Uppföljning granskning av it-säkerhet

Rapport
Västra Mälardalens Kommunalförbund

KPMG AB

2023-12-06

Antal sidor 15

Västra Mälardalens Kommunalförbund
Uppföljning granskning av it-säkerhet

2023-12-06

Innehållsförteckning

1 Sammanfattning

KPMG har av Västra Mälardalens kommunalförbunds revisorer fått i uppdrag att följa upp resultatet av en tidigare genomförd granskning av it-säkerhet från 2021. Revisorerna följer regelbundet upp tidigare genomförda revisionsgranskningar som ett led i att granska om genomförda granskningsinsatser bidragit till att verksamheterna utvecklas. Uppdraget ingår i revisionsplanen för år 2023.

Utifrån genomförd uppföljning är vår sammanfattande bedömning att förbundsdirektionen delvis hörsammat de rekommendationer som lämnades i samband med granskningen av it-säkerhet från 2021.

I den tidigare granskningen bedömdes att förbundet till viss del hade processer, rutiner och kontroll över it-säkerheten, men att arbetet inte bedrevs med ett tillräckligt riskbaserat förhållningssätt. Granskningen rekommenderade därför ett antal åtgärder med syfte att tillse att vidtagna säkerhetsåtgärder utgår från behov och riskbild.

Vi har genom den uppföljande granskningen delgivits ett antal vidtagna förbättringsåtgärder. Bland annat har en informationssäkerhetspolicy beslutats, vilken reglerar uppföljning samt roller och ansvar för det övergripande arbetet.

Dock anser vi att arbetet med riskanalyser har fortsatta utvecklingsbehov. Vi bedömer att förbundsdirektionen inte i tillräcklig omfattning efterfrågat riskanalyser eller bedömt informationssäkerhetsrisker. Vår bedömning är att förbundet i vissa väsentliga avseenden saknar ett systematiskt arbete med riskanalyser och informationsklassningar, vilket riskerar medföra att etablerade it-säkerhetsåtgärder inte motsvarar faktiska behov och aktuell hotbild.

Tidigare rekommendation	Bedömning: delvis	Tillkommande rekommendation
Besluta om att införa ett ledningssystem för informationssäkerhet för förbundet som kan utgöra ett ramverk för styrning och ledning. Därtill behöver erforderliga resurser säkerställas i förhållande till de behov som identifieras vid införandet.	Förbundet ser inte samma behov av ett ledningssystem för informationssäkerhet då det inte har fastställts hur förbundet och medlemskommunerna ska organisera sig i dessa frågor. Förbundsdirektionen och representanter från medlemskommunerna behöver besluta om ansvarsfördelning av uppgifter i arbetet. Detta då väsentliga aktiviteter som behöver genomföras för att it-säkerhetsarbetet i förbundet ska vara ändamålsenligt, inte genomförs i nuläget.	- Föra dialog med medlemskommunerna om gränsdragning mellan medlemskommunerna och förbundet avseende informationssäkerhetsarbetet och systemförvaltningsorganisationen.

Tidigare rekommendation	Bedömning: delvis	Tillkommande rekommendationer
Fastställa styrande dokument som tydliggör ansvar och de krav som ställs på hur arbetet med informationssäkerhet ska bedrivas.	Förbundet har tagit fram en informationssäkerhetspolicy som fastställer övergripande ansvar och roller samt former för uppföljning. Det är av vikt att förbundsdirektionen reviderar riktlinjen för systemförvaltning avseende att tydliggöra vikten av informationsklassningar och riskanalyser.	- Revidera riktlinjen för systemförvaltning med avseende på att tydliggöra vikten av att riskanalyser och informationsklassning genomförs som delar i ett riskbaserat it-säkerhetsarbete. - Föra dialog med medlemskommunerna om gränsdragning mellan medlemskommunerna och förbundet avseende informationssäkerhetsarbetet och systemförvaltningsorganisationen.
Tidigare rekommendation	**Bedömning: nej**	**Tillkommande rekommendationer**
Införa en modell/metod för riskanalys avseende it-infrastruktur som löpande uppdateras för att möta nya risker och hot.	Modell för riskanalys har inte införts. Riskanalys har inte genomförts. I likhet med vad som uppgavs vid den tidigare granskningen baseras därför en fortsatt stor andel av etablerade it-säkerhetsåtgärder på systemleverantörens rekommendationer.	- Införa en modell/metod för riskanalys avseende it-infrastruktur som löpande uppdateras för att möta nya risker och hot.
Tidigare rekommendation	**Bedömning: Delvis**	**Tillkommande rekommendationer**
Säkerställa att förbundet har ett uttalat mandat att ställa krav tillbaka på medlemskommunerna över väsentliga aktiviteter som påverkar förutsättningarna att arbeta med it-säkerhet.	Digitaliseringsrådet har förbättrat samsyn avseende prioriteringar i gemensamma informations- och it-säkerhetsfrågor. Rådet tillmäts viktig betydelse för samordning av it- och informationssäkerhetsarbetet mellan förbundet och medlemskommunerna.	- Förtydliga digitaliseringsrådets roll och ansvar i styrande dokument

Tillkommande revisionsfråga	Bedömning: Nej	Rekommendationer
Har förbundsdirektionen utifrån den ökade hotbild för cyberhot och attacker som funnits under 2022 och 2023 efterfrågat riskanalys eller presentation över förbundets förmåga att skydda information och upprätthålla verksamhet vid säkerhetshändelser inom IT?	Förbundsdirektionen har inte efterfrågat eller bedömt it- eller informationssäkerhetsrisker i tillräcklig omfattning.	- Genomföra en riskanalys som inkluderar informationssäkerhetsrisker för förbundet och utifrån behov vidta åtgärder för att minimera eller eliminera risker för förbundet

2 Bakgrund

Vi har av Västra Mälardalens kommunalförbunds revisorer fått i uppdrag att följa upp resultatet av en tidigare genomförd granskning av IT-säkerhet från 2021. Uppdraget ingår i revisionsplanen för år 2023.

Kommunalförbundets revisorer har efter avslutad granskning lämnat ett antal rekommendationer efter att förbättringsområden identifierats. Förbundsdirektionen har därefter svarat kommunalförbundets revisorer.

En uppföljande granskning av tidigare genomförda granskningar är viktig för att få en uppfattning om i vilken omfattning rapportens likväl som rekommendationerna tagits tillvara av berörda. Resultatet av en sådan uppföljning kan i sin tur ligga till grund för kommande riskanalysarbete.

Västra Mälardalens kommunalförbunds revisorer drar i sin riskanalys slutsatsen att efterlevnaden av kommunrevisionens lämnade rekommendationer i granskning av It-säkerhetsarbetet behöver granskas genom uppföljning.

2.1 Syfte, revisionsfrågor och avgränsning

Det övergripande syftet är att bedöma om förbundsdirektionen har vidtagit åtgärder i enlighet med lämnade rekommendationer.

De svar vi efterfrågar i uppföljningen är:

— Har åtgärder utifrån lämnade rekommendationer vidtagits?

— Har uppföljning av vidtagna åtgärder genomförts?

— Har förbundsdirektionen utifrån den ökade hotbild för cyberhot och attacker som funnits under 2022 och 2023 efterfrågat riskanalys eller presentation över förbundets förmåga att skydda information och upprätthålla verksamhet vid säkerhetshändelser inom IT?

Uppföljningen avser avlämnad revisionsrapport för granskning av It-säkerhet från 2021.

2.2 Revisionskriterier

Vi kommer utifrån genomförda granskning efterfråga svar på vilka åtgärder som vidtagits med anledning av granskningen. Vidare kommer vi att begära att få ta del av revisionsbevis i form av styrdokument, planer och rutiner för att verifiera uppgifter.

2.3 Ansvarig nämnd/styrelse

Granskningen avser förbundsdirektionen.

2.4 Metod

Granskningen har genomförts genom:

- Översiktlig granskning av styrande dokument
- Intervjuer/avstämningar med berörda tjänstepersoner:

Ordförande förbundsdirektionen

Förbundschef

It-chef

Samtliga intervjuade har faktakontrollerat rapporten

3 Resultat av den uppföljande granskningen

3.1 Granskning av IT-säkerhet från år 2021

Syftet med granskningen var att bedöma om förbundet har processer, rutiner och ändamålsenlig kontroll över IT-säkerheten samt bedöma om de åtgärder som vidtas baseras på risker och behov som ansvariga inom medlemskommunerna har fastställt för sina informationstillgångar.

Den sammanfattande bedömningen utifrån granskningens syfte var att förbundet till viss del hade processer, rutiner och kontroll över IT-säkerheten. Det fanns framtagna avtal och överenskommelser om drift och support och förbundet säkerställde löpande ett utvecklingsarbete för IT-infrastruktur för att möta nya risker och behov.

3.2 Uppföljning 2023

I nedanstående stycken presenteras granskningens rekommendationer från 2021 samt vilka åtgärder som vidtagits sedan dess med anledning av lämnade rekommendationer. Efter beskrivna åtgärder redogörs om förbundsdirektionen bedöms ha hörsammat rekommendationen eller inte. En sammanfattande bedömning lämnas efter uppföljningsavsnittet (se kap. 3.3 Sammanfattande bedömning och rekommendationer).

3.2.1 Rekommendation

- Besluta om att införa ett ledningssystem för informationssäkerhet för förbundet som kan utgöra ett ramverk för styrning och ledning. Därtill behöver erforderliga resurser säkerställas i förhållande till de behov som identifieras vid införandet.

Åtgärd

Enligt den tidigare granskningen avsåg förbundsdirektionen att implementera både ett ledningssystem och en organisation för informationssäkerhetsarbete då inget av detta fanns vid genomförandet av granskningen. De styrande dokument som var upprättade hade mer betoning på hantering av it-utrustning och var inte heller kända i tillräcklig omfattning i medlemskommunerna.

Vidare konstaterades att såväl förbundet som medlemskommunerna saknade tillbörliga organisationer för informationssäkerhetsarbetet. Diskussioner hade förts kring att tillsätta en för medlemskommunerna gemensam funktion för informationssäkerhet, samt en it-säkerhetsansvarig inom förbundet. Inget av detta hade realiserats, varvid största delen av arbetet i stället utfördes av förbundets it-chef. En anledning uppgavs vara att förbundet till medlemskommunerna uttryckt behov av, men inte medgivits, ytterligare resurser för att utöka organisationen.

Vid den uppföljande granskningen framkommer att medlemskommunerna anslagit 0,5 tjänst för en kombinerad informationssäkerhetssamordnare och dataskyddsombud. Rekryteringen har inte fullföljts då intresset för tjänsten varit lågt och förbundet inte hittat rätt person. Två medlemskommuner har även etablerat interna organisationer för informationssäkerhet. Som följd av det anses behovet av en gemensam informationssäkerhetssamordnare som stöttar samtliga kommuner ha minskat.

I fråga om implementering av ett ledningssystem för informationssäkerhet konstateras att dylikt inte införts. Givet medlemskommunernas minskade behov av en gemensam informationssäkerhetssamordnare och de nya styrande dokumenten ser intervjuade inget ytterligare behov av ett ledningssystem.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen delvis hörsammats.

Vi uppfattar att förbundet inte ser samma behov av ett ledningssystem för informationssäkerhet vid tid för uppföljningen. Detta mot bakgrund att det inte har fastställts hur förbundet och medlemskommunerna ska organisera sig i dessa frågor. Åtgärder i förhållande till rekommendationen har därigenom prioriterats ned i avvaktan på tydliggjord ansvarsfördelning.

Som vi kommer redogöra för i kommande rapportavsnitt ser vi behov av att förbundsdirektionen och representanter från medlemskommunerna beslutar om ansvarsfördelning av uppgifter i arbetet. Detta då vi kan konstatera att väsentliga aktiviteter som behöver genomföras för att it-säkerhetsarbetet i förbundet ska vara ändamålsenligt, inte genomförs i nuläget.

3.2.2 Rekommendation

- Fastställa styrande dokument som tydliggör ansvar och de krav som ställs på hur arbetet med informationssäkerhet ska bedrivas.

Åtgärd

Av den tidigare granskningen framkom att det saknades styrande dokument som konkretiserar ansvar och krav på informationssäkerhetsarbetet. Granskningen tog upp en riktlinje för systemförvaltning, vilken reglerar att informationsklassning av system ska genomföras, men som inte till fullo var implementerad i medlemskommunerna. Bedömning gjordes att det riskerade försämra möjligheterna för förbundet att upprätthålla det fulla it-säkerhetsansvaret.

Även uppföljning var ett område där den tidigare granskningen pekade ut brister. Uppföljning genomfördes inte regelbundet, vilket bedömdes bero på att det saknades styrande dokument som formaliserade uppföljning.

Genom den uppföljande granskningen ser vi att förbundet tagit fram en informationssäkerhetspolicy[1] och ett par anvisningar för medarbetare, bland annat en informationssäkerhetsanvisning[2]. Policyn fastställer ansvar och roller för det övergripande arbetet inom förbundet medan anvisningarna anger hur informationssäkerhet ska beaktas i det dagliga arbetet. Däremot saknas riktlinjer som kravställer arbetet på en mer konkret nivå. Det framförs av intervjuade att förbundet tagit fram kontinuitetsplaner och aktualiserat förvaltningsplaner för de mest centrala systemen. Som del i det har informationsklassningar genomförts för merparten av dessa system, dock konstateras att informationsklassningar inte genomförs med systematik utan mer situationsbaserat. Detta beskrivs vara en konsekvens av att riktlinjen för systemförvaltning fortfarande inte är helt känd av medlemskommunerna. Riktlinjen var vid tid för granskning under revidering. Ambitionen hos intervjuade är att i ett senare skede etablera den omarbetade riktlinjen i stället för att ta fram nya styrande dokument.

Gällande uppföljning förtydligas av informationssäkerhetspolicyn att informationssäkerhetsarbetet och incidentrapportering ska rapporteras till förbundsdirektionen och förbundsledningen en gång årligen. Efterlevnad av informationssäkerhetsarbetet ska säkerställas genom internkontroll.

I intervju framförs att incidentrapporteringen ännu inte etablerats, men att förbundets samlade säkerhetsarbete rapporteras en gång per år till förbundsdirektionen. Vi har vi tagit del av den återrapportering för 2023 som förbundschef gav till förbundsdirektionen i september månad 2023[3]. Underlaget visar att rapporten utgjordes av en samlad redogörelse för förbundet säkerhetsarbetet, där genomgång av aktiviteter och väsentliga händelser för informations- och it-säkerhetsarbetet var inkluderade.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen delvis hörsammats.

Vi bedömer att förbundsdirektionen formaliserat ändamålsenliga former för uppföljning av informationssäkerhetsarbetet, och att uppföljningen bidrar till att ge en översiktlig bild av förbundets arbete med att förebygga cyberhot och informationssäkerhetsrisker.

För att säkerställa att it-avdelningen ges förutsättningar att upprätta ändamålsenliga säkerhetsåtgärder för att skydda medlemskommunernas informationstillgångar bedömer vi att det är av vikt att förbundsdirektionen reviderar riktlinjen med avseende på att tydliggöra vikten av att informationsklassning och riskanalyser behöver ingå i ett riskbaserat informations- och it-säkerhetsarbete. Likaledes anser vi att förbundet bör ta

[1] Policy för informationssäkerhet, daterad 2022-12-14

[2] Daterad 2023-09-26

[3] Tjänsteskrivelse: uppföljning av säkerhetsarbetet på VMKF, daterad 2023-09-26

initiativ till en dialog om gränsdragning mellan medlemskommunerna och förbundet avseende informationssäkerhetsarbetet och systemförvaltningsorganisationen.

3.2.3 Rekommendation

- Införa en modell/metod för riskanalys avseende it-infrastruktur som löpande uppdateras för att möta nya risker och hot.

Åtgärd

Det fanns inga tydliga processer för riskanalyser avseende it-infrastruktur, enligt vad som framkom vid tidigare granskning. Det visade sig att förbundet dessförinnan genomfört riskanalyser utan systematik, företrädelsevis då behov uttryckts och då med hjälp av en extern leverantör. Det genomfördes heller inget systematiskt arbete med informationsklassning, vilket föranledde att medlemskommunerna sällan kravställde it-säkerhetsåtgärder mot förbundet.

Vid den uppföljande granskningen delges att förbundsdirektionen inte infört någon modell för riskanalys avseende it-infrastruktur, eller genomfört någon dylik analys. Visst riskanalysarbete uppges ha gjorts inom ramen för framtagandet av kontinuitetsplaner, då vissa system informationsklassats. I likhet med vad som uppgavs vid den tidigare granskningen baseras därför en fortsatt stor andel av etablerade it-säkerhetsåtgärder på systemleverantörens rekommendationer.

Däremot framförs att förbundet sedan två år strukturerat upp överenskomna servicenivåer, SLA[4], mellan förbundet och medlemskommunerna vilket anses ha bidragit till att identifiera vissa risker för några system.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte hörsammats.

Likaväl som att enskilda system behöver skyddas av ändamålsenliga säkerhetsåtgärder behöver hot och risker identifieras och förebyggas även för it-infrastrukturen.

[4] ”Service level agreement” motsvarar ett serviceavtal där kravställning av it-driften regleras.

3.2.4 Rekommendation

- Säkerställa att förbundet har ett uttalat mandat att ställa krav tillbaka på medlemskommunerna över väsentliga aktiviteter som påverkar förutsättningarna att arbeta med it-säkerhet.

Åtgärd

Mot bakgrund av att förbundet betraktas som en utförarorganisation uttryckte intervjuade förbundsföreträdare, i samband med tidigare granskning, svårigheter att kravställa ett tillräckligt aktivt arbete från medlemskommunernas sida.

Intervjuade förbundsrepresentanter anser vid den uppföljande granskningen att det inte längre finns behov att förtydliga mandatet. Motiveringen är det digitaliseringsråd som även fanns vid den förra granskningen, där rådsdeltagarna numera upplevs ha bättre samsyn och där diskussion förs kring vilket arbete som ska utföras. Rådet utgörs av förbundschef, förbundets it-chef samt en representant för vardera medlemskommun. Det beskrivs som ett dialog- och samordningsforum där förbundet och medlemskommunerna fattar beslut och gör prioriteringar i gemensamma informations- och it-säkerhetsfrågor.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen delvis hörsammats.

Utifrån intervjuuppgifter uppfattar vi att digitaliseringsrådet tillmäts viktig betydelse för samordning av it- och informationssäkerhetsarbetet mellan förbundet och medlemskommunerna.

För att säkerställa digitaliseringsrådets funktion och ansvar för det gemensamma arbetet bedömer vi att dess roll behöver formaliseras i styrande dokument.

3.2.5 Tillkommande revisionsfråga i uppföljande granskning

- Har förbundsdirektionen utifrån den ökade hotbild för cyberhot och attacker som funnits under 2022 och 2023 efterfrågat riskanalys eller presentation över förbundets förmåga att skydda information och upprätthålla verksamhet vid säkerhetshändelser inom IT?

Åtgärd

Enligt intervjuad direktionsordförande har förbundsdirektionen inte efterfrågat riskanalys eller presentation. Förbundsdirektionen framförs ha hög tilltro till tjänstepersonernas arbete, härvid förväntar sig förbundsdirektionen att tjänstepersonerna delger förbundsdirektionen den information som de anser relevant.

Bedömning

Vi bedömer att förbundsdirektionen inte efterfrågat eller bedömt it- eller informationssäkerhetsrisker i tillräcklig omfattning.

Genom den uppföljande granskningen konstaterar vi att åtgärder vidtagits för att minska hot och risker som förbundet utsätts för, men att arbetet inte är tillräckligt systematiskt för att säkerställa ett ändamålsenligt it-säkerhetsskydd i förhållande till behovs- och riskbild.

.

3.3 Samlad bedömning och rekommendationer

Vår bedömning är att förbundsdirektionen delvis hörsammat de rekommendationer som lämnades i samband med granskningen av it-säkerhet från 2021.

Vi har genom den uppföljande granskningen delgivits ett antal vidtagna förbättringsåtgärder. Dock anser vi att arbetet med riskanalyser har fortsatta utvecklingsbehov. Vi bedömer att förbundsdirektionen inte i tillräcklig omfattning efterfrågat riskanalyser eller bedömt informationssäkerhetsrisker. Vår bedömning är att förbundet i vissa väsentliga avseenden saknar ett systematiskt arbete med riskanalyser och informationsklassningar, vilket riskerar medföra att etablerade it-säkerhetsåtgärder inte motsvarar faktiska behov och aktuell hotbild.

Mot bakgrund av genomförd uppföljning kvarstår följande rekommendationer helt eller delvis till förbundsdirektionen:

- Införa en modell/metod för riskanalys avseende it-infrastruktur som löpande uppdateras för att möta nya risker och hot.

Mot bakgrund av genomförd uppföljning tillkommer följande rekommendation till förbundsdirektionen:

- Revidera riktlinjen för systemförvaltning med avseende på att tydliggöra vikten av att riskanalyser och informationsklassning genomförs som delar i ett riskbaserat it-säkerhetsarbete.
- Föra dialog med medlemskommunerna om gränsdragning mellan medlemskommunerna och förbundet avseende informationssäkerhetsarbetet och systemförvaltningsorganisationen.
- Förtydliga digitaliseringsrådets roll och ansvar i styrande dokument.
- Genomföra en riskanalys som inkluderar informationssäkerhetsrisker för förbundet och utifrån behov vidta åtgärder för att minimera eller eliminera risker för förbundet

2023-12-06

KPMG AB

Jenny Thörn
Kommunal revisor

Sofie Ernerudh
Kommunal revisor

Karin Helin-Lindkvist
Certifierad revisor och kundansvarig