# Revisionsrapport - Granskning av informations- och cybersäkerhet

Dnr 01458-2022

## Förslag till beslut

Regionstyrelsen beslutar att:

1. Ge regiondirektören i uppdrag att säkerställa ett ändamålsenligt arbete kring informations- och cybersäkerhet samt internkontroll enligt de förslag som framkommer i ärendebeskrivningen.
2. Återrapportering med nödvändiga åtgärder sker till styrelsen senast 10 maj 2023.
3. Lägga revisionsrapporten till handlingarna.

## Yttrande till beslutsförslaget

Regionstyrelsen har tagit del av revisorernas granskning av regionens informations- och cybersäkerhet. Styrelsen delar revisorernas bedömning att mer kan göras för att stärka kritiska informationssäkerhetsprocesser inom regionen.

## Sammanfattning

Revisorerna bedömer att Region Norrbotten till viss del säkerställer ett ändamålsenligt arbete kring informations- och cybersäkerhet. Revisorerna presenterar regionens mognadsnivå i de områden som analyserats, samt ger förslag på vilka åtgärder som bör vidtas för att förbättra arbetet.

## Beslutsunderlag

Revisionsrapport Region Norrbotten, Granskning av informations- och cybersäkerhet (juni 2022)

## Ärendet

Revisorerna (PwC) har genomfört en granskning av regionens informations- och cybersäkerhet. Syftet med granskningen var att bedöma om Region Norrbotten säkerställer ett ändamålsenligt arbete kring informations och cybersäkerhet, samt om detta sker med tillräcklig intern kontroll.

Kontrollmålen är baserade på säkerhetsstandarden NIST Cyber Security Framework (CSF) och formulerade för att bedöma regionens förmåga att:

- identifiera säkerhetsrisker och tillgångar
- skydda tillgångar

- upptäcka och analysera säkerhetshändelser
- hantera och kommunicera kring säkerhetshändelser, samt
- återställa verksamheten och IT-miljön efter säkerhetshändelser och lära av dessa.

Efter genomförd granskning bedömer revisorerna att Region Norrbotten till viss del säkerställer ett ändamålsenligt arbete kring informations- och cybersäkerhet. Revisorerna har noterat ett antal områden där arbetet kan förbättras och presenterar även regionens mognadsnivå i de olika kontrollmålen. Mognadsnivån anges utefter en bedömningsskala från 1-5, där 5 är högst och representerar optimerad nivå.

## Resultat

### Identifiera

Mognadsnivån (1.8) återspeglar i huvudsak att Region Norrbotten har ett återstående arbete med att intensifiera och slutföra klassificering av samtliga IT-system inom regionen. Regionen har även ett behov av att säkerställa genomförande av riskanalys på systemnivå i samtliga förvaltningar med bäring på IT- och informationssäkerhet. Slutligen behöver regionen öka sin mognadsnivå med hänsyn till hur uppföljning av säkerhetskrav med leverantör ska ske.

### Skydda

Mognadsnivån (2.2) återspeglar i huvudsak att Region Norrbotten har en begränsad förmåga att proaktivt monitorera och övervaka samtlig IT-infrastruktur. Vidare bör regionen intensifiera planen med att införa obligatoriska, regelbundna utbildningsmoment för samtliga medarbetare inom regionen med bäring på IT- och informationssäkerhet. Vidare behöver regionen intensifiera arbetet med att genomföra mer heltäckande återläsningstester av säkerhetskopior.

### Upptäcka

Mognadsnivån (1.9) återspeglar i huvudsak att Region Norrbotten saknar en centraliserad proaktiv säkerhetsövervakning innefattande logginformation från samtliga kritiska verksamhetsspecifika system. Idag sker majoriteten av säkerhetsövervakningen reaktivt och på förekommen anledning. Ytterligare förbättringsområden finns vad gäller systematisk identifiering av sårbarheter. Roller och ansvar med hänsyn till regionens förmåga att upptäcka säkerhetsincidenter skulle kunna stärkas och förtydligas ytterligare för att maximera nyttan och skapa bättre förutsättningar för proaktiv detektion.

### Hantera/respondera

Mognadsnivån (2.3) återspeglar i huvudsak att Region Norrbotten behöver se över sina incidenthanteringsplaner för prioriterade hot. Detta inkluderar att införa en rutin för att regelbundet genomföra incidentövningar för att

säkerställa att hanteringsregler och eskaleringsrutiner är aktuella och väl införstådda genomgående i regionen.

### Återställa

Mognadsnivån (2.2) återspeglar i huvudsak att regionen saknar heltäckande testade och övade IT-katastrofåterställningsplaner för samtlig IT-infrastruktur. Detsamma gäller även framtagning av kontinuitetsplaner för samtliga verksamhetskritiska system som beskriver vilka alternativa arbetsmetoder som ska aktiveras för att minimera konsekvensen av långvariga IT-avbrott för verksamheten.

### Protokollsutdrag skickas till:

Regionens förtroendevalda revisorer
Regiondirektör
IT/MT-direktör
Verksamhetschef IT/MT-stöd