Granskning av informations-säkerhet

Gästrike Räddningstjänstförbund

Mars 2026

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Gästrike Räddningstjänstförbund genomfört en granskning av informationssäkerhet. Granskningens syfte är att bedöma om direktionen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Vår samlade bedömning är att direktionen **inte helt** har säkerställt ett ändamålsenligt informationssäkerhetsarbete med tillräcklig intern kontroll.

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

Revisionsfrågor	**Bedömning**
1. Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?	Delvis 
2. Arbetar förbundet riskbaserat med informationssäkerhet?	Delvis 
3. Sker efterlevnad av riktlinjer för informationssäkerhet?	Delvis 

Rekommendationer

Med utgångspunkt från de iakttagelser och bedömningar som har framkommit i granskningen lämnar vi följande rekommendationer till direktionen:

- Fortsätta att tydliggöra och formalisera informationssäkerhetsorganisationen. Säkerhetsskyddschefen har idag uppdraget att samordna och driva informationssäkerhetsarbetet och är en del av verksamhetsledningen. Detta bör ytterligare befästas genom att roller, ansvar och rapporteringsvägar dokumenteras och beslutas, samt att ansvarsfördelningen gentemot övriga lednings- och verksamhetsfunktioner klargörs.

- Slutföra framtagandet och beslutsfattandet kring en samlad informationssäkerhetspolicy samt ett övergripande kontrollramverk som tydligt definierar hur informationssäkerhetsarbetet ska styras, följas upp och integreras i verksamheten. Arbetet bör fortsatt utgå från etablerade standarder,

exempelvis ISO/IEC 27000[1]-serien, som anger strukturer och krav för styrning av informationssäkerhet.

- Vidareutveckla det påbörjade riskhanteringsarbetet genom att fullt ut etablera en tydligt definierad IT-riskhanteringsram som anger metodik, ansvarsfördelning och uppföljning. Detta bör innefatta ett dokumenterat riskregister där risker kontinuerligt identifieras, bedöms och prioriteras, samt fastställda mål och mätetal som möjliggör återkommande rapportering och förbättring av risknivåer.

- Fortsatt stärka arbetet med leverantörsrelaterade risker genom att säkerställa att tydliga och dokumenterade krav på informationssäkerhet finns i avtal och upphandlingar, kompletterat med strukturerade uppföljningsprocesser. Detta bör inkludera regelbunden granskning av leverantörers säkerhetsintyg och tredjepartsrapporter, såsom relevanta ISO-certifieringar och SOC-rapporter, för att säkerställa att leverantörer upprätthåller en tillräcklig säkerhetsnivå.

- Slutföra och formalisera interna processer som säkerställer efterlevnad av riktlinjer för informationssäkerhet, genom definierade kontrollmoment, återkommande uppföljningsrutiner och strukturerad rapportering till ledning och direktion. Processerna bör även innefatta hantering av avvikelser och tydlig dokumentation av resultat från genomförda kontroller.

- Tydliggöra hur Gävle kommuns tekniska och operativa säkerhetsåtgärder följs upp och integreras i förbundets egen styrning. Detta innebär att dokumentera hur kommunen ska rapportera relevanta säkerhetskontroller och incidenter till förbundet, samt säkerställa att det finns egna rutiner för att verifiera att riktlinjer och kontroller tillämpas i den egna verksamheten, oavsett att kommunen ansvarar för stora delar av den tekniska miljön.

[1] ISO/IEC 27001 är en internationell standard för ledningssystem för informationssäkerhet

Innehållsförteckning

Inledning

Bakgrund

Kommuner, kommunalförbund och regioner har ett av de mest komplexa uppdragen i samhället, eftersom en stor del av Sveriges samhällsviktiga verksamheter faller under deras ansvarsområde. För kommuner, kommunalförbund och regioner handlar informationssäkerhet att säkerställa att information för medborgare, medarbetare och andra intressenter hanteras med utgångspunkt i konifidientialitet, riktighet, tillgänglighet och spårbarhet. Informationssäkerhet handlar om att skydda information från obehörig åtkomst, ändring eller förstörelse. Det handlar om att säkerställa att informationen är tillgänglig när den behövs, att den är korrekt och pålitlig, samt att den hålls konfidentiell för de som inte har behörighet att ta del av den.

Med ett förändrat geopolitiskt säkerhetsläge och den fortsatt snabba digitaliseringen blir informations- och cybersäkerhet allt viktigare. Brister i informationshantering kan leda till minskat förtroende för tjänster och bakomliggande aktörer. Vid händelse av en informationssäkerhetsincident kan förtroendet för organisationen snabbt raseras, vilket kan ta lång tid att bygga upp. Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering, vilket i sin tur skapar förtroende både internt och externt. Aktiviteter som risk- och sårbarhetsanalys samt klassning av informationstillgångar är viktigt för att säkerställa att den mest skyddsvärda informationen verkligen får det skydd som krävs.

Revisorerna har i sin riskanalys för 2025 bedömt att det finns en risk att direktionen inte har säkerställt att det finns en god informationssäkerhet inom förbundet och har därför gett PwC ett uppdrag att granska området.

Syfte och revisionsfrågor

Granskningens syfte är att bedöma om förbundsstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Revisionsfrågor:

1. Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?
2. Arbetar förbundet riskbaserat med informationssäkerhet?
3. Sker efterlevnad av riktlinjer för informationssäkerhet?

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar. I denna granskning har vi haft följande revisionskriterier:

- Kommunallagen
- IT-styrdokument
- Informationssäkerhetsdokumentation

Avgränsning

I tid avgränsas granskningen till år 2025 samt till granskningens revisionsfrågor.

Metod

Granskningen har genomförts genom intervjuer med förbundets IT-säkerhetsansvarig samt ekonomichef/biträdande förbundsdirektör, tillsammans med inläsning och analys av tillgänglig dokumentation.

Rapporten har kvalitetssäkrats i enlighet med PwC:s interna rutiner och checklistor för kvalitetssäkring.

De intervjuade har beretts möjlighet att sakgranska rapporten.

Granskningsresultat

Organisation med roller och ansvar

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

Iakttagelser

Organisationen har ännu inte etablerat en formellt beskriven struktur för informationssäkerhetsarbetet. Roller, ansvar och rapporteringsvägar för IT-relaterade funktioner är inte dokumenterade eller fastställda av direktionen, det finns däremot en av ledningen utsedd säkerhetsskyddschef som ansvarar för informationssäkerhet. Arbetet med informationssäkerhet utgår i stor utsträckning från Gävle kommuns policyer och processer, då förbundet för närvarande saknar både en egen informationssäkerhetspolicy och ett övergripande kontrollramverk som definierar interna ansvarsförhållanden.

Den praktiska hanteringen av flera delar av informationssäkerhetsarbetet sker genom kommunens etablerade processer, vilket innebär att förbundets interna roll- och ansvarsfördelning inte är fullständigt definierad eller beskriven. Vissa aspekter av ansvar berörs i riktlinjen för säkerhetsskydd, men dessa omfattar inte en heltäckande eller sammanhållen beskrivning av organisationens ansvar inom informationssäkerhetsområdet. Vi noterar att en tydligt formulerad informationssäkerhetsorganisation ännu inte är etablerad.

Bedömning

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

Delvis.

Vår sammanfattande bedömning är att Gästrike Räddningstjänst i nuläget saknar en formellt etablerad och tydligt beskriven informationssäkerhetsorganisation. Roller, ansvar och rapporteringsvägar för IT och informationssäkerhetsrelaterade funktioner är inte fastställda av direktionen, däremot finns det en utsedd funktion på ledningsnivå med ansvar för informationssäkerhet. Förbundet använder i stor utsträckning Gävle kommuns policyer, processer och rutiner, vilket innebär att den interna ansvarsfördelningen inte är definierad i egen styrning. Då en egen informationssäkerhetspolicy och ett övergripande kontrollramverk fortfarande saknas är ansvar och styrning inom informationssäkerhetsområdet inte fullt ut dokumenterat eller strukturerat. Sammantaget bedöms att en tydligare och mer formellt förankrad ansvarsfördelning behöver etableras för att uppnå en sammanhållen informationssäkerhetsorganisation.

Arbetar förbundet riskbaserat med informationssäkerhet?

Revisionsfråga 2: Arbetar förbundet riskbaserat med informationssäkerhet?

Iakttagelser

Förbundet har genomfört en informationssäkerhetsriskanalys genom en workshop med ledningen, och analysen är dokumenterad med en plan för årlig uppföljning. Detta innebär att det finns ett strukturerat moment för att identifiera och bedöma informationssäkerhetsrisker, där metodstödet som används bygger på ISO/IEC 27000[2]-serien. Samtidigt saknas en tydligare, övergripande IT-riskhanteringsram, och något formellt riskregister är inte etablerat. Det finns inte heller dokumenterade informationssäkerhetsmål med kopplade KPI:er eller KRI:er som möjliggör kontinuerlig uppföljning av risknivåer.

Den operativa IT-miljön hanteras i stor utsträckning av Gävle kommun. Kommunen använder verktyg som Microsoft Secure Score och genomför återkommande hälsokontroller av infrastruktur och klienter. Dessa aktiviteter bidrar till att identifiera sårbarheter och tekniska risker men ingår i kommunens driftprocesser och utgör inte ett eget formaliserat riskarbete på förbundsnivå.

När det gäller leverantörsrelaterade risker saknas en separat, dokumenterad strategi för hur IT-tjänster från externa leverantörer ska följas upp ur ett informationssäkerhetsperspektiv. Det finns inte heller en etablerad leverantörsprocess med tydliga informationssäkerhetskrav och återkommande uppföljning, exempelvis genom granskning av ISO eller SOC 2[3].

Förbundet har även tagit fram en hotbildsbeskrivning som identifierar relevanta hot mot information, system och processer. Denna beskrivning fungerar som ett stöd i det fortsatta arbetet med riskanalys men utgör inte ett ramverk för riskhantering.

Sammantaget visar iakttagelserna att förbundet har flera riskrelaterade underlag och aktiviteter på plats, och att dessa delvis tar avstamp i ISO/IEC 27000-serien, men att arbetet ännu inte är samlat i ett helt sammanhållet eller formaliserat riskbaserat arbetssätt.

---

[2] ISO/IEC 27001 är en internationell standard för ledningssystem för informationssäkerhet

[3] SOC-rapport (Service Organization Control report) – oberoende granskningsrapport av en tjänsteleverantörs interna kontroller.

Bedömning

Revisionsfråga 2: Arbetar förbundet riskbaserat med informationssäkerhet?

Delvis.

Vår sammanfattande bedömning är att förbundet i dagsläget ännu inte har etablerat ett fullt ut strukturerat eller formaliserat riskbaserat arbetssätt inom informationssäkerhet. Metodstödet som används för informationssäkerhetsriskanalysen tar visserligen avstamp i ISO/IEC 27000-serien, och det finns både en genomförd och dokumenterad riskanalys samt operativa kontroller som utförs av Gävle kommun. Dessa insatser utgör dock ännu inte ett komplett och sammanhållet ramverk för riskhantering på förbundsnivå.

Avsaknaden av en tydligt definierad IT-riskhanteringsram, ett formellt riskregister samt dokumenterade informationssäkerhetsmål med tillhörande KPI:er/KRI:er innebär att riskarbetet inte är fullt ut konsoliderat eller metodstyrt. Även hanteringen av leverantörsrelaterade risker saknar i nuläget tydliga processer och strukturerad uppföljning.

Sammantaget bedömer vi att förbundet befinner sig i ett tidigt skede i utvecklingen av ett riskbaserat arbetssätt. Grunden är delvis lagd genom ett ISO/IEC 27000-inriktat metodstöd, men flera centrala komponenter behöver fortsatt etableras och integreras för att uppnå en sammanhållen och systematisk riskhantering.

Sker efterlevnad av riktlinjer för informationssäkerhet?

Revisionsfråga 3: Sker efterlevnad av riktlinjer för informationssäkerhet?

Iakttagelser

Förbundet använder i dagsläget Gävle kommuns policyer, riktlinjer och processer som grund för sitt informationssäkerhetsarbete, eftersom en egen informationssäkerhetspolicy ännu inte finns framtagen. Det framgår endast i begränsad utsträckning av det granskade underlaget vilket omfattar bland annat policydokument, riktlinjer för säkerhetsskydd, riskanalysdokumentation samt kommunens och förbundets granskningsunderlag, hur förbundet säkerställer efterlevnaden av de riktlinjer som tillämpas. Det finns vissa kontrollmoment kopplade till informationssäkerhet i förbundets interna kontrollplan, vilket innebär att viss uppföljning sker. Samtidigt beskriver underlaget i övrigt inga mer heltäckande interna rutiner, kontrollmoment eller uppföljningsprocesser som visar hur förbundet systematiskt

verifierar att riktlinjerna följs i den egna verksamheten, och något eget övergripande kontrollramverk som stödjer en samlad efterlevnadsuppföljning är ännu inte etablerat.

En betydande del av det praktiska informationssäkerhetsarbetet, såsom behörighetshantering, tekniska säkerhetskontroller och incidenthantering, utförs av Gävle kommun. Det finns däremot ingen tydlig beskrivning i det granskade materialet av hur förbundet följer upp dessa aktiviteter ur ett efterlevnadsperspektiv. Arbetet framstår därför som beroende av kommunens etablerade rutiner, samtidigt som förbundets egna mekanismer för att säkerställa efterlevnad delvis är odokumenterade och under utveckling.

Det framgår att vissa utvecklingsaktiviteter, såsom riskanalys och planering av framtida styrdokument, pågår. Först när arbetet med att ta fram egna rutiner och riktlinjer har slutförts bedöms det finnas förutsättningar att uppdatera den interna kontrollplanen med fler och mer träffsäkra kontrollmoment. Sammantaget visar iakttagelserna att förbundet har påbörjat ett arbete med intern kontroll kopplad till informationssäkerhet, men att det ännu saknas ett fullt ut etablerat och systematiskt arbetssätt för att följa upp och säkerställa efterlevnad av riktlinjer för informationssäkerhet.

Bedömning

Revisionsfråga 3: Sker efterlevnad av riktlinjer för informationssäkerhet?

Delvis.

Utifrån det samlade granskningsunderlaget framgår att förbundet delvis saknar processer för att säkerställa efterlevnad av riktlinjer för informationssäkerhet. Vissa delar av arbetet är på plats genom att Gävle kommun utför centrala moment såsom behörighetshantering, tekniska säkerhetskontroller och incidenthantering, men på förbundsnivå saknas dokumenterade och formaliserade processer för uppföljning, kontroll och verifiering av efterlevnad.

Det innebär att processer för efterlevnad inte är helt frånvarande, men att de inte är etablerade inom förbundets verksamhet, utan i hög grad hanteras av kommunen. Förbundets egna processer för efterlevnad är därmed inte fullt utvecklade eller beskrivna, utan förekommer endast delvis genom pågående arbete, till exempel utveckling av styrdokument och riskanalys.

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Gästrike Räddningstjänstförbund genomfört en granskning av informationssäkerhet. Granskningens syfte är att bedöma om direktionen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Vår samlade bedömning är att direktionen **inte helt** har säkerställt ett ändamålsenligt informationssäkerhetsarbete med tillräcklig intern kontroll.

Sammanfattande bedömningar utifrån revisionsfrågor

Förbundet saknar en formellt etablerad informationssäkerhetsorganisation med tydligt fastställda roller, ansvar och rapporteringsvägar. Det finns en utsedd säkerhetsskyddschef på ledningsnivå med ansvar för informationssäkerhet, och arbetet bygger till stor del på Gävle kommuns policyer, processer och rutiner. Eftersom en egen informationssäkerhetspolicy och ett övergripande kontrollramverk ännu inte är framtagna, är den interna styrningen av informationssäkerhetsarbetet inte fullt ut dokumenterad eller strukturerad. Detta innebär att förbundet behöver stärka sin formella ansvarsfördelning för att skapa en tydligare organisatorisk grund för informationssäkerhetsarbetet.

Vidare arbetar förbundet endast delvis riskbaserat. Även om en informationssäkerhetsriskanalys har genomförts med metodstöd som bygger på ISO/IEC 27001 och vissa riskrelaterade aktiviteter finns på plats, saknas en definierad IT-riskhanteringsram, ett formellt riskregister samt dokumenterade informationssäkerhetsmål som möjliggör systematisk uppföljning av risknivåer. Den operativa IT-miljön hanteras i stor utsträckning av Gävle kommun, och viktiga riskrelaterade kontroller utförs därför utanför förbundets egen organisation. Det finns även begränsade strukturer för att hantera leverantörsrelaterade risker. Sammantaget innebär detta att förbundet befinner sig i ett tidigt skede av att utveckla ett sammanhållet riskbaserat arbetssätt.

När det gäller efterlevnad av riktlinjer för informationssäkerhet visar granskningen att förbundet delvis saknar dokumenterade och formaliserade processer för uppföljning och kontroll. Förbundet använder Gävle kommuns policyer och processer, men det framgår inte av det granskade materialet hur förbundet säkerställer efterlevnad i den egna verksamheten. De interna mekanismer som behövs för uppföljning, kontrollmoment och verifiering av efterlevnad är inte etablerade, vilket gör att efterlevnadsarbetet i praktiken i stor utsträckning sker genom kommunens befintliga kontroller och rutiner.

Sammanfattningsvis bedömer PwC att Gästrike Räddningstjänstförbund behöver utveckla och stärka såväl organisatoriska strukturer som riskhanteringsprocesser och uppföljningsmekanismer för att säkerställa ett fullt ut ändamålsenligt och internt kontrollerat informationssäkerhetsarbete.

Rekommendationer

Med utgångspunkt från de iakttagelser och bedömningar som har framkommit i granskningen lämnar vi följande rekommendationer till direktionen:

- Fortsätta att tydliggöra och formalisera informationssäkerhetsorganisationen. Säkerhetsskyddschefen har idag uppdraget att samordna och driva informationssäkerhetsarbetet och är en del av verksamhetsledningen. Detta bör ytterligare befästas genom att roller, ansvar och rapporteringsvägar dokumenteras och beslutas, samt att ansvarsfördelningen gentemot övriga ledningss- och verksamhetsfunktioner klargörs.

- Slutföra framtagandet och beslutsfattandet kring en samlad informationssäkerhetspolicy samt ett övergripande kontrollramverk som tydligt definierar hur informationssäkerhetsarbetet ska styras, följas upp och integreras i verksamheten. Arbetet bör fortsatt utgå från etablerade standarder, exempelvis ISO/IEC 27000-serien, som anger strukturer och krav för styrning av informationssäkerhet.

- Vidareutveckla det påbörjade riskhanteringsarbetet genom att fullt ut etablera en tydligt definierad IT-riskhanteringsram som anger metodik, ansvarsfördelning och uppföljning. Detta bör innefatta ett dokumenterat riskregister där risker kontinuerligt identifieras, bedöms och prioriteras, samt fastställda mål och mätetal som möjliggör återkommande rapportering och förbättring av risknivåer.

- Fortsatt stärka arbetet med leverantörsrelaterade risker genom att säkerställa att tydliga och dokumenterade krav på informationssäkerhet finns i avtal och upphandlingar, kompletterat med strukturerade uppföljningsprocesser. Detta bör inkludera regelbunden granskning av leverantörers säkerhetsintyg och tredjepartsrapporter, såsom relevanta ISO-certifieringar och SOC-rapporter, för att säkerställa att leverantörer upprätthåller en tillräcklig säkerhetsnivå.

- Slutföra och formalisera interna processer som säkerställer efterlevnad av riktlinjer för informationssäkerhet, genom definierade kontrollmoment, återkommande uppföljningsrutiner och strukturerad rapportering till ledning och direktion. Processerna bör även innefatta hantering av avvikelser och tydlig dokumentation av resultat från genomförda kontroller.

- Tydliggöra hur Gävle kommuns tekniska och operativa säkerhetsåtgärder följs upp och integreras i förbundets egen styrning. Detta innebär att dokumentera hur kommunen ska rapportera relevanta säkerhetskontroller och incidenter till förbundet, samt säkerställa att det finns egna

rutiner för att verifiera att riktlinjer och kontroller tillämpas i den egna verksamheten, oavsett att kommunen ansvarar för stora delar av den tekniska miljön.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning	
1. Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?	**Delvis**	
2. Arbetar förbundet riskbaserat med informationssäkerhet?	**Delvis**	
3. Sker efterlevnad av riktlinjer för informationssäkerhet?	**Delvis**	

2026-03-05

Cecilia Axelsson

Uppdragsledare

Gabriel Engstrand

Projektledare