Granskning av informationssäkerhet

Rapport

Askersunds kommun

KPMG AB

Datum 2023-01-25

Antal sidor 17

Askersunds kommun
Granskning av informationssäkerhet

2023-01-11

Innehållsförteckning

1 Sammanfattning 3

2 Bakgrund 5

2.1 Syfte, revisionsfrågor och avgränsning 5

2.2 Revisionskriterier 6

2.3 Metod 6

2.4 Metodstöd för systematiskt informationssäkerhetsarbete 7

3 Resultat av granskningen 11

3.1 Iakttagelser 11

3.2 Sammanfattande bedömning och rekommendationer 16

1 Sammanfattning

KPMG har av Askersunds kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsen och nämndernas informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

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

Utifrån granskningens resultat är vår sammanfattande bedömning att kommunstyrelsen och nämnderna inte har säkerställt tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen. Bedömningen baserar vi på att kommunstyrelsen inte tillsett att det finns aktuella och tillräckliga styrdokument som reglerar ansvarsfördelning och hur arbetet ska bedrivas. Det saknas därtill organisation med utsedda funktioner med kompetens och förutsättningar att arbeta med informationssäkerhet. I nuläget saknas ett systematiskt arbete med att identifiera och analysera behov och risker för de informationstillgångar som kommunen hanterar.

Vi kan inte utesluta att det med nuvarande tekniska säkerhetsåtgärder finns risker att kommunens informationstillgångar röjs till obehöriga internt eller externt vid en säkerhetshändelse. Slutligen är vår bedömning att kommunstyrelsen inte har tillsett att det finns etablerade rutiner för informationssäkerhetsincidenter. Detta riskerar att medföra att incidenter inte upptäcks och hanteras tillräckligt skyndsamt. Risken med detta är att det kan leda till större skadeverkan för verksamhetens tillgång till information och förmåga att upprätthålla verksamhetens kontinuitet.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen att:

- Ge kommundirektör i uppdrag att, utifrån MSB:s rekommendationer och metodstöd (avsnitt 2.4), vidta åtgärder i enlighet med dessa så att kommunen etablerar ett systematiskt och riskbaserat informationssäkerhetsarbete.
- Säkerställa att det etableras organisation/funktion med ansvar att leda och samordna informationssäkerhetsarbetet.
- Etablera incidenthanteringsrutiner för informationssäkerhet där ansvar och process för hanteringen tydliggörs.
- Tydliggöra ansvarsfördelning mellan kommunen och gemensam IT-nämnd inom informationssäkerhetsområdet och fastställa vilka tjänster som ingår i förvaltningens uppdrag till kommunerna.

— Efterfråga riskanalys och en nulägesbeskrivning av den tekniska säkerhet som it-nämnden har etablerat för kommunerna för att säkerställa att nuvarande skyddsåtgärder är tillräckliga i förhållande till aktuella hot och risker.

Mot bakgrund av vår granskning rekommenderar vi nämnderna att:

— Säkerställa att en funktion utses med ansvar att leda och samordna nämndens arbete med informationssäkerhet så att det sker med en högre grad av systematik.

— Säkerställa att informationsägare i verksamheten upprätthåller ansvar för informationssäkerhetsfrågorna och initierar ett arbete med riskanalyser och informationsklassning. Analyser bör prioriteras för de system som är mest verksamhetskritiska.

2 Bakgrund

KPMG har av Askersunds kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsen och nämndernas informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används om informationssäkerhet för information som hanteras i kommunens IT-system. Alltmer information hanteras idag med olika tekniska lösningar och aldrig förr har kommunerna hanterat sådana mängder information som görs idag. 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.

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. 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, revisionsfrågor och avgränsning

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

Granskningen ska besvara följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhet?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?

- Sker en kravställning av IT-säkerhetsåtgärder utifrån genomförd riskbedömning och klassning av informationstillgångar som hanteras i system?
- Finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.)?
- Finns incidenthanteringsrutiner och sker en tillräcklig rapportering av inträffade incidenter?
- Görs systematiska uppföljningar av implementerade säkerhetsåtgärder för att kontinuerligt förbättra informationssäkerheten?
- Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?

Granskningen omfattar kommunstyrelsen och samtliga nämnder. Granskningen avser år 2022.

2.2 Revisionskriterier

Vi har bedömt om styrelsen och nämnderna uppfyller

- 6 kap. 6 § kommunallagen (2017:725)
- Tillämpbara interna regelverk, policys och beslut
- MSB[1]: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 av:

- Informationssäkerhetspolicy för Askersunds kommun, 2016-10-04
- Instruktion för informationsklassning, 2022-08-31
- Blankett för genomförande av informationsklassning, 2022-08-31
-

[1] Myndigheten för samhällsskydd och beredskap. MSB har på uppdrag av regeringen ansvar att vara råd- och stödgivande i informationssäkerhetsarbetet och hantera samt förebygga IT-incidenter.

Intervjuer har genomförts med:

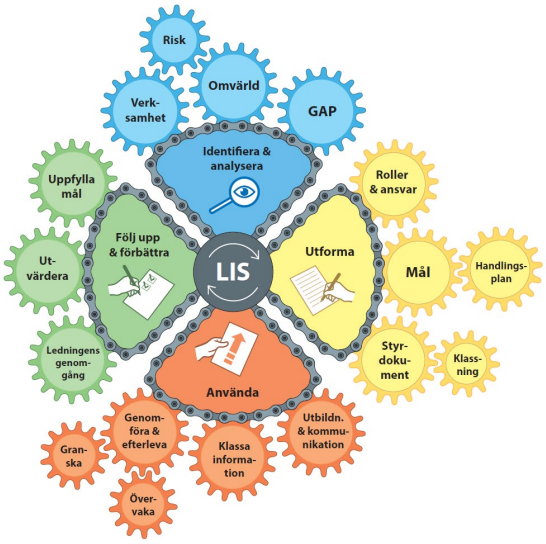
- Administrativ chef, kommunledningsförvaltningen
- Utvecklingsledare och administratör, socialförvaltningen
- Förvaltningschef och IT-strateg, barn- och utbildningsförvaltningen
- Förvaltningschef, tekniska förvaltningen
- Förvaltningschef, förvaltningen för kultur, evenemang och fritid
- Förvaltningschef Sydnärkes IT-förvaltning
- IT-tekniker, Sydnärkes IT-förvaltning

Rapporten är faktakontrollerad av intervjupersoner.

2.4 Metodstöd för systematiskt informationssäkerhetsarbete

MSB har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet 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 Identifiering och analys

Syftet med att analysera 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 Utformning

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

- Organisation
- Informationssäkerhetsmål
- Styrdokument
- Klassningsmodell
- Handlingsplan
- Kontinuitetshantering för informationstillgångar

2.4.3 Användning

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

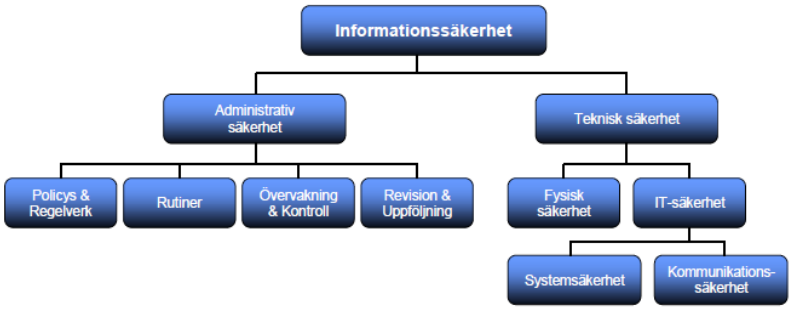
- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet.
- Utbilda och kommunicera informationssäkerhetsfrågor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

2.4.4 Uppföljning och förbättring

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 vägledningen till chefer och övriga medarbetare. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenhet 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 kan 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 ledning, 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 åtskilda från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetssamordnaren både ska granska och vara kravställande gentemot IT-drift och riskerar annars att brista i opartiskhet.

3 Resultat av granskningen

3.1 Iakttagelser

3.1.1 Organisation och styrning

Kommunens informationssäkerhetsarbete tar sin utgångspunkt i en beslutad informationssäkerhetspolicy[2]. Policyn beskriver kommunens mål och inriktning samt styr kommunens informationssäkerhetsarbete. Policyn är framtagen i ett samarbete mellan Askersunds, Hallsbergs, Laxå och Lekebergs kommuner som har en gemensam IT-nämnd och IT-förvaltning.

I informationssäkerhetspolicyn finns en ansvarsfördelning beskriven för informationssäkerhetsarbetet. Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhet. Kommundirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den fastställd informationssäkerhetspolicyn.

Kommundirektörerna i de kommuner som har gemensam IT-förvaltning ska enligt policyn, i samråd med IT-chef, fastslå kommunövergripande regler. Kommundirektören har även ansvar för att utse objektägare för respektive informationssystem. Sydnärkes IT-chef har i ansvar att tillse att driftsäkerheten överensstämmer med objektägarens anvisningar.

I intervjuer framgår att policyn inte har etablerats i kommunens verksamheter. Det finns inte i övrigt några kommunövergripande regler inom informationssäkerhet. Då styrdokument saknas så sker för närvarande ingen uppföljning av efterlevnad av beslut och regler för informationssäkerheten.

Intervjuade beskriver att det saknas funktion som har i ansvar att leda och samordna informationssäkerhetsarbetet i kommunen. Det finns utsedda systemägare för varje system men enligt uppgift så varierar kompetens och förutsättningar i uppdraget mellan systemägarna vilket medför att det inte sker något systematiskt och likvärdigt arbete med systemen i nuläget avseende informationssäkerhet.

[2] Kommunstyrelsen, 2016-10-04

3.1.2 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.

Av intervjuer framgår att det varken finns riktlinjer eller etablerade arbetssätt för att klassa informationen i kommunens system. Det har inte gjorts några informationsklassningar eller andra riskbedömningar av de system som nyttjas i verksamheterna.

Av intervjuade framkommer att det pågår ett arbete att upprätta registerförteckningar för personuppgiftsbehandlingarna i kommunen. Arbetet har fördelats i ledningsgruppen, baserat på tjänstemännens ansvarsområden.

3.1.3 IT-säkerhetsåtgärder

Som vi skrivit i inledningen av rapporten så finns en gemensam IT-nämnd och förvaltning som utgör kommunens IT-funktion. Det tekniska arbetet med drift, support och säkerhet genomförs därigenom av Sydnärkes IT-förvaltning. Internt i kommunen finns vissa kompetenser med uppdrag inom systemförvaltning. Det framgår dock att det är stor variation mellan förvaltningar och verksamheter hur etablerat arbetet med systemförvaltning är och vilka förutsättningar utsedda förvaltare har i sina uppdrag. Det finns en systemförvaltningsmodell men den är inte fullt ut etablerad i kommunen.

Det saknas i nuläget en fastställd tjänstekatalog för de tjänster som ingår och kan förväntas från kommunen av IT-förvaltningens leveranser. Det finns ett upprättat förslag till tjänstekatalog men den har vid tiden för granskningen inte kommunicerats till kommunerna.

Intervjuade uppger att det saknas resurser inom IT-förvaltningen för att genomföra den utveckling och modernisering som det finns behov av. Dels på grund av att det vid övergång till gemensam nämnd och förvaltning fanns en teknikskuld med föråldrade it-komponenter.

De resurser som överfördes till it-nämnden utgick från dåvarande förutsättningar och nivåer i kommunerna och var främst anpassade till att vidmakthålla befintlig it-miljö men tog inte höjd för utveckling. Utvecklingsarbetet har därigenom fått genomföras stegvis utifrån de resurser som finns. Det finns därför enligt uppgift identifierade sårbarheter som behöver åtgärdas. Dessa tas i prioriteringsordning efter budgetförutsättningarna och vissa av dessa är planerade i budget för 2023.

Intervjuade beskriver att det genomförts ett arbete för att höja säkerheten i datahallar och nätverk, bland annat genom nya brandväggar. Det finns till viss del funktioner för övervakning av trafik. Dock saknas i nuläget verktyg för loggning av säkerhetshändelser som med automatik kan agera eller larma om avvikelser. Med nuvarande bemanning finns inte resurser för manuell övervakning

Inom IT-förvaltningen finns etablerade rutiner och processer för säkerhetsuppdateringar som genomförs schematiskt enligt beslutad ordning.

Förvaltningen erhåller regelbundet information om aktuella hot och risker genom omvärldsbevakning från leverantörer och nationella funktionen Cert inom Myndigheten för samhällsskydd och beredskap som har i uppdrag att utveckla och samordna arbetet med IT-incidenter i Sverige.

De skyddsåtgärder som är implementerade har enligt uppgift inte utvärderats. Det finns inte verktyg internt och inte heller uppdrag till extern part att regelbundet genomföra sårbarhetsscanning för nätverk och system. Det pågår dock ett arbete med att se över vilka verktyg som skulle kunna nyttjas av IT-förvaltningen och vilka resurser det i så fall skulle kräva att hantera arbetet som följer med analyserna.

Exempel har framkommit i granskningen som indikerar på brister i integrationer och arkitektur i it-miljön. Verksamheter och användare uppger att de vid tillfällen dels fått ta del av information som de inte är behöriga att ta del av, dels så förloras information utan att det går att felsöka och avhjälpa att så sker. Det har medfört att användare inför egna rutiner och arbetssätt för att spara och lagra information.

3.1.4 Incidenthantering

Vid granskningen framkommer att det finns en rutin avseende incidenthantering för IT-incidenter daterad 2022-09-07, vilken beskriver IT-förvaltningens interna hantering vid incidenter. Därtill finns beslutade rutiner för personuppgifter och hur dessa ska hanteras om de inträffar. Däremot saknas det i nuläget rutin för hur medarbetare ska agera vid informationssäkerhetsincidenter.

3.1.5 Bedömning av revisionsfrågorna

Revisionsfråga	Bedömning
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?	Nej. Den informationssäkerhetspolicy som beslutats av kommunstyrelsen har inte implementerats så att de aktiviteter som policyn ställer krav på genomförts.
Finns en ändamålsenlig organisation för att arbeta med informationssäkerhet?	Nej. Den ansvarsfördelning som beslutats i policy har inte efterlevts av vare sig kommunstyrelsen eller kommundirektören.
Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?	Nej. I avsaknad av etablerade styrdokument och organisation för informationssäkerhetsarbetet sker i nuläget ingen uppföljning av beslut eller krav i arbetet i enlighet med beslutad policy.
Finns ett systematiskt arbete med riskanalyser och informationsklassning?	Nej. Det har inte genomförts några riskanalyser eller informationsklassningar för att bedöma risker för de informationstillgångar som hanteras i kommunens verksamheter.
Sker en kravställning av IT-säkerhetsåtgärder utifrån genomförd riskbedömning och klassning av informationstillgångar som hanteras i system?	Delvis. Rutiner finns för personuppgiftsincidenter men saknas i nuläget för kommunens hantering i händelse av informationssäkerhets-incidenter. IT-förvaltningen har etablerat interna rutiner för hantering av IT-incidenter.

Revisionsfråga	Bedömning
Finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.)?	Delvis. Det finns etablerade rutiner och arbetssätt för it-säkerhetsarbetet för vissa it-komponenter. Vår bedömning är dock att det för närvarande saknas ett antal väsentliga verktyg för att säkerställa en motståndskraft mot exempelvis cyberhot och attacker. Mot bakgrund av de brister vi identifierat i informationssäkerhetsarbetet kan vi inte utesluta att de informationstillgångar som hanteras i kommunen i nuläget utsätts för risk att spridas till obehöriga internt eller externt.
Görs systematiska uppföljningar av implementerade säkerhetsåtgärder för att kontinuerligt förbättra informationssäkerheten?	Nej. I nuläget saknas uppföljning informationssäkerhetsarbetet. Det gäller både de administrativa och organisatoriska åtgärderna men även tekniska säkerhetsåtgärder som implementeras av IT-förvaltningen. Bland annat har inte sårbarhetsscanning eller penetrationstest genomförts för att utvärdera nuvarande motståndskraft och robusthet för kommunens IT-komponenter.
Finns incidenthanteringsrutiner och sker en tillräcklig rapportering av inträffade incidenter?	Nej. Rutiner saknas för kommunens hantering i händelse av incidenter. IT-förvaltningen har etablerat interna rutiner för hantering av IT-incidenter.

3.2 Sammanfattande bedömning och rekommendationer

Utifrån granskningens resultat är vår sammanfattande bedömning att kommunstyrelsen och nämnderna inte har säkerställt tillräcklig intern styrning och kontroll för att tillse ett ändamålsenligt och systematiskt informationssäkerhetsarbete. Kommunen saknar en fastställd organisation med utsedda funktioner med tillräcklig kompetens för att arbeta med informationssäkerhet. I nuläget saknas ett systematiskt arbete med att identifiera och analysera behov och risker för de informationstillgångar som kommunen hanterar för att säkerställa informationssäkerheten.

Vi kan inte utesluta att det med nuvarande tekniska säkerhetsåtgärder finns risker att kommunens informationstillgångar röjs till obehöriga internt eller externt vid en säkerhetshändelse. Slutligen är vår bedömning att kommunstyrelsen inte har tillsett att det finns etablerade incidenthanteringsrutiner för informationssäkerhetsincidenter vilket vid incidenter riskerar att medföra att dessa inte upptäcks och hanteras tillräckligt skyndsamt och kan leda till större skadeverkan för verksamhetens tillgång till information och förmågan att upprätthålla verksamhetens kontinuitet.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen att:

- Ge kommundirektör i uppdrag att, utifrån MSB:s rekommendationer och metodstöd (avsnitt 2.4), vidta åtgärder i enlighet med dessa så att kommunen etablerar ett systematiskt och riskbaserat informationssäkerhetsarbete.
- Säkerställa att det etableras organisation/funktion med ansvar att leda och samordna informationssäkerhetsarbetet.
- Etablera incidenthanteringsrutiner för informationssäkerhet där ansvar och process för hanteringen tydliggörs.
- Tydliggöra ansvarsfördelning mellan kommunen och gemensam IT-nämnd inom informationssäkerhetsområdet och fastställa vilka tjänster som ingår i förvaltningens uppdrag till kommunerna.
- Efterfråga riskanalys och en nulägesbeskrivning av den tekniska säkerhet som it-nämnden har etablerat för kommunerna för att säkerställa att nuvarande skyddsåtgärder är tillräckliga i förhållande till aktuella hot och risker.

Mot bakgrund av vår granskning rekommenderar vi nämnderna att:

- Säkerställa att funktion utses med ansvar att leda och samordna nämndens arbete med informationssäkerhet så att det sker med en högre grad av systematik.
- Säkerställa att informationsägare i verksamheten upprätthåller ansvar för informationssäkerhetsfrågorna och initierar ett arbete med riskanalyser och informationsklassning. Analyser bör prioriteras för de system som är mest verksamhetskritiska.

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal yrkesrevisor

Mikael Lind
Certifierad kommunal revisor