Uppföljande granskning av informationssäkerhet

Askersunds kommun

Mars 2025

Matthew Matti, projektledare

Lars Dahlin, Certifierad kommunal revisor och kvalitetssäkrare

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Askersunds kommun genomfört en granskning. Syftet med granskningen är att bedöma om granskade nämnder och kommunstyrelsen vidtagit tillräckliga åtgärder med anledning av den bedömning och de åtgärdsförslag som lämnats i genomförda granskningar. Utifrån genomförd granskning är vår samlade bedömning att granskade nämnder **inte helt** bedriver tillräcklig styrning och kontroll för att säkerställa en ändamålsenlig uppföljning av informationssäkerhet.

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

Revisionsfrågor	Bedömning
Har revisorernas synpunkter och förslag till åtgärder besvarats av respektive nämnd/styrelse?	Delvis
Har synpunkterna och förslagen åtgärdats?	Delvis

Rekommendationer

- Etablera en tydlig tid- och uppföljningsplan för att slutföra inventering och informationsklassning före 2025.
- Prioritera införandet av incidenthanteringsrutiner och tydliggör ansvar för rapportering och uppföljning.
- Koppla utbildningar till policy och riktlinjer för att säkerställa praktisk efterlevnad.
- Slutför systeminventering och informationsklassning enligt kommunens ledningssystem.

Innehållsförteckning

Inledning

Bakgrund

Revisorerna i Askersunds kommun granskar årligen delårsbokslut och årsredovisning, samt genomför fördjupade granskningar utifrån en risk- och väsentlighetsanalys. De granskningar som revisionen genomför innehåller ofta förslag på åtgärder som bör genomföras. Dessa åtgärder varierar i omfattning och därmed också i tid för genomförande. En viktig del av revisionens arbete är därför att följa upp tidigare genomförda granskningar för att se om åtgärder vidtagits med anledning av dessa och om den granskade organisationen beaktat noterade brister, synpunkter och förslag.

Enligt SKR:s styrdokument God revisionssed i kommunal verksamhet 2018 påtalas även vikten av att följa upp de granskningar revisorerna gjort under året. Genom att regelbundet följa upp genomförda granskningar ges svar på om åtgärder med anledning av revisorernas kritik och rekommendationer har tagits i beaktande. SKR skriver vidare att uppföljningen kan genomföras som en särskild granskningsinsats med skriftlig rapport. Uppföljningen ger också underlag för att bedöma om det finns anledning till förnyad granskning, och blir därmed en grund för riskanalysen inför kommande års revisionsplanering.

Utifrån genomförd riskanalys har revisionen funnit skäl att göra en uppföljande granskning av informationssäkerhet.

Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om granskade nämnder och kommunstyrelsen vidtagit tillräckliga åtgärder med anledning av den bedömning och de åtgärdsförslag som lämnats i genomförda granskningar.

Granskningen har sin utgångspunkt i följande revisionsfrågor:

- Har revisorernas synpunkter och förslag till åtgärder besvarats av respektive nämnd/styrelse
- Har synpunkterna och förslagen åtgärdats?

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.

Följande revisionskriter används i granskningen:

- Kommunallag (2017:725) 6:6
- Revisionsrapport: Granskning av informationssäkerhet, KPMG, Januari 2023

Avgränsning

Totalt görs en uppföljning av en granskning: Granskning av informationssäkerhet

Metod

Genomgång av revisorernas synpunkter och förslag till åtgärder som angetts i lämnade revisionsrapporter och tillhörande missivbrev, samt genomgång och granskning av yttranden som revisorerna erhållit.

Inhämtande av lägesbeskrivningar för respektive granskning genom intervjuer med berörda tjänstemän och/eller politiker. Inhämtande av kompletterande underlag för granskning och verifiering av genomförda åtgärder och utveckling samt övrig materialinsamling nödvändig för att fånga statusen för respektive granskning.

Granskningen sker genom:

- Utskick av skriftliga frågor till förvaltningen samt genomgång av svar.
- Dokumentanalys och genomgång av relevanta protokoll, beslut och handlingar.
- Vid behov kompletterande intervjuer med relevanta tjänstepersoner samt sakavstämning.

De intervjuade har beretts möjlighet att sakgranska rapporten.

Granskningsresultat

Informationssäkerhet

Revisionsfråga 1: Har revisorernas synpunkter och förslag till åtgärder besvarats av respektive nämnd/styrelse?

Iakttagelser

Det gjordes år 2023, på uppdrag av de förtroendevalda revisorerna i Askersunds kommun, en granskning av informationssäkerhet. Syftet med granskningen var att bedöma om kommunstyrelsen och de berörda nämnderna har tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerhet i kommunen. Bedömningen gjordes utifrån 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 incidenthanterings rutiner 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?

Efter genomförd granskning var revisionens samlade bedömning att kommunstyrelsen och de berörda nämnderna **inte** har säkerställt tillräcklig intern styrning och kontroll för att tillse ett ändamålsenligt och systematiskt informationssäkerhetsarbete.

Efter genomförd granskning lämnade revisionen följande rekommendationer till kommunstyrelsen:

- Ge kommundirektör i uppdrag att, utifrån MSB:s rekommendationer och metodstöd, 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 incidenthanterings rutiner 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.

Efter genomförd granskning lämnade revisionen följande rekommendationer till 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 initierar ett arbete med riskanalyser och informationsklassning. Analyser bör prioriteras för de system som är mest verksamhetskritiska.

Yttrande och svar

I kommunfullmäktiges protokoll 2023-06-19 §82 framgår det att kommunfullmäktige har tagit del av återrapportering av revisionens granskning avseende informationssäkerhet.

Uppföljning

Av tjänsteskrivelse 2023-06-09 framgår det att:

- Kommundirektören har tillsatt en informationssäkerhetsgrupp för att arbeta med att stärka informationssäkerheten.
- Nästan alla nämnder har också en utsedd funktion med ansvar att leda och samordna nämndens arbete med informationssäkerhet.
- Den tillsatta informationssäkerhetsgruppen har påbörjat en inventering av system och vilka insatser för informationsklassning som gjorts.
- Kommunstyrelsen har beslutat om policy och riktlinjer för informationssäkerhet.
- Informationssäkerhetsgruppen för en dialog med Sydnärkes IT-förvaltning om ansvarsfördelning och kravställning gällande den tekniska säkerheten och Sydnärkes IT-förvaltning håller även på att ta fram ett dokument som ska tydliggöra ansvarsfördelningen mellan kommunen och IT-nämnden inom olika områden

Bedömning

Har revisorernas synpunkter och förslag till åtgärder besvarats av respektive nämnd/styrelse?

Delvis.

Efter granskningen har flera åtgärder vidtagits för att stärka informationssäkerhetsarbetet, vilket visar att revisorernas synpunkter och förslag delvis har besvarats. Kommunstyrelsen har tagit del av revisionens granskning och rapporterat tillbaka till kommunfullmäktige. Som svar på granskningen har en informationssäkerhetsgrupp tillsatts med uppdraget att stärka informationssäkerheten. Nästan alla nämnder förutom Sydnärkes miljö- och byggnämnd har också utsett en funktion som leder och samordnar informationssäkerhetsarbetet på nämndnivå. Policyn och riktlinjerna för informationssäkerhet har antagits av kommunstyrelsen, och informationssäkerhetsgruppen har initierat en dialog med Sydnärke IT-förvaltning för att tydliggöra ansvarsfördelningen samt kravställningen avseende teknisk säkerhet.

Trots dessa framsteg återstår flera av revisorernas förslag att implementera i sin helhet. Inventeringen av system och informationsklassning har endast påbörjats, och arbetet med att säkerställa att informationsägare upprätthåller sitt ansvar och genomför riskanalyser och informationsklassning är ännu inte fullständigt genomfört. Dessutom saknas fortfarande tydliga incidenthanteringsrutiner, och en systematisk uppföljning av säkerhetsåtgärder har inte rapporterats.

Sammantaget kan konstateras att viktiga steg har tagits för att besvara revisorernas synpunkter, men många av åtgärderna återstår att genomföras och följas upp. Därför är bedömningen att revisorernas synpunkter och förslag endast delvis har besvarats.

Vidtagna åtgärder

Revisionsfråga 2: Har synpunkter och förslagen åtgärdats?

Iakttagelser

Det framgår att det beslutades om en *Policy för informationssäkerhet* den 11 april 2023 §90. Policyn innebär ett uppdrag till förvaltningen att genomföra åtgärder för att stärka informationssäkerheten enligt de strategiska målsättningar som anges i policyn. Kommundirektören har sedan tidigare tillsatt en informationssäkerhetsgrupp bestående av administrativ chef, kommunjurist och representanter för förvaltningarna. Policyn anger bland annat att kommunen ska ha ett ledningssystem för informationssäkerhet, att det ska finnas en hållbar organisation, att utbildning ska genomföras, att informationstillgångar ska informationssäkerhetsklassas, att incidenter ska rapporteras och att kommunen ska ställa relevanta krav på Sydnärke IT och leverantörer vad gäller fysisk och teknisk informationssäkerhet. Informationssäkerhetsgruppens uppdrag är vidta åtgärder för att uppnå de målsättningar som anges i policyn.

Informationssäkerhetsgruppen har samtidigt som man lämnat förslag på Policy för informationssäkerhet också lämnat förslag på Riktlinjer för informationssäkerhet – organisation och roller. Kommunstyrelsen beslutade om dessa riktlinjer den 11 april samtidigt som beslut om policyn. Av riktlinjerna framgår att på övergripande nivå ska finnas en informationssäkerhetssamordnare = Chief Information Security Officer (CISO),

som tillhör kommunledningsförvaltningen och utgör stödfunktion till förvaltningarna. Rollen kommer tillsvidare att upprätthållas av administrativa chefen. På varje förvaltning ska det finnas en informationssäkerhetshandläggare som samordnar informationssäkerhetsarbetet inom respektive förvaltning samt är ett operativt stöd till förvaltningen. Informationssäkerhetshandläggarna bildar tillsammans med informationssäkerhetssamordnaren en informationssäkerhetsgrupp.

En rutin har påbörjats för att tydliggöra ansvarsfördelningen mellan kommunen och den gemensamma IT-nämnden inom informationssäkerhetsområdet. Sydnärke IT-nämnd arbetar med att ta fram ett dokument som ska klargöra ansvarsfördelningen mellan kommunen och IT-nämnden inom olika områden. Frågor kring informationssäkerhet kommer att hanteras inom detta ramverk. Eftersom kommunen äger sina informationstillgångar, ansvarar den också för informationssäkerheten för dessa. Kommunen måste därför tydligt specificera vilka skyddsnivåer som olika informationstillgångar ska ha, vilket förutsätter att dessa tillgångar först klassificeras genom riskanalyser. Oavsett detta ansvarar Sydnärke IT för att upprätthålla en generellt hög grundläggande säkerhetsnivå.

Kommunstyrelsen kommer att efterfråga en riskanalys och nulägesbeskrivning av den tekniska säkerheten som IT-nämnden har etablerat för kommunen. Detta är för att säkerställa att nuvarande skyddsåtgärder är tillräckliga i förhållande till aktuella hot och risker. Informationssäkerhetsgruppen har en dialog med Sydnärke IT-förvaltning om ansvarsfördelningen och kommunens krav på teknisk säkerhet. Gruppen har ett tidsbegränsat uppdrag med kommunledningsgruppen som styrgrupp.

Ytterligare framgår det av intervju att utbildningar har genomförts för personalen, men dessa saknar koppling till policys och riktlinjer, vilket gör att deras praktiska efterlevnad inte kan säkerställas. Vidare framkommer det att inventeringen av system och informationsklassning ännu inte har genomförts, men är planerad att ske under 2025 efter att ansvarsfördelningen mellan kommunen och IT-nämnden har klargjorts.

Bedömning

Har synpunkter och förslagen åtgärdats?

Delvis.

Kommunen har vidtagit flera åtgärder för att förbättra informationssäkerheten, inklusive antagandet av en policy och riktlinjer för informationssäkerhet den 11 april. Dessa styrdokument anger tydliga målsättningar och riktlinjer för hur informationssäkerhetsarbetet ska bedrivas, och en informationssäkerhetsgrupp har etablerats för att driva arbetet framåt. Rollen som Chief Information Security Officer (CISO) har tillsatts och stödstrukturer har skapats genom informationssäkerhetshandläggare på förvaltningsnivå. Vidare har en dialog initierats med Sydnärke IT-nämnden för att tydliggöra ansvarsfördelningen mellan kommunen och IT-nämnden.

Trots detta kvarstår flera brister som indikerar att åtgärderna inte fullt ut har realiserats. Utbildningar har genomförts för personalen, men de saknar koppling till policyn och

riktlinjerna, vilket försvårar möjligheten att säkerställa deras praktiska efterlevnad. Inventeringen av system och informationsklassning, som är en grundläggande del av informationssäkerhetsarbetet, har ännu inte genomförts och planeras först till 2025. Det framgår också att incidenthantering inte är fullt implementerad och att rapporteringsrutiner inte har satt sig i organisationen.

Sammantaget har kommunen gjort framsteg genom att ta fram styrdokument och inleda viktiga processer, men flera av de kritiska åtgärder som revisorerna pekat på återstår att implementera och följa upp. Därför kan det inte bedömas att synpunkterna och förslagen är fullt ut åtgärdade.

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Askersunds kommun genomfört en granskning. Syftet med granskningen är att bedöma om granskade nämnder och kommunstyrelsen vidtagit tillräckliga åtgärder med anledning av den bedömning och de åtgärdsförslag som lämnats i genomförda granskningar. Utifrån genomförd granskning är vår samlade bedömning att granskade nämnder **inte helt** bedriver tillräcklig styrning och kontroll för att säkerställa en ändamålsenlig uppföljning av informationssäkerhet.

Rekommendationer

- Etablera en tydlig tid- och uppföljningsplan för att slutföra inventering och informationsklassning före 2025.
- Prioritera införandet av incidenthanteringsrutiner och tydliggör ansvar för rapportering och uppföljning.
- Koppla utbildningar till policy och riktlinjer för att säkerställa praktisk efterlevnad.
- Slutför systeminventering och informationsklassning enligt kommunens ledningssystem.

2025-03-07

Lars Dahlin	Matthew Matti
Namn	*Namn*