REGION SÖRMLAND

PROTOKOLLSUTDRAG

Datum
2022-06-14

Dokumentnummer
RS-LED22-1197-4

§ 113/22 Yttrande över revisionens granskning - IT/informationssäkerhet år 2022

Diarienummer: RS-LED22-1197

Regionstyrelsens beslut

Yttrandet godkänns.

Yrkande

Bertil Malmberg (-) yrkar bifall till förvaltningens förslag.

Proposition

Ordförande Monica Johansson (S) ställer förvaltningens förslag under proposition och finner att det bifalls.

Ärendet

Revisorerna i Region Sörmland har gett revisionsföretaget KPMG i uppdrag att genomföra en granskning av regionens arbete med IT- och informationssäkerhet. Syftet är att bedöma om regionstyrelsen säkerställer en god internstyrning och kontroll av IT- och informationssäkerhetsarbetet, med syfte att skapa en ändamålsenlig informationssäkerhet och uppnå informationssäkerhetspolicyns mål.

Revisorernas sammanfattande bedömning är att regionstyrelsen delvis säkerställer en god intern styrning och kontroll av sitt IT- och informationssäkerhetsarbete.

Revisorerna har framfört synpunkter gällande att IT-säkerheten endast regleras på en övergripande nivå, att uppföljningen sker endast på övergripande nivå och att en intern kontroll av efterlevnad bör etableras. Revisorerna identifierar också brister i kraven på IT-säkerhet och hur uppföljningen ska ske. Det finns även brister i hur många medarbetare som genomför regionens obligatoriska utbildningar inom informationssäkerhet, vilket leder till risker.

Regionstyrelsen ställer sig bakom revisorernas rekommendationer, vilka stämmer överens med styrelsens egna ambitioner gällande IT- och informationssäkerhet. I regionstyrelsens yttrande framför vikten av att etablera intern kontroll för att säkerställa uppföljning av regionens styrande dokument på dessa områden.

Gränsdragningen mellan IT- och informationssäkerhet och resp. verksamhets ansvarsområden utreds och ska inarbetas i regionens styrande dokument. Även en komplettering av styrande dokument kommer att ske vid behov.

Kontinuitetsplanering ska bli en integrerad del i arbetet med att skydda IT- och informationssäkerhet genom ett förbättrat metodstöd riktat till verksamheterna. Sammanfattningsvis avser Region Sörmland att fortsätta det systematiska och riskbaserade IT- och informationssäkerhetsarbetet samt att stärka styrning, kontroll och uppföljning på området.

Beslutsunderlag

Tjänsteutlåtande
Yttrande över revisionens granskning av IT/informationssäkerhet
År 2022 - Granskning av IT/informationssäkerhet

Beslutet expedieras till

Revisionen
Jan Grönlund, regiondirektör
Urban Petrén, IT-direktör
Jonas Jensen, Informationssäkerhetschef
Akten

REGION SÖRMLAND

Handläggare
Jonas Jensen
Informationssäkerhetsenheten (1)

Datum
2022-04-26

Dokumentnummer
RS-LED22-1197-3

Ärendegång
Regionstyrelsen

Yttrande över revisionens granskning - IT/informationssäkerhet år 2022

Förslag till beslut

Regionstyrelsens beslut

Yttrandet godkänns.

Ärendet

Revisorerna i Region Sörmland har gett revisionsföretaget KPMG i uppdrag att genomföra en granskning av regionens arbete med IT- och informationssäkerhet. Syftet är att bedöma om regionstyrelsen säkerställer en god internstyrning och kontroll av IT- och informationssäkerhetsarbetet, med syfte att skapa en ändamålsenlig informationssäkerhet och uppnå informationssäkerhetspolicyns mål.

Revisorernas sammanfattande bedömning är att regionstyrelsen delvis säkerställer en god intern styrning och kontroll av sitt IT- och informations-säkerhetsarbete.

Revisorerna har framfört synpunkter gällande att IT-säkerheten endast regleras på en övergripande nivå, att uppföljningen sker endast på övergripande nivå och att en intern kontroll av efterlevnad bör etableras. Revisorerna identifierar också brister i kraven på IT-säkerhet och hur uppföljningen ska ske. Det finns även brister i hur många medarbetare som genomför regionens obligatoriska utbildningar inom informationssäkerhet, vilket leder till risker.

Regionstyrelsen ställer sig bakom revisorernas rekommendationer, vilka stämmer överens med styrelsens egna ambitioner gällande IT- och informationssäkerhet. I regionstyrelsens yttrande framför vikten av att etablera intern kontroll för att säkerställa uppföljning av regionens styrande dokument på dessa områden.

Gränsdragningen mellan IT- och informationssäkerhet och resp. verksamhets ansvarsområden utreds och ska inarbetas i regionens styrande dokument. Även en komplettering av styrande dokument kommer att ske vid behov.

Kontinuitetsplanering ska bli en integrerad del i arbetet med att skydda IT- och informationssäkerhet genom ett förbättrat metodstöd riktat till verksamheterna.

REGION SÖRMLAND

Handläggare
Jonas Jensen
Informationssäkerhetsenheten (1)

Datum
2022-04-26

Dokumentnummer
RS-LED22-1197-3

Sammanfattningsvis avser Region Sörmland att fortsätta det systematiska och riskbaserade IT- och informationssäkerhetsarbetet samt att stärka styrning, kontroll och uppföljning på området.

Beslutsunderlag

Yttrande över revisionens granskning av IT/informationssäkerhet
År 2022 - Granskning av IT/informationssäkerhet

Beslutet expedieras till

Revisionen
Jan Grönlund, regiondirektör
Urban Petrén, IT-direktör
Jonas Jensen, Informationssäkerhetschef
Akten

REGION SÖRMLAND

Handläggare
Jonas Jensen
Informationssäkerhetsenheten (1)

Datum
2022-04-26

Dokumentnummer
RS-LED22-1197-3

Yttrande över revisionens granskning - IT/informationssäkerhet

Regionstyrelsen har mottagit en granskningsrapport från revisionen gällande arbetet med IT- och informationssäkerhet. Regionstyrelsen ska yttra sig senast den 23 juni 2022.

Regionstyrelsen ser positivt på granskningen och ställer sig bakom revisionens rekommendationer. Region Sörmland har för ambition att leva upp till lagstiftarens krav gällande hantering av personuppgifter och övriga informationstillgångar.

I det fortsätta arbete med att stärka ett systematiskt IT- och informationssäkerhetsarbete kommer regionstyrelsen att överväga frågan ifall resurstilldelning behöver öka för att möta lagstiftarens krav. Frågan kommer att hanteras inom ramen för budgetberedning för de kommande åren.

Regionstyrelsen ser nämligen ett behov av att utveckla stöd till verksamheterna på områdena IT- och informationssäkerhet. Bland annat ska följsamhet av regionens styrande dokument samt medarbetarnas genomförande av obligatoriska utbildningar att säkerställas.

RSIT och Informationssäkerhetsenheten har sedan årsskiftet 2021/2022 arbetat med att utvärdera och tydliggöra ansvarsfördelning och gränsdragning mellan områdena IT- och informationssäkerhet; utvärderingen förväntas bli klar under våren 2022. Inom ramen för detta arbete kommer även en översyn av styrande dokument och eventuella kompletteringar att ske.

Kontinuitetsplanering av verksamheten kommer att analyseras och utvecklas bland annat genom tydliggörande av krav och metodstöd för hantering av informationstillgångar, test och övningar.

Monica Johansson (S)
Regionstyrelsens ordförande

Jan Grönlund
Regiondirektör