Granskning av informationssäkerhet

Rapport

Region Gävleborg

2025-11-18

Antal sidor 26

Bilagor 2

1 INNEHÅLLSFÖRTECKNING

1 Sammanfattning 3

2 Bakgrund 6

3 Syfte, revisionsfrågor och avgränsning 6

3.1 Avgränsning 7

4 Revisionskriterier 7

5 Metod 7

6 Resultat av granskningen 9

6.1 Ledningssystem för informationssäkerhet 9
6.1.1 Säkerhetspolicy 9
6.1.2 Riktlinjer inom informationssäkerhet 9
6.1.3 Övriga styrande och stödjande dokument 9
6.1.4 Bedömning 10

6.2 Organisation 10
6.2.1 Regionstyrelsens och nämndernas ansvar 10
6.2.2 Ansvarsfördelning centrala funktioner 11
6.2.3 Informationssäkerhetsansvar som följer med verksamhetsansvaret i styrelser och nämnder 12
6.2.4 Informationssäkerhetsråd och Systemägarråd 14
6.2.5 Bedömning 14

6.3 Rutiner för riskhantering 14
6.3.1 Riskanalys 14
6.3.2 Informationsklassning och riskbedömning för informationstillgångar 15
6.3.3 Bedömning 16

6.4 Rutiner för personalrelaterad säkerhet 16
6.4.1 Utbildning och information 16
6.4.2 Bedömning 17

6.5 Hantering av informationssäkerhetsincidenter 18
6.5.1 Bedömning 19

6.6 Uppföljning av informationssäkerhetsarbetet 19
6.6.1 Uppföljning av informationssäkerhet 19
6.6.2 Övrig rapportering 20
6.6.3 Kontroll av dataskyddsarbetet 20
6.6.4 Bedömning 21

7 Samlad bedömning och rekommendationer 22

8 Bilaga 1 24

9 Bilaga 2 25

1 SAMMANFATTNING

Azets har av Region Gävleborgs revisorer fått i uppdrag att granska regionens arbete med informationssäkerhet.

Syftet med granskningen har varit att bedöma om regionstyrelsen, hälso- och sjukvårdsnämnden samt hållbarhetsnämnden säkerställt att informationssäkerhetsarbetet är systematiskt i enlighet med lagkrav och interna beslut.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen, hälso- och sjukvårdsnämnden samt hållbarhetsnämnden endast delvis har säkerställt att informationssäkerhetsarbetet är systematiskt i enlighet med lagkrav och interna beslut.

Bakgrunden till vår samlade bedömning är att granskningen visat att det finns ett antal styrande dokument som utgör grund för regionens ledningssystem för informationssäkerhet. Vi noterar dock dels att de styrande dokumenten inte är politiskt antagna, dels att ledningssystemet i dess nuvarande form inte är komplett och saknar hierarkisk ordning och struktur. Vi ser en risk att detta kan medföra svårighet för verksamheterna att tillämpa reglerna effektivt. De mest väsentliga bristerna i arbetet uppfattar vi är riskhantering och att åtgärder vidtas för att dessa ska vara på en acceptabel nivå samt att arbetet med uppföljning och kontroll stärks så att regionen i högre grad utvärderar följsamhet till lagkrav, föreskrifter och interna styrdokument inom informationssäkerhet.

I det följande redovisas samlad bedömning av revisionsfrågan per revisionsobjekt.

Finns ett ledningssystem för informationssäkerhet som reglerar ansvar och krav för regionens informationssäkerhetsarbete?	
Regionstyrelsen	Endast delvis
Finns en organisation för informationssäkerhetsarbetet som är anpassad efter ledningssystemets omfattning?	
Regionstyrelsen	I allt väsentligt
Hälso- och sjukvårdsnämnden	I allt väsentligt
Hållbarhetsnämnden	I allt väsentligt
Finns dokumenterade rutiner avseende riskhantering och genomförs arbetet med en tillräcklig systematik så att säkerheten är anpassad efter skyddsbehov hos informationstillgångar?	
Regionstyrelsen	Endast delvis

Hälso- och sjukvårdsnämnden	Endast delvis
Hållbarhetsnämnden	Endast delvis
Har säkerhetsåtgärder vidtagits för att säkerställa personalrelaterad säkerhet?	
Regionstyrelsen	Endast delvis
Hälso- och sjukvårdsnämnden	Endast delvis
Hållbarhetsnämnden	Endast delvis
Finns etablerade rutiner och arbetssätt för att effektivt hantera informations-säkerhetsincidenter?	
Regionstyrelsen	Endast delvis
Hälso- och sjukvårdsnämnden	Endast delvis
Hållbarhetsnämnden	Endast delvis
Sker en regelbunden uppföljning av arbetet samt kontroll över att informationssäkerhetsarbetet efterlever lagkrav och interna beslut?	
Regionstyrelsen	Nej
Hälso- och sjukvårdsnämnden	Nej
Hållbarhetsnämnden	Nej

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen att:

- Tillse att övergripande styrdokument för informationssäkerhet antas politiskt för att tydliggöra de förtroendevaldas viljeriktning och krav på förvaltningarnas arbete.
- Tillse att nuvarande LIS utvärderas, kompletteras och struktureras i syfte att säkerställa tillämpning av regionens regelverk inom informationssäkerhet.
- Besluta om riktlinjer för regionens övergripande riskhantering och tillse att riskanalyser minst årligen genomförs med inriktning på informationssäkerhet.
- Utvärdera nuvarande personalsäkerhetsåtgärder för att bedöma om de är tillräckliga i syfte att etablera en säkerhetskultur i enlighet med beslutade riktlinjer för informationssäkerhet.
- Stärka styrningen av informationssäkerhetsarbetet där uppföljning och rapportering efterföljs av beslut om handlingsplaner för väsentliga och prioriterade förbättringsåtgärder.

- Utvärdera nuvarande it-säkerhetsåtgärder i relation till kommande lagkrav samt aktuella hot och risker, särskilt med beaktande på förmåga att upptäcka och hantera avvikelser i form av it-säkerhetshändelser.
- Säkerställa att uppföljning och rapportering genomförs i enlighet med beslutade rutiner samt tydliggöra krav på nämndernas ansvar för uppföljning och rapportering av informationssäkerhetsarbetet. I uppföljning bör kontroll av att de beslutade styrdokumenten efterlevs ingå.

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

- Slutföra arbetet enligt rutinen för POIK.
- Efterfråga förtydligande över nämndens ansvar för uppföljning av det egna informationssäkerhetsarbetet.
- Efterfråga förtydligande över på vilka sätt informationsägaren ska involveras i analys och bedömning av informationssäkerhetsincidenter samt vilka krav som finns för när nämnden ska få kännedom om inträffade incidenter.
- Etablera regelbunden, minst årlig, uppföljning informationssäkerhetsarbetet så att nämnden ges förutsättningar att fatta beslut om inriktning och förstärkningar.

Utifrån resultatet av vår granskning rekommenderar vi hållbarhetsnämnden att:

- Tillse att samverkan och samsyn stärks internt mellan funktioner för informationssäkerhet och systemenhet samt även mellan systemenhet och avdelning för IT och verksamhetsutveckling.
- Efterfråga förtydligande över nämndens ansvar för uppföljning av det egna informationssäkerhetsarbetet.
- Efterfråga förtydligande över på vilka sätt informationsägaren ska involveras i analys och bedömning av informationssäkerhetsincidenter samt vilka krav som finns för när nämnden ska få kännedom om inträffade incidenter.
- Etablera regelbunden, minst årlig, uppföljning informationssäkerhetsarbetet så att nämnden ges förutsättningar att fatta beslut om inriktning och förstärkningar.

2 BAKGRUND

Azets Revision & Rådgivning har av de förtroendevalda revisorerna i Region Gävleborg fått i uppdrag att genomföra en granskning av regionens arbete med informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2025.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Informationssäkerhet innebär att all skyddsvärd information ska vara tillgänglig, konfidentiell och spårbar.

Regionens har verksamhet som är identifierad som samhällsviktig verksamhet och samhällsviktig tjänst. Det finns därigenom förstärkta krav på att informationssäkerhetsarbetet ska vara systematiskt och riskbaserat så att de samhällsviktiga funktionerna ska vara robusta och inte drabbas utav störningar eller avbrott.

Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Ett flertal offentliga organisationer har under de senaste åren utsatts för cyberattacker med stora konsekvenser som följd. Exempelvis har skyddsvärd information förlorats eller röjts till obehöriga eller den bristande hanteringen lett att organisationer drabbats av ekonomisk skada eller förtroendeskada.

Ett vanligt tillvägagångssätt har varit att rikta hot direkt mot användare för att på så sätt utnyttja sårbarheter för att komma åt organisationens information eller för att hindra väsentliga processer. Detta innebär att organisationer måste ha ett proaktivt arbete med etablering av säkerhetsåtgärder och rutiner för att säkerställa en tillräcklig personalsäkerhet där utbildning och information bidrar till säkerhetskultur hos de som använder verksamhetssystem och applikationer. Därtill krävs verktyg och applikationer som hindrar eller detekterar hot som riktas mot användare samt en effektiv incidenthanteringen om ändå incidenter inträffar.

Europaparlamentet beslutade 2022 om ett nytt NIS2-direktiv med förstärkta krav om informations- och cybersäkerhet inom unionen. Under 2025 ska ny svensk lagstiftning, Cybersäkerhetslagen, införas som reglering av direktivet. I nuvarande förslag anges offentlig förvaltning vara en egen sektor som ska omfattas av lagkraven. Detta innebär i sin tur att regioner omfattas i sin helhet och därigenom har att efterleva de krav på ett systematiskt informationssäkerhetsarbete som lagen ställer. För många verksamheter innebär detta stora förändringar och behov av anpassningar både organisatoriskt och tekniskt.

Mot bakgrund av ovan har revisorerna bedömt att det finns behov av att genomföra en fördjupad granskning av regionens arbete med informationssäkerhet.

3 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

Syftet med granskningen har varit att bedöma om regionstyrelsen och nämnderna säkerställt att informationssäkerhetsarbetet är systematiskt i enlighet med lagkrav och interna beslut.

Granskningen har omfattat följande revisionsfrågor:

- Finns ett ledningssystem för informationssäkerhet som reglerar ansvar och krav för regionens informationssäkerhetsarbete?
- Finns en organisation för informationssäkerhetsarbetet som är anpassad efter ledningssystemets omfattning?

- Finns dokumenterade rutiner avseende riskhantering och genomförs arbetet med en tillräcklig systematik så att säkerheten är anpassad efter skyddsbehov hos informationstillgångar?
- Har säkerhetsåtgärder vidtagits för att säkerställa personalrelaterad säkerhet?
- Har insatser varit tillräckliga för att etablera en medvetenhet om hot som riktas direkt mot användare?
- Finns etablerade rutiner och arbetssätt för att effektivt hantera informations-säkerhetsincidenter?
- Sker en regelbunden uppföljning av arbetet samt kontroll över att informationssäkerhetsarbetet efterlever lagkrav och interna beslut?

3.1 AVGRÄNSNING

Granskningen har avgränsats till styrning och ledning av informationssäkerhetsarbetet. Varken Azets eller revisorerna har tagit del av säkerhetsklassad information i enlighet med säkerhetsskyddslagen.

Granskningen har avsett revisionsåret 2025.

Granskningen har avsett regionstyrelsen, hälso- och sjukvårdsnämnden samt hållbarhetsnämnden (kollektivtrafikverksamheten).

4 REVISIONSKRITERIER

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen 6 kap. 6 §
- Reglementen för styrelser och nämnder RS 2022/1307
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och tillhörande Föreskrift (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster
- SS-ISO/IEC 27001 krav om ledningssystem för informationssäkerhet samt 27002 säkerhetsåtgärder
- Säkerhetspolicy RS 2023/2757
- Tillämpbara interna regelverk, policys och beslut

5 METOD

Granskningen har genomförts genom:

- Dokumentstudier, se bilaga 1.
- Intervjuer, se bilaga 2.
- Stickprovsvisa kontroller av upprättad dokumentation för informationsklassningar samt riskanalyser.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.

Rapporten är faktakontrollerad av företrädare som deltagit i intervjuer.

6 RESULTAT AV GRANSKNINGEN

6.1 LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET

6.1.1 Säkerhetspolicy

Region Gävleborg har en beslutad Säkerhetspolicy[1]. Syftet med policyn uppges vara att tydliggöra förhållningssätt till säkerhet för allt arbete inom regionen. Säkerhetspolicyn framhåller att Region Gävleborg ska bedriva ett systematiskt informationssäkerhetsarbete för att skydda informationstillgångarnas konfidentialitet, riktighet och tillgänglighet.

Vi noterar att policyn refererar till andra styrande dokument inom informationssäkerhet som inte är gällande längre. Exempelvis Övergripande direktiv för informationssäkerhet samt Grundläggande regler för it-säkerhet – direktiv Region Gävleborg. Dessa har ersatts av nedan beskrivna Riktlinjer för informationssäkerhet.

6.1.2 Riktlinjer inom informationssäkerhet

Övergripande riktlinje för informationssäkerhet[2]. Av underlaget framgår att riktlinjen utgör grunden för regionens ledningssystem för informationssäkerhet (LIS). Ledningssystemet omfattar samtliga verksamheter i Region Gävleborg.

Regionen har genom beslut av riktlinjen fastställt att informationssäkerhetsarbetet ska eftersträva att följa informationssäkerhetsstandarden ISO 27001:2022. Standarden har som krav att högsta ledningen ska besluta om en informationssäkerhetspolicy. I den övergripande riktlinjen anges att denna avser motsvara det ställda kravet på en informationssäkerhetspolicy. Vi noterar av underlaget att det är beslutat av förvaltningschef.

Riktlinjen beskriver övergripande målsättningen för informationssäkerhetsarbetet samt organisationens åtagande om att uppfylla tillämpliga krav på informationssäkerhet. Underlaget beskriver även lagområden som regionen har att förhålla sig till, övergripande ansvarsfördelning samt målsättning för arbetet. Ansvarsfördelningen konkretiseras i *Riktlinje för ansvar och roller*[3] Även denna riktlinje har beslutats av förvaltningschef.

6.1.3 Övriga styrande och stödjande dokument

Riktlinjerna konkretiseras av ett stort antal underliggande rutiner och instruktioner (vi har i granskningen tagit del av 40-tal dokument). Dessa ger operativ vägledning för avgränsade processer och moment inom både informationssäkerhets- och dataskyddsarbetet. Vi noterar genom dokumentgranskning att dokumenten i hög grad är aktuella med beslutsdatum eller revidering under 2024 och 2025.

Några exempel är:

- Instruktion för e-post
- Rutin för hantering av personer med skyddade personuppgifter
- Instruktion för lagring och kommunikation i digitala kanaler
- Instruktion för registrering i registerförteckning
- Övergripande rutin för personuppgiftsbehandling

[1] Beslutad av regionfullmäktige 2024-03-26 RS 2023/2757
[2] Beslutad 2025-02-19
[3] Beslutad 2025-02-19

Under granskningen förevisas den yta på regionens intranät där den samlade dokumentationen från ledningssystemet har tillgängliggjorts. Genom intervjuer ges en entydig bild av att ledningssystemet är användbart och värdeskapande, men att det skulle tjäna på att vara verksamhetsanpassat i högre grad.

En uppfattning som förmedlas av flera intervjuade är att antalet styrande och stödjande dokument är stort och för den enskilda svårt att förhålla sig till. Nyckelfunktioner är därför de verksamhetsnära informationsförvaltningssamordnare som på daglig basis kan ge vägledning och stöd i operativa frågor och även ta fram dokument från intranätet som efterfrågas av verksamheterna. En annan utmaning som lyfts är tolkningen av informationssäkerhetskrav som ställs i de styrande dokumenten i relation till funktionalitet eller behov inom verksamheter, främst inom medicinsk teknik.

6.1.4 Bedömning

Vår bedömning är att regionstyrelsen endast delvis säkerställt att det finns ett ledningssystem för informationssäkerhet som reglerar ansvar och krav för regionens informationssäkerhet.

Vi baserar vår bedömning på att det i nuläget saknas en politiskt beslutad styrning för regionens informationssäkerhetsarbete utöver det som övergripande framgår av Säkerhetspolicyn. Vi ser det som väsentligt att krav på arbetet samt övergripande ansvarsfördelning, mål och inriktning fastställs av behörig instans då styrningen omfattar hela regionens verksamhet. Därunder kan delegation finnas för beslut om verksamhetsanpassade och konkretiserande anvisningar, rutiner och instruktioner så länge dessa linjerar med policy och riktlinjer på övergripande nivå.

Vi konstaterar att det stora antalet dokument i ledningssystemet samt att det inte är organiserat i en hierarkisk struktur av styrande och stödjande dokument kan innebära att förutsättningarna för verksamheterna att tolka och tillämpa gällande regelverk försvåras.

6.2 ORGANISATION

6.2.1 Regionstyrelsens och nämndernas ansvar

Enligt Reglemente för regionstyrelsen och nämnder[4] har regionstyrelsen ansvar för interna säkerhets- och beredskapsfrågor. Övriga nämnders ansvar för säkerhetsfrågor regleras inte i reglementet. Regionstyrelsen respektive nämnderna ansvarar för de personuppgifter som nämnden hanterar i sin verksamhet.

Vidare anges krav om att nämnderna bedriver verksamheten i enlighet med de mål och riktlinjer som fullmäktige har bestämt, föreskrifter i lag eller förordningar samt bestämmelser i reglementet.

Styrande dokument inom säkerhet och informationssäkerhet är inte samstämmiga avseende vem som har det yttersta ansvaret för säkerhetsarbetet. Säkerhetspolicyn saknar uppgift om regionstyrelsens ansvar trots att reglementet anger regionstyrelsen som ansvariga för det interna säkerhets- och beredskapsarbetet. Den övergripande riktlinjen för informationssäkerhet reglerar att regionstyrelsen har det yttersta ansvaret för detta.

[4] Fastställt av regionfullmäktige 2022-05-31 RS 2022/1307

6.2.2 Ansvarsfördelning centrala funktioner

I *Säkerhetspolicyn* tillskrivs koncernledningen det yttersta ansvaret för säkerhetsarbetet i Region Gävleborg. Koncernledningen ansvarar även för att tillsätta adekvata resurser, så att verksamheterna har möjligheter att bedriva ett aktivt säkerhetsarbete. Vidare beskrivs att säkerhet- och beredskapsavdelningen och informationssäkerhetsenheten har sakkunniga inom respektive verksamhetsområde vars uppgifter är att stötta övriga verksamheter i koncernen i deras säkerhetsarbete. I avdelningens ansvar ingår regionövergripande internkontroller samt att tillse att lag, förordning och riktlinjer efterlevs.

Enligt *Övergripande riktlinje för informationssäkerhet* ansvarar regiondirektören för att tillse att arbetet följer vad som anges i riktlinjen. På verksamhetsnivå ansvarar respektive chef för informationssäkerheten som del av linjeansvaret.

En central informationssäkerhetsfunktion ska uppbära det strategiska och operativa ledningsansvaret. I uppdraget ligger att ta fram en årlig plan för aktiviteter och åtgärder i syfte att stärka informationssäkerhetsarbetet på både central och verksamhetsnära nivå. Ansvar för centrala funktioner i informationssäkerhetsarbetet konkretiseras i en särskild *Riktlinje för ansvar och roller*[5]. I dokumentet anges även att regionens säkerhetschef har ansvar för att samordna och leda säkerhetsarbetet.

Iakttagelser från våra intervjuer är att det har genomförts en omorganisation där tidigare Informationssäkerhetsenheten har flyttats till Juridikavdelningen från Säkerhetsavdelningen.

Regionens chefsjurist är tillförordnad informationssäkerhetsansvarig och dataskyddsombud. Därutöver finns en informationssäkerhetssamordnare samt en verksamhetsutvecklare som ålagts ansvar för dataskyddsfrågor och som numera tillhör den centrala informationssäkerhetsfunktionen. Ytterligare en informationssäkerhetssamordnare hade rekryterats men inte påbörjat sin anställning då våra intervjuer hölls. Att den centrala informationssäkerhetsfunktionen utökas uttrycks vara ett medvetet vägval då arbetet tidigare uppfattas att ha varit beroende av en enskild funktion. Därför finns en tanke att skapa en enhet som bygger på funktion snarare än person. Likaså finns en ambition att verksamheterna ska bli mer autonoma i sitt arbete då de centrala funktionerna i dagsläget är involverade i verksamheternas arbete i stor omfattning.

I riktlinjen finns särskild skrivelse angående ansvar för IT-säkerhet. Inom IT-förvaltningen ska finnas funktioner som säkerställer IT-säkerhetsåtgärder som följd av krav härledda från informationssäkerhetsarbetet. IT-förvaltningen uppges ha ett särskilt ansvar att omsätta funktionella krav på säkerhet till tekniska lösningar.

Inom regionen fungerar avdelningen för IT och verksamhetsutveckling som IT-förvaltning enligt de styrande dokumentens beskrivning. Inom avdelningen arbetar närmare 150 medarbetare vilket är en ökning de senaste fem åren med cirka 50 personer. Intervjuade beskriver att arbetssätt och strukturer är under utveckling. Avdelningen har identifierat behov av en strategi för det samlade it-säkerhetsarbetet men den saknas för närvarande. Det finns en digitaliseringsstrategi och handlingsplan för verksamheterna.

Funktioner inom avdelningen är bland annat it-säkerhetsansvarig och it-säkerhetsarkitekt. Flertalet funktioner uppfattas för närvarande ha ett nyckelpersonsberoende vilket utgör en sårbarhet och flaskhals i vissa processer. Därtill lyfts att det finns stora grundbehov med säkerhetsåtgärder som behöver prioriteras som avdelningen har svårt att möta.

[5] Beslutad 2025-02-19

I dagsläget saknas full samsyn kring gränsdragningen mellan informationssäkerhetsfunktionen och avdelningen för IT och verksamhetsutveckling där det uttrycks olika uppfattning kring i vilken utsträckning som IT-teknisk kompetens involveras i informationssäkerhetsarbetet samt hur olika avvägningar och tolkningar görs från informationssäkerhetsfunktionen och ansvariga inom IT. Utifrån intervjuer uppfattar vi att det finns en ömsesidig vilja att utveckla samarbetet.

I upprättad årsrapport för informationssäkerhetsarbetet 2024 anges fokusområde för 2025 vara att säkerställa specialistkompetens för det systematiska informationssäkerhetsarbetet. Rapporten innehåller dock inte någon beskrivning över vad som ligger till grund för det valda fokusområdet.

6.2.3 Informationssäkerhetsansvar som följer med verksamhetsansvaret i styrelser och nämnder

Ansvaret för det linjebaserade informationssäkerhetsarbetet som följer med verksamhetsansvaret utgörs av rollerna informationsägare och resursägare. Informationsägare är den funktion som uppdragits verksamhetsansvar, som därmed ansvarar för informationssäkerheten inom respektive verksamhetsområde. Resursägare är den funktion som ansvarar för den IT-resurs som hanterar en informationstillgång. Resursägarens ansvar är att tillse att IT-resurser uppfyller de säkerhetskrav som är tillbörliga som skydd för informationstillgången. Enligt riktlinjen för ansvar och roller har IT-direktören det övergripande ansvaret för alla Region Gävleborgs IT-resurser. Vidare ska arbetet genomföras i enlighet med Region Gävleborgs systemförvaltningsmodell.

Vi har tagit del av *Region Gävleborgs systemförvaltningsmodell*[6]. I den benämns ett antal roller, däribland systemägare, systemförvaltare och systemadministratör. Även informationsägare nämns, dock saknas förtydligande av rollen resursägare. Enligt styrdokumentet för systemförvaltningsmodellen så arbetar systemförvaltare kontinuerligt med informationssäkerhet och tillhörande modell för arbetet. Vi har inte kunnat spåra vilken modell som avses i denna skrivelse. I underlaget framgår att systemets nivå för krav på tillgänglighet, riktighet och sekretess ska anges och krav för dessa aspekter dokumenteras i en handlingsplan.

Vi har i intervjuer försökt klarlägga ansvar och roll för funktionen ”resursägare” då förtydligande beskrivning saknas i dokumentationen. Från de intervjuade ges olika svar varför vi inte får någon tydlig bild av funktionen och hur denna roll förhåller sig till exempelvis rollen systemägare.

Som stöd till informationsägaren ska en lokal informationsförvaltningssamordnare finnas inom varje förvaltning. Dessa har i uppgift att samordna och stötta informationsägaren i det lokala informationssäkerhetsarbetet.

I enlighet med reglering i den övergripande riktlinjen samt riktlinjen för roller och ansvar har respektive nämnd utsett lokala informationsförvaltningssamordnare. Dessa utgör dels kontaktyta och stöd för de centrala informationssäkerhetssamordnarna, dels är utförare av det operativa informationssäkerhetsarbetet inom respektive verksamhet.

Organisation under hälso- och sjukvårdsnämnden

”Verksamhetsområde digital vård” är ett av hälso- och sjukvårdsnämndens 20 verksamhetsområden. Området omfattar ett tiotal medarbetare och beskrivs som en både operativ och strategisk part i arbete och frågor som är kopplade till digitalisering, till exempel informationssäkerhet, dataskyddsfrågor och upphandlingsstöd vid IT-införanden.

Två av medarbetarna var tidigare utsedda informationsförvaltningssamordnare och deltog i regionens centrala informationssäkerhetsråd (se vidare nästa avsnitt). Då granskningen

[6] Fastställd av Lena Grudén 2024-11-11

genomfördes hade en av dem nyligen flyttat över till juridikavdelningen, där regionens centrala informationssäkerhetssamordnare är placerade. De intervjuade framför att hälso- och sjukvårdsnämnden i regel haft flera informationsförvaltningssamordnare.

På verksamhetsnivå finns runt 70 utsedda ”registeransvariga” som är kontaktpersoner och engagerade i respektive verksamhets lokala informationssäkerhetsarbete. Vår uppfattning är att dataskyddsfrågor är de registeransvariga primära ansvar, men att informationssäkerhet lagts till ansvaret. Registeransvariga utpekas som nyckelfunktioner och har en tät samverkan med nämndens informationsförvaltningssamordnare.

Strukturen, med verksamhetsområde digital vård och de registeransvariga, beskrivs ha skapats i syfte att både ha verksamhetsanknutna ”ambassadörer” som utför operativa, lokala uppgifter samtidigt som den centraliserade funktionen kan stötta chefer i mer strategiska beslut och driva större processer med bäring på informationssäkerhet och digitalisering. På operativ nivå har nämnden dock inte utvärderat eller på annat sätt analyserat eller bedömt om befintlig organisation omfattar tillräckliga resurser för att bedriva ett systematiskt informationssäkerhetsarbete.

Organisation under hållbarhetsnämnden

Kollektivtrafikavdelningen utgörs av fem enheter där varje enhet har en uttalad registeransvarig. De registeransvariga utgör en arbetsgrupp som hanterar och driver avdelningens informationssäkerhetsarbete. Gruppen leds av avdelningens informationsförvaltnings-samordnare vars ordinarie arbetsuppgift är chefssekreterare inom förvaltningsstaben.

Arbetsgruppen träffas regelbundet och arbetet uppges följa det centrala informationssäkerhetsrådets årshjul, men med verksamhetsspecifika anpassningar. Förutsättningarna för de registeransvariga ser lite olika ut avseende tid att lägga på uppgifter men beskrivs även påverkas av hur väl dessa känner till LIS och övrig kompetens inom dataskydd och informationssäkerhet.

Vidare finns inom avdelningen en separat systemenhet bestående av en enhetschef och en handfull anställda. Enheten driftar och utför systemförvaltning för de cirka 50 IT-system som tillhör verksamheten. Enheten beskrivs som delaktig i vissa informationssäkerhetsmoment, men besitter inte tillräcklig kompetens eller kunskap för att kunna genomföra sådana aktiviteter fullt ut självständigt. Det ges även uttryck för att avdelningens IT-verksamhet inte är fullt ut integrerad i regionens övriga IT-processer. Detta framstår som en konsekvens av att avdelningen driftar sina egna system medan beslut om inköp av nya system eller avtalsförlängningar tas i det centrala systemägarrådet där avdelningen för IT och verksamhetsstöd agerar kravställare å IT-verksamhetens vägnar.

6.2.4 Informationssäkerhetsråd och Systemägarråd

Samordningen mellan de centrala informationssäkerhetssamordnarna och informationsförvaltningssamordnarna kanaliseras genom informationssäkerhetsrådet. Informationssäkerhetsrådet nämns i både den övergripande riktlinjen för informationssäkerhet liksom i riktlinjen för roller och ansvar. Dock förtydligar inget av dokumentet rådets ansvar, mandat eller uppgift. Enligt information på intranätet i regionen har rådet tillsatts för att samordna arbetet kring informationssäkerhet och dataskydd i ett helhetsperspektiv.

Rådet består av representanter från samtliga förvaltningar (genom informationsförvaltningssamordnarna), IT-chef, IT-säkerhetsansvarig, chefsjurist, säkerhetsansvarig och chef för informationsförvaltningen.

Genom våra intervjuer har vi fått en samstämmig bild att informationssäkerhetsrådet är ett centralt forum med avgörande betydelse för samordning men också för exempelvis utbildningsinsatser. Vi har tagit del av informationssäkerhetsrådets årshjul vilket tagits fram i syfte att ge en systematik till arbetet. Vi har även tagit del av minnesanteckningar från rådets möten och kan genom det verifiera att det rådet träffas med regelbundenhet där de frågor som tagits upp ligger i linje med uppdraget om samordning och informationsdelning.

Det sker även samverkan inom ramen för regionens systemförvaltning där ett systemägarråd träffas månadsvis. Enligt Systemägarråd, rutin, Region Gävleborg så är rådets uppdrag att bereda och prioritera beslut kring Region Gävleborgs IT-landskap. Detta ska ske genom en gemensam helhetssyn för vilka utvecklingsinitiativ som ska resurssättas och uppföljning av fattade beslut. Intervjuade beskriver att samverkan har bidragit till att systemägarna i stor utsträckning stöttas av avdelningen för IT och verksamhetsutveckling i många av de operativa uppgifterna genom utsedda systemförvaltare och systemadministratörer.

6.2.5 Bedömning

Vår bedömning är att regionstyrelsen, hälso- och sjukvårdsnämnden samt hållbarhetsnämnden i allt väsentligt etablerat en organisation för informationssäkerhetsarbetet som är anpassad efter ledningssystemets omfattning.

Vi baserar vår bedömning på att det dels finns tydligt dokumenterad ansvarsfördelning, dels utgör grund för arbetet i praktiken. Även om vi bedömer organisationen som i allt väsentligt anpassad efter krav och behov ser vi ändå behov av att lyfta att vi ser risk för påverkan på arbetet genom den brist på samsyn som lyfts mellan de olika funktionerna. Det är därtill väsentligt att det inom respektive verksamhet säkerställs att utsedda funktioner har mandat och förutsättningar i arbetstid och kompetens för att utföra informationssäkerhetsarbetet på ett effektivt sätt.

6.3 RUTINER FÖR RISKHANTERING

6.3.1 Riskanalys

Enligt de övergripande riktlinjerna för informationssäkerhet ska regiondirektören och ledningsgruppen ha en uppdaterad lägesbild över identifierade risker avseende

informationshantering och besluta om hur dessa risker ska hanteras. Arbetet med lägesbilden ska när så är lämpligt samordnas med Region Gävleborgs övriga riskhantering.

Utöver ovan beskrivning har vi inte erhållit underlag i form av rutin eller instruktion som beskriver hur regionens rutiner eller metoder för riskanalyser inom informationssäkerhet ska genomföras.

Vi har tagit del av riskbedömning avseende regionens nuläge i relation till lagkrav samt ISO 27000-serien, som gjorts i form av en GAP-analys. Sammanställningar visar att arbetet är tillräckligt i vissa delar men för flertalet områden uppges som status att det inte är tillräckligt och måste hanteras. Det framgår inte av de underlag vi erhållit eller av intervjuer om genomförda riskbedömningar har rapporterats till regiondirektör eller ledningsgrupp så att de har en uppdaterad lägesbild, i enlighet med kravet i riktlinjerna. Underlagen saknar även uppgift om datum för bedömning, vem/vilka som deltagit. Riskbedömningen saknar även tilldelning av ansvar för att vidta åtgärder för områden som identifierats som otillräckliga.

Vi har även erhållit en dokumenterad riskanalys specifikt för hälso- och sjukvården. Enligt uppgift har de fått stöd av den tidigare informationssäkerhetssamordnaren i genomförandet. Analysen resulterade i ett antal förbättringsområden, däribland behov av utbildningsinsatser.

Inom avdelning IT och verksamhetsutveckling har flertalet genomlysningar gjorts genom självskattningar och mappning mot bland annat Myndigheten för samhällsskydd och beredskaps rekommendationer samt ”best practice”, det vill säga empiriskt förvärvade erfarenheter. Det har gjorts initiala analyser i relation till NIS2-regleringen.

Avdelningen har en priolista med sex-sju områden/åtgärder som bedöms vara högst prioriterade. Dessa har varit kända några år men det har saknats ekonomiska resurser för att vidta åtgärder.

6.3.2 Informationsklassning och riskbedömning för informationstillgångar

Av riktlinjen för informationssäkerhet anges att IT-säkerhetsåtgärder ska vidtas baserat på informationsklassning och riskanalyser. Ansvar för detta åligger informationsägaren medan resursägaren ansvarar för implementering av IT-säkerhetsåtgärderna.

Befintliga styrdokument saknar uppgift om huruvida någon särskild modell för informationsklassning och riskanalys ska användas. Vi har däremot tagit del av underlaget Processorienterad informationskartläggning (POIK) rutin för genomförande i Region Gävleborg[7]. I underlaget ingår informationsklassning och riskanalys (steg 6) samt införa nya eller kontrollera befintliga säkerhetsåtgärder (steg 7).

Summariskt handlar processen om att kartlägga vilka informationstillgångar som hanteras i olika arbetsprocesser. För informationsklassning finns en dokumenterad mall som ger konkret stöd för denna del av processen. Resultat av dessa genererar IT-säkerhetsåtgärder som ska baseras på en kravkatalog som är generisk för hela regionen. Avdelningen för IT- och verksamhetsutveckling höll på att ta fram denna då granskningen genomfördes och vi har tagit del av utkast till kravkatalog.

Vi har kunnat verifiera att arbetssättet är etablerat och vi har i granskningen tagit del av dokumentation från arbetet enligt POIK. Dock beskrivs arbetet ha kommit olika långt i verksamheterna. Inom kollektivtrafiken har samtliga informationstillgångar genomlysts och klassats. Inom hälso- och sjukvården finns exempel på processer där detta har genomförts men intervjuade uppger att det kvarstår arbete för att gå igenom samtliga informationstillgångar. En

[7] Processorienterad informationskartläggning (POIK) rutin för genomförande i Region Gävleborg, daterad 2025-05-25

orsak som nämns till att arbetet inte kommit längre är införandet av nytt journalsystem vilket krävt fokus från funktioner som behöver ingå i arbetet med POIK. Vi har tagit del av underlag för informationsklassning och riskbedömning för det nya journalsystemet.

I fråga om riskanalyser och informationsklassningar framgår av ovan nämnda GAP-analys att momenten inte genomförts i tillräcklig omfattning. Samstämmiga uppgifter i granskningen är dock att informationsklassning och riskbedömning är obligatorisk och sker med systematik vid nyanskaffning eller avtalsförlängning av IT-system. Som stöd vid inköp av IT-system finns också ett dokumenterat beslutsstöd som flera intervjuade hänvisar till, där även informationssäkerhetsaspekter beaktas.

6.3.3 Bedömning

Vår bedömning är att det endast delvis finns dokumenterade rutiner avseende riskhantering. Vi bedömer vidare att arbetet endast delvis genomförs med en tillräcklig systematik så att säkerheten är anpassad efter skyddsbehov hos informationstillgångar.

Vi baserar vår bedömning på att det saknas reglering för hur regionens övergripande rutiner för riskhantering ser ut. Vi bedömer därtill att arbetet inte sker tillräckligt formaliserat och strukturerat. Underlag saknar väsentliga uppgifter i syfte att fördela ansvar så att risker omhändertas för att nå en acceptabel nivå, nå lagefterlevnad eller krav i vedertagen informationssäkerhetsstandard som regionen har att följa. Det finns också väsentliga risker identifierade i underlag utan att dessa emotsetts med vidtagna åtgärder vilket kan innebära förhöjd risk för regionens säkerhet.

Vi bedömer att rutin för processorienterad informationskartläggning som etablerats kan bidra med väsentliga bedömningar och analyser i syfte att anpassa säkerhetsåtgärder utifrån behov och krav. Vi ser det som positivt att samtliga revisionsobjekt påbörjat arbetet. Samtidigt är det väsentligt att arbetet slutförs så att det inte finns informationstillgångar som inte genomlysts och har behov av säkerhetsåtgärder som ännu inte identifierats.

6.4 Rutiner för personalrelaterad säkerhet

6.4.1 Utbildning och information

Enligt den övergripande riktlinjen för informationssäkerhet ansvarar den centrala informationssäkerhetsfunktionen för att tillhandahålla obligatoriska utbildningar inom informationssäkerhet och dataskydd. Regionens medarbetare ansvarar för att genomföra de obligatoriska utbildningarna.

Uppföljning av genomförda introduktionsutbildningar visar att cirka hälften av alla påbörjade utbildningssessioner avslutats under respektive år.

År	Antal deltagare Informationssäkerhet	Antal slutförda utbildningar	Antal deltagare Dataskydd	Antal slutförda utbildningar
2023	1533	822 (54 %)	1507	836 (55 %)
2024	2117	1099 (52 %)	2052	1055 (51 %)

2025	874	347 (40 %)	872	374 (43 %)

Tabellen visar deltagarfrekvens i utbildningar inom informationssäkerhet och dataskydd. Källa: Region Gävleborg.

För hälso- och sjukvården visar uppföljning av utbildningar att 5500 medarbetare genomfört utbildning inom informationssäkerhet och cirka 4400 inom dataskydd. Datan i tabellen ovan kan därigenom tolkas som att flertalet medarbetare har genomfört utbildningen tidigare än de år som tabellen visar, men att dessa medarbetare därefter inte repeterat genomförandet med regelbundenhet.

Utöver ovan utbildning har vi tagit emot underlag för andra utbildningar riktade till olika målgrupper, exempelvis informationsägare, informationsförvaltningssamordnare samt registeransvariga inom olika verksamheter. Intervjuade anser att de utbildningar som tillhandahållits via den centrala informationssäkerhetsfunktionen fungerat bra. Chefer uppfattas även ha följt upp vilka anställda som har gjort utbildningarna.

Vi har tagit del av årsrapport för informationssäkerhetsarbetet. I rapporten presenteras en självskattning av informationssäkerhetsarbetet som kallas mognadsdialog. Dialogen är genomförd inom informationssäkerhetsrådet där informationssäkerhetschef ansvarat för sammanställningen. I rapporten har rådet bedömt att regionen uppnår ett betyg 4 gällande kompetens. För att nå betyg 4 krävs bland annat att ”*arbetssätt för utbildning sker enligt plan utifrån identifierade behov. Olika metoder används och utbildning och träning genomförs i alla relevanta processer utan personberoende. Verksamheten mäter och följer upp både deltagande och effekt. Även utbildningsprocessen följs och förbättras utifrån verksamhetens behov*”.

Utöver utbildningarna enligt ovan så framhålls de nätverk och råd som vi beskrivit tidigare som viktiga för både omvärldsbevakning och kunskapshöjande insatser för de nyckelfunktioner som deltar i dessa.

Andra informationsinsatser är bland annat nyheter på intranät under informationssäkerhetsmånaden eller på förekommen anledning för att uppmärksamma medarbetare på aktuella händelser eller information inom informationssäkerhet.

6.4.2 Bedömning

Vår bedömning är att det endast delvis vidtagits säkerhetsåtgärder för att säkerställa personalrelaterad säkerhet.

Vi bedömer att centrala funktioner i enlighet med sitt ansvar har tillsett att utbildningar inom informationssäkerhet och dataskydd är tillgängliga för olika målgrupper. Vi konstaterar dock att genomförande av utbildningar är bristfälligt och innebär risk att säkerhetskultur inom informationssäkerhet inte är tillräcklig. Vi noterar även att vår granskning av insatser inte är överensstämmande med bedömning som regionen själva gjort i årsrapport för informationssäkerhetsarbetet 2024. Vi bedömer att det medför risk att behov av utbildning, mätning av effekter samt justering av utbildningsprocessen inte utvärderas löpande i syfte att stärka regionens arbete med säkerhetsmedvetenhet och kunskap.

6.5 HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER

I Riktlinje för ansvar och roller framgår att det för samtliga IT-resurser ska finnas en incidenthanteringsrutin. Rutinen ska linjera med krav avseende dataskyddslagstiftning och Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Incidentrapportering ska följa regionens gängse rutiner för incidenthantering och ska genomföras av regionens centrala informationssäkerhetsfunktion.

Befintlig incidenthanteringsrutin[8] följer vad som anges i riktlinjen där incidentrapportering kravställs utifrån regulatoriska bestämmelser. Vidare anges att regionen ska utreda incidenter i syfte att minska risken för att de inträffar igen. För mer direkta åtgärder i syfte att reducera incidentens påverkan ansvarar informationsägaren.

Av incidenthanteringsrutinen framgår vidare att medarbetare ska anmälda misstänkta informationssäkerhetsincidenter, och att det ska ske via intranätet eller telefon eller e-post. Anmälningar via e-post och telefon tas emot och handläggs av regionens centrala informationssäkerhetsfunktion tillsammans med dataskyddsombud. Enligt uppgift är personuppgiftsincidenter vanligast förekommande.

De intervjuade uppfattar att anmälningsskyldigheten är väletablerade bland anställda. En förklaring som ges är att regionens tidigare informationssäkerhetssamordnare var drivande i att identifiera och tillse dokumenterade anmälningar av incidenter. Samstämmiga uppgifter i granskningen är att hantering av incidenter sköts centralt av informationssäkerhetsfunktionen.

En risk som lyfts av intervjuade är sammanblandning mellan avvikelsehantering och incidenter inom informationssäkerhet. När dessa anmäls som avvikelser fördröjs hanteringen då inte it-funktionerna får kännedom om dessa på samma sätt som när de anmäls enligt incidenthanteringsrutinen.

Enligt incidenthanteringsrutinen så ansvar informationsägaren för att genomföra åtgärder och kan i det ta stöd från IT-förvaltningen eller central informationssäkerhetsfunktion.

I praktiken beskrivs dock hanteringen främst vara att informationssäkerhetsfunktionen överlämnar incidenthanteringen till avdelning IT och verksamhetsutveckling som påbörjar teknisk analys och bedömning. Om incidenten är av användarkaraktär så analyserar informationssäkerhetsfunktionen detta och skriver en rapport som delges informationsägaren. Processen uppfattas som strukturerad och tydlig.

Enligt årsrapport för regionens informationssäkerhetsarbete 2024[9] utvärderades under året 50 informationssäkerhetsincidenter, varav 13 var anmälningspliktiga enligt lag. Många av incidenterna uppges ha härrört till ”Min Vård Gävleborg” och störningar i de digitala lösningarna.

Det skedde 219 personuppgiftsincidenter varav 60 var av karaktären att det krävdes en anmälan till Integritetsskyddsmyndigheten. Den enskilt största orsaken till att incidenter skett var den mänskliga faktorn, 155 av de 219 incidenter bedömdes bero på detta. Tekniska fel stod för 15 av incidenterna.

Vad gäller IT-säkerhetsmässiga åtgärder för att stärka förmåga och beredskap att hantera och reducera incidenter framgår att regionen saknar teknisk kapacitet att logga och övervaka försök till intrång och andra riskassocierade händelser. Försök att upphandla en extern leverantör för

[8] Rutin för hantering av informationssäkerhetsincidenter, daterad 2025-02-25
[9] Informationssäkerhet, årsrapport 2024, ej daterad

övervakning av IT-miljön uppges ha gjorts under tre års tid, och var även pågående då granskningen genomfördes. Den avgörande faktorn uppges vara ekonomiska resurser.

Avdelningen IT och verksamhetsutveckling hade vid tid för intervjuerna ett pågående arbete att formalisera och etablera interna incidenthanteringsprocesser. Arbetet hade emellertid inte blivit tillräckligt konkret och dokumenterat vid granskningen.

Vissa utmaningar för att få rutinerna på plats lyftes, bland annat olika regelverk och synsätt kring incidenter inom IT-verksamheten respektive hälso- och sjukvården. Därtill uppfattades det saknas tydlighet och enhetlighet kring hur incidenter ska anmälas och hanteras inom regionen.

Ett förbättringsområde som poängterades i intervjuer var att incidenter inte dokumenterades tillräckligt för att kunna användas i lärandesyfte, samt att den interna jourberedskapen inom it var bristfällig, vilket försämrar förutsättningarna för en effektiv incidenthantering.

6.5.1 Bedömning

Vår bedömning är att regionstyrelsen endast delvis har etablerade rutiner och arbetssätt för att effektivt hantera informationssäkerhetsincidenter.

Vi baserar vår bedömning på att det finns dokumenterad rutin och etablerade arbetssätt för processen att anmäla och utreda incidenter. Vi ser särskilt positivt på att central informationssäkerhetsfunktion har en samlad bild över inträffade incidenter då det kan utgöra en väsentlig information för att identifiera behov av förbättringsåtgärder på både regionövergripande nivå samt förvaltningsspecifik nivå.

Vi bedömer däremot att nuvarande tekniska förmåga samt organisation för beredskap för it-säkerhetsincidenter är bristfällig i relation till de hot och risker som föreligger mot särskilt hälso- och sjukvårdsverksamheter, med stor ökning av antagonistiska hot. Det finns därtill lagförslag som träder i kraft inom kort där övervakning och förmåga att hantera och avvärja cyberhot ingår.

Vår bedömning är att hälso- och sjukvårdsnämnden och hållbarhetsnämnden i allt väsentligt har etablerade rutiner och arbetssätt för att effektivt hantera informationssäkerhetsincidenter.

Vi baserar vår bedömning på att nämnderna har att efterleva den regiongemensamma rutinen vilket vi bedömer att de i hög grad gör. Vi noterar dock att det kan finnas behov av att ytterligare tydliggöra hur informationsägaren förväntas vara involverad i bedömning och analys av inträffade incidenter. Detta så att det finns en delaktighet och förståelse för de förbättringsåtgärder som det kan finnas behov av så att inte incidenter inträffar på nytt.

6.6 Uppföljning av informationssäkerhetsarbetet

6.6.1 Uppföljning av informationssäkerhet

Enligt den övergripande riktlinjen för informationssäkerhet ska uppföljning av Region Gävleborgs arbete med informationssäkerhet ske på ett regelbundet och strukturerat sätt samt utföras genom interna kontroller och revisioner av oberoende part.

Regiondirektören och regionledningsgruppen ska ha en lägesbild avseende risker och informationssäkerhet som är tillräckligt uppdaterad för att kunna fatta beslut om riskhantering.

I riktlinjen för ansvar och roller framgår vidare att den centrala informationssäkerhetsfunktionen har ett nyckelansvar avseende uppföljning. Funktionen ska två gånger per år sammanställa och rapportera informationssäkerhetsarbetet till regionens säkerhetschef. Denna rapportering ska inkluderas i den säkerhetsrapport som säkerhetschefen presenterar för regionstyrelsen och regiondirektören en gång per år.

Årsrapport för informationssäkerhet

I granskningen har vi tillhandahållits den skriftliga sammanställningen av regionens informationssäkerhetsarbete för 2024. Rapporten ger en översiktlig beskrivning där mognadsgrad inom ett antal områden presenteras tillsammans med uppställning av inträffade incidenter innevarande år. Rapporten har föreslagit två fokusområden för 2025.

1. Säkerställa specialistkompetens för det systematiska informationssäkerhetsarbetet.
2. Tillse att för de mest samhällsviktiga och kritiska processerna har fungerande kontinuitetshantering.

Enligt intervjuer tillsänds rapporten regiondirektör per e-post, samt delges regionstyrelsen för kännedom. Rapporten har inte föredragits muntligen för vare sig regionledningen eller regionstyrelsen.

Den reglering enligt ovan, att uppföljningen ska integreras i säkerhetschefens säkerhetsrapport, samt rapporteras till regionstyrelsen och regiondirektören är det ingen av intervjupersonerna som känner till.

Intern kontroll

I regionstyrelsens internkontrollplan 2025 ingår risken ”*att vi inte når lagkrav med informationssäkerhet och IT-säkerhet som förväntas av en region, vilket kan leda till oönskad sårbarhet genom obehörig eller otillåten behandling, förlust, förstöring eller skada genom olyckshändelse*”.

Internkontrollplanen saknar uppgift om ansvarig för kontrollen eller när kontrollen ska genomföras. Vi har i granskningen inte erhållit något underlag som presenterar resultat för kontrollen.

Hälso- och sjukvårdsnämnden och hållbarhetsnämnden saknar kontrollområden kopplat till informationssäkerhet i sina beslutade internkontrollplaner för 2025.

6.6.2 Övrig rapportering

Enligt muntliga uppgifter har it-säkerhetsfunktionerna på avdelning IT och verksamhetsutveckling tagit fram underlag till IT-direktören för en presentation hos regionledning och regionstyrelsen. Vi har dock inte kunnat verifiera genom underlag eller sammanträdesprotokoll att så har skett eller vad rapporteringen ledde till.

6.6.3 Kontroll av dataskyddsarbetet

Enligt riktlinjer för informationssäkerhet ska Region Gävleborgs dataskyddsombud genomföra fortlöpande kontroller, säkerställa att dataskyddet fungerar enligt ovanstående och, om så inte

sker, rapportera till personuppgiftsansvariga och regiondirektören samt i vissa fall till dataskyddsmyndigheten[10].

Vi har i granskningen inte erhållit några granskningsrapporter över personuppgiftsansvarigas efterlevnad till dataskyddsförordningen.

6.6.4 Bedömning

Vår bedömning är att regionstyrelsen, hälso- och sjukvårdsnämnden och hållbarhetsnämnden inte har säkerställt att det sker en regelbunden uppföljning av arbetet samt kontroll över att informationssäkerhetsarbetet efterlever lagkrav och interna beslut.

Vi baserar vår bedömning på att det finns tydliggjorda krav för uppföljning och rapportering av informationssäkerhetsarbetet på övergripande nivå. Vi bedömer dock att nuvarande former för uppföljning och rapportering inte efterlever beslutade rutiner. Vi bedömer att nuvarande underlag inte i tillräcklig nivå uppnår syftet att ge regiondirektör och regionledning en lägesbild avseende risker och informationssäkerhet för att kunna fatta beslut om riskhantering.

Förutom att nuvarande rapport är sparsam i omfattning saknas uppföljning av regionens behov av säkerhetsåtgärder inom de områden som ISO27002 ställer krav på, exempelvis it-säkerhet. Vi anser att fokusområden för 2025 i högre grad borde ha utgått från de riskanalyser och underlag som finns tillgängliga och inte på den självskattning av mognadsgrad som informationssäkerhetsnätverket genomfört.

Det saknas i nuläget tydlighet i styrande dokument avseende ansvar för nämndernas uppföljning och krav om rapportering. Någon strukturerad uppföljning och rapportering har inte genomförts inom vare sig hälso- och sjukvårdsnämnden eller hållbarhetsnämnden. Vi ser det som väsentligt att former för detta beslutas och att uppföljning sker då informationssäkerhetsansvaret följer verksamhetsansvaret.

[10] Enligt riktlinjer för informationssäkerhets benämning. Tidigare var tillsynsmyndigheten Datainspektionen, numera Integritetsskyddsmyndigheten.

7 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

Syftet med granskningen har varit att bedöma om regionstyrelsen, hälso- och sjukvårdsnämnden samt hållbarhetsnämnden säkerställt att informationssäkerhetsarbetet är systematiskt i enlighet med lagkrav och interna beslut.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen, hälso- och sjukvårdsnämnden samt hållbarhetsnämnden endast delvis säkerställt att informationssäkerhetsarbetet är systematiskt i enlighet med lagkrav och interna beslut.

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen att:

- Tillse att övergripande styrdokument för informationssäkerhet antas politiskt för att tydliggöra de förtroendevaldas viljeriktning och krav på förvaltningarnas arbete.
- Tillse att nuvarande LIS utvärderas, kompletteras och struktureras i syfte att säkerställa tillämpning av regionens regelverk inom informationssäkerhet.
- Besluta om riktlinjer för regionens övergripande riskhantering och tillse att riskanalyser minst årligen genomförs med inriktning på informationssäkerhet.
- Utvärdera nuvarande personalsäkerhetsåtgärder för att bedöma om de är tillräckliga och effektiva i syfte att etablera en säkerhetskultur i enlighet med beslutade riktlinjer för informationssäkerhet.
- Stärka styrningen av informationssäkerhetsarbetet där uppföljning och rapportering efterföljs av beslut om handlingsplaner för väsentliga och prioriterade förbättringsåtgärder.
- Utvärdera nuvarande it-säkerhetsåtgärder i relation till kommande lagkrav samt aktuella hot och risker, särskilt med beaktande på förmåga att upptäcka och hantera avvikelser i form av it-säkerhetshändelser.
- Säkerställa att uppföljning och rapportering genomförs i enlighet med beslutade rutiner samt tydliggöra krav på nämndernas ansvar för uppföljning och rapportering av informationssäkerhetsarbetet. I uppföljning bör kontroll av att de beslutade styrdokumenten efterlevs ingå.

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

- Slutföra arbetet enligt rutinen för POIK.
- Efterfråga förtydligande över nämndens ansvar för uppföljning av det egna informationssäkerhetsarbetet.
- Efterfråga förtydligande över på vilka sätt informationsägaren ska involveras i analys och bedömning av informationssäkerhetsincidenter samt vilka krav som finns för när nämnden ska få kännedom om inträffade incidenter.
- Etablera regelbunden, minst årlig, uppföljning informationssäkerhetsarbetet så att nämnden ges förutsättningar att fatta beslut om inriktning och förstärkningar.

Utifrån resultatet av vår granskning rekommenderar vi hållbarhetsnämnden att:

- Tillse att samverkan och samsyn stärks internt mellan funktioner för informationssäkerhet och systemenhet samt även mellan systemenhet och den centrala IT-funktionen.
- Efterfråga förtydligande över nämndens ansvar för uppföljning av det egna informationssäkerhetsarbetet.
- Efterfråga förtydligande över på vilka sätt informationsägaren ska involveras i analys och bedömning av informationssäkerhetsincidenter samt vilka krav som finns för när nämnden ska få kännedom om inträffade incidenter.
- Etablera regelbunden, minst årlig, uppföljning informationssäkerhetsarbetet så att nämnden ges förutsättningar att fatta beslut om inriktning och förstärkningar.

Datum som ovan

Azets Revision & Rådgivning AB

Jenny Thörn	Sofie Ernerudh
Verksamhetsrevisor	*Verksamhetsrevisor*

8 BILAGA 1

Följande funktioner har intervjuats för granskningen:

Säkerhetschef

Chefsjurist

Informationssäkerhetssamordnare

Avdelningschef på IT och verksamhetsutveckling

IT-säkerhetsarkitekt

Trafikdirektör

Chefssekreterare/Handläggare/Samordnare Kultur och kompetensförvaltningen

Regiondirektör

Utvecklingschef Hälso-och sjukvård

Verksamhetsutvecklare/e-hälsoutvecklare digital vård

Kvalitetssamordnare verksamhetsområdet digital vård.

Hållbarhetsnämndens presidium

Hälso-och sjukvårdsnämndens presidium

Regionstyrelsens presidium

9 BILAGA 2

Följande dokument har ingått i granskningen:

Säkerhetspolicy

Övergripande riktlinje för informationssäkerhet

Instruktion för e-post

Rutin för hantering av personer med skyddade personuppgifter

Instruktion för lagring och kommunikation i digitala kanaler

Instruktion för registrering i registerförteckning

Övergripande rutin för personuppgiftsbehandling

Reglemente för regionstyrelsen och nämnder

Riktlinje för ansvar och roller

Uppdrag VO Digital Vård

Region Gävleborgs systemförvaltningsmodell

Årshjul för informationssäkerhetsrådet

Informationssäkerhetsråd 2024-12-12

Informationssäkerhetsråd 20241114

Informationssäkerhetsrådet

Systemägarråd, rutin, Region Gävleborg

Processorienterad informationskartläggning rutin för genomförande i Region Gävleborg

POIK genomlysning ambulanssjukvården

Prioritering POIK

Riskanalys mall

Övergripande GAP-analys säkerhetsåtgärder

GAP-analys ISO 27001

Övergripande riskanalys avseende informationssäkerhet för Hälso- och sjukvården

Riskanalys för driftsättning Cosmic

Övergripande riskanalys informationssäkerhet o lagkrav Q1 2025

Generella kravkatalogen 1.0

Mall informationsklassning

Dataskydd statistik

Informationssäkerhet statistik

Informationssäkerhet årsrapport 2024

Rutin för hantering av informationssäkerhetsincidenter