Granskning av informations- och cybersäkerhet

Rapport

Region Gotland

KPMG AB

2023-09-18

Antal sidor: 27

Innehållsförteckning

1 Sammanfattning

KPMG har av Region Gotlands förtroendevalda revisorer fått i uppdrag att genomföra en granskning av regionens arbete för att upprätthålla en god informations- och cybersäkerhet. Granskningen syftar till att bedöma om regionstyrelsen, hälso- och sjukvårdsnämnden, socialnämnden och tekniska nämnden har säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Utifrån genomförd granskning bedömer vi att regionstyrelsen och nämnderna i allt väsentligt har säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vi gör bedömningen utifrån att regionstyrelsen har etablerat ett ledningssystem för informationssäkerhet som omfattar beskrivningar av processer och stödmaterial för det operativa arbetet. Styrande dokument är aktuella samt tydliggör ansvar och krav på hur informationssäkerhetsarbetet ska genomföras. Däremot saknas förvaltningsspecifika rutiner och vi bedömer att detta kan riskera att verksamhetsspecifika förutsättningar inte har beaktats tillräckligt.

Vi anser även att samtliga revisionsobjekt till stora delar har en ändamålsenlig organisation. Dock är vår bedömning att nuvarande organisationsstruktur påvisar en avsaknad av prioritering för informationssäkerhetsfrågor utifrån informationssäkerhetschefens roll och placering i regionen.

Vi bedömer att det verktyg som utvecklats och nyttjas som stöd för genomförandet av riskbedömning och informationsklassning säkerställer att tillgångarna klassas i förhållande till interna och externa krav som verksamheterna har att förhålla sig till. Dock är vår bedömning att samtliga revisionsobjekt behöver stärka det befintliga risk- och klassningsarbetet i enlighet med beslutad objektförvaltningsmodell då en avsaknad av kontinuitet i arbetet kan bidra till en ökad risk för sårbarheter i verksamhetssystemen. Riskbedömningar på verksamhetsnivå har främst gjorts som en del i internkontrollarbetet och vi ser en risk att informationssäkerhetsrisker inte i tillräcklig grad kan beaktas i den strukturen och risker kan missas som har betydelse för säkerheten på en övergripande nivå.

Som en del i regionens säkerhetsarbete och för att stärka regionens säkerhetskultur är vår bedömning att regionstyrelsen bör utveckla nuvarande insatser så att dessa sker med en regelbundenhet, är obligatoriska och även utifrån behov omfattar riktade utbildningsinsatser. Att medarbetare har en tillräcklig kunskap och medvetenhet är en avgörande faktor och kan bidra till att minska risken för att incidenter inträffar, dels interna risker på grund av felaktig hantering, dels externa risker då hotaktörer ofta riktar sig till medarbetare.

Regionstyrelsen har i huvudsak säkerställt att den tekniska säkerheten är ändamålsenlig inom regionen i relation till aktuella hot och risker. Systematiska uppföljningar och kontroller av vidtagna säkerhetsåtgärder har genomförts. Det finns även upprättade och dokumenterade reserv- och återgångsrutiner. Vi anser dock att regionen bör stärka sin förmåga för övervakning samt att säkerhetshändelser samlas i loggar i syfte att uppnå en mer effektiv hantering av hot och sårbarheter.

Vidare är vår bedömning att det verktyg som används i informationssäkerhetsarbetet ger tillräckliga möjligheter i syfte att kunna följa upp arbetet med klassningar samt vilka åtgärder som behöver vidtas i syfte att stärka skyddet.

Däremot anser vi att samtliga revisionsobjekt kan stärka uppföljningsarbetet genom att upprätta mål- och handlingsplaner för det fortsatta informationssäkerhetsarbetet, i syfte att ge en överblick över nuläge samt vilka erforderliga åtgärder som krävs för att uppnå eller bibehålla tillräcklig informationssäkerhet.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi regionstyrelsen att:

- Se över organisationsstrukturen avseende informationssäkerhetschefens roll och placering i regionen.
- Säkerställa att objektsförvaltningsmodellen och dess aktiviteter implementeras fullt ut.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.
- Säkerställ att regionövergripande utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
- Säkerställ att övervakning av it-system sker i tillräcklig utsträckning samt att säkerhetshändelser loggas.
- Säkerställ att inträffade incidenter analyseras i syfte att identifiera eventuella åtgärder som behöver vidtas.
- Följa upp informationssäkerhetsarbetet både på förvaltningsnivå och regionövergripande nivå i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi hälso- och sjukvårdsnämnden att:

- Säkerställa att objektsförvaltningsmodellen och dess aktiviteter implementeras fullt ut.
- Utvärdera behov av resurser i syfte att kunna etablera ett systematiskt informationssäkerhetsarbete som uppnår krav i NIS-direktivet.
- Se över behov av förvaltningsspecifika rutiner för informationssäkerhetsarbetet.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.
- Säkerställ att utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
- Följa upp informationssäkerhetsarbetet i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi socialnämnden att:

- Se över behov av förvaltningsspecifika rutiner för informationssäkerhetsarbetet.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.
- Säkerställ att utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
- Följa upp informationssäkerhetsarbetet i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi tekniska nämnden att:

- Säkerställa att objektsförvaltningsmodellen och dess aktiviteter implementeras fullt ut.
- Utvärdera behov av resurser i syfte att kunna etablera ett systematiskt informationssäkerhetsarbete som uppnår krav i NIS-direktivet.
- Se över behov av förvaltningsspecifika rutiner för informationssäkerhetsarbetet.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.
- Säkerställ att utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
- Följa upp informationssäkerhetsarbetet i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

2 Bakgrund

KPMG har av Region Gotlands förtroendevalda revisorer fått i uppdrag att genomföra en granskning av regionens arbete för att upprätthålla en god informations- och cybersäkerhet. Uppdraget ingår i revisionsplanen för år 2023.

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. Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Utvecklingen och den förändrade användningen av ny teknik innebär också att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. Den digitala utvecklingen måste följas av ett anpassat och balanserat säkerhetsarbete för att säkerställa att inte de system och digitala tjänster som nyttjas för informationshantering och lagring är exponerade och tillgängliga för cyberhot och angrepp. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer.

Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för kommunen. Det är således väsentligt att kommunen har en tillräcklig intern styrning och kontroll av sitt it-säkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att arbetet med informations- och it-säkerhet behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningen syftar till att bedöma om regionstyrelsen och nämnderna har säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Granskningen har besvarat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
- Har kunskapshöjande insatser genomförts så att en säkerhetskultur är etablerad?
- Sker ett systematiskt arbete med riskanalyser och informationsklassning?
  - Vidtas tekniska säkerhetsåtgärder som ett resultat av åtgärdsplaner från riskanalyser och klassningar?
- Finns ett systematiskt arbetssätt med it-säkerhetsåtgärder för central it-infrastruktur (nätverk, servrar, klienter mm.)?
- Finns en tillräcklig kontroll för att upptäcka eventuella hot om intrång eller andra säkerhetshändelser i it-miljön?

— Finns det en tillräcklig uppföljning av att de säkerhetsåtgärder som är vidtagna fungerar ändamålsenligt?
— Finns etablerade rutiner med tydliggjorda eskaleringsvägar vid säkerhetshändelser och incidenter?
— Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?
— Finns en etablerad uppföljning av informations- och it-säkerhetsarbetet som rapporteras till styrelse och nämnder med regelbundenhet?
    - Har styrelse utifrån genomförd uppföljning fattat beslut om åtgärder för att stärka informations- och cybersäkerheten?
    - Har nämnderna utifrån genomförd uppföljning fattat beslut om åtgärder för att stärka informationssäkerheten?

2.2 Revisionskriterier

Vi har i granskningen utgått från följande kriterier:

— Kommunallagens (2017:725) 6 kap. 6 §
— Tillämpbara interna regelverk, policys och beslut
— MSB:s metodstöd och rekommendationer avseende Ledningssystem för informationssäkerhet samt it-säkerhetsåtgärder
— Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster där detta är tillämpbart

2.3 Ansvarig nämnd och styrelse

Granskningen omfattar regionstyrelsens övergripande ansvar för informationssäkerhet och it- och cybersäkerhet samt regionstyrelsens, hälso- och sjukvårdsnämnden, socialnämnden och tekniska nämndens ansvar för informationssäkerhet i enlighet med verksamhetsansvaret för de informationstillgångar som hanteras inom respektive nämnd.

2.4 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer/avstämningar med berörda tjänstemän och politiker.

3 Inledning

3.1 Metodstöd för systematiskt informationssäkerhetsarbete och säkerhetsåtgärder

Som revisionskriterium i granskningen utgår vi från MSB:s metodstöd och rekommendationer för ett systematiskt informationssäkerhetsarbete och säkerhetsåtgärder med fokus på nedanstående områden.

Standard och krav

Metodstödet bygger på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien och då främst på SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 om ledningssystem för informationssäkerhet.

Ledningssystem för informationssäkerhet

Ett ledningssystem för informationssäkerhet (ofta förkortat LIS) är den del av ledningssystemet som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, som planering och uppföljning. Det innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och kontroller samt ser över styrdokumenten med jämna mellanrum.

Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare om vilka krav som ställs i arbetet. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer.

Ansvar och organisation

Metodstödet beskriver hur ansvaret för arbetet med informationssäkerhet bör fördelas i organisationen samt tydliggör betydelsen av ledningens förståelse och engagemang i informationssäkerhetsarbetet för att det ska lyckas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, chefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten. Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Utbildning och kommunikation

MSB:s metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet. Utbildning och kommunikation ökar också acceptansen av och förståelsen för de säkerhetsåtgärder som implementeras.

Riskanalys och informationsklassning

Genom en riskanalys ska verksamheten identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen. Riskanalyser kan göras verksamhetsövergripande, för en process eller för ett enskilt objekt. Risker och potentiella händelser som kan leda till negativa konsekvenser beskrivs och bedöms sedan avseende sannolikheten att de inträffar samt potentiella konsekvenser.

Metodstödet anger vidare att informationsklassning är en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet. Skyddsnivåerna beskriver säkerhetsåtgärder som informationens värde kräver. Identifierat behov av säkerhetsåtgärder utgör ett viktigt underlag vid exempelvis kravställning av tjänster, som interna och externa it-tjänster. De identifierade behoven av säkerhetsåtgärder bör dokumenteras i en åtgärdsplan. It-säkerhetsåtgärder rent tekniskt kan vara en del men klassningen kan även ha identifierat behov av kompletterande risk- och konsekvensanalyser, förbättrade rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Skyddsåtgärder

Informationstillgångar består av information och resurser som används för att hantera information. Själva informationen är den primära tillgången som ska klassas. Resurser som används för att hantera informationen, till exempel it-system och fysiska tillgångar, samt rutiner i verksamheten ska sedan utformas enligt skyddsnivåer som matchar klassningens resultat. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

I MSB:s föreskrift för säkerhetsåtgärder i informationssystem framgår att systemägaren behöver ha en dialog med berörda informationsägare inom organisationens olika verksamheter för att införa de säkerhetsåtgärder som ger rätt nivå av skydd för informationssystemet. Behovet av säkerhetsåtgärder identifieras utifrån de informationsklassningar och riskbedömningar som informationsägaren har genomfört, samt systemägarens egna riskbedömningar för informationssystemet.

MSB:s metodstöd beskriver att övervakning anger status för ett system, en process eller en aktivitet. Övervakning sker ofta kontinuerligt genom exempelvis att loggar i ett it-system övervakas och avvikelser automatiskt rapporteras. Övervakning och mätning görs för att bedöma om implementerade säkerhetsåtgärder har avsedd verkan och fungerar tillfredsställande.

Uppföljning och förbättringsarbete

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i organisationen behöver det ske en övergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning.

Resultatet från ledningens genomgång ska dokumenteras och bevaras.

3.2 Interna styrdokument

Enligt MSB bör ledningen se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan ledningen ge vägledning till chefer och övriga medarbetare över de krav och förhållningssätt som gäller i informationssäkerhetsarbetet.

I riktlinjer är det vanligt att det förs in bestämmelser om till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet
- incidenthantering
- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning

Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.

4 Resultat av granskningen

4.1 Styrning och organisering av informationssäkerhetsarbetet

4.1.1 Ledningssystem för informationssäkerhet (LIS)

Alla regioner har verksamhet som är identifierad som samhällsviktig och står under kraven i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, även kallat NIS-direktivet. I lagen ställs krav på att verksamheter som är identifierade som samhällsviktiga ska ha ett etablerat ledningssystem för informationssäkerhet, ett så kallat LIS.

Region Gotland som är en regionkommun, bedriver samhällsviktiga tjänster inom hälso- och sjukvårdsnämnden samt inom tekniska nämnden. Övriga nämnder inom den kommunala verksamheten är inte identifierad som samhällsviktig utifrån NIS-direktivet. Dock så ingår övrig verksamhet i den gemensamma it-infrastrukturen varpå ett systematiskt och riskbaserat informationssäkerhetsarbete behöver bedrivas.

Av Region Gotlands ledningssystem för informationssäkerhet framgår att det är informationssäkerhetspolicyn tillsammans med riktlinjer för informationssäkerhet som utgör grunden för regionens arbete. Policyn och tillhörande riktlinjer har nyligen reviderats och fastställdes av regionfullmäktige i juni 2023[1].

Som en del i ledningssystemet har regionen utvecklat ett eget informationssystem i syfte att vara ett stöd i informationssäkerhetsarbetet samt utgöra en samlad plats för dokumentation. Systemet används vid riskbedömning och klassning av verksamhetssystem och den information som hanteras i systemet samt för att dokumentera förvaltningsplaner. *Verktyget*[2] innehåller en kravkatalog som utgår från ISO 27000-serien för informationssäkerhet samt lagkrav som regionens verksamheter har att förhålla sig till. Intervjuade uppger att det finns en ambition att uppdatera kravkatalogen vid behov, exempelvis utifrån nya externa krav eller interna säkerhetsnivåer. Intervjuade uppger att kravkatalogen har uppdaterats med nya lagkrav som tillkommit över tid, exempelvis säkerhetsskyddslagen och Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Intervjuade ser dock en risk för att resursbrist påverkar hur snabbt uppdateringar kan genomföras efter förändringar.

Syftet med informationssäkerhetsarbetet är enligt policyn att skydda den information som hanteras inom regionens verksamheter och att arbetet därför ska vara prioriterat och bedrivas både metodiskt och långsiktigt. Målet är att information ska vara tillgänglig för den som har behörighet, att medborgare ska ha verksamhetsinsyn, att den personliga integriteten skyddas samt att regionen ska skyddas mot hot och intrång.

Av riktlinjer för informationssäkerhet konkretiseras policyn genom beskrivning av vad som måste etableras i syfte att uppnå policyns syfte och mål. Utifrån riktlinjerna ska varje förvaltning upprätta rutiner som detaljerat redogör för hur aktiviteter och säkerhetslösningar ska utformas och tillämpas i syfta att efterleva policy och riktlinjer.

[1] Protokoll, Regionfullmäktige, 2023-06-19, § 107
[2] Vidare i rapporten benämns detta som *verktyget*.

Vi har i granskningen inte erhållit förvaltningsspecifika rutiner men uppfattar att de övergripande styrdokumenten är kända och att verksamheterna utgår från dessa i sitt informationssäkerhetsarbete.

Enligt regionstyrelsens verksamhetsplan för 2023 ska en ny styrmodell implementeras. Med utgångspunkt i den nya styrmodellen ska enligt verksamhetsplanen ett ledningssystem utvecklas med styrande dokument. Intervjuade uppfattar att utvecklingsarbetet troligen kommer att påverka informationssäkerhetsarbetet då ledningssystemet för informationssäkerhet behöver kopplas ihop med det övergripande ledningssystemet samt inarbetas i ordinarie strukturer, arbetssätt och rutiner.

4.1.2 Regionstyrelsens övergripande ansvar för informationssäkerhet

Enligt Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster ska leverantörer utifrån identifierade risker och behov tydliggöra ledningens och övriga organisationens ansvar avseende informationssäkerhetsarbetet samt tilldela nödvändiga resurser, mandat och befogenheter för de funktioner som arbetet med informationssäkerhet kräver. Därtill ska leverantören säkerställa att informationssäkerhetsarbetet regelbundet och vid behov utvärderas och anpassas.

Av tidigare nämnda riktlinjer framgår att regionstyrelsen innehar det yttersta ansvaret för Region Gotlands informationssäkerhetsarbete och ska utarbeta, fastställa och följa upp riktlinje för informationssäkerhet. Det framgår även att ansvaret för informationssäkerhet är kopplat till det delegerade verksamhetsansvaret. Varje nämnd ansvarar därmed för att policy och riktlinjer efterlevs samt att det inarbetas i den egna verksamhetens lokala handlingsplaner och rutiner.

Av styrande dokument framgår att det är informationsägarna som ansvarar för hur informationen får hanteras och av vem. Informationsägarna ska klassificera informationen samt ange vilka lagar, regler, avtal och förordningar som informationen omfattas av.

Regionen har en informationssäkerhetschef som är organiserad under enheten för informationsförvaltning. Regionens informationssäkerhetschef har det övergripande och strategiska ansvaret att leda, samordna och utveckla informationssäkerhetsarbetet. Funktionen utgör vid tid för granskningen utifrån egen uppskattning 60 % av en heltidstjänst. De aktiviteter som funktionen fokuserat på har varit centrala delar så som revidering av styrande dokument och utbildningsinsatser. Funktionen har inte i sitt uppdrag att bistå i förvaltningarnas operativa informationssäkerhetsarbete och har i nuläget inte heller uppdraget att göra uppföljning eller kontroll av det informationssäkerhetsarbete som genomförs hos nämnder och styrelse.

Rollen informationssäkerhetschef har över tid bytt organisationstillhörighet inom regionen. Oaktad placering så uppfattar vi att det funnits utmaningar med tydlighet kring rollens uppdrag och mandat. Nuvarande organisering upplevs ha försvårat samverkan med funktioner med arbetsuppgifter som tangerar informationssäkerhet.

Utifrån beskrivningar i styrande och stödjande dokument kan vi konstatera att utsedda roller i regionens objektsförvaltningsmodell har ansvar i det operativa informationssäkerhetsarbetet. Ett antal roller finns etablerade i syfte att hantera it-

system på ett strukturerat sätt. Enligt riktlinjer för informationssäkerhet är det objektägarna som har det övergripande ansvaret för respektive system och dess användning och förvaltning. Vi har i granskningen tagit del av en beskrivning av Region Gotlands objektsförvaltningsmodell[3] som på en detaljerad nivå beskriver syfte med objektsförvaltning och hur arbetet inkluderar informationssäkerhetsarbetet. Intervjuade anger att modellen för objektsförvaltningen är känd i hela regionen och att ett arbete med att etablera roller och ansvar pågår men inte är slutfört vid tid för granskningen.

Regionens digitaliseringsavdelning är organiserad inom regionstyrelseförvaltningen och ansvar för drift av it-infrastrukturen. Inom avdelningen finns ett antal medarbetare som har högre kompetens inom it-säkerhet. Ansvaret är dock fördelat på flera funktioner inom avdelningen som arbetar utifrån perspektivet it-säkerhet inom respektive funktionsområde. Avdelningen har utöver detta en intern säkerhetsgrupp som hanterar aktuella frågor inom bland annat it-säkerhetsområdet som träffas månatligen.

Intervjuade beskriver att digitaliseringsdirektör under 2022 initierade ett uppdrag till extern konsult att göra en genomlysning av regionens it-styrning. Genomlysningen resulterade i ett antal rekommendationer avseende organisation och processer, däribland identifierades vissa brister inom informations- och cybersäkerhet. Denna genomlysning utmynnande enligt intervjuade i en samsyn hos koncernledningen om prioriteringar och aktiviteter. Det arbete som har genomförts uppges ha ett till att både informationssäkerhetsarbetet och arbetet utifrån objektsförvaltningen har utvecklats inom samtliga förvaltningar.

Som en del i att stärka det centrala stödet i regionens informationssäkerhetsarbete har ett forum kallat Arbetsgrupp informationssäkerhet (kallat Ag infosäk av företrädare från regionen). I gruppen ingår representanter från digitaliseringsavdelningen och samtliga förvaltningar. Ledningspersoner erhåller kallelser och medverkar utifrån behov. Gruppen innehar inget beslutsmandat utan ska fungera som råd och vägledande i informationssäkerhetsarbetet.

4.1.3 Regionstyrelsens och nämndernas verksamhetsansvar för informationssäkerhet och informationstillgångar

4.1.3.1 Regionstyrelsen

Intervjuade från regionstyrelseförvaltningen anger att genomlysningen av it-styrning under 2022 bidrog till ett förtydligande i ansvarsfördelningen samt att etablering av objektsförvaltningsmodellen kunde genomföras. Ledningsgruppen har etablerat en objektsstruktur i syfte att få en tydlig styrning av objektsförvaltningen.

Inom regionstyrelseförvaltningen saknas det en särskild funktion som arbetar med digitalisering eller it och vid behov av resurser efterfrågas detta från digitaliseringsavdelningen.

Informationssäkerhetschef är organiserad inom förvaltningen men som vi beskrivit tidigare så är inte chef operativ i arbetet på förvaltningsnivå.

[3] Upprättat dokument fastställdes av tf regiondirektör 2023-05-01.

4.1.3.2 Hälso- och sjukvårdsnämnden

Inom hälso- och sjukvårdsförvaltningen finns en digitaliseringschef samt en funktion som bland annat arbetar med informationssäkerhetsfrågor. Arbetet med informationssäkerhet uppges av förvaltningen vara i behov av fler resurser och stöd än de haft tillgång till för att kunna etablera ett systematiskt informationssäkerhetsarbete i tillräcklig utsträckning.

Det uppges även att utvecklingsarbetet har påverkats negativt av personalomsättning. Det arbete som pågår för att etablera objektsförvaltningsmodellen, kräver ytterligare resurser, rekrytering av dessa pågår vid tid för granskningen och beräknas vara på plats senast vid årsskiftet.

Intervjupersoner anger att förvaltningen det senaste året har genomfört ett strukturerat arbete, men att det fortfarande finns mycket kvar att göra.

De styrande dokument som upprättats på regionövergripande nivå upplevs inte alltid anpassade efter hälso- och sjukvårdsverksamheten, förvaltningen arbetar därför med att upprätta interna riktlinjer och rutiner som komplement.

4.1.3.3 Socialnämnden

Intervjuade anger att socialförvaltningen har etablerat objektsförvaltningsmodellens roller och ansvar samt grupperat samtliga objekt. Utöver detta har förvaltningen upprättat en objektstyrgrupp bestående av förvaltningschef, administrativ chef, avdelningschefer, representanter från it, chef för systemförvaltare samt förvaltningens utvecklingsledare. Gruppen träffas minst två gånger per år.

Socialförvaltningens utvecklingsledare arbetar med informationssäkerhetsfrågor inom förvaltningen och intervjuade anger att de får ett tillräckligt stöd från centrala funktioner i informationssäkerhetsarbetet.

4.1.3.4 Tekniska nämnden

Tekniska förvaltningen har en it-samordnare som bland annat arbetar med digitalisering och informationssäkerhetsfrågor inom den egna förvaltningen.

Vid intervjuer uppges att förvaltningen arbetar med att implementera ledningssystemet men att resursbrist har försvårat för förvaltningen att genomföra arbetet. Det har i sin tur påverkat förutsättningarna att nå en efterlevnad av NIS-direktivets krav. Intervjuade anger att de erhåller centralt stöd från Ag-infosäk utifrån behov. VA-verksamhetens säkerhetsansvarig sitter även med Ag-infosäk och intervjuade anger att de får hjälp med att identifiera förbättringsåtgärder inom den egna förvaltningen. Vissa roller i objektsförvaltningsorganisationen har funnits sedan tidigare men aktiviteter som behöver genomföras är i ett uppstartsskede.

Objektsförvaltningsorganisationen uppges ha varit etablerad sedan innan.

4.1.4 Bedömning

Vår bedömning är att regionstyrelsen har säkerställt att det finns aktuella styrdokument och att dessa tydliggör ansvar och krav på hur informationssäkerhetsarbetet ska genomföras. Regionstyrelsen har etablerat ett ledningssystem för informationssäkerhet som innehåller beskrivningar av processer och stödmaterial för det operativa arbetet.

Därtill har ett systemstöd utvecklats i syfte att samtliga verksamheter ska få stöd och vägledning i väsentliga processer i informationssäkerhetsarbetet. Vi konstaterar att systemstödet inkluderar en kravkatalog med både externa krav och interna krav på säkerhetsnivåer som regionens verksamheter måste förhålla sig till.

I nuläget saknas förvaltningsspecifika rutiner och vi bedömer att detta kan riskera att det för exempelvis hälso- och sjukvårdsnämnden och tekniska nämnden innebär att verksamhetsspecifika förutsättningar inte har beaktats tillräckligt.

Vår bedömning är att samtliga revisionsobjekt i allt väsentligt har säkerställt en ändamålsenlig organisation för informationssäkerhetsarbetet men att den i vissa delar har behov av att anpassas utifrån ledningssystemets omfattning och de krav som regionen har på ett systematiskt och riskbaserat informationssäkerhetsarbete.

Vi bedömer att organisationen skulle kunna stärkas ytterligare genom att regionstyrelsen och dess förvaltning ser över informationssäkerhetschefens roll och placering i regionen. Vi ser behov av att rollen stärks med ett tydligare uppdrag att leda, stödja, samordna och följa upp informationssäkerhetsarbetet i regionen. Nuvarande organisationsstruktur påvisar en avsaknad av prioritering för informationssäkerhetsfrågor inom regionen vilket riskerar att påverka mandat och uppdrag för rollen i förhållande till styrelser och nämnder.

Vi bedömer även att regionstyrelsen ur ett övergripande perspektiv samt hälso- och sjukvårdsnämnden och tekniska nämnden bör utvärdera nuvarande organisation så att roller och funktioner som är tillgängliga i informationssäkerhetsarbetet är anpassade utifrån externa krav och ledningssystemets omfattning. Detta avser bland annat roller i objektsförvaltningsmodellen men även om det finns behov av kompetensförstärkning för en intern samordning av informationssäkerhetsarbetet.

4.2 Riskbedömning och informationsklassning

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantör av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Utifrån detta har MSB rekommendationer avseende säkerhetsåtgärder i syfte att öka skyddet mot angrepp eller minimera eventuell skada. Rekommendationerna omfattar bland annat säkerhetsuppdateringar, säkerhetskopiering samt förmågan att upptäcka säkerhetshändelser.

4.2.1 Riskanalys

Riskanalyser genomförs som del i flera processer och på olika nivåer inom regionens verksamheter. Av riktlinjer för informationssäkerhet framgår att samtliga verksamheter ska genomföra regelbundna och systematiska risk- och sårbarhetsanalyser i syfte att ge underlag för krishantering i verksamheten.

Riskanalyser genomförs därtill som en del i styrelser och nämnders internkontrollarbete samt för enskilda informationstillgångar som en del i objektsförvaltningsarbetet (se avsnitt informationsklassning nedan).

Vi har i granskningen tagit del av regionstyrelsens riskanalys med tillhörande internkontrollplan för år 2023. Flera kontrollmoment syftar till att ge regionen förutsättningar att hantera samhällsstörningar och bli en mer robust och motståndskraftig organisation.

Flertal kontrollmoment som berör granskningsområdet är inkluderat i planen. Bland andra att system och applikationer införskaffas eller används utan genomförd informationsklassning. Som förslag på åtgärd är att regionstyrelseförvaltningens funktioner för dataskydd och informationssäkerhet ska fortsätta sitt arbete tillsammans med digitaliseringsavdelningen i syfte att utveckla arbetet inom informationssäkerhet och dataskydd. Regionstyrelsen har även valt att inkludera kontrollmoment inom informationsåtkomst, behörighet och it-tekniska säkerhetsåtgärder. Kontroller ska genomföras av digitaliseringsdirektör genom stickprov.

Vid tid för granskningen hade ingen uppföljning hunnit genomföras av kontrollmomenten.

4.2.2 Informationsklassning

Av riktlinjer för informationssäkerhet framgår att informationen som hanteras inom Region Gotland ska klassas i syfte att utgöra underlag för behov av skydd för informationstillgångar. I syfte att ge vägledning i klassningsarbetet har regionen tagit fram en guide[4] för informationsklassning.

Det framgår i guiden att objektsförvaltaren praktiskt har hand om förvaltningen av informationsmängden och informationssystemet. Klassningen ska ske utifrån perspektiven konfidentialitet, tillgänglighet, riktighet och spårbarhet samt följande konsekvensnivåer: försumbar skada, måttlig skada, betydande skada och allvarlig skada. Genomförd klassning ska dokumenteras i *verktyget*. I guiden finns en tydlig

[4] Version 04, daterad 2022-04-08

beskrivning av vad som ska ingå i dokumentationen. Det framgår vidare att klassning och riskanalys ska genomföras före upphandling av nya verksamhetssystem.

Det framgår i dokumentet för objektsförvaltning att årliga aktiviteter i årshjul för objektsförvaltning är att årligen i december uppdatera:

- Informationsklassningar
- Risk och sårbarhetsanalyser
- Förvaltningsplaner
- Återkommande revision

Intervjuade anger att de system som finns inlagda i *verktyget* är de som verksamheterna manuellt har registrerat och att det saknas en fullständig systemförteckning. Det finns därför en risk att verksamheterna nyttjar system som inte registrerats i *verktyget* och som därmed inte genomgår klassning och riskbedömning.

Som en del i granskningen har vi fått en genomgång av *verktyget* och den dokumentation som lagras där. Utifrån detta kan vi konstatera att samtliga revisionsobjekt löpande genomför de moment som det ställs krav på, nya klassningar har tillkommit och ett stort antal klassningar har uppdaterats i närtid. Enligt uppgift så saknas dock genomförda moment för att täcka regionens informationstillgångar.

Risk- och sårbarhetsanalyser är en del i arbetet för objekt och informationstillgångar och vid genomgången noterade vi att förvaltningsplaner finns tillgängliga i *verktyget*. Intervjuade uppger dock att det saknas förvaltningsplaner och att det arbete som pågår med att etablera objektsförvaltningsmodell och roller kan bidra i att fler planer registreras.

En risk som lyfts av intervjuade är att en bristande kunskap kan leda till att vissa klassningar inte är korrekt bedömda avseende skyddsvärde och de åtgärdsplaner som dessa genererar. Det upplevs finnas behov av att stärka förvaltningarnas kunskap i syfte att klassningarna som genomförs ska bli korrekta.

4.2.3 Åtgärdsplan

I guiden för informationssäkerhet framgår att klassningsarbetet genererar ett klassningsresultat och en revisionsplan. Detta resultat presenteras sedan i form av en åtgärdsplan med aktiviteter som verksamheten genomför utifrån relevans och behov inom en tre-årsperiod. Detta finns tillgängligt i det verktyg som regionen nyttjar för riskbedömning och informationsklassning.

Vi uppfattar dock av intervjuade att det förekommer att inte åtgärder vidtas som planen visat behov av, eller att behov inte kommuniceras till digitaliseringsavdelningen så att tekniska säkerhetsåtgärder kan etableras.

4.2.4 Styrelsen och nämndernas arbete med riskanalys, informationsklassning och åtgärdsplaner

4.2.4.1 Regionstyrelsen

Intervjuade anger att riskanalyser och informationsklassningen finns i *verktyget*, men det uppges saknas ett tillräckligt systematiskt arbete med att uppdatera dessa med årlig kontinuitet.

4.2.4.2 Hälso- och sjukvårdsnämnden

Intervjuade anger att förvaltningen har tagit del av den kartläggning som digitaliseringsavdelningen har gjort av sårbarheter i operativsystem och applikationer. Arbetet identifierade ett antal sårbarheter som genererade en handlingsplan och intervjuade anger att de mest kritiska riskerna har åtgärdats men att vissa väsentliga åtgärder kvarstår att hantera. Utöver detta har förvaltningen inte genomfört någon ytterligare riskanalys på verksamhetsnivå och intervjuade anger att det finns behov av att stärka riskanalysarbetet på regionövergripande nivå med tydligare metoder och exempelvis ett årshjul att följa.

Intervjuade anger att *verktyget* inte är kompatibelt med den verksamhet som bedrivs inom hälso- och sjukvårdsnämnden och förvaltningen därför arbetar med att upprätta egna rutiner för klassning av informationstillgångar. Vid tid för granskningen uppges att förvaltningsplaner finns för de större objekten samt att det finns behov av att komplettera för övriga objekt.

4.2.4.3 Socialnämnden

I intervju uppges att socialförvaltningen inte har medverkat i ett regionövergripande riskanalysarbete samt att förvaltningen inte har genomfört någon övergripande riskanalys på verksamhetsnivå. Intervjuade anger även att nämnden har gjort bedömningen att verksamheten inte omfattas av NIS-direktivet.

Intervjuade anger att klassning och riskbedömning görs i samband med att ett nytt system ska implementeras eller i det fall det sker organisatoriska förändringar. Vidare uppges att det finns behov av att stärka klassningsarbetet i samband med upphandling av ett system. Socialförvaltningen har även genomfört riskbedömning och klassning på samtliga av de system som är implementerade i verksamheten. Klassningsarbetet utgår från objektförvaltningsmodellen och uppdateras årligen.

Riskbedömning och klassningsarbetet uppges ha identifierat krav på nya säkerhetsskydd som förvaltningen arbetar med att införa. Efter resultat sker en kommunikation om säkerhetsåtgärder med digitaliseringsavdelningen.

4.2.4.4 Tekniska nämnden

I intervjuer framgår att det inte har genomförts någon riskanalys på verksamhetsnivå, utan att arbetet utgår från en övergripande riskanalys som genomfördes på ledningsnivå. Riskanalysen omfattar även andra verksamhetsområden och har därför inte endast perspektivet informationssäkerhet. Vidare uppges att förvaltningen arbetar med att upprätta riskanalys för samtliga objekt i objektens förvaltningsplaner.

I intervjuer framgår att det främst är kritiska system inom den tekniska förvaltningen som genomgått klassning. De system som saknar antingen en genomförd eller uppdaterad klassning uppges inte hantera känslig information och de har därför prioriterats bort till fördel för system inom exempelvis VA-verksamheten. I faktakontrollen framgår att det saknas upprättade förvaltningsplaner för objekt inom tekniska förvaltningens verksamhetsområde.

4.2.5 Bedömning

Vår bedömning är att regionstyrelsen genom styrande dokument för internkontroll samt inom informationssäkerhet har ställt krav på riskbedömning på verksamhetsnivå samt för system och information.

Riskbedömningar på verksamhetsnivå har främst gjorts som del i internkontrollarbetet och vi ser risker att informationssäkerhet inte i tillräcklig grad beaktas inom den strukturen. Utifrån lagkrav så ska organisationen regelbundet genomföra riskbedömning avseende informationssäkerhetsriskerna för att säkerställa att organisationen har förutsättningar att genomföra det systematiska informationssäkerhetsarbetet i enlighet med ledningssystemets krav. Vi noterar att det inom vissa verksamheter upplevs saknas tillräckliga resurser för att möta nuvarande kravställning.

Arbetet med riskbedömningar skulle kunna stärkas genom att etablera en gemensam riskmodell och tydliggöra hur riskarbetet ska genomföras både inom förvaltningarna och på regionövergripande nivå.

Vi bedömer att det verktyg som utvecklats och nyttjas som stöd för genomförandet av riskbedömning och informationsklassning säkerställer att tillgångarna klassas i förhållande till interna och externa krav som verksamheterna har att förhålla sig till. Vi noterar dock att hälso- och sjukvårdsnämndens verksamheter inte fullt ut uppfattar att de kan nyttja verktyget för de informationstillgångar som hanteras inom nämnden. Vi ser det som väsentligt att åtgärder vidtas i syfte att säkerställa att regionens samtliga tillgångar finns dokumenterade i verktyget och att åtgärder vidtas så att hälso- och sjukvårdsnämndens informationstillgångar registreras i det gemensamma verktyget.

Vidare är vår bedömning att styrelsen och nämnderna som omfattas av granskningen behöver stärka det befintliga risk- och klassningsarbetet i enlighet med beslutad objektsförvaltningsmodell och att tillgångarna registreras i verktyget så att förteckningen är aktuell och uppdaterad. Avsaknad av kontinuitet i arbetet kan riskera att bidra till ökad risk för sårbarheter i verksamhetssystemen som i sin tur kan leda till en ökad risk för intrång.

4.3 Säkerhetskultur

Av riktlinjer för informationssäkerhet framgår att samtliga anställda, förtroendevalda, utförare och konsulter löpande ska göras medvetna om sitt ansvar för informationssäkerheten. Vidare framgår att de även ska ges den kunskap i informationssäkerhet som behövs för att de ska kunna utföra sina uppdrag.

Innan coronapandemin bröt ut genomförde informationssäkerhetschefen egenutformade utbildningar som omfattade informations- och it-säkerhet. Utbildningen uppges ha genomförts för ca 2 200 anställda. Intervjuade anger att det därefter inte har genomförts några riktade utbildningar. I stället har material angående informationssäkerhet lagts upp på regionens intranät och det pågår ett arbete med att inkludera materialet i introduktionen för nyanställda. Det saknas däremot en formaliserad uppföljning för vilka som har tagit del av materialet.

4.3.1 Bedömning

Vår bedömning är att regionstyrelsen och samtliga nämnder inte har säkerställt en tillräcklig säkerhetskultur. De regionövergripande insatserna i syfte att stärka regionens säkerhetskultur kan utvecklas ytterligare och bör omfatta riktade utbildningsinsatser utöver nuvarande material på regionens intranät. Utbildningsinsatser bidrar till att öka kunskap och medvetenhet hos medarbetare och förtroendevalda, vilket i sin tur kan leda till att risken för att incidenter inträffar minskar.

Utbildningarna bör vara obligatoriska både för att säkerställa samtligas deltagande och för att regionstyrelsen genom detta påvisar vikten av att kunskapen kring informationssäkerhet ökas.

4.4 It-säkerhet

4.4.1 Riskanalys och omvärldsbevakning

Intervjuade anger att arbetet med it-tekniska säkerhetsåtgärder till viss del har utgångspunkt i riskanalyser, men bygger även på omvärldsbevakning genom nätverk med andra kommuner och regioner. Digitaliseringsavdelningen har även bevakning på den information som MSB samlar in och presenterar utifrån den omvärldsbevakning som myndigheten har i uppdrag att tillhandahålla.

Under 2022 genomförde digitaliseringsavdelningen en risk- och sårbarhetsanalys för it-infrastruktur och system. Vi har endast tagit del av muntlig information om sårbarheter och hur dessa har prioriterats och åtgärder vidtagits.

4.4.2 Implementerade skyddsåtgärder

Digitaliseringsavdelningen har utifrån genomförd risk- och sårbarhetsanalys och den åtgärdslista som MSB upprättat vidtagit flertalet åtgärder för att uppnå en säker it-miljö, bland annat följande:

- Nätverkssegmentering.
- Regelbunden installation av säkerhetsuppdateringar samt sårbarhetsskanning.
- Åtstramning av behörigheter. Antalet med höga behörigheter har minskat. Applikationer med känslig information hanteras med identifiering via e-legitimation. Utöver detta har multifaktorautentisering införts i vissa delar av regionens organisation som hanterar skyddsvärd information.

Utöver detta har Digitaliseringsavdelningen tillsammans med respektive förvaltning genomfört en kartläggning avseende de system som bör ses över med anledning av systemens ålder. Upprättade förvaltningsplaner ska hantera systemens livscykel vilket saknas för system och det uppges finnas föråldrade system som kan utgöra sårbarheter för förvaltningarnas informationstillgångar men även regionenens it-miljö på övergripande nivå.

Efter att verksamheterna har genomfört riskbedömning och klassning i *verktyget* genereras som tidigare nämnt en åtgärdsplan. I åtgärdsplanen framgår vem som ansvarar för genomförande av respektive åtgärd, exempelvis Digitaliseringsavdelningen eller verksamheten. Intervjuade uppger dock att det saknas en upprättad kommunikationsväg mellan verksamheterna och Digitaliseringsavdelningen när det finns en uppdaterad åtgärdsplan. Digitaliseringsavdelningen får därför manuellt gå in i systemet för att ta del av uppdaterad information.

Utifrån åtgärdsplanerna upprättas förvaltningsplaner för systemet och Digitaliseringsavdelningen upprättar SLA[5] mellan dem och berörd verksamhet. Det är sedan enligt objektsförvaltningsmodellen upp till objektsförvaltarna att följa upp att säkerhetsåtgärderna har införts.

[5] Service Level Agreement

Intervjuade anger att det inte har uppstått några hinder för att införa de säkerhetsåtgärder som har identifierats utifrån genomförda klassningar och omvärldsbevakning.

Digitaliseringsavdelningen har påbörjat ett utvecklingsarbete genom att utbilda egna medarbetare i syfte att kunna genomföra egna penetrationstester. I dagsläget genomförs externa penetrationstest på årlig basis. Utöver detta har socialförvaltningen beställt egna penetrationstester som utförts av extern leverantör.

4.4.3 Övervakning och säkerhetsloggar

Övervakning av it-miljön är automatiserad med i nuläget saknas en automatisk övervakning av säkerhetshändelser. För vissa typer av attacker finns automatiska funktioner implementerade genom externa leverantörer. Intervjuade uppger att det finns tillräckliga resurser för den manuella övervakningen, men att det finns behov att se över arbetssättet i syfte att eventuellt uppdatera dessa för att utöka omfattningen på övervakningen. Vid eventuella händelser skickas en automatisk varning till Digitaliseringsavdelningens beredskapsfunktion.

Regionen har utöver detta ett skanningsprogram som veckovis söker efter sårbarheter i it-miljön.

Den loggning som sker av aktiviteter i system och nätverk som övervakningen registrerar är i dagsläget spridd inom olika delar av infrastrukturen. Intervjuade uppger att Digitaliseringsavdelningen ser över de alternativ som finns för att införa en samlad loggningsfunktion.

4.4.4 Reserv- och återgångsrutiner

Regionen har etablerade rutiner för säkerhetskopiering för system och information som sker med en frekvens så att minimalt med information ska förloras vid avbrott.

Med anledning av att regionen har drabbats av driftstörning på central hårdvara har Digitaliseringsavdelningen tillsammans med hälso- och sjukvårdsnämnden samt socialnämnden upprättat en prioriteringsordning för respektive nämnds system.

Inom hälso- och sjukvårdsförvaltningen har det genomförts en kartläggning över reserv- och återgångsrutiner för kritiska system.

4.4.5 Bedömning

Vår bedömning är att regionstyrelsen i huvudsak har säkerställt att den tekniska säkerheten är ändamålsenlig inom regionen i relation till aktuella hot och risker. Vi ser behov av att regionen förstärker sin förmåga för övervakning och att säkerhetshändelser samlas i loggar för en mer effektiv hantering av hot och sårbarheter. Regionstyrelsen har säkerställt att reserv- och återgångsrutiner upprättats och att dessa är dokumenterade.

Vi bedömer att det genomförts systematiska uppföljningar och kontroller av vidtagna säkerhetsåtgärder för att upptäcka eventuella brister, genom exempelvis penetrationstester och regelbunden sårbarhetsskanning.

Vidare gör vi bedömningen att respektive styrelse och nämnd som omfattas av granskningen bör tydliggöra hur klassningsresultat ska kommuniceras till

digitaliseringsavdelningen när det finns behov av att etablera kompletterande tekniska säkerhetsåtgärder.

4.5 Incidenthantering

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantör av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

4.5.1 Rutiner

Av riktlinjer för informationssäkerhet framgår att Region Gotland ska ha ett system för rapportering av incidenter så att de blir dokumenterade på ett enhetligt sätt. Vidare framgår att regionen ska ha en etablerad kontakt med Sveriges nationella CSIRT (Computer Security Incident Respons Team). Detta saknas dock.

Regionstyrelseförvaltningen har tagit fram ett rutindokument som beskriver hantering av en större incident eller driftstörning. Bland annat framgår att ett incidentteam ska tillsättas samt att en incident manager ska tillsättas. I det fall regionen drabbas av en allvarlig störning som ger stora konsekvenser för verksamheten ska regionens tjänsteman i beredskap informeras av incident manager (digitaliseringsavdelningens rutiner).

Utöver detta finns rutiner i *verktyget* för hur en anmälan ska genomföras. Detta avser även NIS-incidenter. Dock uppger intervjupersoner att det saknas tydliga instruktioner för vad det är för typ av händelse som ska anmälas.

Intervjuade anger att det inom it finns rutiner och arbetssätt för eskalering och arbetsfördelning vid allvarliga händelser.

4.5.2 Arbetssätt och ansvar

Intervjuade anger att intern anmälan av en inträffad incident sker via *verktyget* eller via e-post till objektägare för *verktyget*. I *verktyget* får incidenten en ägare (incident manager) som sedan kan skapa underärenden för att på så sätt involvera andra funktioner som behöver bistå hantering av incidenten. Objektägare får även en notis om att incidenten har inträffat.

Incidenter som inkommer via e-post sänds vidare till objektägaren för det system som incidenten uppstått i.

Systemet saknar funktion angående kravställning att eskalera incidenter vidare internt. Detta innebär exempelvis att vissa funktioner inte automatiskt informeras vid en inträffad incident. Den kravställning som finns avser anmälan till berörd myndighet beroende på vilken typ av incident som inträffat.

Vidare anges att det finns en upplevelse av att antalet anmälningar är för få utifrån Region Gotlands organisationsstorlek och att det finns svårigheter med att sprida kunskap kring incidentanmälan. Intervjuade lyfter även att det i nuläget saknas en

tillräcklig tydlighet angående vad som är en incident och vad som medarbetarna är skyldiga att anmäla.

4.5.3 Dokumentation och uppföljning

Samtliga incidenter som anmälts internt finns lagrade i *verktyget*. Samtidigt lyfts att det i nuläget finns svårigheter med att sortera bland anmälda incidenter i *verktyget* och få en tillräckligt bra överblick.

Incidenter gås igenom i AG-infosäk men enligt uppgift sker inget strukturerat förbättringsarbete utifrån dessa utan lyfts främst som en information till de representanter som ingår i forumet.

4.5.4 Bedömning

Vår bedömning är att regionstyrelsen har etablerat incidenthanteringsrutiner som inkluderar hur incidenter ska dokumenteras och följas upp. Det finns tydliga eskaleringsvägar beskrivna i det verktyg som används vid anmälan om en incident.

Vår bedömning är att det finns behov av att tydliggöra vad som är en informationssäkerhetsincident, både i det verktyg som nyttjas samt genom kompetenshöjande insatser som utbildning. Syftet är att minska risken för att incidenter inträffar samt att säkerställa att kunskap finns om vad en incident är vilket ökar chansen för att dessa anmäls.

Utöver detta är vår bedömning att samtliga revisionsobjekt kan stärka arbetet med att analysera inträffade incidenter i syfte att identifiera eventuella åtgärder som behöver vidtas för att minska risken för att incidenten inträffar igen.

4.6 Uppföljning och återrapportering

Av 6 kap. 6 § Kommunallagen (2017:725) framgår att nämnder inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten. De ska även se till att den interna kontrollen är tillräcklig och att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Vidare framgår av MSB:s metodstöd att för att ledningen på en strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i kommunen behöver det ske en kommunövergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning. Resultatet från ledningens genomgång ska dokumenteras och bevaras.

4.6.1 Uppföljning

Utifrån den genomlysning som genomfördes år 2022 har koncernledningsgruppen aktivt arbetat med att etablera objekt och objektägareskap för system på ett övergripande plan inom regionen. Arbetet har även inneburit en översyn av befintliga system samt att avtal upprättats i syfte att identifiera och prioritera åtgärder mellan systemen.

Det saknas en dokumenterad styrning i Region Gotland avseende hur uppföljning av informationssäkerhetsarbetet och hur återrapportering till ledningsgrupp ska ske. I *verktyget* finns en samlad uppföljning angående de system som registrerats i systemet. Uppföljningen visar vilka system som har en uppdaterad klassning. Det går även i systemet att se när den senaste klassningen har genomförts.

Utöver den uppföljning som sker i *verktyget* görs ingen ytterligare samlad uppföljning i någon av de nämnder eller styrelser som granskningen omfattar. Det saknas även sammanställda rapporter/berättelser över det informationssäkerhetsarbete som sker, både i respektive nämnd och styrelse samt på regionövergripande nivå.

I intervju uppges även att det saknas en strukturerad uppföljning av att styrande dokument efterlevs.

4.6.2 Ledningens genomgång eller annan rapportering till styrelse och nämnder

Intervjuade anger att engagemanget kring informationssäkerhetsarbetet har ökat i regionens ledningsgrupper, men att det saknas ett formaliserat arbete för återrapportering till regionstyrelsen av den uppföljning som sker i *verktyget*. Vidare anges att regionstyrelsen inte har efterfrågat någon särskild rapportering från regionens informationssäkerhetschef angående informationssäkerhetsarbetet.

Intervjuade anger att det inom regionstyrelseförvaltningen har etablerats återrapportering till regionstyrelsen med anledning av ett ökat krav om återrapportering på grund av GDPR.

Inom hälso- och sjukvårdsförvaltningen sker ingen särskild återrapportering till ledningsgruppen avseende informationssäkerhetsarbetet.

Inom socialnämndens förvaltning sker en återrapportering till styrgruppen.

Inom tekniska nämnden genomför it-samordnaren återkommande muntlig återrapportering till förvaltningens ledningsgrupp.

4.6.3 Beslut om förbättringar

Det saknas en samlad mål- och handlingsplan för samtliga nämnder/styrelser samt på regionövergripande nivå som omfattas av granskningen i den uppföljning som verktyget *verktyget* genererar.

Med anledning av den genomlysning som genomfördes 2022 samt den utveckling som sker i omvärlden uppger intervjuade att medvetenheten och förståelsen för vikten av att ha en säker it-miljö har ökat, bland annat hos regionens politiker. Regionstyrelsen har därför i investeringsplanen[6] beslutat om att utöka Digitaliseringsavdelningens investeringsbudget. Det framgår av beslutet att mot bakgrund av det skärpta säkerhetsläget behöver Region Gotland investera, för att så långt som möjligt, säkerställa en fortsatt och säker drift av it-infrastrukturen. I intervju uppges dock att investeringsbehoven har bordlagts i väntan på besked om ekonomiska förutsättningar.

4.6.4 Bedömning

Vår bedömning är att det verktyg som används i informationssäkerhetsarbetet ger tillräckliga möjligheter i syfte att kunna följa upp arbetet med klassningar samt vilka åtgärder som behöver vidtas i syfte att stärka skyddet. Vi anser dock att det i befintliga dokument kan tydliggöras hur styrelser och nämnder ska följa upp informationssäkerhetsarbetet i syfte att utgöra en del av regionstyrelsens styrning inom området.

Vidare är vår bedömning att även samtliga nämnder och styrelser kan stärka uppföljningsarbetet genom att upprätta mål- och handlingsplaner för det fortsatta arbetet inom den egna förvaltningen. Sådana planer bidrar till att ge styrelsen/nämnden en överblick över nuläge samt vilka erforderliga åtgärder som krävs för att uppnå och/eller bibehålla tillräcklig informationssäkerhet inom den egna förvaltningen.

Vi anser även att den uppföljning som sker på regionövergripande nivå bör stärkas så att nuläge och förutsättningar för hela organisationen kan utvärderas i förhållande till hot och risker samt kontroll av efterlevnad av styrande dokument. Detta för att regionstyrelsen på en övergripande nivå kan fatta beslut om mål- och handlingsplan för erforderliga åtgärder.

[6] Långsiktig investeringsplan 2023–2032, Regionstyrelsen, 2022-01-024

5 Slutsats och rekommendationer

Vår bedömning utifrån granskningens syfte är att regionstyrelsen och nämnderna i all väsentlighet har säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vi gör bedömningen utifrån att regionstyrelsen har etablerat ett ledningssystem för informationssäkerhet som omfattar beskrivningar av processer och stödmaterial för det operativa arbetet. Styrande dokument är aktuella samt tydliggör ansvar och krav på hur informationssäkerhetsarbetet ska genomföras.

Vi anser även att samtliga revisionsobjekt till stora delar har en ändamålsenlig organisation. Dock är vår bedömning att nuvarande organisationsstruktur påvisar en avsaknad av prioritering för informationssäkerhetsfrågor utifrån informationssäkerhetschefens roll och placering i regionen.

Vi bedömer att det verktyg som utvecklats och nyttjas som stöd för genomförandet av riskbedömning och informationsklassning säkerställer att tillgångarna klassas i förhållande till interna och externa krav som verksamheterna har att förhålla sig till. Dock är vår bedömning att samtliga revisionsobjekt behöver stärka det befintliga risk- och klassningsarbetet i enlighet med beslutad objektförvaltningsmodell då en avsaknad av kontinuitet i arbetet kan bidra till en ökad risk för sårbarheter i verksamhetssystemen.

Regionstyrelsen har i huvudsak säkerställt att den tekniska säkerheten är ändamålsenlig inom regionen i relation till aktuella hot och risker samt att reserv- och återgångsrutiner upprättats och dokumenterats. Vi anser dock att regionen bör stärka sin förmåga för övervakning.

Vidare är vår bedömning att samtliga revisionsobjekt kan stärka uppföljningsarbetet genom att upprätta mål- och handlingsplaner för det fortsatta informationssäkerhetsarbetet, i syfte att ge en överblick över nuläge samt vilka erforderliga åtgärder som krävs för att uppnå eller bibehålla tillräcklig informationssäkerhet.

5.1 Rekommendationer

Utifrån våra iakttagelser och vår bedömning rekommenderar vi regionstyrelsen att:

- Se över organisationsstrukturen avseende informationssäkerhetschefens roll och placering i regionen.
- Säkerställa att objektsförvaltningsmodellen och dess aktiviteter implementeras fullt ut.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.
- Säkerställ att regionövergripande utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
- Säkerställ att övervakning av it-system sker i tillräcklig utsträckning samt att säkerhetshändelser loggas.

- Säkerställ att inträffade incidenter analyseras i syfte att identifiera eventuella åtgärder som behöver vidtas.
- Följa upp informationssäkerhetsarbetet både på förvaltningsnivå och regionövergripande nivå i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi hälso- och sjukvårdsnämnden att:

- Säkerställa att objektsförvaltningsmodellen och dess aktiviteter implementeras fullt ut.
- Utvärdera behov av resurser i syfte att kunna etablera ett systematiskt informationssäkerhetsarbete som uppnår krav i NIS-direktivet.
- Se över behov av förvaltningsspecifika rutiner för informationssäkerhetsarbetet.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.
- Säkerställ att utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
- Följa upp informationssäkerhetsarbetet i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi socialnämnden att:

- Se över behov av förvaltningsspecifika rutiner för informationssäkerhetsarbetet.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.
- Säkerställ att utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
- Följa upp informationssäkerhetsarbetet i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi tekniska nämnden att:

- Säkerställa att objektsförvaltningsmodellen och dess aktiviteter implementeras fullt ut.
- Utvärdera behov av resurser i syfte att kunna etablera ett systematiskt informationssäkerhetsarbete som uppnår krav i NIS-direktivet.
- Se över behov av förvaltningsspecifika rutiner för informationssäkerhetsarbetet.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.

— Säkerställ att utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
— Följa upp informationssäkerhetsarbetet i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

Datum som ovan

KPMG AB

Ida Larsson
Kommunal revisor

Jenny Thörn
Kommunal revisor

Magnus Larsson
Certifierad kommunal revisor
Kundansvarig