Granskning av IT-säkerhet

Rapport
Nerikes Brandkår

KPMG AB

2022-12-13

Antal sidor 15

Nerikes Brandkår
Granskning av IT-säkerhet

2022-12-13

Innehållsförteckning

1 Sammanfattning

KPMG har av Nerikes Brandkårs revisorer fått i uppdrag att granska om förbundet säkerställt en tillräcklig uppföljning och kontroll av sin IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2022.

Syftet med granskningen har varit att bedöma om direktionen har en tillräcklig styrning och intern kontroll över sin IT-säkerhet. Därtill syftar granskningen till att följa upp de rekommendationer som lämnats i tidigare granskning för att bedöma om direktionen säkerställt att förbättringsåtgärder vidtagits.

Vår sammanfattande bedömning utifrån granskningens syfte är att direktionen inte har en tillräcklig styrning och intern kontroll över sin IT-säkerhet. Bland annat saknas i nuläget krav på vad Nora kommun som IT-driftsleverantör med ansvar för IT-säkerhet förväntas leverera till förbundet. Avtalet tydliggör i nuvarande form inte kravnivåer vilket försvårar möjligheter för förbundet att följa upp avtal genom efterlevnadskontroller. De krav som direktionen beslutat som gällande för förbundets interna informationssäkerhetsarbete måste även ställas som ett minimum till externa leverantörer.

Mot bakgrund av vår bedömning och slutsats rekommenderar vi direktionen att:

- Beakta och vidta åtgärder för de tidigare lämnade rekommendationerna från granskning av informationssäkerhet 2020, se sid 9.
- Revidera avtal med Nora kommun för att tydliggöra förbundets behov och krav avseende support och IT-säkerhet.
- Stärka dialog och uppföljning med Nora kommun som It-driftsleverantör och andra externa systemleverantörer där risker och hot kopplat till informations- och IT-säkerhet behandlas och dokumenteras regelbundet.
- Klassificera informationstillgångar i system så att resultat kan utgöra underlag för kravställning och beställning av it-säkerhetsåtgärder som står i relation till bedömt skyddsvärde på informationen som hanteras.
- Etablera en regelbunden uppföljning och återrapportering av det informationssäkerhetsarbete som genomförs så att direktionen har kännedom om aktuella hot och risker som förbundet behöver beakta för att skydda verksamheten.

2 Bakgrund

Vi har av Nerikes Brandkårs revisorer fått i uppdrag att granska om förbundet säkerställt en tillräcklig uppföljning och kontroll av sin IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2022.

Under 2020 genomfördes en fördjupad granskning av förbundets arbete med informationssäkerhet. Resultatet av granskningen visade på en del brister som även har en påverkan på förutsättningar att skydda information med tekniska IT-säkerhetsåtgärder. I granskningen identifierades därtill en otydlighet i ansvarsförhållandet mellan förbundet och dess IT-leverantör Nora kommun. När IT-verksamheten är outsourcad ställs ytterligare krav på interna arbetssätt och processer för att riskbedöma och klassa information för att kunna ställa krav om tekniska åtgärder hos leverantören eller andra externa systemleverantörer. Genom denna ansvarsfördelning behöver verksamheten säkerställa att det finns en tillräcklig beställarkompetens och tydliggjorda strukturer för att följa upp leveransen och kontrollera att den säkerhet som är etablerad står i relation till krav som förbundet har att efterleva.

Sedan granskningen av informationssäkerhet genomfördes har verksamheters beroende av robust och säker IT ökat i takt med att alltmer information hanteras i verksamhetssystem. Därtill finns i nuläget en förhöjd hotbild mot svenska kommuner, regioner och andra verksamheter genom cyberangrepp som får stora konsekvenser för verksamheters kontinuitet. Sårbarheter i IT-säkerheten kan nyttjas av interna eller externa hotaktörer och riskerar därför att leda till både ekonomisk skada och förtroendeskada för förbundet.

Nerikes Brandkårs revisorer har i sin riskanalys dragit slutsatsen att förbundets IT-säkerhet behöver granskas. I samband med granskningen önskar därtill revisorerna att de rekommendationer som lämnades i tidigare granskning av informationssäkerhet följs upp då dessa i stor del påverkar förutsättningarna för IT-säkerheten.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen är att bedöma om direktionen har en tillräcklig styrning och intern kontroll över sin IT-säkerhet. Därtill syftar granskningen till att följa upp de rekommendationer som lämnats i tidigare granskning för att bedöma om direktionen säkerställt att förbättringsåtgärder vidtagits.

De revisionsfrågor som besvaras:

- Har direktionen vidtagit erforderliga åtgärder utifrån resultatet av tidigare genomförd granskning?
- Har informationsklassning och riskbedömning gjorts för förbundets informationstillgångar som hanteras i system, som ligger till grund för kravställning och implementering av tekniska IT-säkerhetsåtgärder?
- Finns etablerade strukturer för dialog mellan förbundet och IT-leverantören där uppföljning och kontroll kan genomföras?
- Har direktionen efterfrågat riskanalys eller på annat sätt informerat sig om leverantörens förmåga utifrån den ökade hotbilden kring IT-angrepp och intrång?
- Har direktionen vidtagit åtgärder utifrån den ökade hotbilden kring IT-angrepp och intrång?

2.2 Revisionskriterier

- Utgångspunkt för uppföljning är granskningsrapport för förbundets informationssäkerhet från 2020.
- Interna styrdokument

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier av:
  - Policy – Informationssäkerhet, 2020-12-11
  - Riktlinje – Informationssäkerhet inom Nerikes Brandkår, 2021-03-08
  - Systemdokumentation verksamhetssystem
- Intervjuer har genomförts med
  - Brandchef
  - Vice brandchef
  - IT-chef på Nora kommun.

Samtliga intervjupersoner har fått möjlighet att faktakontrollera rapporten.

3 Resultat av uppföljande granskning

3.1 Granskning av informationssäkerhet, 2020

Under år 2020 genomförde KPMG på uppdrag av de förtroendevalda revisorerna en granskning av förbundets rutiner kring informationssäkerhet. I granskningen framkom bland annat att förbundets informationssäkerhetspolicy inte uppdaterats och förbundets organisation för informationssäkerhetsarbetet saknade tydliggjorda roller. Klassningar av förbundets informationstillgångar föreslogs att genomföras så att resurser kunde anpassas efter den information som bedömdes mest kritisk för verksamheten. Vidare framkom att avtalet med Nora kommun som IT-leverantör var otydligt och att roller och ansvar mellan förbundet och Nora kommun avseende informationssäkerhetsarbetet borde tydliggöras, detta för att undvika att delar av informationssäkerhetsarbetet förbises.

Sammanfattningsvis gjordes bedömningen att förbundet inte hade ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

3.1.1 Rekommendationer och nuläge

Utifrån den tidigare genomförda granskningen av informationssäkerhet 2020 har vi följt upp lämnade rekommendationer. Nedan presenteras iakttagelser om nuläge för arbetet och de åtgärder som vidtagits som ett resultat av lämnade rekommendationer.

Rekommendation 1
Genom arbetsordningar eller delegationsordning tydliggöra ansvar för förbundets system.

I uppföljning kan vi konstatera att ansvaret för förbundets system har inte reglerats i arbetsordning eller delegationsordning. Däremot är ansvaret tydliggjort i förbundets informationssäkerhetspolicy. Där framgår följande ”grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Brandkårens informationssäkerhetsansvarige och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till Brandkårens verksamhet för att fullfölja informationssäkerhetsansvaret”.

Rekommendation 2

Se över förbundets informationssäkerhetspolicy och riktlinjer för informationssäkerhet för att säkerställa dess relevans.

Sedan tidigare genomförd granskning har både policyn och riktlinjen för informationssäkerhet uppdaterats. Policy för informationssäkerhet antogs av direktionen 2020-12-11 och Riktlinje – Informationssäkerhet inom Nerikes Brandkår antogs av ledningsgruppen 2021-03-08. Riktlinjen är mer detaljerad och konkretiserar informationen i informationssäkerhetspolicyn.

Vid intervjuer framkommer att den uppdaterade policyn och riktlinjen inte fullt ut är implementerad i verksamheten och det har inte gjorts någon kontroll över hur den efterlevs i verksamheten.

Rekommendation 3

Utse en informationssäkerhetssamordnare inom förbundet med en tydlig rollbeskrivning.

Informationssäkerhetsarbetet inom Brandkåren leds och samordnas av en informationssäkerhetsansvarig. Informationssäkerhetsansvarig ansvarar för:

- att brandkårens styrande dokument inom området är aktuella, som informationssäkerhetspolicy och riktlinjer för informationssäkerhet,
- att stödja verksamheterna i frågor som rör informationssäkerhet,
- kontroll och uppföljning av informationssäkerheten och
- omvärldsbevakning inom informationssäkerhetsområdet.

Vid intervjuer framkommer att den tidigare anställda brandingenjören haft rollen som informationssäkerhetssamordnare men sedan denne slutat är uppdraget vakant.

Rekommendation 4

I avtalet med Nora kommun tydliggöra gränsdragningarna i ansvarsförhållandena mellan förbundet och Nora kommun. Det bör inkludera att genom SLA[1] tydliggöra kravställandet på Nora kommun som IT-leverantör. Samt att tydliggöra ansvar avseende informationssäkerhetsarbetet för att undvika att delar förbises.

Avtalet med Nora kommun har sedan tidigare genomförd granskning inte uppdaterats.

[1] Service Level Agreement

Rekommendation 5
Framarbeta en rutin för behörighetskontroller.

Vid intervjuer framkommer att det inte finns någon rutin för behörighetskontroller. Vissa stickprov genomförs av vice brandchef.

Rekommendation 6
Utveckla kortsiktiga mål för informationssäkerhetsarbetet med tillhörande handlingsplaner.

I förbundets policy för informationssäkerhet anges ett antal mål för informationssäkerheten:

” Brandkåren ska uppnå och upprätthålla en informationssäkerhet som:

- innebär en robust, säker och tillförlitlig informationshantering,
- möjliggör ett aktivt medverkande i det digitala samhället,
- bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personliga integritet,
- motsvarar medborgares och externa verksamheters behov och förväntningar,
- uttrycks i aktuella styrdokument som policy och riktlinjer,
- efterlever krav i lagar, förordningar, föreskrifter och avtal.”

Av vår granskning framgår att inga kortsiktiga mål för informationsarbetet med tillhörande handlingsplaner tagits fram.

Rekommendation 7
Säkerställa att arbetet med att identifiera och analysera risker sker regelbundet.

Förbundet har identifierat ett antal risker kopplat till informationssäkerhet, bland annat kring risk för driftstopp. Av de underlag vi tagit del av kan vi inte se att åtgärder har vidtagits som ett resultat av de identifierade riskerna.

3.1.2 Bedömning

Vår bedömning är att åtgärder vidtagits för följande lämnade rekommendationer i tidigare genomförd granskning av informationssäkerhet från år 2020:

- Tydliggöra ansvar för förbundets system.
- Se över förbundets informationssäkerhetspolicy och riktlinjer för informationssäkerhet för att säkerställa dess relevans.
- Utse en informationssäkerhetssamordnare inom förbundet med en tydlig rollbeskrivning.
- Säkerställa att arbetet med att identifiera och analysera risker sker regelbundet.

Dock ser vi att de rekommendationer där åtgärder genomförts i vissa delar är i behov av ytterligare förtydligande och konkreta aktiviteter för att anses tillräckliga. För att uppnå en högre efterlevnad av de nya styrdokumenten som beslutats behöver dessa implementeras tydligare i verksamheten. Därtill behöver en ny informationssäkerhetsansvarig utses med uppdrag att leda och samordna förbundets arbete utifrån de styrande dokumenten och andra krav som finns på informationshantering i förbundet. Åtgärder behöver vidtas som står i relation till de risker som identifierats för att säkerställa att verksamheten kan upprätthållas med minimerad skadeverkan i händelse av störning eller avbrott med påverkan på förbundets informationstillgångar.

Vår bedömning är att åtgärder inte vidtagits för följande lämnade rekommendationer i tidigare genomförd granskning av informationssäkerhet från år 2020 och kvarstår därigenom för direktionen att åtgärda:

- I avtalet med Nora kommun tydliggöra gränsdragningarna i ansvarsförhållandena mellan förbundet och Nora kommun. Det bör inkludera att genom SLA tydliggöra kravställandet på Nora kommun som IT-leverantör. Samt att tydliggöra ansvar avseende informationssäkerhetsarbetet för att undvika att delar förbises.
- Framarbeta en rutin för behörighetskontroller.
- Utveckla kortsiktiga mål för informationssäkerhetsarbetet med tillhörande handlingsplaner.

4 Resultat av fördjupad granskning av IT-säkerhet

4.1 Organisation

4.1.1 Informationssäkerhet

I förbundets riktlinje för informationssäkerhet framgår grundprincipen att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från direktionen och ledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Vidare framgår att direktionen för Nerikes Brandkår har det yttersta ansvaret för informationssäkerheten inom förbundet.

I förbundet finns en organisering med brandchef som övergripande ansvarig för förbundets verksamhet och två vice brandchefer. En uppdelning har gjorts mellan de vice brandcheferna där den operativa verksamheten är den ena delen och förebyggande arbete, utbildning och information ingår i den andra delen. Ansvar för information och IT tillhör den förebyggande sidan. Som vi beskrivit tidigare i avsnitt 3.1.1, så har vice brandchef ansvar för vissa system som är verksamhetsspecifika. Förbundet har tidigare haft en ansvarig för GDPR och en informationssäkerhetsansvarig. Utsedd person har dock slutat inom förbundet och i nuläget har endast GDPR-ansvaret tilldelats ny funktion.

4.1.2 IT-säkerhet

Förbundet har genom avtal med Nora kommun outsourcat sin IT-drift. Anledningen till det beslutet var att förbundet växte med flera medlemskommuner vilket medförde att det inte längre fungerade att sköta IT-frågorna internt med den bemanning och organisation som förbundet hade vid tiden.

Som vi nämnt i avsnitt 3.1.1 avseende uppföljning av tidigare genomförd granskning så har det avtal som förbundet och kommunen tecknat inte uppdaterats i enlighet med lämnad rekommendation. Intervjupersoner uppger att avtalet är i behov av revidering och att det ska genomföras under kommande år.

Det innebär att det inte vid tiden för granskningen är tydliggjort några specifika krav på leveranser avseende IT-drift och IT-säkerhet mer än det som framgår av förbundets riktlinje för informationssäkerhet. Där finns på övergripande nivå följande beskrivning av kommunens uppdrag och ansvar som leverantör:

> ”IT-enheten, Nora kommun, ansvarar för att säkerheten i Nerike Brandkårs IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet.”

Förbundet erhåller enligt intervjuade en likvärdig IT-funktion som kommunen har och följer de rutiner och arbetssätt som IT-enheten etablerat för den kommunala verksamheten. Intervjupersoner uppger att avtalet är i behov av revidering och att det ska genomföras under kommande år. Det har enligt intervjuade inte gjorts någon mer formell kontroll eller revision av att avtalet efterlevs. Dock framgår av intervjuer att förbundet varit nöjda med leveransen och inte har identifierat något behov av att ställa andra krav än vad leverantören har levererat.

4.1.3 Dialog mellan förbundet och IT-leverantör

Vid intervjuer framkommer att förbundet och kommunens IT-chef i huvudsak är nöjd med den dialog de har etablerat. Brandchef och vice brandchef genomför fyra gånger per år eller vid behov möten med IT-chef i Nora kommun. Intervjupersoner uppger att aktuella driftsfrågor hanteras i dialogen tillsammans med utvärdering av etablerade skyddsåtgärder i syfte att upptäcka sårbarheter. Förbundet anger att de får råd från IT-funktionen avseende behov om ökade skyddsbehov, exempelvis införande av säkrare inloggningsfunktioner med mera.

En hög personalomsättning på IT-enheten uppges däremot ha påverkat samarbetet och lett till en sämre funktion och support det senaste året. En ny IT-chef har dock tillträtt och de inledande samtalen har uppfattats positiva.

4.1.4 Bedömning

Vår bedömning är att det finns etablerade strukturer för dialog mellan förbundet och IT-leverantören. I nuvarande form är dock avtal inte utformade så att det går att utföra en kvalitativ uppföljning och kontroll av de leveranser som förbundet erhåller. Vi konstaterar dock att förbundet varit nöjda med leverantörens leverans av IT-drift.

Utifrån direktionens övergripande ansvar för informationssäkerheten och det verksamhetsansvar som informationssäkerheten utgår från rekommenderar vi att dialog och uppföljning stärks genom att i regelbundna dialoger inkludera mer strategiska frågor utifrån upprättade riskanalyser där IT-säkerhet ingår.

4.2 IT-säkerhetsåtgärder

4.2.1 Riskhantering och informationsklassning

Av policyn för informationssäkerhet framgår att informationsklassning ska tillämpas med syfte att ge känslig och kritisk information ett starkare skydd än annan information, och på så sätt kan en anpassad och effektiv informationssäkerhet skapas. I riktlinjen kompletteras informationen avseende informationsklasser och det anges att det inom förbundet finns tre klasser för hur känslig informationen är och hur den får spridas; Öppen, Intern eller Konfidentiell.

Informationsklass	Behörighet/spridning	Exempel
2 Konfidentiell information	Konfidentiell information får endast vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen.	▪ Känsliga personuppgifter ▪ Sekretessbelagd information
1 Intern information	Intern information ska endast spridas till medarbetare inom Nerikes Brandkår och till externa som har behov av informationen.	▪ Riktlinje ▪ Instruktioner ▪ Information på intranät
0 Öppen information	Öppen information kan spridas fritt inom och utom Nerikes Brandkår.	▪ Pressmeddelanden ▪ Broschyrer ▪ Information på externwebb

Modellen baseras på Sveriges nationella modell för informationsklassning som är utgiven av MSB och SIS, men är anpassad till brandkårens behov. Den klassade informationen utgör ett underlag för en verksamhet vid kravställning av tjänster, exempelvis IT-tjänster, både internt och externt. Klassningsmodellen kan därigenom fungera som ett gemensamt ramverk och kommunikationsmodell vid förhandling mellan beställare och leverantör av tjänster. Vidare anges att identifiering och klassificering av information bör ske initialt när informationssäkerhetsbehovet ska analyseras, men även som ett led i löpande förbättring eller vid förändringar av verksamheter eller IT-system.

Som vi beskrivit tidigare så följer informationssäkerhetsansvaret med linjeansvaret. I det ansvaret ingår därigenom att genomföra riskbedömning och klassificering av den information som hanteras Därtill ingår att se till att sina medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att

informationssäkerheten i verksamheten kan uppnås. Arbetet med klassningar har inte kommit i gång ännu och klassningar har endast genomförts vid införande av molntjänster. Då förbundet inte genomfört klassningar har inte IT-enheten heller erhållit krav om kompletterande IT-säkerhetsåtgärder.

Förbundet har förutom eget ansvar för system och Nora kommun som systemansvarig ett antal externa leverantörer som driftar system och säkerställer säkerhet för dessa. Bland annat har vi i granskningen tagit del av dokumentation avseende det verksamhetssystem som räddningstjänsten nyttjar i den operativa verksamheten. För systemet finns upprättade avtal och en så kallad SLA, som är ett servicenivåavtal. Detta reglerar krav på leverantörens hantering och återställning om systemet inte är tillgängligt för förbundet. Intervjuade uppger att förbundet identifierat en sårbarhet kring systemleverantören då majoriteten av räddningstjänster i Sverige nyttjar systemet. Det skulle innebära att en allvarligare störning hos leverantören skulle kunna påverka kontinuiteten i verksamheten då information inte är tillgänglig. Dialog pågår på nationell nivå om åtgärder för att minska denna sårbarhet. Intervjupersoner uppger dock att räddningstjänsten i huvudsak skulle kunna upprätthålla sin operativa verksamhet utan tillgång till systemet.

Enligt intervjuade ingår det i avtalet mellan förbundet och Nora kommun att IT-enheten vidtar vissa skyddsåtgärder i IT-miljöns komponenter, som servrar, nätverk och datorer. Det finns bland annat brandväggslösningar och inbyggda skydd för plattform och e-post.

Intervjupersoner uppger att det pågår ett arbete vid IT-enheten med att byta ut nätverksutrustning vilket kommer generera bättre möjligheter till att övervaka och upptäcka eventuella hot. Det finns i dagsläget inget etablerat arbetssätt eller metod för att regelbundet bevaka nya hot och risker. I syfte att minimera förlust eller skada av information vid ett intrång genomför IT-enheten regelbundna backuper.

4.2.2 Bedömning

Vår bedömning är att informationsklassning och riskbedömning inte genomförs systematiskt i enlighet med beslutade styrdokument eller de rekommendationer som MSB ger. Då inte klassningar genomförts i någon större utsträckning, utan mer i undantagsfall vid nya systeminförandet, saknas underlag för att ställa krav om tekniska skyddsåtgärder för förbundets informationstillgångar som hanteras i system.

Nora kommun har inom sitt ansvar som leverantör för förbundet etablerat ett antal tekniska skyddsåtgärder för att skydda den information som lagras eller kommuniceras åt förbundet. Utan informationsklassning och bedömningar gjorda av förbundet kan det dock inte säkerställas att dessa åtgärder står i relation till informationens skyddsvärde.

4.3 Åtgärder utifrån ökad hotbild kring IT-angrepp

Av protokollsgenomläsning kan vi konstatera att direktionen inte under 2022 haft något ärende i syfte att informera sig om förbundets förmåga att stå emot cyberhot eller intrångsförsök. Av intervjuuppgifter framgår att direktionen inte efterfrågat riskanalys eller att förbundsledningen lämnat någon särskild information rörande ökad hotbild kring IT-angrepp och intrång. Det föranleder att inga beslut om åtgärder har fattats av direktionen.

Intervjupersoner beskriver att förbundet inte har ställt krav eller efterfrågat denna information från IT-leverantören utan litar på det arbete som utförs inom IT-enheten i Nora kommun mot bakgrund av den verksamhet och den information som hanteras internt i kommunen. Dessa nivåer uppfattas tillräckliga även för hantering av förbundets informationstillgångar och system.

4.3.1 Bedömning

Vår bedömning är att direktionen inte har efterfrågat riskanalys eller på annat sätt informerat sig om leverantörens förmåga utifrån den ökade hotbilden kring IT-angrepp och intrång. De har därigenom inte vidtagit åtgärder utifrån den ökade hotbilden kring IT-angrepp och intrång.

5 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att direktionen i nuläget inte har en tillräcklig styrning och intern kontroll över sin IT-säkerhet.

Bedömningen baserar vi på att det i nuläget saknas krav på vad Nora kommun som IT-driftsleverantör med ansvar för IT-säkerhet ska tillhandahålla för säkerhetsnivåer. Detta försvårar möjligheter för förbundet att följa upp avtal genom efterlevnadskontroller. De krav som direktionen beslutat om ska gälla för förbundets interna informationssäkerhetsarbete måste även ställas som ett minimum till externa leverantörer.

Direktionen har i viss utsträckning vidtagit åtgärder utifrån de rekommendationer som revisorerna lämnat i tidigare granskning. Vår bedömning är att rekommendationer kvarstår samt att det finns behov av ytterligare konkreta aktiviteter för de rekommendationer som hittills beaktats av direktionen.

Mot bakgrund av vår bedömning och slutsats rekommenderar vi direktionen att:

- Beakta och vidta åtgärder för de tidigare lämnade rekommendationerna från granskning av informationssäkerhet 2020, se sid 9.
- Revidera avtal med Nora kommun för att tydliggöra förbundets behov och krav avseende support och IT-säkerhet.
- Stärka dialog och uppföljning med Nora kommun som It-driftsleverantör och andra externa systemleverantörer där risker och hot kopplat till informations- och IT-säkerhet behandlas och dokumenteras regelbundet.
- Klassificera informationstillgångar i system så att resultat kan utgöra underlag för kravställning och beställning av it-säkerhetsåtgärder som står i relation till bedömt skyddsvärde på informationen som hanteras.
- Etablera en regelbunden uppföljning och återrapportering av det informationssäkerhetsarbete som genomförs så att direktionen har kännedom om aktuella hot och risker som förbundet behöver beakta för att skydda verksamheten.

Nerikes Brandkår
Granskning av IT-säkerhet

2022-12-13

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Linnéa Grönvold
Certifierad kommunal revisor

Mikael Lind
Certifierad kommunal revisor