Revisorerna

Region Gotland

2024-11-06

Till:
Regionstyrelsen, hälso- och sjukvårdsnämnden, socialnämnden samt bolagsstyrelsen i AB Gotlandshem.

För kännedom:
Regionfullmäktige
Valnämnden
Överförmyndarnämnden

Granskning av kontinuitetsplanering för it-avbrott

KPMG har av Region Gotlands revisorer fått i uppdrag att granska om regionstyrelsen, hälso- och sjukvårdsnämnden och socialnämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

KPMG:s samlade bedömning utifrån granskningens syfte är att regionstyrelsen och nämnderna delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser.

I revisionsrapporten som bifogas framgår väsentliga iakttagelser. Utifrån våra iakttagelser och bedömningar rekommenderar vi **regionstyrelsen** att:

- Förtydliga hur arbetet med kontinuitetsplanering är tänkt att bedrivas utifrån befintliga riskprocesser i regionen.
- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna sker enligt en av regionstyrelsen beslutad systematik.
- Tillse att det är tydligt på vilket sätt kritiska beroenden till informationssystem ska beaktas i verksamheternas kontinuitetsplanering.
- Säkerställa att de egna verksamheterna beaktar kritiska beroenden till informationssystem i sin kontinuitetsplanering.
- Tillse att informationsklassningen för måltidsverksamhetens kritiska system slutförs.
- Säkerställa att avtalad servicenivå och beredskap baserad på skyddsvärde och behov av tillgänglighet framtas för måltidsverksamheten verksamhetskritiska informationssystem.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Säkerställa att det är tydligt på vilket sätt kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar.
- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad regionövergripande systematik.

Utifrån resultatet av vår granskning rekommenderar vi **hälso- och sjukvårdsnämnden** att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna sker enligt en av regionstyrelsen beslutad systematik.

- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad regionövergripande systematik

Utifrån resultatet av vår granskning rekommenderar vi **socialnämnden** att:

- Även om nämnden har en god planering i nuläget kan det finnas behov av att anpassa denna om beslut fattas av regionstyrelsen över krav och gemensamma arbetssätt.

- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad regionövergripande systematik.

AB Gotlandshem:

Syftet med granskningen har varit att bedöma om AB Gotlandshem har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

KPMG:s bedömning är att bolagsstyrelsen i AB Gotlandshem i allt väsentligt har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser

- Beakta på vilka sätt bolaget behöver anpassa sina arbetssätt i förhållande till de av regionfullmäktige beslutade styrdokumenten som även reglerar bolagens krisberedskapsarbete.

- Utifrån av bolaget identifierade risker inom cybersäkerhet säkerställa att det finns en tydlig struktur och process för att identifiera och vidta åtgärder som säkerställer en tillräcklig planering så att kontinuitet i verksamheten vid kritiska it-säkerhetshändelser upprätthålls.

- I högre utsträckning bedriva kontinuitetsplaneringsarbetet i en mer sammanhållen process som inkluderar både systemnära åtgärder och åtgärder i verksamhetens rutiner.

- Tillse att det finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheten fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

Vi emotser nämndens samt AB Gotlandshem yttrande till våra iakttagelser och rekommendationer i bifogad rapport senast 2025-02-10. Yttrandet expedieras till Klara.lowenberg@kpmg.se samt Barbro.Hejdenberg-Ronsten@gotland.se

De förtroendevalda revisorerna i Region Gotland,
Barbro Hejdenberg Ronsten
Ordförande