Svar på revisionsrapport - Uppföljande granskning - Informations- och cybersäkerhet

Sammanfattning

Revisorerna i Region Gävleborg har beslutat att genomföra en uppföljande granskning av informations- och cybersäkerhet inom Region Gävleborg. Granskningen som genomfördes av revisionsbiträdet PwC under 2021 hade som syfte att besvara om ändamålsenliga åtgärder vidtagits med anledning av 2019 års granskning.

Revisionsrapporten överlämnades av regionfullmäktige den 16 februari 2022 till regionstyrelsen för beredande av svar.

Kommentarer

Regionstyrelsen lämnar följande kommentarer till revisionsrapporten.

Övergripande kommentarer

Regionstyrelsen välkomnar att revisorerna än en gång har uppmärksammat området informations- och cybersäkerhet. Informationssäkerhet- och cybersäkerhet får en allt viktigare betydelse för att kunna tillgodose Region Gävleborgs verksamheter och medborgares behov. Det finns även högre krav på lagefterlevnad inom området än tidigare.

Sedan 2019 har ett systematiskt arbete bedrivits inom informations- och cybersäkerhet, vilket har medfört förbättringar. Det systematiska regiongemensamma informationssäkerhetsarbetet är avgörande för de förbättringar som påvisas i revisorernas rapport. Dessa förbättringar speglas även i de mätningar som Myndigheten för samhällsskydd och beredskap (MSB) har genomfört i omgångar och även i den interna uppföljningen. Området är ständigt föränderligt och kräver ett kontinuerligt lärande och kontinuerliga förbättringar. Dessutom behöver vi identifiera och möta både nya och befintliga hot och sårbarheter, samt tillse att Region Gävleborg har ändamålsenliga säkerhetsåtgärder implementerade.

Revisorerna har fokuserat på den övergripande styrningen av informationssäkerhet samt tittat på några IT-säkerhetsområden. Utöver de frågor som revisorerna har adresserat så bör också nämnas

- IT-förvaltningen arbetar utifrån en treårsplan för att förbättra Region Gävleborgs cybersäkerhetsförmåga.

- Arbetet med att identifiera, informationsklassa samt genomföra riskanalyser pågår för samtlig information som hanteras inom Region Gävleborg (processorienterad informationskartläggning).
- Samverkan på området sker med andra regioner, SKR samt statliga myndigheter exempelvis MSB.

Regionstyrelsens kommentarer angående revisorernas bedömningar
Regionstyrelsen lämnar följande kommentarer till revisionsrapporten kopplat till respektive revisionsfråga

Revisionsfråga 1 – Har regionen fastställt styrande dokument inom både informations- och cybersäkerhet?

Revisorernas bedömning är att kontrollmålet är helt uppfyllt.

Regionstyrelsen delar revisorernas bedömning. Styrdokument revideras vid behov och som minst årligen för att möta lagkrav, omvärldsläget och verksamhetens behov.

Revisionsfråga 2 - Har regionen fastställt dokumenterade processer för arbetet med informations- och cybersäkerhet?

Revisorernas bedömning är att kontrollmålet är till övervägande del är uppfyllt.

Regionstyrelsen delar revisorernas bedömning. Den processorienterade informationskartläggningen har återupptagits efter pandemin och arbetet fortlöper. Under 2022 kommer ett systematiskt arbetssätt för uppföljning av informationssäkerhet att implementeras, uppföljning kommer att dokumenteras.

Revisionsfråga 3 - Har regionen formaliserat och systematiserat arbetet med informationssäkerhetsrisker?

Revisorernas bedömning är att kontrollmålet är uppfyllt till övervägande del.

Regionstyrelsen delar revisorernas bedömning. Det finns ett formaliserat och systematiserat arbetssätt avseende informationssäkerhetsrisker som tillämpas i samtliga verksamheter inom Region Gävleborg. Inom Region Gävleborg pågår dessutom ett antal förbättringsåtgärder kopplat till IT-säkerhet kring många av de punkter som ingår i granskningen.

Revisionsfråga 4 - Har regionen en incidenthanteringsprocess som samordnas genom samverkan mellan informationssäkerhetsavdelningen och IT-avdelningen?

Revisorernas bedömning är att kontrollmålet är uppfyllt till övervägande del.

Regionstyrelsen delar revisorernas bedömning. Arbete med kontinuitetshantering har påbörjats och kommer genomföras för verksamhets- och samhällskritiska processerna inom Region Gävleborg. I frågan ingår även kontinuitetshantering av centrala IT-processer. Detta arbete har påbörjats och arbetet med kontinuitetshantering och katastrofplaner för regionens IT-miljö kommer att pågå under 2022-2023.

Revisionsfråga 5 - Har regionen säkerställt att funktionen för informationssäkerhet har tillräckligt med mandat för att bedriva sitt uppdrag och att de förvaltar sin egen budget?

Revisorernas bedömning är att kontrollmålet är uppfyllt till övervägande del.

Regionstyrelsen delar bedömningen, genom att förändra organisationen så att informationssäkerhet är en egen enhet och att IT-utveckling, -drift och -förvaltning numera sker samlat i en egen förvaltning så har ytterligare tyngd lagts på dessa områden.

Revisionsfråga 6 - Har regionen genomfört, samt fortsätter att genomföra, utbildningar och kompetenshöjande aktiviteter inom området cybersäkerhet?

Revisorernas bedömning är att kontrollmålet är uppfyllt till övervägande del.

Regionstyrelsen delar bedömningen. Det finns sedan tidigare obligatoriska grundutbildningar inom området, dessutom publiceras information regelbundet för att höja medvetenheten kring informations- och cybersäkerhet. Kampanjer inom området, ofta kopplade till omvärldshändelser, kommer även fortsättningsvis att prioriteras.

Regionstyrelsens kommentarer angående revisorernas rekommendationer

- Fastställ dokumentet (rutinen) ”Livscykelhantering i Region Gävleborg”.

  Regionstyrelsen delar rekommendationen. Arbetet kommer att genomföras under 2022.

- Slutför och dokumentera den påbörjade processkartläggningen, med fokus på de återstående kärnprocesserna, då dessa torde ha högre prioritet än

resterande stöd- och ledningsprocesser. Sammanställ processkartläggningen på ett sätt som skapar överblick och som underlättar uppföljning och styrning.

Regionstyrelsen delar rekommendationen om genomförande av den processorienterade informationskartläggningen ska slutföras och arbetet återupptogs under hösten 2021

- Stärk arbetet med uppföljning av tidigare upphandlingar genom tydligt utpekat ansvar och genom stickprov samt ett dokumenterat systematiskt arbete relaterat till uppföljning.

  Regionstyrelsen delar rekommendationen. Ett systematiskt arbetssätt, som även omfattar upphandlingar, för operativ, taktisk samt strategisk uppföljning kommer att implementeras under 2022.

- Förtydliga hur arbetet med området för informationssäkerhet ska följas upp, med tydliga mål och planer för hur detta ska ske.

  Regionstyrelsen delar rekommendationen. Ett systematiskt arbetssätt för operativ, taktisk samt strategisk uppföljning kommer att implementeras under 2022.

- Slutför arbetet med utformandet av en övergripande kontinuitetsplan och säkerställ att arbetet med nedbrutna och anpassade planer för verksamheterna slutförs.

  Regionstyrelsen delar uppfattningen. Verksamhets- och samhällskritiska processer har prioriterats på ett övergripande plan och genomförande har påbörjats tillsammans med Säkerhets- och beredskapsavdelningen.

- Överväg att skapa ett dokumenterat rollbaserat utbildningspaket för olika personalgrupper inom organisationen.

  Regionstyrelsen delar inte uppfattningen fullt ut. Det finns redan idag rollbaserad utbildningspaket, dessa kan dock förbättras och utökas.

- Överväg att utveckla dokumenterade rollbaserade eller individuella utbildningsplaner, vilka följs upp för att säkerställa att obligatoriska moment verkligen genomförts.

  Regionstyrelsen delar inte uppfattningen fullt ut, detta sker redan idag i Kompetensportalen likt annan utbildning inom Region Gävleborg.

- Överväg att genomföra ytterligare medvetandehöjande kampanjer kring ransomware, nätfiske eller lösenordsbyte, gärna vid olika tidpunkter varje år.

Regionstyrelsen delar uppfattningen att detta är ett prioriterat område. Befintligt arbete med informationsspridning kommer att ske fortlöpande.

Regionstyrelsen

Eva Lindberg
Regionstyrelsens ordförande

Markus Bylund
IT-direktör