats för att öka medvetenhet och kunskap på bred front.

Kommunen har även erbjudit utbildningar utifrån dataskyddslagstiftningen samt inom offentlighet och sekretess.

3.2.4 Bedömning

Vår bedömning är att det till viss del finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet. Det finns framtagna anvisningar och mallar för att göra riskbedömning och informationsklassning. Riskbedömning och informationsklassning görs främst inför implementering och vidareutveckling av system, på initiativ från LKDATA. Rutiner saknas däremot för att regelbundet ompröva de genomförda informationsklassningar och riskanalyser som gjorts för att möta nya risker och behov när systemen är i drift. Detta ansvar behöver etableras hos informationsägarna och rutiner inrättas.

Krav på dokumenterade informationsklassningar för samtliga informationstillgångar ställs i den nyligen beslutade informationssäkerhetshandboken där även rutiner för uppföljning finns dokumenterat. Vi bedömer att det kan ge kommunen stärkta möjligheter att säkerställa att risker för samtliga informationstillgångar identifieras och möts med åtgärder.

Utbildningsinsatser har endast till viss del genomförts och det kan därför finnas risk att de som hanterar kommunens information inte har tillräcklig kunskap och en medvetenhet om säker informationshantering som inte utsätter tillgångarna för risker. Utbildningsinsatser planeras att genomföras i samband med implementeringen av informationssäkerhetshandboken med start under hösten 2021 vilket vi ser som positivt.

3.3 Incidenthantering

Av riktlinjerna för informationssäkerhet framgår att incidenter och säkerhetsmässiga svagheter, utan dröjsmål, ska rapporteras till närmast överordnade chef enligt gällande rutiner för Linköpings kommun.

Enligt intervju har det under de senaste åren skett en ökning av incidentrapporteringar vilket enligt intervjupersoner tolkas som en indikation på högre medvetenhet om frågorna. Det avser främst personuppgiftsincidenter och anges bero på att det har funnits ett strukturerat arbete med dataskydd i kommunen med utbildningar, aktiviteter och utsedda representanter i respektive förvaltning.

Efter att rapportering skett så fördelas ärenden till olika funktioner beroende på typ av incident. Roller finns tilldelade i systemet så information går till den funktion som finns angiven beroende på om det är en personuppgiftsincident, tillgänglighetsstörning i system eller annan form av händelse eller störning. Efter rapportering startas utredning och om behov finns så sker en rapportering till tillsynsmyndighet.

Det inkommer även en stor andel frågeställningar från medarbetare till dataskyddsombud, jurister samt LKDATA över hur de ska bedöma incidenter och om händelser som skett skulle kunna vara en incident som behöver anmälas.

Vad gäller informationssäkerhetsincidenter anges i intervjuer att det finns en större otydlighet avseende rutiner för att hantera och rapportera dessa. Det har inträffat incidenter som inte uppfattats så allvarliga från början men som senare i processen visat en annan allvarsgrad. Det anges vara långa eskaleringsvägar tills någon med rätt kunskap bedömer vad som inträffat och dess konsekvenser.

Inom LKDATA finns standardiserade processer för incidenthantering som avser IT-incidenter. De har en stor andel tekniska implementationer för att skydda kommunens system och information som löpande övervakar trafik på nätet i syfte att upptäcka incidenter. Om det sker en allvarlig incident så finns framtagna rutiner och processer för detta.

I den nyligen antagna informationssäkerhetshandboken finns information om rapportering av informationssäkerhetsincidenter med tillhörande instruktioner. Det pågår ett utvecklingsarbete för att etablera en liknande rutin och hantering som för personuppgiftsincidenter men är vid tiden för granskningen inte slutfört.

Enligt uppgift har ett antal incidenter rapporterats, främst till integritetsmyndigheten. Dessa har dels varit kopplade till system, dels information på papper.

3.3.1 Bedömning

Vår bedömning är att kommunens incidenthanteringsprocess i vissa delar och för vissa typer av incidenter i huvudsak är ändamålsenlig. Detta avser främst personuppgiftsincidenter samt IT-säkerhetsincidenter där vi konstaterar att det finns etablerade rutiner för anmälan och hantering av inträffade incidenter.

Det finns däremot risk att informationssäkerhetsincidenter inte upptäcks i tillräckligt hög grad. Det kan medföra att incidenter sker som inte utreds och kan utgöra grund i det löpande förbättringsarbetet. Därtill kan inträffade incidenter, om de inte upptäcks tillräckligt skyndsamt, leda till allvarliga konsekvenser för kommunens informationstillgångar. Vi bedömer att informations- och utbildningsinsatser bör genomföras över vad som är incidenter och hur dessa ska hanteras så att en tillräcklig medvetenhet och kunskap finns i verksamheten.

Inträffade incidenter bör därtill dokumenteras och analyseras på kommunövergripande nivå så att ansvariga, exempelvis informationssäkerhetsrådet, kan bedöma om det finns behov av rutiner, utbildningsinsatser eller annan åtgärd för att ytterligare stärka kommunens incidenthanteringsprocess.

3.4 Uppföljning, intern kontroll och rapportering

3.4.1 Intern kontroll och uppföljning

Styrelsen och varje nämnd har det yttersta ansvaret och ska upprätthålla en tillfredsställande internkontroll, det vill säga de ska med rimlig grad av säkerhet säkerställa att bland annat att efterlevnad av tillämpliga lagar, föreskrifter, riktlinjer sker.

Det har enligt uppgift inte funnits någon etablerad struktur för uppföljning av informationssäkerhetsarbetet fram till nu. Handboken avser dock att bidra med en tydliggjord struktur när arbetet är implementerat. I handboken finns i avsnitt 3.12 beskrivet hur efterlevnad och granskning ska organiseras. Bland annat anges att det ska ske genom ordinarie verksamhetsuppföljning, intern kontroll och kontroller utförda av kommunrevisionen. Informationssäkerhetssamordnaren har inte genomfört några interna revisioner för att kontrollera efterlevnad av beslutade policys och riktlinjer som funnits innan handboken fastställdes.

Informationssäkerhetssamordnaren och informationssäkerhetsrådet anges vara nyckelfunktioner i granskning och uppföljning i det kommande arbetet utifrån ledningssystem för informationssäkerhet.

Inom LKDATA finns det enligt uppgift kontrollpunkter avseende informationssäkerhet i internkontrollplan. LKDATA har även genomfört sårbarhetsanalyser och planer för åtgärder inom informationssäkerhet, dessa är dock sekretessbelagda av säkerhetsskäl och vi har i granskningen inte tagit del av dessa underlag.

Utifrån LKDATA:s certifiering enligt 20000-1 genomförs årliga externa revisioner med uppföljning av rutiner och arbetssätt där förbättringsåtgärder identifieras och rekommenderas.

3.4.2 Rapportering

Enligt MSB:s metodstöd för ett systematiskt informationssäkerhetsarbete som vi beskrivit inledningsvis i rapporten så är ledningens förståelse för och engagemang i informationssäkerhet grundläggande för att lyckas. Med andra ord måste ledningen få kunskap om hur de kan leda och styra verksamheten på ett effektivt sätt för att åstadkomma god informationssäkerhet. Ledningens stöd är också oumbärlig för att frågan ska få acceptans och ett engagemang från andra roller i organisationen.

I ett ledningssystem för informationssäkerhet är en årlig rapportering till ledningen en avgörande punkt för att följa upp det arbete som skett inom informationssäkerhet samt få beslut om prioriteringar och åtgärder för att förbättra arbetet under kommande år.

Intervjupersoner beskriver att det inte finns någon etablerad rapportering till kommunstyrelsen eller nämnderna. Funktioner från säkerhetsavdelningen, LKDATA och objektledare har dock deltagit i sammanträden för att föredra aktuella ärenden och ge information om projekt mm.

I informationssäkerhetshandboken hänvisas till MSB:s planerings- och uppföljningscykler i ett ledningssystem för informationssäkerhet. Därtill beskrivs att kommunens ledningssystem ska utgår från verksamhetens planerings- och uppföljningscykler vilket innebär att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och verksamhetskontroller samt regelbundet ser över styrdokument.

3.4.3 Bedömning

Vår bedömning är att kommunstyrelsen och nämnderna inte har etablerat arbetssätt och rutiner för att systematiskt följa upp genomförda åtgärder. Det finns därigenom inte någon dokumenterad uppföljning där underlag kan ligga till grund för beslut om förbättringsåtgärder för att utveckla informationssäkerheten.

Informationssäkerhetsarbetet inom LKDATA följs upp kontinuerligt i arbetet med intern kontroll samt genom de externa revisioner som görs utifrån certifiering där förslag om förbättringar ingår.

Vår bedömning är att det saknas rutiner för att löpande följa upp att beslut och styrande dokument för informationssäkerhet efterlevs. Det har inte gjorts några interna revisioner eller inkluderats i den interna kontrollen.

Den fastställda informationssäkerhetshandboken avser att tydliggöra ansvar, krav och uppföljningsrutiner för att säkerställa en tillräcklig efterlevnad. Handboken var vid tiden för granskningen inte implementerad i verksamheterna vilket innebär att arbetssätt och krav inte etablerats fullt ut.

4 Slutsats och rekommendationer

4.1 Svar på revisionsfrågor

Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i kommunen?

Vår bedömning är att det i huvudsak finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågor i kommunen. Kommunstyrelsen har genom beslut av styrande dokument och uppdrag till verksamheten tydliggjort ansvarsfördelning och de aktiviteter som ingår i kommunens ledningssystem för informationssäkerhet. Den informationssäkerhetshandbok som nyligen fastställts har dock vid tiden för granskningen inte hunnit implementeras så att ansvar och krav i arbetet är etablerat.

Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?

Vår bedömning är att kommunens förvaltningsstyrningsmodell har bidragit till att etablera en tydlig roll- och ansvarsfördelning mellan verksamhet och IT-organisation. Inom IT-verksamheten finns tydliggjorda rutiner i arbetet där informationsägare och andra representanter kallas för att delta i processer i informationssäkerhetsarbetet.

Arbetar kommunens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?

Vår bedömning är att det finns anvisningar och mallar för att göra riskbedömning och informationsklassning och att dessa används för dokumentation vid genomförande. Riskbedömning och informationsklassning görs dock främst inför implementering av nya system eller vidareutveckling av befintliga system efter initiativ från LKDATA. Rutiner saknas för att regelbundet ompröva de genomförda informationsklassningar och riskanalyser för att möta nya risker och behov när systemen är i drift. Detta ansvar behöver etableras hos informationsägarna och rutiner inrättas.

Krav på dokumenterade informationsklassningar för samtliga informationstillgångar ställs i den nyligen beslutade informationssäkerhetshandboken där även rutiner för uppföljning finns dokumenterat. Vi bedömer att det kan ge kommunen stärkta möjligheter att säkerställa att risker för samtliga informationstillgångar identifieras och möts med åtgärder.

Finns det ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet (dokumenterat och förankrat i kommunens verksamheter)?

Vår bedömning är att det till viss del finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet. Vi konstaterar att det främst är kopplat till den information som hanteras i system och inte för kommunens samtliga informationstillgångar.

Utbildningsinsatser har endast till viss del genomförts och det kan därför finnas risk att de som hanterar information inte har tillräcklig kunskap och medvetenhet om säker informationshantering för att inte utsätta informationstillgångarna för risker. Utbildningsinsatser planeras att genomföras i samband med implementering av informationssäkerhetshandboken, med start under hösten 2021, vilket vi ser som positivt.

Är kommunens incidenthanteringsprocess ändamålsenlig?

Vår bedömning är att kommunens incidenthanteringsprocess i vissa delar och för vissa typer av incidenter i huvudsak är ändamålsenlig. Detta avser främst personuppgiftsincidenter samt IT-säkerhetsincidenter där vi konstaterar att det finns etablerade rutiner för anmälan och hantering av inträffade incidenter.

Det finns däremot risk att informationssäkerhetsincidenter inte upptäcks i tillräckligt hög grad. Det kan medföra att incidenter sker som inte utreds och kan utgöra grund i det löpande förbättringsarbetet. Därtill kan inträffade incidenter, om de inte upptäcks tillräckligt skyndsamt, leda till allvarliga konsekvenser för kommunens informationstillgångar.

Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?

Vår bedömning är att kommunstyrelsen och nämnderna inte har etablerat arbetssätt och rutiner för att systematiskt följa upp genomförda åtgärder. Det finns därigenom inte någon dokumenterad uppföljning där underlag kan ligga till grund för beslut om förbättringsåtgärder för att utveckla informationssäkerheten.

Informationssäkerhetsarbetet inom LKDATA följs upp kontinuerligt i arbetet med intern kontroll samt genom de externa revisioner som görs utifrån certifiering där förslag om förbättringar ingår.

Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?

Vår bedömning är att det saknas rutiner för att löpande följa upp att beslut och styrande dokument för informationssäkerhet efterlevs. Det har inte gjorts några interna revisioner eller inkluderats i den interna kontrollen.

Den fastställda informationssäkerhetshandboken avser att tydliggöra ansvar, krav och uppföljningsrutiner för att säkerställa en tillräcklig efterlevnad. Handboken var vid tiden för granskningen inte implementerad i verksamheterna vilket innebär att arbetssätt och krav inte etablerats fullt ut.

4.2 Slutsats

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnderna till viss del har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Vår bedömning är att kommunstyrelsen genom beslut av styrande dokument och uppdrag till verksamheten har tydliggjort styrningen för ett systematiskt och ändamålsenligt arbetssätt för att uppnå en god informationssäkerhet. Vi konstaterar dock att den höga ambitionsnivån som beslutats för kommunens arbete behöver mötas med en strukturerad kommunikation, utbildning, stöd och resurser. Utan detta finns en risk att handboken upplevs alltför omfattande och verksamheterna därför brister i efterlevnad. Det i sin tur riskerar att leda till att kommunens informations-säkerhetsarbete inte når de intentioner och förväntningar som finns.

Vår bedömning är vidare att uppföljning av efterlevnad av styrande dokument samt de insatser som genomförs i syfte att förbättra informationssäkerheten behöver utvecklas då det i nuläget inte sker på ett strukturerat vis. Rutiner bör därtill inrättas så att verksamheterna med regelbundenhet uppdaterar sina riskanalyser och informationsklassningar så att nya krav och behov kan värderas och nya åtgärder vid behov vidtas för att kommunens informationstillgångar ska ha säkerhetsåtgärder som står i relation till dess skyddsvärde.

4.3 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Följa upp att implementeringen av informationssäkerhetshandboken följer projektplanen och når de milstolpar och mål som finns beslutade.
- Säkerställa att de krav och förväntningar som finns i utvecklingsarbetet tilldelas tillräckliga resurser i form av stöd och utbildning så att den ansvarsfördelning som etableras kan upprätthållas.
- Inrätta kommungemensamma incidenthanteringsrutiner och erbjuda utbildnings- och informationsinsatser så att incidenter upptäcks och hanteras.
- Säkerställa att uppföljning av efterlevnad av styrande dokument görs, exempelvis genom interna revisioner.
- Säkerställa att det arbete och de åtgärder som genomförs i syfte att stärka informationssäkerheten följs upp och löpande utvärderas.

Utifrån vår bedömning och slutsats rekommenderar vi nämnderna att:

- Säkerställa att de roller som beskrivs i styrande dokument etableras så att det finns en organisation och resurser för informationssäkerhetsarbetet.
- Inrätta rutiner för att regelbundet följa upp de riskanalyser och informationsklassningar som gjorts för att möta nya risker och behov.
- Inrätta uppföljningsrutiner för att säkerställa en tillräcklig efterlevnad av de styrande dokumenten för informationssäkerhet.

2022-02-07

KPMG AB

Jenny Thörn	Karin Helin Lindqvist
Kommunal revisor	Certifierad kommunal revisor