Rcvisionsskrivclse

Datum 2020-04-08

Regionstyrelsen

Granskning av informations- och cybersäkerhet

På uppdrag av oss, de förtroendevalda revisorerna i Region Gotland, har PwC, genomfört en granskning av informations- och cybersäkerhet i regionen.

Den pågående digitaliseringen ger möjligheter att höja kvalitet, säkerhet och effektivitet i regionens olika verksamheter och förbättra service till medborgare, organisationer och företagare. Den andra sidan av myntet målar dock en annan bild, nämligen att allt fler inom privat- som offentlig sektor drabbas av allvarliga attacker, intrång, läckage och avbrott.

I syfte att bedöma om regionstyrelsens har en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet har en granskning genomförts. Granskningens inriktning har baserats på en förstudie som genomförts under året. Granskningen har avgränsats till att omfatta regionstyrelseförvaltningen (kontoret) och teknikfötvaltningen.

Efter genomförd granskning görs bedömningen att regionstyrelsen delvis säkerställt en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet.

Kontrollmålen som varit ledande i granskningen är baserade på förmågan att **identifiera** säkerhetsrisker och tillgångar; **skydda** tillgångar och IT-miljön; **upptäcka** och analysera säkerhetshändelser; **hantera** och kommunicera kring säkerhetshändelser samt **återställa** verksamheten och IT-miljön efter säkerhetshändelser och lära av dessa. Revisionskritetietna ir baserade på säkerhetsstandarden *1\|/S T (ybenemri(y Framework (CSF).*

Postadress SE-621 81 Visby
Telefon +46 (0)498 26 90 00 vxl
E-post regiongotland@gotland.se
Org nr 212000-0803
Webbplats www.gotland.se

Bedömningen bygger i huvudsak på att:

- Region Gotland har ett väl etablerat ledningssystem för informationssäkerhet.
- Det finns en central grupp med ansvar att samordna säkerhetsfrågor i regionen och att stötta och informera verksamhet och ledning i dessa frågor.
- Det pågår en digitaliseringsförändring i IT-miljön i stort som medför en minskad riskexponering.
- Det läggs ett stort ansvar på systemägare och verksamhetsansvariga i organisationen utan stöd från ledning eller säkerhetsorganisation.
- Flera av de största riskerna som identifierats i granskningen avser förmågan att upptäcka säkerhetshändelser. Regionen är välmedveten om detta och utvärderar vidare åtgärder.

Revisionen överlämnar revisionsrapporten till regionstyrelsen för yttrande med anledning av granskningens resultat och lämnade rekommendationer. Svar önskas senast den 28 september 2020.

Svaret skickas till registrator i Region Gotland på adress registrator-rs@gotland.se med kopia till sakkunnigt biträde carin.hultgren@pwc.com

För Region Gotlands revisorer,

Mats Ågren

Orr!frirande