Revisionsrapport

Granskning av regionens arbete med cybersäkerhet

November 2025

Qualitarium AB
559155-9652
Turning Torso, 211 15 Malmö
qualitarium.se

Innehållsförteckning

Sammanfattning

Granskningens syfte har varit att bedöma om regionstyrelsen säkerställt att Region Dalarnas arbete med cybersäkerhet är ändamålsenligt. Den samlade revisionella bedömningen är att regionstyrelsen **till viss del** har säkerställt detta.

Granskningens fokus har varit styrningen av cybersäkerhetsarbetet inom Region Dalarna. Tekniska aspekter har endast behandlats i mycket begränsad omfattning och enbart i den mån det har varit nödvändigt för att belysa hur regionstyrelsen styr, följer upp och skapar förutsättningar för arbetet med cybersäkerhet.

Granskningen visar att det finns viktiga initiativ, vissa tekniska lösningar och lokala strukturer, men att det saknas en helhetsstyrning, systematik och integrering i den ordinarie styrmodellen. Cybersäkerhetsarbetet bedrivs till stor del som separata aktiviteter utan samlad uppföljning eller analys, vilket medför att regionstyrelsen har begränsade förutsättningar att bedöma om arbetet ger tillräckligt skydd i förhållande till de risker som finns.

Det finns ett stort antal styrande dokument inom cybersäkerhetsområdet, men dokumentationen utgör i praktiken inte ett fungerande styrsystem. Flera respondenter beskriver svårigheter med att veta vilka dokument som gäller, var de finns och hur de hänger ihop. Det saknas vägledning och struktur för hur dokumenten ska tillämpas och följas upp.

Ansvarsfördelningen för cybersäkerhet är till viss del tydlig i styrande dokument, men upplevs i praktiken som otydlig. Flera respondenter beskriver osäkerhet kring mandat, roller och gränsdragningar, särskilt i skärningspunkten mellan IT, informationssäkerhet, dataskydd och verksamhet. ISSO-funktionen finns, men dess förutsättningar varierar. Organisationen för cybersäkerhetsarbetet är inte samordnad och saknar gemensam styrning, koordinering och uppföljning. Förutsättningarna att bedriva arbetet varierar, och det saknas samlat systemstöd för riskhantering, dokumentation och uppföljning. Kompetensförsörjningen är en utmaning, särskilt inom specialistområden.

Cybersäkerhetsarbetet omfattar till viss del människor, processer och tekniska lösningar, men inte på ett systematiskt och integrerat sätt. Informationsinsatser och utbildning är oregelbundna, och det saknas struktur för att sprida och följa upp stödmaterial. Incidenthantering sker inte enhetligt i organisationen.

Regionstyrelsen har uppmärksammat cybersäkerhetsfrågor i vissa beslut och budgetförslag, men stödet är inte samordnat eller systematiskt. Det saknas underlag och analyser som möjliggör strategisk styrning, och området saknas i den formella internkontrollplanen.

Riskanalyser och egenkontroller förekommer, men det saknas struktur för att följa upp eller återrapportera cybersäkerhetsrelaterade risker. Åtgärder genomförs inte alltid, och det saknas samordning i arbetet med riskhantering och återrapportering till politisk nivå.

Regionen har inte genomfört någon GAP-analys i förhållande till NIS2, och det saknas samlad planering för hur kommande krav ska uppfyllas. Cybersäkerhetsarbetet bedrivs i olika delar av organisationen utan samlad styrning, och det saknas dokumentation som visar efterlevnad.

Cybersäkerhetsfrågorna är inte integrerade i regionens övergripande styrning, planering eller intern kontroll. Arbetet bedrivs i separata spår, och resultaten från egenkontroller återförs inte systematiskt till regionstyrelsen.

Upphandlingar och avtal innehåller i vissa fall relevanta cybersäkerhetskrav, men arbetet är inte systematiserat. Det saknas stöd, struktur och uppföljning, särskilt i direktupphandlingar och mindre avrop. Varje verksamhet ansvarar själv för kravställning och uppföljning, vilket innebär en betydande risk.

Sammantaget visar granskningen att cybersäkerhetsfrågorna inte är en integrerad del av Region Dalarnas ordinarie styrning, planering eller uppföljning.

Mot bakgrund av granskningens resultat lämnas följande rekommendationer till regionstyrelsen:

1. **Integrera cybersäkerhetsfrågorna i regionens övergripande styrning, planering och uppföljning.**

   Regionstyrelsen bör säkerställa att cybersäkerhet betraktas som en ledningsfråga och integreras i verksamhetsplanering, internkontroll, målstyrning och riskhantering – inte hanteras i separata spår.

2. **Genomför en nulägesanalys i förhållande till NIS2 och ta fram en samlad åtgärdsplan för att säkerställa efterlevnad.**

   Detta bör inkludera roller, ansvar, uppföljningsmodeller och dokumentation som visar hur kraven i NIS2 uppfylls – inklusive styrning av leverantörsled, incidenthantering och utbildningsinsatser.

3. **Utveckla en strukturerad och sammanhållen modell för cybersäkerhetsrelaterad riskhantering.**

   Modellen bör möjliggöra att risker identifieras, dokumenteras, aggregeras och analyseras på regional nivå. Det bör också finnas tydliga strukturer för att ta fram, följa upp och återrapportera åtgärder kopplade till riskanalyser och handlingsplaner.

4. **Säkerställ att samtliga verksamheter och nivåer i organisationen har tillgång till kompetens, vägledning och stöd i cybersäkerhetsarbetet.**

   Detta innefattar systemstöd, rollbeskrivningar, utbildning till alla medarbetare samt metodstöd som gör det möjligt att arbeta systematiskt i vardagen.

5. **Stärk cybersäkerheten i leverantörsledet genom enhetliga krav, tydlig ansvarsfördelning och systematisk uppföljning.**

   Det bör finnas en modell för hur cybersäkerhetsrisker identifieras, hanteras och följs upp vid upphandlingar, avrop och andra leverantörsrelationer – oavsett omfattning och typ av tjänst.

6. **Säkerställ ledningens kompetens och beslutsstöd i cybersäkerhetsfrågor.**

   Regionstyrelsen och andra beslutsfattare behöver återkommande analysunderlag och riskbilder för att kunna styra området proaktivt. Det bör även finnas strukturer för kompetensutveckling kopplat till cybersäkerhet i styrande roller.

1. Inledning

1.1 Syfte och revisionsfrågor

Syftet med granskningen är att ge revisorerna underlag för att bedöma om regionstyrelsen säkerställt att regionens arbete med cybersäkerhet är ändamålsenligt.

Granskningen besvarar följande revisionsfrågor:

- Finns aktuella och ändamålsenliga dokument som styr cybersäkerhetsarbetet i regionen?
- Är ansvar och roller för arbetet med cybersäkerhet tydliga och kända?
- Är organisationen för arbetet med cybersäkerhet ändamålsenlig och finns nödvändiga resurser för arbetet (kompetensmässigt, ekonomiskt, systemstöd etc.)?
- Omfattar regionens cybersäkerhetsarbete i tillräcklig grad såväl människor (t.ex. anställdas säkerhetsmedvetande) som processer och tekniska lösningar?
- Har cybersäkerhetsarbetet ett tillräckligt och ändamålsenligt stöd från regionens ledning?
    - Beaktas t.ex. cybersäkerhetsaspekter i tillräcklig grad vid olika verksamheters önskemål om utvecklad digitalisering i regionen?
- Bedrivs ett systematiskt arbete med att identifiera (t.ex. via riskanalyser), hantera och åtgärda risker och behov för att säkerställa en ändamålsenlig cybersäkerhet?
    - Är berörd personal och politisk ledning medvetna om de eventuella brister som finns i cybersäkerhetsarbetet?
    - Genomförs t.ex. systematiska uppföljningar och kontroller av vidtagna åtgärder för att upptäcka eventuella brister?
- Håller cybersäkerhetsarbetet i regionen sådan standard att regionen kan förväntas leva upp till kraven i kommande lagstiftning?
    - Om inte, vad saknas för att göra detta?
- Har regionen säkerställt att cybersäkerhetsarbetet är integrerat i den övergripande styrningen och det interna kontrollsystemet på ett sätt som omfattar både organisatoriska, tekniska och verksamhetsmässiga perspektiv?
- Beaktas cybersäkerhet vid upphandlingar för att säkerställa att regionens informations- och IT-säkerhet inte hotas?

1.2 Metod

Granskningen har genomförts med hjälp av:

- Dokumentstudier av styrande dokument, handlingsplaner, riskanalyser, internkontrollplaner, strategier, utbildningsmaterial m.m.
- Semistrukturerade intervjuer med företrädare för regionstyrelsen, regiondirektören, IT-direktörer, informationssäkerhetschef, säkerhetschef, HR-direktör, informationssäkerhetssamordnare, upphandlingschef samt andra nyckelfunktioner inom regionens organisation. Totalt har 19 intervjuer genomförts.
- Stickprov av utvalda upphandlingar och gällande avtal med leverantörer.

Teknisk analys

Som en del av granskningen har en teknisk analys genomförts av Orange Cyberdefense, som granskat vissa delar av regionens cybersäkerhetsstruktur och gett kompletterande inspel till bedömningen. Resultatet återfinns i bilaga 3 och har vävts in i analysen där det varit relevant.

Bedömningsskala

För varje revisionsfråga görs en samlad revisionell bedömning. Bedömningen baseras på i vilken utsträckning de kriterier som ligger till grund för granskningen är uppfyllda. Skalan som använts är:

- Ja – Revisionskriterierna bedöms vara uppfyllda i allt väsentligt.
- Till stor del – Revisionskriterierna är i huvudsak uppfyllda, med vissa mindre avvikelser.
- Till viss del – Revisionskriterierna är endast delvis uppfyllda, och det finns flera brister.
- Nej – Revisionskriterierna är inte uppfyllda.

1.3 Avgränsningar

Granskningen fokuserar på regionstyrelsens ansvar för cybersäkerhetsarbetet och omfattar organisatoriska och styrningsrelaterade aspekter. Tekniska detaljer kring skyddsåtgärder, sårbarheter, nätverkslösningar och incidenthantering har endast översiktligt analyserats och inkluderas som en del av granskningens helhetsbedömning.

Granskningen omfattar främst nuläget under 2025, med tillbakablickar där det är relevant för att förstå utvecklingen över tid.

1.4 Revisionskriterier

Granskningen har utgått från följande revisionskriterier:

- Kommunallagen (2017:725)
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Regionstyrelsens reglemente
- Regionplan 2025–2027
- Andra styrande dokument och riktlinjer inom informations- och IT-säkerhetsområdet

Bedömningar som rör *kommande lagstiftning* avser i denna granskning i första hand NIS2-direktivet, som enligt SOU 2024:18 föreslås införas i svensk rätt genom en ny cybersäkerhetslag från 15 januari 2026. Granskningen har i dessa delar utgått från de förväntade krav som beskrivs i SOU 2024:18 *"Nya regler om cybersäkerhet"* samt i andra tillgängliga källor om föreslagna regeländringar.

1.5 Ansvarig nämnd

Ansvarig nämnd är regionstyrelsen.

1.6 Kvalitetssäkring

Kvalitetssäkring har skett genom Qualitariums interna kvalitetsprocesser. Ett utkast till rapport har varit föremål för faktagranskning av intervjupersonerna, i syfte att säkerställa att sakuppgifter är korrekt återgivna.

1.7 Förkortningar

Förkortning	Betydelse
MIT	Medicinsk teknik och IT (enhet under regionstyrelsens förvaltning)
ISSO	Information Security Support Officer (informationssäkerhetssamordnare på förvaltningsnivå)
IAM	Identity and Access Management (identitets- och behörighetshantering)
NIS2	EU:s nya cybersäkerhetsdirektiv (Network and Information Security Directive 2)
UoT	Uttalande om tillämplighet (Statement of Applicability enligt ISO 27001)
ISAK	Region Dalarnas mall för informationssäkerhetsbedömning
PUB-avtal	Personuppgiftsbiträdesavtal (enligt GDPR)
Synergi	Regionens IT-verktyg för rapportering av avvikelser, tillbud eller risk

2. Bakgrund

Region Dalarna bedriver en omfattande verksamhet och hanterar stora mängder känslig information. Hanteringen av denna information är i allt väsentligt digitaliserad, vilket ställer höga krav på säkerheten i system och processer. Samtidigt utvecklas både tekniken och hotbilden snabbt – något som har lett till att flera svenska kommuner och regioner drabbats av omfattande cyberincidenter med allvarliga konsekvenser.

Cybersäkerhet omfattar de processer, metoder och tekniska lösningar som syftar till att skydda viktiga system och nätverk från digitala angrepp. Ett effektivt cybersäkerhetsarbete innefattar både tekniska aspekter och organisatoriska åtgärder och behöver involvera hela organisationen – från ledning till medarbetare.

Regelverket kring cybersäkerhet är under utveckling. Under 2025 förväntas EU:s NIS2-direktiv införlivas i svensk rätt genom en ny cybersäkerhetslag som ersätter nuvarande lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Även det så kallade CER-direktivet väntas införlivas i svensk lagstiftning under året. Tillsammans innebär dessa nya regelverk skärpta krav på både informationssäkerhet och förmågan att hantera störningar inom samhällsviktiga verksamheter.

Regionens arbete med IT- och informationssäkerhet har tidigare granskats år 2011 och 2018. Vid den senaste granskningen konstaterades att säkerhetsarbetet generellt var välfungerande, men att utvecklingstakten var låg och stödet från ledningen bristfälligt.

Mot bakgrund av digitaliseringens omfattning, den förändrade hotbilden samt det ökade regeltrycket har revisorerna beslutat att följa upp cybersäkerhetsarbetet inom Region Dalarna under 2025.

3. Granskningens resultat

Utifrån det granskade materialet och de genomförda intervjuerna redovisas svaren på granskningens kontrollfrågor i detta kapitel. Avsnitten är uppdelade i en del som beskriver våra iakttagelser och en del som återger våra kommentarer och bedömningar. Svaren på kontrollfrågorna ligger till grund för våra bedömningar kopplade till granskningens huvudfråga och syfte samt till de rekommendationer som lämnas. I Region Dalarna används vanligtvis begreppen IT-säkerhet och informationssäkerhet. Begreppet cybersäkerhet används mer sällan och förekommer inte konsekvent i styrdokument, planer eller andra dokument. Detta bör beaktas vid tolkning av frågorna i denna granskning.

3.1 Finns aktuella och ändamålsenliga dokument som styr cybersäkerhetsarbetet i regionen?

Iakttagelser

Det finns ett stort antal dokument som styr cybersäkerhetsområdet i Region Dalarna. Dokumentationen omfattar flera nivåer och typer av styrning, däribland policyer, strategier, handlingsplaner, riktlinjer, rutiner och mallar. I bilaga 1 finns en sammanställning av samtliga styrande dokument som ingår i denna granskning.

Regionen har bland annat en informationssäkerhets- och dataskyddspolicy från 2022 och en övergripande säkerhetspolicy från 2025. Det finns också en digitaliseringsstrategi för 2024–2028 med tillhörande handlingsplan, där flera av aktiviteterna berör cybersäkerhetsområdet. Därtill finns dokument såsom Handlingsplan för informationssäkerhet och dataskydd 2025, riktlinjer för identitets- och åtkomsthantering, rutin för riskhantering, checklista för egenkontroll, samt utbildnings- och kommunikationsplaner. Regionen har också ett ledningssystem för informationssäkerhet och dataskydd, vilket i handlingsplanen beskrivs som ramverk för det systematiska arbetet.

Många av dokumenten har uppdaterats under perioden 2023–2025, men det förekommer även äldre handlingar. Flera dokument är försedda med giltighetsdatum, vilket innebär att det finns en grundläggande struktur för dokumenthantering och uppdatering. Dokumenten som ingår i denna granskning är i huvudsak framtagna centralt inom ramen för exempelvis IAM-programmet eller Medicinsk teknik och IT (MIT). Lokalt i verksamheterna finns framtagna riktlinjer, rutiner, anvisningar och mallar.

Granskningen visar att det finns en stor mängd dokument inom området. Flera intervjuade personer, särskilt på operativ nivå, uppger att det är svårt att överblicka vilka dokument som gäller, var de finns och hur de hänger ihop. Det är inte alltid tydligt vilket dokument som gäller i vilken situation, särskilt i de fall där innehållet överlappar mellan olika styrdokument. Under granskningen har det inte heller identifierats någon tydlig vägledning som visar hur dokumenten förhåller sig till varandra och vilka som gäller för vem.

I vissa av styrdokumenten, exempelvis handlingsplanen för 2025, finns hänvisning till skärpta krav och kommande lagstiftning, däribland EU:s NIS2-direktiv.

Bedömning

Vår sammanfattande bedömning är att det **till stor del** finns aktuella och ändamålsenliga dokument inom cybersäkerhetsområdet, men dessa dokument är inte fullt ut styrande och implementerade i arbetet med cybersäkerhet över hela organisationen.

Analys och motivering

Region Dalarna har ett stort antal styrande dokument som rör cybersäkerhetsområdet. Det finns policyer, riktlinjer, handlingsplaner, strategier och operativa stöddokument som täcker flera viktiga delar, såsom informationsklassning, riskhantering, incidentrapportering och åtkomstkontroll. Innehållet är i flera fall uppdaterat och delvis anpassat till kommande lagkrav, t.ex. genom hänvisningar till NIS2-direktivet. Dokumenten har i många fall angivna giltighetstider, vilket bidrar till en grundläggande struktur för uppdatering och översyn.

Granskningen visar samtidigt att dokumentationen i praktiken inte utgör ett fullt ut fungerande styrsystem. Flera intervjuade beskriver svårigheter med att veta vilka dokument som gäller i vilken situation, och var de finns. Det saknas en tydlig struktur för hur dokumenten hänger samman, samt vägledning för tillämpning på olika nivåer i organisationen.

Det framgår också att vissa dokument inte används konsekvent. Exempelvis uppger flera respondenter att centralt framtagna mallar och checklistor inte alltid är kända eller används i verksamheten. Det saknas en systematisk struktur för att följa upp dokumentens tillämpning eller analysera hur väl de efterlevs i praktiken. Detta innebär att dokumenten inte får fullt genomslag som styrning i organisationen.

Därutöver har det i granskningen identifierats ett antal äldre dokument som fortfarande är i bruk. Mot bakgrund av kraven i kommande lagstiftning och tillämpliga standarder, t.ex. ISO 27001, bör samtliga styrande dokument valideras årligen.

3.2 Är ansvar och roller för arbetet med cybersäkerhet tydliga och kända?

Denna fråga fokuserar på hur ansvar och roller för cybersäkerhetsarbetet är definierade, fördelade och kända i organisationen ur ett individ- och rollperspektiv. Det handlar om i vilken utsträckning berörda aktörer har ett tydligt uppdrag och mandat. Fråga 3.3 behandlar de organisatoriska och resursmässiga förutsättningarna för dessa roller.

Iakttagelser

Region Dalarna har definierat ett antal funktioner med roller kopplade till informations- och cybersäkerhet:

- Informationssäkerhetschef – placerad på koncernstaben, med ansvar för metodstöd och styrning av informationssäkerhetsarbetet.
- Informationssäkerhetssamordnare (ISSO:er) – utsedda personer på verksamhetsnivå som samordnar det för förvaltningen gemensamma informationssäkerhetsarbetet samt utformar förslag till verksamhetsspecifika rutiner och informationssäkerhetsplan.
- IT-direktörer och teknisk chef – på MIT-enheten, med ansvar för teknisk infrastruktur, säkerhetsarkitektur och systemdrift.
- Säkerhetschef – ansvarar för fysisk säkerhet, krisberedskap och säkerhetsskydd.
- IAM-programledare –fungerar som en länk mellan den operativa arbetsgruppen för IAM och det strategiska programrådet. Rollen beskrivs i intervjuerna som samordnande snarare än ansvarsbärande i sakfrågor kring identitet och åtkomst.
- Dataskyddsombud – ansvarar för dataskyddsfrågor enligt dataskyddsförordningen (GDPR).

- Förvaltningschefer – anges enligt styrdokument och intervjusvar som ansvariga för informations- och cybersäkerhet inom respektive förvaltning.

Rollbeskrivningar återfinns i styrdokument som säkerhetspolicyn, handlingsplaner och dokument kopplat till IAM-programmet. I ett verkställighetsbeslut anges exempelvis att IT-direktören har ett brett ansvar inom MIT-enheten, men att informationssäkerhetsansvaret ska utövas i samverkan med andra funktioner.

Enligt intervjuerna upplevs ansvarsfördelningen som otydlig i vissa delar. Det förekommer osäkerhet kring roller, mandat och gränsdragningar, särskilt i skärningspunkten mellan IT, informationssäkerhet, dataskydd, fysisk säkerhet och verksamhet. Flera personer uppger att funktioner inte alltid känner till varandras uppdrag.

ISSO:er beskrivs som ansvariga för operativ informationssäkerhet på verksamhetsnivå. Det finns dokumenterade uppdragsbeskrivningar där ISSO-rollen definieras som en stödjande funktion. Enligt intervjuer varierar förutsättningarna för att fullgöra uppdraget, bland annat gällande avsatt tid, tydlighet i uppdraget och gränsdragning mot andra funktioner.

Det formella ansvaret för informations- och cybersäkerhet ligger enligt styrdokument och intervjuer på förvaltningscheferna. I intervjuer beskrivs att cheferna inte alltid får särskild utbildning eller stöd kopplat till detta ansvar. Det anges att ISSO:er, IT-funktioner eller centrala aktörer ofta utgör stöd i säkerhetsfrågor i verksamheterna.

Inom regionen finns flera forum för cybersäkerhetsfrågor (vilka behandlas vidare i kommande avsnitt 3.3), såsom ISSO-nätverket, MIT:s ledningsgrupp samt interna styr- och arbetsgrupper kopplade till informationssäkerhetsfunktionen.

Bedömning

Vår sammanfattande bedömning är att ansvar och roller för cybersäkerhetsarbetet är **till viss del** tydliga och kända.

Analys och motivering

Region Dalarna har definierat ett antal funktioner med ansvar inom informations- och cybersäkerhet. Rollbeskrivningar förekommer i flera styrdokument, och det finns exempel på centrala funktioner med tydliga uppdrag, såsom informationssäkerhetschef, IT-direktör, dataskyddsombud och ISSO:er på verksamhetsnivå. Det finns även en uttalad fördelning där förvaltningschefer bär det övergripande ansvaret i respektive förvaltning, i enlighet med regionens styrmodell.

Trots denna formella struktur framkommer i granskningen att ansvarsfördelningen i praktiken inte alltid upplevs som tydlig. Flera respondenter beskriver osäkerhet kring mandat, roller och gränsdragningar, särskilt i skärningspunkten mellan IT, informationssäkerhet, dataskydd, fysisk säkerhet, upphandling och verksamhet. Det förekommer exempel på att olika funktioner inte känner till varandras uppdrag, vilket försvårar samordning.

ISSO-funktionen finns i hela regionen, men uppdragets omfattning, förutsättningar och mandat varierar.

Det har också framkommit att vissa förvaltningschefer saknar särskilt stöd eller utbildning för att utöva sitt formella ansvar inom cybersäkerhet, vilket medför att mycket av arbetet förväntas ske genom stödfunktioner. Detta kan leda till en otydlig ansvarsfördelning, särskilt i de delar av organisationen där varken ISSO-roll eller andra stödfunktioner har tillräcklig kapacitet.

Det finns flera interna forum och nätverk där cybersäkerhetsfrågor hanteras, bland annat inom MIT och genom ISSO-nätverket.

3.3 Är organisationen för arbetet med cybersäkerhet ändamålsenlig och finns nödvändiga resurser för arbetet (kompetensmässigt, ekonomiskt, systemstöd etc.)?

Denna fråga fokuserar på vilka organisatoriska och resursmässiga förutsättningar som finns för att bedriva ett systematiskt cybersäkerhetsarbete. Det rör såväl personal, kompetens och ekonomi som systemstöd, verktyg och samverkansformer. Frågan har nära koppling till föregående fråga som behandlar ansvar och roller.

Iakttagelser

Regionen har flera organisatoriska funktioner som arbetar med cybersäkerhet på olika nivåer:

- **MIT-enheten** ansvarar för teknisk infrastruktur, IT-säkerhet, SOC och säkerhetsarkitektur. Cybersäkerhet hanteras i flera avdelningar inom enheten och ingår i verksamhetsplaneringen.
- **Koncernstaben** ansvarar bland annat för framtagande av styrdokument och metodstöd för dataskydd och informationssäkerhet.
- Ett **programråd** bestående av regionens direktörer ger uppdrag och beslutar gällande IAM.
- **Verksamhetsnära funktioner**, exempelvis ISSO:er, arbetar med säkerhetsfrågor i respektive förvaltnings kontext

Enligt intervjuerna finns det inte någon samlad struktur för samordning av cybersäkerhetsarbetet idag. Arbetet beskrivs bedrivas inom olika delar av organisationen, och det uppges i flera fall vara oklart var det övergripande ansvaret ligger. En ny ledningsgrupp under regiondirektören som bland annat kommer att hantera cybersäkerhetsfrågor har inrättats. Gruppen hade vid granskningstillfället ännu inte sammanträtt.

Ekonomiska resurser för cybersäkerhetsarbete hanteras främst inom ordinarie ramar hos respektive förvaltning. Det finns inte någon samlad översikt på regionnivå över hur mycket resurser som avsätts för cybersäkerhet. I regionstyrelsens budgetförslag för 2026 föreslås att 10 miljoner kronor avsätts för att förstärka cybersäkerhetsarbetet. Enligt flera intervjuer är syftet att möta ökade krav kopplat till bland annat tekniska lösningar, överblick och systemförvaltning. Det har även nämnts att en del av medlen kommer att användas för att hantera teknisk skuld, exempelvis genom utbyte eller uppgradering av äldre IT-system.

Resurstillgången inom vissa centrala funktioner, såsom informationssäkerhetschef och dataskyddsombud, beskrivs i intervjuerna som begränsad i förhållande till uppdragets omfattning. Även MIT-enheten lyfter att uppdragen inom säkerhet och digitalisering har vuxit. ISSO-funktionen är organiserad på liknande sätt i hela regionen, men enligt intervjuerna varierar de faktiska förutsättningarna att fullgöra uppdraget. Det beskrivs exempelvis att vissa ISSO:er har ett tydligt uppdrag med avsatt tid och mandat, medan andra utför uppgiften som ett tilläggsansvar.

Regionen använder flera systemstöd för att hantera cybersäkerhetsrelaterade frågor. ISAK-verktyget används för informationsklassning och riskanalyser. Det finns dock inte något digitalt systemstöd för att dokumentera och följa upp identifierade risker och åtgärder på en samlad nivå. Systemet Synergi används i vissa delar av organisationen för avvikelsehantering, men används inte konsekvent för cybersäkerhetsrelaterade incidenter.

Enligt intervjuerna efterfrågas digitala verktyg inom flera delar av cybersäkerhetsområdet, såsom behörighetsstyrning, logghantering, stöd för säkerhetskrav vid upphandlingar samt dokumentation kopplad till efterlevnad av NIS-regelverket.

Kompetensförsörjning lyfts i intervjuerna som en utmaning, särskilt inom specialiserade områden som NIS, SOC, IAM och säkerhetsarkitektur. Det beskrivs som svårt att rekrytera och behålla personal inom dessa områden. Det uppges även finnas behov av ökad kunskap om cybersäkerhet i verksamheterna, särskilt vid upphandlingar och i samband med förändringsarbete.

Bedömning

Vår sammantagna revisionella bedömning är att organisationen för arbetet med cybersäkerhet **till viss del** är ändamålsenlig och att det till viss del finns nödvändiga resurser för arbetet (kompetensmässigt, ekonomiskt, systemstöd etc.).

Analys och motivering

Regionen har inrättat flera organisatoriska funktioner med ansvar inom cybersäkerhetsområdet, både på strategisk och operativ nivå. Det finns också definierade roller inom IT, informationssäkerhet, dataskydd och fysisk säkerhet. Dessa funktioner är nödvändiga för att hantera cybersäkerhetsfrågor, men i praktiken är ansvarsfördelningen inte fullt ut tydlig eller samordnad.

Cybersäkerhetsarbetet bedrivs i dag inom flera organisatoriska enheter utan en sammanhållen modell för styrning, koordinering och uppföljning. Det förekommer överlapp och otydligheter i gränsdragningar mellan funktioner, vilket påverkar förutsättningarna för ett effektivt arbete. Det finns initiativ för att stärka samordningen, men dessa har ännu inte hunnit få genomslag.

Förutsättningarna att utföra cybersäkerhetsuppdraget varierar mellan olika delar av organisationen. Vissa funktioner har avsatt tid och mandat, medan andra hanterar uppdraget som ett tilläggsansvar vid sidan av övriga arbetsuppgifter. Detta gäller bland annat ISSO:erna, vars roll i praktiken skiljer sig åt mellan olika förvaltningar. För att stärka cybersäkerhetsarbetet i verksamheterna behövs både ökad kompetens och operativ kapacitet. I dagsläget saknar flera ISSO:er tillräckligt med tid och förutsättningar att arbeta operativt, vilket begränsar deras möjligheter att stödja verksamheterna i det dagliga säkerhetsarbetet. Vi bedömer att det finns behov för ökad tillgång till utbildning för chefer, nyckelpersoner och ISSO:er för att höja den operativa förmågan.

Kompetensförsörjningen är en utmaning för regionen. Det gäller särskilt inom specialistområden som identitetshantering, behörighetshantering, incidenthantering och säkerhetsarkitektur. Det finns också ett behov av ökad kunskap i verksamheterna, vilket är särskilt relevant i samband med upphandlingar, systemförändringar och implementering av nya säkerhetskrav. Vi bedömer att det behövs utbildningsinsatser till medarbetare i hela organisationen på ett mer systematiskt sätt än vad som erbjuds idag.

Vad gäller systemstöd bedöms befintliga verktyg inte ge tillräckligt stöd för ett samlat, effektivt och uppföljningsbart cybersäkerhetsarbete. Det saknas gemensamma digitala lösningar för riskuppföljning, dokumentation av åtgärder och incidenthantering. Existerande verktyg som ISAK och Synergi används i viss utsträckning, men inte konsekvent eller i samordning. Respondenterna efterfrågar stöd för bland annat logghantering, åtkomstkontroll och dokumentation av efterlevnad kopplad till NIS-krav. Vi bedömer att ett gemensamt systemstöd för riskhantering, uppföljning och aggregering saknas, och att detta bör prioriteras. Ett sådant stöd skulle möjliggöra att risker hanteras på flera nivåer och följas upp på ett enhetligt sätt.

Ekonomiska resurser hanteras i huvudsak inom förvaltningarnas ordinarie budgetramar. Det finns ingen sammanställd bild av hur mycket som totalt avsätts till cybersäkerhetsområdet. Regionstyrelsen föreslår dock att 10 miljoner kronor avsätts för cybersäkerhetsarbete i budgeten för 2026, vilket indikerar en ökad politisk prioritering av området. Det återstår dock att säkerställa att dessa medel används på ett sätt som möter behoven inom teknik, kompetens och styrning.

3.4 Omfattar regionens cybersäkerhetsarbete i tillräcklig grad såväl människor (t.ex. anställdas säkerhetsmedvetande) som processer och tekniska lösningar?

Denna fråga fokuserar på hur cybersäkerhetsarbetet omsätts i praktiken och hur väl det omfattar både tekniska system, organisatoriska processer och människors kunskap och beteenden. I tidigare frågor har förutsättningarna för arbetet beskrivits. Här belyses hur dessa faktorer samverkar i det operativa säkerhetsarbetet.

Iakttagelser

Informationssäkerhetsfrågor kommuniceras i viss utsträckning till medarbetare via intranät, APT:er och interna nätverk. ISSO:er uppger att de informerar om säkerhetsfrågor vid t.ex. personalmöten, och informationssäkerhetschefen nämns som en aktiv kommunikatör internt. Regionen deltar i den nationella säkerhetsveckan, då informationsinsatser riktade till medarbetare genomförs under en begränsad period.

Det finns informationsmaterial tillgängligt på intranätet, men flera intervjuade uppger att det kan vara svårt att hitta och veta vad som gäller. Det förekommer introduktionsmoment kopplade till informationssäkerhet för nyanställda, men det varierar mellan verksamheter och nivåer hur omfattande dessa moment är.

Regionen har tagit fram ett antal centrala dokument som ska stödja informationssäkerhetsarbetet i praktiken, t.ex. mallar för informationsklassning och ISAK-analyser, checklistor för egenkontroll samt riktlinjer för riskhantering och incidentrapportering. Under granskningen har inte identifierats någon tydlig struktur för hur dokumenten sprids, tillämpas eller följs upp. Respondenter beskriver att det varierar mellan verksamheter hur dokumenten används, vilket försvårar enhetlighet och kvalitetssäkring i det operativa arbetet.

Frågor kopplade till tekniska verktyg, systemstöd och digitala lösningar behandlas under fråga 3.3. Där beskrivs att det finns vissa verktyg för t.ex. IAM och informationsklassning, men att flera respondenter efterfrågar ytterligare systemstöd, bland annat för incidenthantering, uppföljning och övervakning.

När det gäller processer för kravställning i upphandlingar hänvisar vi till fråga 3.9 som visar att det saknas enhetliga arbetssätt för att beakta cybersäkerhet i leverantörsrelationer. Granskningen visar också att det inte alltid genomförs strukturerad informationsklassning inför upphandling eller avrop, även i fall där känsliga personuppgifter hanteras.

Bedömning

Vår sammantagna revisionella bedömning är att arbetet med cybersäkerhet **till viss del** omfattar människor, processer och tekniska lösningar.

Analys och motivering

Granskningen visar att regionen har vidtagit åtgärder för att höja anställdas medvetenhet om informationssäkerhet, bland annat genom riktad kommunikation, deltagande i säkerhetsveckan och vissa utbildningsmoment. Det finns även framtagna dokument, rutiner och mallar som syftar till att stödja ett systematiskt arbete. Dessa initiativ bidrar till att området omfattar flera dimensioner av cybersäkerhet.

Samtidigt visar granskningar att det finns ett antal begränsningar. Informationsinsatserna beskrivs som oregelbundna och svåra att hitta. Det finns skillnader mellan verksamheterna i hur introduktion, rutiner

och stödmaterial används, vilket påverkar förutsättningarna för ett enhetligt arbetssätt. Det saknas struktur för hur dokument och instruktioner sprids och följs upp. Det saknas även samlad uppföljning av om anställda har tagit del av informationssäkerhetsutbildning eller genomfört egenkontroller.

När det gäller processer är det särskilt relevant att notera att cybersäkerhet inte integreras på ett systematiskt sätt i upphandlingar, avtal och leverantörsrelationer, vilket framgår av iakttagelserna under fråga 3.9. Trots att vissa krav förekommer är det inte alltid tydligt hur risker ska hanteras eller hur säkerhetsklassning ska genomföras. Detta påverkar helheten i cybersäkerhetsarbetet.

Vad gäller tekniska lösningar finns grundläggande verktyg på plats, inklusive stöd för loggning och säkerhetsövervakning. Samtidigt efterfrågar flera intervjuade utökade funktioner och förbättrad systematik, särskilt kopplat till incidenthantering, uppföljning och överblick. Det saknas i dagsläget ett samlat tekniskt systemstöd som ger en heltäckande bild av cybersäkerhetsrelaterade aktiviteter.

Sammantaget innebär detta att cybersäkerhetsarbetet visserligen omfattar såväl människor, processer som tekniska lösningar, men att arbetet inte är fullt ut integrerat eller systematiskt på alla nivåer. Den genomförda tekniska analysen (bilaga 3) bekräftar också att arbetet med incidenthantering inte är enhetligt. Det framkommer att det finns olika arbetssätt för att rapportera incidenter och i vissa fall sker rapportering endast till närmaste chef, utan skriftlig dokumentation. Detta innebär att det finns en betydande risk att identifierade säkerhetsrisker inte hanteras systematiskt eller når upp till ledningen, vilket ytterligare försvårar ett sammanhållet och effektivt cybersäkerhetsarbete.

3.5 Har cybersäkerhetsarbetet ett tillräckligt och ändamålsenligt stöd från regionens ledning?

- Beaktas t.ex. cybersäkerhetsaspekter i tillräcklig grad vid olika verksamheters önskemål om utvecklad digitalisering i regionen?

Denna fråga belyser hur cybersäkerhetsarbetet prioriteras och hanteras på högsta strategiska nivå i regionen. Det handlar om i vilken utsträckning regionens ledning initierar, följer upp och stödjer arbetet, samt hur säkerhetsaspekter integreras i övergripande styrning och i beslut om digital utveckling. Frågan har kopplingar till tidigare frågor om organisation och samordning (se särskilt fråga 3), men fokuserar här på ledningsnivåns engagemang och styrning.

Iakttagelser

En genomgång av regionstyrelsens protokoll visar att styrelsen hanterat flera ärenden med koppling till informations- och cybersäkerhet, inklusive strategiska satsningar och rapportering av säkerhetsrelaterade händelser. I förslaget till regionstyrelsens budget för 2026 ingår en post om 10 miljoner kronor avsatt för att stärka cybersäkerhetsarbetet.

Det framkommer i intervjuerna att cybersäkerhetsområdet har fått ökad uppmärksamhet på strategisk nivå. Samtidigt beskrivs det som komplext och svåröverblickbart, vilket kan göra det utmanande att bedöma hur arbetet bör följas upp och prioriteras. Några respondenter uttrycker att bristen på samlad analys och rapportering kan försvåra styrning och uppföljning.

Regionstyrelsens internkontrollplan för 2025 innehåller ett kontrollområde kopplat till robusthet och RSA (risk- och sårbarhetsanalyser). Det finns däremot inte något uppdrag i planen som explicit rör cybersäkerhet eller informationssäkerhet. I 2024 års internkontrollplan fanns ett sådant uppdrag, men det togs bort inför 2025. Enligt intervju med representanter för regionstyrelsen berodde detta på att området inte visade på några avvikelser, medan andra områden prioriterades.

Det har inte framkommit någon enhetlig beskrivning av hur cybersäkerhetsaspekter vägs in i digitaliseringsarbetet. Regionens digitaliseringsstrategi och tillhörande handlingsplan innehåller vissa formuleringar som rör cybersäkerhet, exempelvis kopplat till ansvarsfördelning, informationsklassning och säker utveckling. Det finns även en digitaliseringsberedning under regionstyrelsen, med uppdrag att hantera strategiska digitaliseringsfrågor. Flera personer med ansvar för informations- och cybersäkerhet nämner dock inte dessa dokument eller beredningen spontant i intervjuerna, och beskriver i stället att arbetet sker i olika strukturer.

Bedömning

Vår sammantagna revisionella bedömning är att cybersäkerhetsarbetet **till viss del** har ett tillräckligt och ändamålsenligt stöd från regionens ledning.

Analys och motivering

Vi bedömer att cybersäkerhetsaspekter inte beaktas på ett systematiskt sätt vid olika verksamheters önskemål om digitalisering. Även om det finns strategiska dokument och vissa beredningar på plats, är inte arbetet tillräckligt integrerat i styrningen av digitala utvecklingsinsatser. Därför bedömer vi att detta endast till viss del är uppfyllt.

Granskningen visar att regionstyrelsen har hanterat ett antal ärenden med koppling till cybersäkerhet, och att området har uppmärksammats i budgetförslag och vissa protokoll. Det finns också exempel på att strategiska dokument, som digitaliseringsstrategin och tillhörande handlingsplan, innehåller hänvisningar till säkerhetsfrågor såsom ansvarsfördelning och informationsklassning. Detta tyder på att frågorna finns på agendan och att ledningen i viss utsträckning stödjer cybersäkerhetsarbetet.

Samtidigt framkommer att detta stöd inte är samordnat eller systematiskt. Cybersäkerhetsområdet uppfattas som komplext och svårt att överblicka, och det saknas samlade analyser, riskbilder eller rapporter som ger underlag för strategiska beslut. Detta minskar regionstyrelsens möjlighet att bedriva ett proaktivt och prioriterat arbete inom området.

Att det i internkontrollplanen för 2025 inte ingår något uppdrag kopplat till cybersäkerhet innebär också att området inte följs upp eller kontrolleras inom ramen för den ordinarie styrningen, vilket försvagar möjligheten till kontinuerlig ledningsstyrning. Även om robusthetsfrågor finns med i planen, hanteras inte cybersäkerhet som en integrerad del av regionstyrelsens kontrollfunktioner.

Det saknas också en tydlig koppling mellan cybersäkerhet och digitaliseringsstyrning. Flera personer med ansvar för informations- och cybersäkerhet känner inte till digitaliseringsstrategin eller digitaliseringsberedningens arbete, vilket tyder på bristande kännedom och koppling mellan centrala funktioner. Utan en strukturerad samordning riskerar säkerhetsaspekter att hanteras ad hoc eller lämnas utanför i samband med utvecklingsinitiativ.

Bristerna i koppling mellan cybersäkerhet och den övergripande styrningen bekräftas även i den tekniska analysen (bilaga 3), som visar att säkerhetsrelaterade initiativ ofta drivs parallellt med ordinarie styrningsprocesser. Det saknas strukturer för att säkerställa att säkerhetsfrågor beaktas systematiskt vid digitalisering, upphandling, planering och ledningsbeslut. Liknande analys framkommer även nedan i fråga 3.8, där tydliggörs att cybersäkerhet inte utgör en integrerad del av verksamhetsutvecklingen eller den interna kontrollen.

3.6 Bedrivs ett systematiskt arbete med att identifiera, hantera och åtgärda risker och behov för att säkerställa en ändamålsenlig cybersäkerhet?

- Är berörd personal och politisk ledning medvetna om de eventuella brister som finns i cybersäkerhetsarbetet?
- Genomförs t.ex. systematiska uppföljningar och kontroller av vidtagna åtgärder för att upptäcka eventuella brister?

Denna fråga fokuserar på hur regionen arbetar med att systematiskt identifiera, hantera och följa upp cybersäkerhetsrelaterade risker. Den omfattar både det löpande arbetet med riskanalyser och upprättande av åtgärder, samt vilken struktur som finns för uppföljning och återrapportering. Frågan berör även i vilken utsträckning berörd personal och politisk ledning har kännedom om eventuella brister i cybersäkerhetsarbetet.

Iakttagelser

Regionen arbetar med riskanalyser genom verktyget ISAK, som enligt riktlinjerna ska användas vid förändringar som påverkar informationshantering, t.ex. införande av nya system eller ändrade arbetssätt. Det finns instruktioner för användningen av ISAK, men enligt flera intervjupersoner är det otydligt i vilka situationer det ska tillämpas.

I praktiken varierar tillämpningen av ISAK mellan olika verksamheter. Enligt intervju med medarbetare inom upphandling finns varken fastlagda rutiner för hur urval av cybersäkerhetskrav ska göras, eller för vilket förarbete som ska föregå urvalet. Samtidigt pågår ett utvecklingsarbete för att skapa tydligare stöd i dessa delar.

Riskanalyser som genomförs kan leda till framtagande av lokala handlingsplaner. Flera respondenter uppger dock att det förekommer att åtgärder inte genomförs fullt ut, till exempel på grund av resursbrist eller otydlig ansvarsfördelning. Risker som identifieras förs ibland vidare till kommande års planering. Det har inte identifierats någon gemensam struktur för hur dessa åtgärder dokumenteras, följs upp eller återrapporteras på regional nivå.

Det saknas ett system för att samla in, följa upp och analysera risker och åtgärder på övergripande nivå. Riskbedömningar görs lokalt i verksamheterna, men aggregeras inte till en gemensam regional lägesbild. Enligt flera intervjuer har detta tidigare inneburit att endast ett begränsat antal risker nått ledningen. Under 2025 har förändringar genomförts för att förbättra återrapporteringen, men det finns fortfarande inte någon etablerad modell för samlad analys.

Verksamheterna genomför årliga egenkontroller inom informationssäkerhet, baserat på centralt framtagen mall. Flera personer beskriver att dessa uppfattas som en formalitet och att resultaten sällan återförs till central nivå för analys eller vidare åtgärder.

Det finns strukturer för återkoppling av risker till politisk nivå, exempelvis genom internkontrollplaner och verksamhetsrapporter. Det har dock inte framkommit att cybersäkerhetsrelaterade risker regelbundet ingår i dessa återrapporteringar, eller att det finns en samlad bild av cybersäkerhetsläget i regionstyrelsens riskhantering.

Bedömning

Vår sammantagna revisionella bedömning är att Region Dalarna **till viss del** bedriver ett systematiskt arbete med att identifiera, hantera och åtgärda risker och behov kopplat till cybersäkerhet.

Analys och motivering

Vi bedömer vidare att berörd personal till viss del är medveten om de brister som finns i cybersäkerhetsarbetet, men att denna kännedom inte systematiskt återförs till politisk ledning. Bristande struktur för återrapportering, i kombination med begränsade och oregelbundna utbildningsinsatser, innebär en risk för att ledning och nyckelpersoner saknar tillräcklig överblick över aktuella brister.

Vi bedömer också att systematiska uppföljningar och kontroller av vidtagna åtgärder inte genomförs. Egenkontroller och riskanalyser förekommer, men används inte konsekvent som underlag för styrning, prioritering eller lärande på övergripande nivå.

Regionen har vissa strukturer för att identifiera och hantera cybersäkerhetsrisker, men arbetet saknar samordning och enhetlighet. Det finns ingen övergripande struktur för att följa upp eller återrapportera risker på regionnivå, vilket försvårar lärande och prioritering.

Riskanalyser och egenkontroller genomförs, men används inte systematiskt som styr- eller uppföljningsunderlag. Det förekommer att åtgärder skjuts upp eller inte genomförs fullt ut, ibland utan dokumenterade skäl. Arbetet präglas av otydlighet och bristande samordning. Det finns ingen gemensam struktur för att aggregera, följa upp eller återrapportera cybersäkerhetsrelaterade risker. Riskanalyser och egenkontroller används inte systematiskt som underlag för styrning eller förbättringsarbete.

Cybersäkerhetsrisker rapporteras i vissa fall vidare till nästa års planering utan dokumentation av skäl, och det finns exempel på att åtgärder inte genomförs fullt ut. Detta minskar möjligheten till lärande och prioritering utifrån en samlad riskbild.

Det är också oklart i vilka situationer riskanalyser ska genomföras, till exempel vid upphandlingar, och det råder olika tolkningar inom organisationen. Det saknas beslutsstöd och vägledning för när och hur dessa analyser ska göras, vilket påverkar kvaliteten i kravställning och säkerhetsåtgärder.

Avsaknaden av samordning och systematik försvårar en strategisk hantering av cybersäkerhetsrisker och innebär att risker hanteras reaktivt snarare än proaktivt.

Även den tekniska analysen (bilaga 3) pekar på brister i regionens systematiska cybersäkerhetsarbete. Bland annat lyfts avsaknad av gemensamt systemstöd för riskhantering, begränsad spårbarhet i dokumentation och behov av förbättrad uppföljning. Analysen bekräftar att det saknas struktur för att aggregera och följa upp identifierade risker på regionnivå, samt att mognadsnivån inom flera områden behöver stärkas.

Det finns etablerade standarder och lösningar för att hantera risker inom informationssäkerhet, till exempel ISO 27005 och olika kommersiella systemstöd. Den genomförda tekniska analysen betonar också vikten av att genomföra riskanalyser vid alla typer av beslut, inte enbart vid införande av nya system. Detta understryker behovet av en mer systematisk och konsekvent tillämpning av riskanalysverktyg som ISAK i regionens arbete, samt behovet av att införa ett samlat stöd för riskhantering som kan användas på alla nivåer i organisationen och möjliggör uppföljning, aggregering och lärande.

Granskningen visar även att medvetenheten om brister i cybersäkerhetsarbetet varierar inom organisationen. Flera respondenter på operativ nivå uttrycker kännedom om utmaningar kopplat till resurser, ansvarsfördelning och brist på systemstöd, medan denna bild inte i samma utsträckning verkar nå den politiska ledningen. Risker lyfts i vissa fall till kommande planering, men det finns inte något strukturerat arbetssätt för att återföra brister till ledningsnivå på ett samlat sätt.

Vidare framkommer att det saknas en etablerad modell för att systematiskt följa upp och kontrollera att vidtagna åtgärder genomförs och får önskad effekt. Egenkontroller genomförs, men resultaten återförs

inte konsekvent till central nivå och används inte för gemensam analys. Detta innebär att brister riskerar att kvarstå över tid utan att åtgärdas fullt ut eller följas upp på ett lärande och systematiskt sätt.

3.7 Håller cybersäkerhetsarbetet i regionen sådan standard att regionen kan förväntas leva upp till kraven i kommande lagstiftning?

- Om inte, vad saknas för att göra detta?

Denna fråga fokuserar på i vilken utsträckning Region Dalarnas cybersäkerhetsarbete är anpassat för att möta kraven i kommande lagstiftning, framför allt EU:s nya NIS2-direktiv, som ska implementeras i svensk rätt genom en ny cybersäkerhetslag. Kraven i den nya lagstiftningen är mer långtgående än tidigare och omfattar bland annat:

- Tydlig ansvarsfördelning och ledningsengagemang i cybersäkerhetsarbetet.
- Systematiskt arbete med riskhantering, incidentrapportering och kontinuitetsplanering.
- Återkommande uppföljning och kontroll av skyddsåtgärder.
- Dokumentation av säkerhetsarbetet och möjlighet att visa efterlevnad.
- Säkerhetsåtgärder som omfattar både teknik, processer och människor.
- Kompetenskrav för berörda roller samt krav på utbildning och medvetandegörande.

Iakttagelser

Det har inte genomförts någon samlad analys (t.ex. gap-analys) för att bedöma hur väl organisationen i dagsläget uppfyller kraven i den kommande lagstiftningen. I flera intervjuer uppges att regionen ännu inte bedöms leva upp till samtliga krav, men många nämner pågående utvecklingsarbeten. Det finns ett antal initiativ och funktioner inom regionen som berör områden som regleras i NIS2, exempelvis:

- MIT:s arbete med tekniska säkerhetslösningar, och säkerhetsövervakning.
- ISSO-funktioner som arbetar med informationsklassning och riskanalyser.
- Centralt framtagna riktlinjer och mallar för riskanalyser, incidentrapportering och egenkontroller.
- IAM-programråd
- En nyinrättad ledningsgrupp som kommer bl.a. att hantera cybersäkerhetsfrågor.

Det finns även ett dokument kallat “Uttalande om tillämplighet” (UoT), som beskriver vilka säkerhetsåtgärder regionen anser relevanta. Dokumentet saknar dock datum.

Riskanalyser genomförs i samband med förändringar som påverkar informationshantering, t.ex. vid införande av nya system. Arbetet sker i huvudsak inom förvaltningarna, och resultaten dokumenteras lokalt. Det finns inga samlade systemstöd eller rutiner för att följa upp eller aggregera riskanalyser på regional nivå.

Cybersäkerhetsrelaterade incidenter hanteras i första hand lokalt, och det förekommer olika arbetssätt för rapportering. Systemstödet Synergi används inom vissa delar av organisationen, men det används inte konsekvent för incidenter kopplade till informationssäkerhet.

Flera personer uppger i intervjuer att ansvars- och rollfördelning inom cybersäkerhetsområdet inte alltid är tydlig, särskilt i gränsytor mellan funktioner. Det förekommer olika tolkningar av hur cybersäkerhets-frågorna ska kopplas till digitaliseringsarbetet, och flera respondenter beskriver att frågorna hanteras inom separata strukturer.

Det har i granskningen inte identifierats någon samlad översikt över hur arbetet med att uppfylla kommande krav enligt NIS2 bedrivs inom regionen.

Bedömning

Vår sammantagna revisionella bedömning är att Region Dalarnas cybersäkerhetsarbete **inte** håller sådan standard att regionen kan förväntas leva upp till kraven i kommande lagstiftning.

För att regionen ska kunna leva upp till kraven i kommande lagstiftning behöver bland annat följande utvecklingsområden adresseras:

- En samlad gap-analys och övergripande plan för efterlevnad
- Systematik i säkerhetsarbetet med e6 riskbaserat arbetssä6 utifrån allriskperspektivet
- Tydlig ansvarsfördelning och styrstruktur
- Systematik i incident- och kontinuitetshantering
- Systematik i behörighets- och ändringshantering
- Höjning av kunskapsnivån gällande cybersäkerhet hos alla medarbetare
- Systematik i hantering av leverantskedjor

Analys och motivering

Regionen har inlett flera initiativ som ligger i linje med de krav som ställs i NIS2-direktivet. Det handlar bland annat om tekniska lösningar som IAM och säkerhetsövervakning, riktlinjer för incidenthantering, mallar för riskanalyser, och rollbeskrivningar för ISSO:er. En ny ledningsgrupp som bland annat kommer att hantera cybersäkerhet har också bildats på ledningsnivå.

Trots detta saknas en samlad plan för hur regionen ska möta kraven i den kommande lagstiftningen. Någon GAP-analys har inte genomförts, och det finns inget övergripande program som kopplar samman de olika delarna av arbetet. Krav på ansvarsfördelning, uppföljning, dokumentation och ledningsengagemang hanteras i olika delar av organisationen, men utan en gemensam struktur.

Det finns inte heller någon dokumentation som visar hur efterlevnaden ska bedömas eller följas upp. Incidenter hanteras på olika sätt i olika delar av organisationen, och gränsdragningar mellan funktioner upplevs som oklara. Flera respondenter beskriver dessutom att kopplingen mellan cybersäkerhet och digitalisering är svag, med arbete som bedrivs i separata spår.

Avsaknaden av en samlad bild av cybersäkerhetsläget innebär att regionen inte har tillräckligt beslutsunderlag för att bedöma vilka brister som finns eller vilka åtgärder som bör prioriteras. Arbetet bedrivs i praktiken fragmentariskt, med varierande ambition och struktur. Det finns därmed en påtaglig risk att regionen inte kan möta kraven på ansvar, rapportering och tillsyn när den nya lagstiftningen träder i kraft.

Även den tekniska analysen (bilaga 3) pekar på att regionens mognadsnivå är låg i förhållande till NIS2-kraven. Analysen visar bland annat att det saknas tydliga spår av en enhetlig struktur för styrning, att incidenthantering inte är konsekvent implementerad, och att dokumentationen inte håller tillräcklig nivå för att visa efterlevnad. Brister identifieras i förutsättningarna att följa upp åtgärder, säkerställa kompetens och få överblick över cybersäkerhetsläget. Sammantaget bekräftar analysen att regionen har långt kvar till att fullt ut möta kraven i den kommande lagstiftningen.

Vad saknas för att möta kraven?

För att Region Dalarna ska kunna leva upp till kraven i den kommande lagstiftningen saknas flera grundläggande komponenter. Det behövs en samlad strategi och plan för hur NIS2-kraven ska uppfyllas, inklusive en gap-analys som visar vilka brister som finns. Regionens styrning, uppföljning och

incidenthantering behöver samordnas och dokumenteras, så att ansvarsfördelning, åtgärder och efterlevnad blir tydliga. Det saknas också strukturer för att följa upp och rapportera cybersäkerhetsarbete till ledningsnivå. Slutligen behövs förstärkt kompetens och utbildningsinsatser samt ett ökat ledningsengagemang för att driva det systematiska arbetet framåt.

Utöver detta bedömer vi att cybersäkerhetsarbetet behöver baseras på ett helhetsperspektiv på risk, där både kända och okända hot, sårbarheter och konsekvenser beaktas. Det innebär att regionen inte enbart bör arbeta med enstaka riskbedömningar kopplade till specifika projekt eller system, utan även genomföra en samlad och kontinuerlig riskanalys för hela organisationen utifrån ett allriskperspektiv. Ett sådant angreppssätt kräver struktur och stöd för att identifiera, värdera, dokumentera och hantera olika typer av cybersäkerhetsrelaterade risker, inklusive beroenden mellan system, leverantörer, dataflöden och processer. I dag saknas verktyg och rutiner för detta, vilket försvårar möjligheten att agera proaktivt och prioritera rätt åtgärder. Att etablera ett systematiskt riskhanteringsramverk är därmed en nödvändig komponent för att kunna uppfylla NIS2-kraven och skapa motståndskraft mot framtida cyberhot.

3.8 Har regionen säkerställt att cybersäkerhetsarbetet är integrerat i den övergripande styrningen och det interna kontrollsystemet på ett sätt som omfattar både organisatoriska, tekniska och verksamhetsmässiga perspektiv?

Frågan belyser hur cybersäkerhetsarbetet är integrerat i Region Dalarnas övergripande styrmodell, inklusive planering, uppföljning och intern kontroll. Detta omfattar både organisatoriska, tekniska och verksamhetsmässiga perspektiv, och har även koppling till krav i kommande lagstiftning såsom NIS2.

Iakttagelser

Cybersäkerhetsrelaterade frågor behandlas i flera av regionens styrdokument. I Regionplan 2025–2027 lyfts målsättningar om att vara en trygg och robust region, och insatsområden kopplade till beredskap och informationssäkerhet finns med. Digitalisering beskrivs som en viktig drivkraft, men det framgår inte hur säkerhetsaspekter integreras i det övergripande styr- och utvecklingsarbetet.

Regionstyrelsen får löpande information i ärenden där IT-säkerhet, informationssäkerhet eller dataskydd aktualiseras. I budgetförslaget för 2026 föreslås särskilda medel avsättas för att förstärka cybersäkerhetsarbetet, vilket hanteras inom den ordinarie styr- och planeringsprocessen.

Internkontrollplanen för 2025 innehåller inte något särskilt uppdrag som rör informationssäkerhet eller cybersäkerhet. I 2024 års plan fanns däremot två uppdrag kopplade till området robusthet, samt ett uppdrag kopplat till informationssäkerhet. Av intervjun med representanter för regionstyrelsen framgår att området informationssäkerhet togs bort i planeringen inför 2025, då det inte bedömdes visa på några avvikelser, medan robusthetsrelaterade uppdrag kvarstod. Det anges som vanligt förekommande att fokus i internkontrollen ändras från år till år.

Egenkontroller inom informationssäkerhet genomförs årligen av verksamheterna enligt en centralt framtagen mall, men dessa hanteras inte inom ramen för den formella internkontrollplanen. Det har inte identifierats någon samlad modell för hur resultaten från egenkontrollerna återförs till regionstyrelsen.

Cybersäkerhetsrelaterade frågor hanteras inom flera stödfunktioner, däribland MIT och koncernstaben. I intervjuerna beskrivs att frågor kopplade till säkerhet, digitalisering och planering hanteras i olika processer och av olika funktioner.

Bedömning

Vår sammantagna revisionella bedömning är att Region Dalarna **inte** har säkerställt att cybersäkerhetsarbetet är integrerat i den övergripande styrningen och det interna kontrollsystemet, på ett sätt som omfattar organisatoriska, tekniska och verksamhetsmässiga perspektiv.

Analys och motivering

Cybersäkerhetsområdet finns omnämnt i flera övergripande dokument, och regionstyrelsen hanterar ärenden med koppling till informationssäkerhet och IT. I förslag till budget för 2026 föreslås även riktade medel till cybersäkerhetsarbete, vilket tyder på att området uppmärksammas på strategisk nivå.

Granskningen visar samtidigt att det saknas en struktur för att integrera cybersäkerhetsarbetet i den ordinarie styrningen. Cybersäkerhet nämns i styrdokument och målformuleringar, men inte som en integrerad komponent i verksamhetsutveckling, målstyrning eller planering. Arbetet sker ofta i separata spår: digitalisering, säkerhet, robusthet, snarare än som en sammanhållen helhet. Avsaknaden av en integrerad modell blir särskilt relevant i ljuset av kommande krav i NIS2, där just styrning, kontroll och ansvarsfördelning är centrala delar.

Internkontrollplanen för 2025 innehåller inte något uppdrag kopplat till cybersäkerhet, och resultaten från egenkontroller inom området återförs inte systematiskt till regionstyrelsen. Det saknas också strukturer för att väga samman verksamhets-, teknik- och säkerhetsperspektiv i styrningen.

Det finns därmed en risk att cybersäkerhetsfrågor inte hanteras på ett enhetligt och proaktivt sätt i planering och uppföljning. Samtidigt är området tekniskt komplext och förutsätter tillgång till rätt kompetens. I dag finns inga strukturer för återkommande kompetenshöjande insatser för regionstyrelsen eller andra beslutsfattare, vilket kan försvåra möjligheten att tolka och agera på information från verksamheten.

Även den tekniska analysen (bilaga 3) bekräftar bilden av att cybersäkerhetsarbetet i nuläget inte är tillräckligt integrerat i regionens övergripande styrmodell. Analysen visar att det saknas en sammanhållen struktur för styrning, dokumentation och uppföljning, samt att informations- och cybersäkerhetsfrågorna hanteras isolerat från andra styr- och kontrollsystem. Det efterlyses ett övergripande riskramverk som integrerar dessa frågor på alla nivåer av verksamheten. Detta ligger i linje med kommande krav enligt NIS2, där styrning, kontroll och ansvarsfördelning utgör grundläggande komponenter.

3.9 Beaktas cybersäkerhet vid upphandlingar för att säkerställa att regionens informations- och IT-säkerhet inte hotas?

Inledning

Cybersäkerhet i leverantörsledet är en viktig aspekt av det övergripande säkerhetsarbetet. Region Dalarna anlitar ett stort antal externa leverantörer inom både teknikintensiva områden och verksamhetsnära tjänster. Det innebär att en betydande del av regionens informationshantering, systemförvaltning och tekniska infrastruktur hanteras av aktörer utanför den egna organisationen.

Mot denna bakgrund har vi valt att lyfta frågan om kravställning i upphandling som en egen kontrollfråga. Det bedöms som en fråga med tydlig bäring på övriga delar av cybersäkerhetsarbetet, bland annat styrning, riskhantering, tekniska lösningar och incidentberedskap. Frågan ryms inom projektplanens formulering om att granska om regionens cybersäkerhetsarbete är systematiskt och ändamålsenligt, och ligger i linje med såväl gällande lagstiftning som kommande krav enligt EU:s NIS2-direktiv.

Relevanta krav och kriterier

Enligt NIS2-direktivet ska offentliga aktörer som omfattas av lagstiftningen vidta lämpliga säkerhetsåtgärder för att skydda sina nätverks- och informationssystem. Detta inkluderar säkerställande av cybersäkerhet i hela värdekedjan, inklusive hos leverantörer. I artikel 21 anges att organisationer ska vidta åtgärder för att hantera risker i samband med användningen av leverantörer eller tredjepartsleverantörer. Detta krav återkommer i flera andra regelverk, bland annat:

- **ISO/IEC 27001**: kräver hantering av informationssäkerhetsrisker i leverantörsledet
- **GDPR**: ställer krav på att personuppgiftsbiträden ska ha tillräckliga tekniska och organisatoriska skyddsåtgärder
- **Lagen om offentlig upphandling (LOU)**: medger kravställning kopplad till säkerhet och riskhantering när det är motiverat av kontraktets art
- **MSB:s vägledning**: betonar vikten av säker upphandling i offentlig sektor

Stickprovskontroll

För att belysa hur cybersäkerhetskrav hanteras vid upphandlingar och i avtal har vi genomfört en stickprovskontroll av fem upphandlingar och fem avtal. Urvalet har gjorts ur en bruttolista av pågående och nyligen avslutade upphandlingar under 2025 samt avtal tecknade under 2023. Urvalet gjordes slumpmässigt, men med hänsyn till att täcka olika verksamhetsområden (t.ex. tekniska system, vårdnära tjänster, konsulttjänster, kommunikationslösningar och stödprocesser).

I stickproven har vi granskat följande aspekter:

- Förekomst av krav på informationssäkerhet
- Förekomst av tekniska säkerhetskrav
- Krav på incidenthantering
- Förekomst av informationsklassning
- Förekomst av personuppgiftsbiträdesavtal (PUB)
- Förekomst av sekretessklausuler
- Krav på robusthet, tillgänglighet eller kontinuitet

Stickproven och bedömningarna återges i sin helhet i bilaga 2.

Iakttagelser

Stickprovskontrollen visar att Region Dalarna ställer cybersäkerhetsrelaterade krav i vissa upphandlingar och avtal, men att tillämpningen saknar enhetlighet. Kravens omfattning varierar beroende på upphandlingens eller avtalets art och det finns inte någon fastställd modell för vad som ska krävas vid olika typer av avrop eller avtalstecknande.

I ett fall (doshanteringssystem) återfanns ett flertal detaljerade krav som rörde både tekniska, organisatoriska och juridiska säkerhetsaspekter, inklusive informationsklassning, IT-standarder och eKlientmiljö. I andra fall (exempelvis upphandling av psykologiska testverktyg) saknades motsvarande krav trots att upphandlingens innehåll innebar potentiella cybersäkerhetsrisker.

I flera upphandlingar och avtal förekommer personuppgiftsbiträdesavtal, sekretessklausuler eller andra legala krav. Däremot saknas ofta tekniska säkerhetskrav, hänvisningar till relevanta standarder, krav på informationsklassning eller beskrivning av hur incidenter ska hanteras. Det framgår inte heller att någon systematisk informationsklassning har genomförts inför upphandlingarna.

Enligt intervjuer med upphandlingschef, kravställande funktioner och säkerhetsansvariga saknas i dagsläget:

- En övergripande modell eller metodstöd för cybersäkerhetsrelaterad kravställning
- Fastställda rutiner för när och hur säkerhetskompetens ska involveras i upphandlingar
- En modell för uppföljning av ställda säkerhetskrav i avtal
- Resurser i form av avtalscontroller

Enligt upphandlingsenheten är resurserna begränsade. Det finns inte tillräcklig kapacitet att ge verksamheterna stöd i kravställningen. Verksamheterna är avtalsägare och därmed ansvarar för avtalsuppföljning, inklusive uppföljning av säkerhetsrelaterade villkor i avtalen, men beroende på klassificering av avtalet kan andra stödfunktion hjälpa till med avtalsuppföljning.

I flera av de granskade upphandlingarna och avtalen framgår att det finns en rutin för att konsulter eller leverantörer ska underteckna ett sekretess- och tystnadspliktsavtal i samband med uppstart av leverans. Dessa hanteras också av linjeverksamheten direkt, utan stöd från upphandlingsenheten eller gemensam uppföljning.

Av intervjuerna framgår att ansvaret för att formulera kravställning vid upphandling samt följa upp avtal ligger på verksamheterna, men beroende på klassificering av avtal kan stöd som behövs från andra stödfunktioner inom regionen fås. Upphandlingsenheten fungerar som en stödfunktion, men uppger att den saknar resurser för att aktivt stötta verksamheterna i säkerhetsfrågor. Det innebär att varje verksamhet själv behöver identifiera behov och formulera relevanta krav, även i upphandlingar där cybersäkerhetsaspekter är centrala. Inom upphandlingsenheten finns viss sakkunskap om cybersäkerhet. En funktion ansvarar för att förvalta och uppdatera den tekniska kravlista som används som stöd i upphandlingar. Enligt intervju med tjänstepersonen innebär uppdraget att ge stöd i att välja lämpliga krav från listan. Det saknas dock rutiner för hur urvalet ska göras, när kravlistan ska användas eller hur tidigare urval har dokumenterats. Upphandlingsenheten påpekar att ansvaret för detta åligger helt rollen "IT-kravledare" som jobbar inom MIT, inte upphandlingen. Det pågår ett utvecklingsarbete hos MIT, men i nuläget är stödet beroende av enskilda personers initiativ och bedömningar.

Granskningen visar att det råder oenighet om i vilka situationer en ISAK-analys ska genomföras inför en upphandling. Vissa anser att det endast bör ske vid upphandling av IT-system, medan andra menar att analysen bör göras även när upphandlingen gäller tjänster som innebär hantering av information. Avsaknaden av gemensam tolkning och tillämpning innebär att riskbedömningar inte genomförs på ett enhetligt sätt inför upphandlingar, vilket påverkar kravställningen. Upphandlingsenheten påpekar behovet för att ansvariga för informationssäkerhet inom regionen ska tydligt definiera när ISAK ska göras.

Direktupphandlingar där värdet understiger 100 tkr genomförs direkt av verksamheterna, utan att upphandlingsenheten involveras. Det finns i nuläget ingen systematisk kontroll eller dokumentation av vilka krav som ställs i dessa upphandlingar. Samtidigt bedömer upphandlingsavdelningen att även dessa mindre upphandlingar kan omfatta lösningar där cybersäkerhetsrisker förekommer, till exempel där personuppgifter hanteras eller systemanslutning sker.

Bedömning

Vår sammantagna revisionella bedömning är att cybersäkerhet vid upphandlingar beaktas **till viss del** för att säkerställa att regionens informations- och IT-säkerhet inte hotas.

Analys och motivering

Det finns exempel på upphandlingar där Region Dalarna har ställt genomtänkta krav kopplade till cybersäkerhet – både legala, tekniska och organisatoriska. I upphandlingen av doshanteringssystemet och i

biljettsystemets avtal går det att se hur kravställningen har tagit höjd för risker och säkerhetsaspekter. Dessa exempel visar att det finns förutsättningar för ett fungerande arbetssätt när rätt kompetens involveras och frågan hanteras tidigt i processen.

Samtidigt visar granskningen att detta inte är den generella bilden. Kravställningen är varken enhetlig eller strukturerad. Det saknas vägledning för hur cybersäkerhetsrisker ska analyseras och hur krav ska utformas beroende på upphandlingens innehåll. I praktiken innebär det att upphandlingar med potentiella säkerhetsrisker kan genomföras utan tillräcklig förberedelse. Som vi visade ovan i fråga 3.6 finns det även brister i den övergripande riskhanteringen, vilket påverkar möjligheten att identifiera säkerhetskrav på ett systematiskt sätt.

Granskningen visar att det inte finns någon samlad funktion för uppföljning av cybersäkerhetskrav i avtal. Detta innebär att det i praktiken är upp till varje verksamhet att säkerställa att krav efterlevs, vilket kan vara svårt när kraven inte är tydligt formulerade eller när verksamheterna saknar expertstöd.

Avsaknaden av struktur, metodstöd och uppföljning gör att regionen i nuläget inte säkerställer att cybersäkerhetsrisker i leverantörsledet hanteras på ett enhetligt och riskbaserat sätt. Mot bakgrund av de krav som följer av NIS2-direktivet och andra regelverk bör detta ses som ett viktigt utvecklingsområde.

Intervjuerna och den tekniska analysen pekar också på att det i dag saknas en sammanhållen modell som täcker hela inköpskedjan, från direktupphandlingar och avrop till mer omfattande upphandlingar. Vi bedömer att cybersäkerhet bör hanteras utifrån en gemensam process med dokumenterade kriterier, tröskelvärden och vägledande stöd, oavsett upphandlingens storlek eller karaktär. En sådan modell bör även innehålla strukturer för när säkerhetskompetens ska involveras och hur uppföljning av säkerhetskrav ska genomföras. Avsaknaden av en sådan helhet innebär att cybersäkerhetsrisker i leverantörsledet riskerar att förbises, särskilt i mindre upphandlingar där säkerhetsaspekterna kan vara svårare att identifiera.

4. Sammanfattande bedömning och rekommendationer

Syftet med granskningen har varit att ge revisorerna underlag för att bedöma om regionstyrelsen säkerställt att regionens arbete med cybersäkerhet är ändamålsenligt. Vår samlade revisionella bedömning är att regionstyrelsen **till viss del** har säkerställt att arbetet med cybersäkerhet är ändamålsenligt.

Granskningen visar att det finns viktiga initiativ, vissa tekniska lösningar och lokala strukturer, men att det saknas en helhetsstyrning, systematik och integrering i den ordinarie styrmodellen. Cybersäkerhetsarbetet bedrivs till stor del som separata aktiviteter utan samlad uppföljning eller analys, och regionstyrelsen har därmed begränsade förutsättningar att bedöma om arbetet ger tillräckligt skydd i förhållande till de risker som finns.

Nedan redovisas granskningens svar på respektive revisionsfråga:

Revisionsfråga	Bedömning	Kort motivering
3.1 Finns aktuella och ändamålsenliga dokument som styr cybersäkerhetsarbetet i regionen??	**Till stor del**	Det finns ett stort antal styrande dokument som berör cybersäkerhetsarbetet, men vi bedömer samtidigt att dokumentationen i praktiken inte utgör ett fullt ut fungerande styrsystem.
3.2 Är ansvar och roller för arbetet med cybersäkerhet tydliga och kända??	**Till viss del**	Vissa roller är tydligt definierade i styrande dokument, men trots denna formella struktur upplevs ansvarsfördelningen i praktiken inte alltid som tydlig.
3.3 Är organisationen för arbetet med cybersäkerhet ändamålsenlig och finns nödvändiga resurser för arbetet (kompetensmässigt, ekonomiskt, systemstöd etc.)?	**Till viss del**	Cybersäkerhetsarbetet bedrivs i dag inom flera organisatoriska enheter utan en sammanhållen modell för styrning, koordinering och uppföljning. Förutsättningarna för att bedriva arbetet varierar mellan verksamheterna. Kompetensförsörjningen är en utmaning för regionen. Det gäller särskilt inom specialistområden som identitetshantering, behörighetshantering, incidenthantering och säkerhetsarkitektur. Vad gäller systemstöd bedöms befintliga verktyg inte ge tillräckligt stöd för ett samlat, effektivt och uppföljningsbart cybersäkerhetsarbete.
3.4 Omfattar regionens cybersäkerhetsarbete i tillräcklig grad såväl människor (t.ex. anställdas säkerhetsmedvetande) som processer och tekniska lösningar?	**Till viss del**	Regionen har vidtagit åtgärder för att höja anställdas medvetenhet om informationssäkerhet, men insatserna beskrivs som oregelbundna. När det gäller processer är det särskilt relevant att notera att cybersäkerhet inte integreras på ett systematiskt sätt i upphandlingar, avtal och leverantörsrelationer.
3.5 Har cybersäkerhetsarbetet ett tillräckligt och ändamålsenligt stöd från regionens ledning?	**Till viss del**	Området uppmärksammas, men saknar genomgående prioritering, samlad återrapportering och strategisk styrning. Vi bedömer att stödet inte är samordnat eller systematiskt. Området uppfattas som komplext och det saknas samlade analyser, riskbilder eller rapporter som ger underlag för strategiska beslut.
3.6 Bedrivs ett systematiskt arbete med att identifiera, hantera och åtgärda risker och behov för att	**Till viss del**	Regionen har vissa strukturer för att identifiera och hantera cybersäkerhetsrisker, men arbetet saknar samordning och enhetlighet. Det finns ingen övergripande struktur för att följa upp eller

säkerställa en ändamålsenlig cybersäkerhet?		återrapportera risker på regionnivå, vilket försvårar lärande och prioritering. Även den tekniska analysen lyfter avsaknad av gemensamt systemstöd för riskhantering, begränsad spårbarhet i dokumentation och behov av förbättrad uppföljning.
3.7 Håller cybersäkerhetsarbetet i regionen sådan standard att regionen kan förväntas leva upp till kraven i kommande lagstiftning?	**Nej**	Flera funktioner berör kraven i NIS2, men någon samlad analys, planering eller översikt finns inte. Avsaknaden av en samlad bild av cybersäkerhetsläget innebär att regionen inte har tillräckligt beslutsunderlag för att bedöma vilka brister som finns eller vilka åtgärder som bör prioriteras.
3.8 Är cybersäkerhetsarbetet integrerat i den övergripande styrningen och interna kontrollen?	**Nej**	
3.9 Beaktas cybersäkerhet vid upphandlingar för att säkerställa att regionens informations- och IT-säkerhet inte hotas?	**Till viss del**	Enstaka upphandlingar innehåller relevanta krav, men arbetet är inte systematiserat, stödet är otillräckligt och uppföljning saknas.

Rekommendationer

Mot bakgrund av granskningens resultat lämnas följande rekommendationer till regionstyrelsen:

1. **Integrera cybersäkerhetsfrågorna i regionens övergripande styrning, planering och uppföljning.**

   Regionstyrelsen bör säkerställa att cybersäkerhet betraktas som en ledningsfråga och integreras i verksamhetsplanering, internkontroll, målstyrning och riskhantering – inte hanteras i separata spår.

2. **Genomför en nulägesanalys i förhållande till NIS2 och ta fram en samlad åtgärdsplan för att säkerställa efterlevnad.**

   Detta bör inkludera roller, ansvar, uppföljningsmodeller och dokumentation som visar hur kraven i NIS2 uppfylls – inklusive styrning av leverantörsled, incidenthantering och utbildningsinsatser.

3. **Utveckla en strukturerad och sammanhållen modell för cybersäkerhetsrelaterad riskhantering.**

   Modellen bör möjliggöra att risker identifieras, dokumenteras, aggregeras och analyseras på regional nivå. Det bör också finnas tydliga strukturer för att ta fram, följa upp och återrapportera åtgärder kopplade till riskanalyser och handlingsplaner.

4. **Säkerställ att samtliga verksamheter och nivåer i organisationen har tillgång till kompetens, vägledning och stöd i cybersäkerhetsarbetet.**

   Detta innefattar systemstöd, rollbeskrivningar, utbildning till alla medarbetare samt metodstöd som gör det möjligt att arbeta systematiskt i vardagen.

5. **Stärk cybersäkerheten i leverantörsledet genom enhetliga krav, tydlig ansvarsfördelning och systematisk uppföljning.**

   Det bör finnas en modell för hur cybersäkerhetsrisker identifieras, hanteras och följs upp vid upphandlingar, avrop och andra leverantörsrelationer – oavsett omfattning och typ av tjänst.

6. **Säkerställ ledningens kompetens och beslutsstöd i cybersäkerhetsfrågor.**

   Regionstyrelsen och andra beslutsfattare behöver återkommande analysunderlag och riskbilder för att kunna styra området proaktivt. Det bör även finnas strukturer för kompetensutveckling kopplat till cybersäkerhet i styrande roller.

Malmö den 13 november 2025

Teodora Heim

Qualitarium erbjuder kvalificerade tjänster inom revision, utvärdering, konsultation och rådgivning till offentliga och privata aktörer. Varje uppdrag utförs med högsta professionalitet och noggrannhet för att säkerställa kvalitet och värde för våra kunder.

Qualitarium AB är ett svenskt aktiebolag. För mer information om vårt företag och våra tjänster vänligen besök vår webbplats på qualitarium.se eller kontakta våra delägare:

Teodora Heim

Delägare
Specialist inom organisation, styrning och ledning av offentliga organisationer

E-post: teodora.heim@qualitarium.se
Telefon: 0733-976304

Mattias Holmetun

Delägare
Specialist inom ledning, styrning och samverkan

E-post: mattias.holmetun@qualitarium.se
Telefon: 0706-946091