Granskning

Västra Götalandsregionens arbete med informations- och cybersäkerhet

Rapport
Västra Götalandsregionen

KPMG AB

Datum 2022-12-14

Antal sidor 49

Antal bilagor 2

Västra Götalandsregionen
Granskning av informations- och cybersäkerhet

2022-12-14

Innehållsförteckning

1 Sammanfattning

KPMG har av Västra Götalandsregionens revisorer fått i uppdrag att granska regionens arbete med informations- och cybersäkerhet. Uppdraget ingår i revisionsplanen för år 2022. Syftet med granskningen har varit att bedöma om nämnder och styrelser har en tillräcklig styrning och intern kontroll av informationssäkerhetsarbetet för att säkerställa att arbetet sker på ett ändamålsenligt sätt.

Vår sammanfattande bedömning utifrån granskningens syfte är att regionstyrelsen, inom ramen för sitt övergripande ledningsansvar, inte har etablerat en tillräcklig styrning av informations- och cybersäkerhetsarbetet. Det ramverk som utgörs av regionens ledningssystem för informationssäkerhet innehåller riktlinjer, rutiner och instruktioner för hur arbetet ska bedrivas men är i behov av revidering och komplettering för att informationssäkerhetsarbetet ska vara ändamålsenligt. Ledningssystemet har inte anpassats till lagar och regler som tillkommit efter år 2015. Därtill är beskrivningar av ansvar och roller i de styrande dokument som ingår i ledningssystemet inte överensstämmande med nuvarande organisation. Det innebär att funktioner och nyckelroller i arbetet, exempelvis Enhet säkerhet och beredskap samt Enhet cybersäkerhet, inte finns omnämnda i de styrande dokumenten. Vi ser därför en risk att otydlighet i roller och ansvar både på strategisk och operativ nivå kan leda till brister i genomförandet. Enligt beslut 2019 ska nya styrdokument fastställas, vi anser att regionstyrelsen brustit i sin uppföljning då detta ännu inte är verkställt.

Vår sammanfattande bedömning är att styrelsen för regionhälsan och fastighetsnämnden i huvudsak har en tillräcklig styrning av informationssäkerhetsarbetet för att säkerställa att det sker på ett ändamålsenligt sätt. Ansvar är tydliggjort och informationssäkerhetssamordnare finns utsedda, som tillsammans med informationsägare, i huvudsak utför informationssäkerhetsarbetet i enlighet med interna beslut.

Vår bedömning är att styrelsen för Skaraborgs sjukhus inte har en tillräcklig styrning av informationssäkerhetsarbetet och det i nuläget inte sker på ett ändamålsenligt sätt. Väsentliga aktiviteter som informationsklassning och riskbedömning har inte

genomförts i enlighet med interna beslut. Då inte heller utbildningar har genomförts i någon större utsträckning ser vi att det i nuläget finns en risk för informationshanteringen både ur ett tekniskt och ett organisatoriskt perspektiv.

Det saknas i nuläget i vissa delar inom samtliga revisionsobjekt ett systematiskt arbete för att identifiera, hantera och åtgärda risker för att säkerställa en robust informationshantering. Vi gör bedömningen utifrån att det för samtliga styrelser och nämnd som ingår i granskningen saknas en tillräcklig mognad och medvetenhet i respektive organisation i syfte att skydda information mot interna och externa hot. Detta då utbildningar inom informationssäkerhet inte har genomförts i tillräckligt hög grad för att en grundkunskap och förståelse för risker och hot ska finnas. Utifrån detta ser vi ett behov av att regionstyrelsen inför obligatoriska utbildningar för samtliga medarbetare och förtroendevalda i regionen samt att deltagandet följs upp på respektive förvaltning. Därtill bör nämnder utvärdera om det finns behov av kompletterande utbildningar utifrån den information och de risker som verksamheten hanterar.

Ur ett tekniskt perspektiv är vår bedömning att regionen har stärkt sin förmåga att identifiera och agera på risker, exempelvis cyberhot och intrångsförsök genom det arbete som cybersäkerhetsenheten har etablerat. De arbetssätt och metoder som nyttjas är i stora delar ändamålsenliga för att identifiera, hantera och åtgärda risker. Vi ser dock behov av att arbetet dokumenteras i högre grad för att minska risk att det finns ett personberoende i arbetsuppgifter eller att underlag saknas vilket kan leda till bristande förutsättningar att genomföra uppföljning av arbetet.

Vår bedömning är att samtliga revisionsobjekt har behov av en stärkt intern kontroll. I nuläget saknas kontrollmoment i samtliga internkontrollplaner för 2022 och det saknas en samlad uppföljning av regionens informationssäkerhetsarbete. Den uppföljning som genomförs och som presenteras bedömer vi inte vara tillräcklig i syfte att utgöra underlag för utvärdering och beslut om åtgärder. Utifrån detta är vår sammanfattande bedömning att det saknas en tillräcklig intern kontroll av informationssäkerhetsarbetet och att samtliga revisionsobjekt behöver vidta åtgärder i syfte att stärka sitt uppföljningsarbete så att arbetet sker på ett ändamålsenligt sätt.

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen inom ramen för sitt övergripande ledningsansvar att:

- Revidera och komplettera LIS i enlighet med granskningens resultat, främst med avseende på:
    - De kompletterande riktlinjer, planer och rutiner som enligt tidigare beslut fattade av regionstyrelsen och regiondirektören upprättas.
    - Gällande lagar, regler och nya krav inom området.
    - Beskrivning av ansvar och roller på både strategisk och operativ nivå så att det överensstämmer med nuvarande organisation.
    - Rutiner för uppföljning och kontroll.
- Säkerställa att det regelbundet genomförs obligatoriska utbildningar i informationssäkerhet för medarbetare.
- Förstärka uppföljning, intern kontroll och uppsikt av informationssäkerhetsarbetet för att säkerställa följsamhet till interna krav och gällande regelverk.
- Etablera en årlig rapportering från samtliga nämnder och styrelser i syfte att ge styrelsen en samlad bild av regionens informationssäkerhet.

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen, styrelsen för regionhälsan, fastighetsnämnden och styrelsen för Skaraborgs sjukhus att:

- Upprätta förvaltningsspecifika rutiner avseende hantering av behörighet som kopplar an mot de regionövergripande riktlinjerna samt säkerställa att kontroller av tilldelade behörigheter genomförs.
- Säkerställa att obligatoriska utbildningar som svarar mot verksamhetens behov genomförs och att deltagandet följs upp.
- Upprätta kontinuitetsplaner för att säkerställa verksamhetens fortgående vid en eventuell incident samt säkerställa att dessa testas med regelbundenhet.
- Vidta åtgärder i syfte att stärka uppföljningsarbetet samt upprätta former för kontinuerlig återrapportering till styrelse/nämnd av det informationssäkerhetsarbete som bedrivs.

Vi rekommenderar Styrelsen för Skaraborgs sjukhus att även:

- Säkerställa att riskbedömning och informationsklassning genomförs av den information som hanteras inom styrelsens verksamhet.

2 Bakgrund

Västra Götalandsregionen hanterar stora mängder känslig och skyddsvärd[1] information. Regionens verksamhet är i stora delar identifierad som samhällsviktig, vilket ställer höga krav på ett systematiskt och riskbaserat informationssäkerhetsarbete där ett ledningssystem för informationssäkerhet[2] är etablerat. Informationssäkerhet innebär att all skyddsvärd information ska vara tillgänglig, riktig, konfidentiell och spårbar. Informationssäkerhet är en fråga som inte bara berör verksamhetens ledning och säkerhetspersonal. Samtliga anställda i en verksamhet har ett ansvar för att uppnå och behålla en god informationssäkerhet. Det är därför viktigt att fördela och tydliggöra ansvar och roller i verksamheten samt att utbilda anställda i förhållande till arbetsuppgifter och ansvar.[3] Styrningen av informationssäkerhetsarbetet behöver vara integrerat i verksamhetens övriga former för styrning.

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

---

[1] Skyddsvärd innebär att informationen är värd att skydda med hänsyn till vad konsekvensen av skadan blir om tillgänglighet, riktighet och konfidentialitet röjs.

[2] Alla organisationer har ett ledningssystem, eller ett "system" för att leda verksamheten. Det handlar helt enkelt om hur ledningen styr verksamheten. Ett ledningssystem för informationssäkerhet (LIS) är den del av ledningssystemet som styr informationssäkerheten i verksamheten. Ett LIS innebär att organisationens ledning på ett systematiskt sätt kan styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra verksamhetens informationshantering. Ett LIS kan bygga på etablerade standarder inom området såsom ISO 27000-serien. Standarderna 27001 och 27002 i denna serie, visar hur ett LIS kan se ut och ger god ledning när det gäller vad som kan och bör ingå i organisationens LIS.

[3] Myndigheten för samhällsskydd och beredskap (2015). *En bild av kommunernas informationssäkerhetsarbete 2015* samt Riksrevisionen (2016). *Informationssäkerhetsarbete på nio myndigheter. En andra granskning av informationssäkerheten i staten*. RIR 2016:8.

och lagring är exponerade och tillgängliga för cyberangrepp. 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 regionen. Det är således väsentligt att Västra Götalandsregionen har en tillräcklig intern styrning och kontroll av sitt informations- och cybersäkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

Mot denna bakgrund har Västra Götalandsregionens revisorer beslutat att genomföra en granskning av regionens arbete med informations- och cybersäkerhet.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen har syftat till att bedöma om nämnder och styrelser har en tillräcklig styrning och intern kontroll av informations- och cybersäkerhetarbetet för att säkerställa att arbetet sker på ett ändamålsenligt sätt.

Följande revisionsfrågor besvaras i granskningen:

- Finns aktuella och ändamålsenliga styrande dokument som tydliggör krav och hur arbetet ska bedrivas?
- Är roller och ansvar tydliggjorda så att beslutad ansvarsfördelning upprätthålls?
- Har styrelser och nämnder säkerställt en tillräcklig mognad och medvetenhet i organisationen för att skydda information mot interna och externa hot?
- Finns ett systematiskt arbete för att identifiera, hantera och åtgärda risker och behov för att säkerställa en robust informationshantering?

- Genomförs systematiska uppföljningar och kontroller av vidtagna säkerhetsåtgärder för att upptäcka eventuella brister?
- Har styrelser och nämnder säkerställt en ändamålsenlig incident- och kontinuitetshantering?
- Finns etablerade uppföljnings- och rapporteringsrutiner i enlighet med krav i ledningssystem för informationssäkerhet?

Inom ramen för uttrycket *ändamålsenligt* avser vi att granska om det finns tillräckliga förutsättningar för verksamheterna, om verksamheterna lever upp till de krav och mål som gäller för verksamheten enligt riktlinjer och föreskrifter inom informations- och cybersäkerhetsområdet samt om ansvariga nämnder och styrelser har en uppföljning och kontroll mot dessa bestämmelser.

Inom ramen för ett *ändamålsenligt* informations- och cybersäkerhetsarbete avser vi även att granska om verksamheterna arbetar systematiskt med informationsklassning, riskanalyser, incidenthantering, kontinuitetsplanering samt uppföljning och kontroll, det vill säga bedriver ett systematiskt informations- och cybersäkerhetsarbete.

Granskningen kommer att omfatta de organisatoriska och administrativa aspekterna av informationssäkerhet samt att bedöma regionens förmåga att möta cyberhot.

Regionstyrelsen, styrelsen för Regionhälsan, styrelsen för Skaraborgs sjukhus och fastighetsnämnden är ansvariga styrelser och ansvarig nämnd för det som granskningen omfattar.

2.2 Revisionskriterier

Vi har bedömt om arbetet uppfyller

- Kommunallagens (2017:725) 6 kap. 1, 6§§
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster med tillhörande förordning och föreskrifter
- Policy för styrning i Västra Götalandsregionen (RS 2019–02491)
- Policy för säkerhet och beredskap (RS 2018–00129)
- Regionstyrelsens reglemente (2018–0353)

2.3 Metod

Granskningen har utförts genom dokumentstudier av regelverk och styrdokument samt intervjuer med ansvariga tjänstepersoner inom koncernkontoret och inom respektive förvaltning. För fullständig förteckning av dokument och regelverk se bilaga A. För fullständig förteckning av intervjupersoner se bilaga B.

Samtliga deltagare har getts möjlighet att faktagranska rapporten.

3 Resultat av granskningen

3.1 Styrande dokument

3.1.1 Bakgrund

Av regionfullmäktiges protokoll från 2018-11-27 framgår att regionstyrelsen har gett regiondirektören i uppdrag att under hösten 2018 presentera nya styrande dokument inom säkerhet och beredskap. Bakgrunden till uppdraget uppges vara att Västra Götalandsregionen har haft ett stort antal styrande dokument som rör säkerhet och beredskap och uppdraget är tänkt att leda till färre styrande dokument samt ny dokumentstruktur för området.

Den 27 november 2018 fattar regionfullmäktige beslut att anta Policy för säkerhet och beredskap[4] vilken beskrivs i avsnitt 3.1.2.

Av protokollet framgår att följande dokument då upphör att gälla från och med 2018-12-31:

- Säkerhetspolicy för Västra Götalandsregionen
- Regional strategi för säkerhetsarbetet i Västra Götalandsregionens verksamheter
- Krishanteringsplan 2015–2018
- Riktlinjer informationssäkerhet
- Säkerhetspolicy för publikt när i VGR

Regionstyrelsen fattade därefter beslut om en ny Riktlinje för informationssäkerhet[5]. Denna beskrivs i avsnitt 3.1.3.

[4] Fastställd av Regionfullmäktige, 2018-11-27

[5] Regionstyrelsen 2018-12-11, dnr: RS 2018–00129

Med anledning av att den nya säkerhetspolicyn samt de nya riktlinjerna för informationssäkerhet avsågs kompletteras med ytterligare riktlinjer och rutiner fattade regiondirektören ett verkställighetsbeslut[6] att återinföra tidigare regiongemensamma riktlinjer, rutiner och planer. Detta då de nya styrdokumenten inte var kompletta och det fanns risk för luckor mellan tidigare och nya styrdokument. Beslutet innebar att de tidigare styrdokumenten fortsatt skulle tillämpas fram till att nya styrdokument upprättats och fastställts.

Enligt beslutet fick Enhetschef säkerhet och beredskap ansvar för att nya regiongemensamma riktlinjer, planer och rutiner inom säkerhets- och beredskapsområdet skulle tas fram samt att upprätta en tidsplan med tillhörande prioritering.

I den bifogade listan med återinförda styrdokument finns den tidigare Säkerhetspolicyn inkluderad. Intervjupersoner uppger dock att den tidigare säkerhetspolicyn inte längre är gällande, utan att endast den nya policyn för säkerhet och beredskap ska ses som den gällande vid tiden för granskningen.

I regionstyrelsens reglemente[7] framgår att styrelsen ansvarar för att en effektiv och ändamålsenlig organisation upprätthålls samt att styrelsen får besluta om regiongemensamma riktlinjer och tillhörande rutiner och anvisningar inom området säkerhet och beredskap. Utöver detta ska regionstyrelsen utfärda de anvisningar till övriga nämnder och styrelser som följer av styrelsens roll att leda och samordna förvaltningen av Västra Götalandsregionens angelägenheter och ha uppsikt över verksamheten. Intervjuade bekräftar att inga nya styrdokument har upprättats och fastställts i enlighet med uppdrag i verkställighetsbeslutet. Den främsta orsaken till det uppges vara den resursbrist som funnits inom Enhet Säkerhet och beredskap samt att resurserna har behövt prioriteras för att hantera andra säkerhetsrisker, först utifrån pandemin och sedan utifrån Ukrainakrisen.

[6] Regiondirektör, verkställighetsbeslut, 2019-03-08, Dnr: RS 2019–01501

[7] Reglemente för regionstyrelsen i Västra Götalandsregionen, Regionfullmäktige, 10-11 juni 2019

3.1.2 Policy för säkerhet och beredskap

Policy för säkerhet och beredskap är enligt dokumentet det övergripande styrdokumentet för Västra Götalandsregionens säkerhetsarbete. Policyn innehåller grundläggande värderingar, principer och förhållningssätt för arbetet med säkerhet och beredskap i regionen. Policyn beskriver ansvarsfördelning vid särskilda händelser med eskaleringsvägar både på tjänstepersonsnivå och för den politiska nivån. Policyn saknar i övrigt reglering avseende roller och ansvar samt uppföljningsrutiner avseende säkerhetsarbetet.

3.1.3 Ledningssystem för informationssäkerhet, LIS

Det finns krav på att regioner, utifrån att de bedriver samhällsviktig verksamhet med krav om efterlevnad av NIS-direktivet[8], har ett etablerat ledningssystem för informationssäkerhet (LIS).

Västra Götalandsregionen har samlat sina beslutade riktlinjer, rutiner, anvisningar och mallar i ett LIS på intranätet. Ledningssystemet utgör de samlade krav som ställs i regionens informationssäkerhetsarbete. Styrningen utgörs främst av Riktlinje för informationssäkerhet, vilken beskrivs nedan.

Intervjuade ger en samstämmig bild att de känner till de krav som ställs i arbetet utifrån regionens etablerade LIS. Intervjuuppgifter gör därtill gällande att det finns behov av att revidera innehållet i LIS och etablera nya och uppdaterade styrdokument. Som vi angett tidigare i avsnitt 3.1.1 finns ett tilldelat uppdrag att revidera LIS och ett arbete är enligt uppgift uppstartat inom Enhet säkerhet och beredskap.

[8] The Directive on security of network and information systems vilken i Sverige införts i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Riktlinjer för informationssäkerhet 2015

Riktlinjer för informationssäkerhet antogs av regionstyrelsen 2015-09-01[9]. Av dokumentet framgår att riktlinjerna utgår från den tidigare Säkerhetspolicyn i Västra Götalandsregionen. Riktlinjerna omfattar hur informationssäkerhetsarbetet i regionen ska bedrivas samt beskrivning av roller och ansvar. Av dokumentet framgår dock att övergripande roller och ansvar regleras i den tidigare säkerhetspolicyn samt att koncernsäkerhetschefen ska utse en eller flera som ansvarar för informationssäkerheten.

Riktlinjen är omfattande med en detaljerad beskrivning av olika delar som ingår i informationssäkerhetsarbetet. Som vi nämnt ovan så ingår det därtill ett antal kompletterande riktlinjer, rutiner och instruktioner inom olika områden som ytterligare konkretiserar hur arbetet i regionen ska bedrivas.

Riktlinje för informationssäkerhet 2018

Den nya riktlinjen för informationssäkerhet antogs i december 2018 och är enligt dokumentet en övergripande ram för området och utgår från standarden för informationssäkerhet ISO 27 000. I riktlinjen regleras att varje nämnd och styrelse ansvarar för att det finns en förteckning av bland annat informationsägare och systemägare inom sitt verksamhetsområde. Riktlinjerna innehåller även en beskrivning av modell för informationsklassning.

IS/IT Styrmodell

Regionen har sedan 2019 en beslutad styrmodell för IS/IT, (Informationssystem/Informationsteknik). Styrmodellen beskriver hur olika delar inom VGR ska verka för att regionen som helhet ska nå effektiv användning och nytta av IS/IT som möjligt. Styrmodellen beskriver samverkan och samspel mellan

[9] Riktlinjer för informationssäkerhet i Västra Götalandsregionen, Regionstyrelsen, 2015-09-01,

verksamheterna och IT. Styrmodellen beskriver bland annat roller och ansvar, beslutsforum, beslutsstruktur och ärendegång.

Intervjupersoner uppger att styrmodellen för IS/IT inte längre är gällande. Det finns ett pågående utvecklingsarbete mot processtyrning i stället för den tidigare objektsstyrningen som varit etablerad. Vi har dock inte tagit del av några beslutade dokument som tydliggör den nya styrningen. Vi har däremot fått del av presentationsmaterial som beskriver förflyttning och nuläge i arbetet.

3.1.4 Bedömning

Vår bedömning är att regionstyrelsen inte har tillsett att det finns aktuella styrande dokument. Det finns för närvarande en otydlighet i gällande styrdokument med två säkerhetspolicys och två riktlinjer för informationssäkerhet som utgör styrningen parallellt. Majoriteten av styrdokument inom säkerhetsområdet har upphävts och sedan återaktualiserats genom verkställighetsbeslut. Vi bedömer att det är en brist i hanteringen att det inte vid tiden fanns en struktur och planering för inrättande av nya styrande dokument inom säkerhetsområdet. Det uppdrag som tilldelats att upprätta nya styrdokument har inte verkställts vilket innebär att regionens etablerade ledningssystem för informationssäkerhet inte är överensstämmande med regionens nuvarande organisation och de roller som är utsedda i det strategiska och operativa arbetet. Därtill saknas i nuläget anvisningar utifrån gällande lagar och regler inom området, exempelvis dataskyddsförordningen och NIS-direktivet. LIS är i behov av revidering och komplettering för att kunna utgöra en ändamålsenlig styrning som tydliggör krav och hur arbetet ska bedrivas. Regionstyrelsen har haft en bristande styrning i process för att upprätta nya styrdokument och har inte bevakat att detta verkställts av verksamheten. Vi anser därmed att regionstyrelsen inte lever upp till kraven i styrelsens reglemente angående ansvar att utfärda anvisningar till övriga nämnder och styrelsen utifrån styrelsens roll att leda och samordna förvaltningen.

3.2 Roller och ansvar

3.2.1 Regionstyrelsens styrning av ansvar

Riktlinjen för informationssäkerhet 2015 hänvisar till att det övergripande ansvaret för informationssäkerhet beskrivs i den tidigare Säkerhetspolicyn. Då denna ersatts av en ny policy för säkerhet och beredskap, där ansvaret inte finns beskrivet, saknas i nuläget dokumenterad ansvarsfördelning för regionfullmäktige, regionstyrelsen, regiondirektör, nämnder samt styrelser i informationssäkerhetsarbetet.

Av riktlinjer för informationssäkerhet från 2015 framgår ansvarsfördelningen avseende informationssäkerhet. Som utgångspunkt följer ansvaret för informationssäkerhet samt informationsägarskapet linjeansvaret i regionen.

I övrigt ser ansvarsfördelningen ut som följande enligt riktlinjer för informationssäkerhet 2015:

- Koncernsäkerhetschef – Ansvarar för informationssäkerheten.
- Personaldirektören – Ansvarig för att säkerhetskrav införs i personalhanteringsprocessen före, under och efter anställning.
- Fastighetsdirektören – Ansvarar för att kraven på fysiskt skydd beaktas i byggnadsprocessen.
- IS/IT-direktören – Ansvarar för att IT-säkerheten (teknisk säkerhet, ansvar och rutiner) motsvarar ställda krav.
- Chef inköpsorganisation – Ansvarar för att informationsägarens säkerhetskrav beaktas i inköpsprocessen.

Utöver detta beskrivs att koncernsäkerhetschefen utifrån ansvar för samordning och uppföljning leder ett informationssäkerhetsråd där sakkunniga, med mandat att företräda förvaltning, samt relevanta experter ingår.

Vidare ska det enligt riktlinjerna finnas ett regionalt riskhanteringsråd. Det framgår inte av riktlinjerna vilka som ingår i rådet, men rådet har som roll att bereda hot och risker som eskalerats till koncernsäkerhetschef som sedan regiondirektören eller lämplig

politisk församling beslutar angående. Enligt intervjupersoner finns riskhanteringsrådet vid tid för granskningen inte kvar i organisationen.

Utöver detta finns det roll och ansvar på förvaltningsnivå beskrivet. På varje förvaltning ska det finnas en samordnare för informationssäkerhet eller motsvarande. Denne har som uppgift att samordna och följa upp informationssäkerhetsarbetet i den egna verksamheten och rapportera direkt till förvaltningschefen.

Förvaltningschefen ansvarar för tillämpning av ledningssystemets regelverk i den egna förvaltningen, för att utforma lokala regelverk samt återrapportera status på informationssäkerhetsarbetet till nämnd/styrelse.

Verksamhetschefen ansvarar för att informationssäkerhet inom den egna verksamheten och ska se till att medarbetarna får utbildning i informationssäkerhet.

Genom dokumentgranskning kan vi konstatera att nuvarande organisation och ansvar inte överensstämmer med det som finns reglerat i riktlinjer och andra styrdokument. Omorganisationer inom koncernkontoret har genererat nya enheter och benämningar på vissa roller. Enheten för säkerhet och beredskap (ESB) är ny sedan 2015 och omnämns inte i styrande dokument, detsamma gäller för Koncernstab digitalisering som tidigare gick under namnet VGR IT, en förändring som skedde under 2021. Därtill pågår som vi beskrivit tidigare en förändring där den tidigare IS/IT-styrmodellen inte längre ska utgöra regionens objektsförvaltningsmodell, vilket även får en påverkan i informationssäkerhetsarbetet. Detta då roller enligt modellen innehar visst ansvar i det operativa arbetet. Nya roller som exempelvis regional processägare uppges inte vara definierat i nuläget och därigenom försvåras för verksamheten att etablera informationsägarskapet och det ansvar som följer med rollen.

3.2.2 Enheten för säkerhet och beredskap

Det saknas vid tiden för granskningen en dokumenterad uppdrags-, roll- och ansvarsbeskrivning för ESB. Enligt intervjuade är det dock enheten som har det övergripande ansvaret för regionens styrning och samordning av informationssäkerhetsarbetet. Den bemanning som finns inom ESB för arbetet med informationssäkerhet har funnits på plats sedan våren 2022. I arbetet ingår dock även

området säkra och robusta samband, bland annat inom signalskydd. Inom enheten finns en funktionsansvarig för informationssäkerhet och dataskydd. Funktionsansvarig har sedan april 2022 sex medarbetare som arbetar med informationssäkerhet, dataskydd, säkra kommunikationer samt säker lagring. Fram till december 2021 bestod funktionen av två medarbetar varav den ena var dedikerad till arbetet med FVM (Framtidens vårdinformationsmiljö).

Inom regionstyrelsens verksamheter har ESB samordningsansvar angående informationssäkerhetsarbetet. Det uppges i intervjuer att det inom enheten finns en samordnande tjänst som vid tid för granskningen innehas av en tillfällig resurs från annan enhet. Intervjupersoner uppger att det finns behov av att arbeta närmare verksamheterna i syfte att kunna identifiera verksamheternas behov.

Som tidigare nämnts har regionen haft en styrmodell för IS/IT. Enligt riktlinjer för informationssäkerhet anges en koppling mellan ansvariga roller i styrmodellen och roller i informationssäkerhetsarbetet. Då roller och processer är i förändring uppfattar vi av intervjuade att det skapar en viss otydlighet i hur ansvar i nuläget är fördelat och vilka som formellt är de rätta kontaktpersonerna inom olika frågor.

3.2.3 Koncernstab digitalisering

Det framgår i intervjuer att det som tidigare benämndes VGR IT har omorganiserats till koncernstab digitalisering. Omorganisationen har resulterat i att tidigare roll- och ansvarsbeskrivningar inte längre är aktuella. I nuläget saknas en dokumenterad beskrivning av uppdrag och ansvar för koncernstab digitalisering samt de enheter och funktioner som är organiserade inom staben.

Koncernstab digitalisering leds av en digitaliseringsdirektör och enligt den organisationsskiss vi tagit del av har staben ett övergripande ansvar för regionens IT-drift och säkerhet. Det tekniska säkerhetsarbetet hanteras inom avdelningen Infrastruktur och cybersäkerhet på cybersäkerhetsenheten. Cybersäkerhetsenheten består av två undergrupper där Revision/Kontroll/Analys är en och SOC (Security Operations Center) är en. SOC är en virtuell funktion som övervakar internettrafik, intern nätverksinfrastruktur, klienter, servrar, databaser, applikationer samt andra

system i syfte att identifiera potentiella säkerhetsincidenter. För hanteringen inom SOC finns en arbetsgrupp med tilldelade ansvar för förvaltning och utveckling av olika komponenter samt övervakning och loggkontroll.

Ett nära samarbete uppges finnas inom avdelningen för infrastruktur och cybersäkerhet och med övriga avdelningar inom koncernstab digitalisering då integrationer och komponenter i IT-miljön är beroende av varandra. Intervjupersoner uppger att det i nuläget saknas en sammanhållande resurs inom koncernstab digitalisering som kan hålla ihop övergripande frågor inom IT-säkerhet, exempelvis i form av en IT-säkerhetssamordnare. Det behövs bland annat forum att kunna hantera utbildningsbehov, samverkansbehov och andra mer generella frågor kring information- och cybersäkerhet mellan avdelningar.

3.2.4 Samordning

Intervjuade uppger att avsaknad av tydlighet och att den nya objektsstyrningen inte är fastlagd, utan endast testad i pilotverksamheter, är förenat med vissa risker inom informations- och cybersäkerhet. Det gäller särskilt när frågor behöver kommuniceras eller eskaleras kring sårbarheter eller hot. I intervjuer uppges att det inte har skett en tillräcklig kommunicering av de organisationsförändringar som genomförts vilket innebär en risk för att det saknas kännedom om ansvarsfördelning och uppdrag för olika avdelningar, enheter och den processtyrning som ska etableras i regionens verksamheter.

Intervjupersoner beskriver därtill att det finns behov av att definiera begreppet informationssäkerhet och de delar som ingår. Regionen har med nuvarande organisation separerat den administrativa informationssäkerheten från cybersäkerhet och IT-säkerhet, som båda tillhör informationssäkerhetsarbetet. Intervjuade menar att det i nuläget inte finns samsyn över hur arbetet ska organiseras och hur ansvarsfördelningen ska se ut. Enligt uppgift från intervjupersoner upplevs ett behov av att ha informationssäkerhetsfunktioner närmare digitaliseringsfunktionen, detta då en stor del av det praktiska informationssäkerhetsarbetet genomförs i nära anslutning till systemförvaltning och utveckling samt etablering av nya system och tjänster.

3.2.5 Styrelsen för Regionhälsan

Inom styrelsen för regionshälsans förvaltning är informationssäkerhetsarbetet organiserat utifrån följande:

- Dataskyddsombud – Är ett stöd för personuppgiftsansvarig. Kontrollerar att dataskyddsförordningen följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.
- Säkerhetsansvarig – Leder och skapar förutsättningar för säkerhetsarbetet inom Regionhälsans verksamhetsområde.
- Informationssäkerhetssamordnare – Arbetar med utveckling och förvaltning av informationssäkerhetsarbetet, identifierar risker och möjliga åtgärder, omvärldsbevakar utifrån nytillkomna lagar och regler.
- Jurist – Stöttar förvaltningen med tolkning av lagar samt bistår med bedömningar och utredningsarbete.

Intervjupersoner uppger att funktionerna informationssäkerhetssamordnare samt IT-chef innehas av verksamhetschefen för eHälsa och Säkerhet.

3.2.6 Styrelsen för Skaraborgs sjukhus

Inom förvaltningen för Skaraborgs sjukhus är det verksamhetschefen för Stöd och Service som innehar rollen som informationssäkerhetssamordnare sedan februari 2022. Det är förvaltningens jurist som innehar rollen som dataskyddsombud och förvaltningen har på grund av uppsägning rekryterat en ny jurist som tillträder i december. Utöver detta har även strategen på kvalitet- och utvecklingsenheten involverats i informationssäkerhetsarbetet och arbetar bland annat med att anmäla incidenter till IMY[10].

[10] Integritetsmyndigheten

Det framgår av intervjuer att det informationssäkerhetsarbete som sker inom förvaltningen har sin utgångspunkt i det som finns fastställt på regionövergripande nivå. Förvaltningen har därmed inte brutit ned och anpassat reglering och metoder.

3.2.7 Fastighetsnämnden

Inom fastighetsnämndens förvaltning Västfastigheter finns utsedd informationssäkerhetssamordnare som har i uppgift att leda och samordna det informationssäkerhetsarbete som sker inom Västfastigheter. Utöver detta medverkar samordnaren vid informationsklassningar och risk- och sårbarhetsanalyser samt ser över hur väl förvaltningens system hanterar informationen på ett säkert sätt. Informationssäkerhetssamordnaren involverar representanter från verksamheten vid bland annat informationsklassningar. Utöver detta söker samordnaren stöd regionalt om det finns behov av detta.

3.2.8 Bedömning

Vår bedömning är att regionstyrelsen genom styrande dokument har tydliggjort det linjeansvar som informationssäkerhetsarbetet utgår från. Granskade nämnder och styrelser har uppfattat linjeansvaret i enlighet med reglering i styrande dokument.

Vår bedömning är regionstyrelsen i övrigt har brustit i att tydliggöra roller och ansvar så att beslutad ansvarsfördelning upprätthålls i informationssäkerhetsarbetet. I nuläget överensstämmer inte de i praktiken etablerade enheter, funktioner, roller och processer med reglering i styrande dokument.

Utöver detta saknas dokumenterade uppdragsbeskrivningar för enheter inom koncernkontoret. Uppdragsbeskrivningar är viktigt för att internt kommunicera ansvar och gränsytor för en tydlighet mellan enheter och minimera att missförstånd sker. Vi ser det som särskilt viktigt att ansvarsfördelning och gränsytor mellan ESB och Enheten för cybersäkerhet tydliggörs då det finns en del närliggande frågor som kan behöva fördelas. Vi anser därmed att regionstyrelsen inte lever upp till kraven i styrelsens reglemente när det gäller ansvaret för att upprätthålla en ändamålsenlig organisation.

Utifrån ovan beskrivning anser vi att tydliggörande av roller och uppdrag bör prioriteras då otydligheten kan bidra till svårigheter att ställa krav samt att följa upp att ansvar upprätthålls i enlighet med interna beslut. Det kan därtill leda till att väsentliga delar i det systematiska informationssäkerhetsarbetet inte genomförs.

3.3 Riskhantering och informationsklassning

3.3.1 Regionövergripande

Informationsklassning

Av riktlinjen för informationssäkerhet från 2015 framgår att nämnder och styrelser ska klassificera sina informationstillgångar i syfte att avgöra lämpliga skyddsåtgärder. Utifrån riktlinjerna har dåvarande koncernsäkerhetschef upprättat en rutin för genomförande av riskanalys[11]. Rutinerna innehåller bland annat en detaljerad och tydlig beskrivning av bedömningsmetod i syfte att identifiera risker och analysera dess sannolikhet att inträffa samt konsekvens i det fall det sker. I VGR klassificeras information i fyra klasser och informationens skyddsbehov avgör skyddsnivå.

Av intervjuer framgår att ansvar för att informationsklassning genomförs, följer linjeansvaret och är därmed ett ansvar för förvaltningscheferna i regionen. Vidare uppges i intervjuer att klassningar till största del genomförs vid införande av nya system samt vid större förändringar av system. Av riktlinjerna från 2018 framgår att klassificering ska genomföras i samband med förändringar i organisation, process och teknik samt vid etablering av nya IS/IT-system eller IS/IT-tjänster som kan påverka informationshanteringen.

Intervjuade uppfattar att klassningar ska diarieföras, dock framhåller vissa att det kan vara förenat med risk vid de tillfällen där klassningar har bedömt att information har ett högt skyddsvärde som övergår diariesystemets acceptabla skyddsklass.

Vidare framgår av riktlinjerna från 2015 att det är resursägaren som ansvarar för att det finns tekniska lösningar och administrativa rutiner som motsvarar informationsägarens klassificering. Det framgår även att resursägaren ansvarar för att regelbundet uppdatera skyddsåtgärder och att dessa ingår som krav om verksamheten har externa leverantörer av IS/IT-tjänst.

[11] Rutin för riskanalys, koncernsäkerhetschef, 2015-11-09

Behörighetshantering

Av riktlinjerna för informationssäkerhet från 2018 framgår att nämnder och styrelser ska ansvara för att behörighet till informationstillgångar ges restriktivt och styras utifrån krav som arbetssituationen kräver. Intervjupersoner uppger att det pågår ett arbete med att se över hur ansvaret för behörighetshantering ska se ut och att det finns ett behov av att upprätta en behörighetsstruktur. Intervjupersoner uppger att ledningssystemet för informationssäkerhet behöver bli tydligare avseende behörighetshantering.

Regionen har infört multifaktorautentisering (MFA)[12] på vissa av regionens system. Ett inriktningsbeslut har fattats att införa MFA och arbetet bedrivs enligt intervjuuppgifter som ett projekt. Det framgår dock att det i vissa verksamheter har uppstått en problematik med anledning av att MFA införts per system vilket av verksamheten uppfattas leda till effektivitetsbortfall. För att komma vidare med införandeprojektet har inriktning gjorts att införa MFA på klientnivå (samtliga datorer), vilket uppges påverka verksamheterna mindre negativt.

3.3.2 Regionstyrelsen

Koncernkontoret har i arbetet med informationsklassning och riskhantering ett dubbelt ansvar. Dels som styrande och samordnande funktion, dels i arbetet med den egna informationssäkerheten. I det samordnande uppdraget framgår att ESB inte har genomfört någon uppföljning eller kontroller av de informationsklassningar som genomförts, vare sig inom koncernkontoret eller för övriga verksamheter. Det lyfts som en försvårande faktor att det i nuläget inte finns något systemstöd eller gemensam lagringsyta för de klassningar som har genomförts. I ett uppföljande syfte anges det därigenom alltför tids- och resurskrävande att få del av dokumentation av riskanalyser och informationsklassningar. Det pågår en förstudie för att undersöka hur behovet ser

[12] Multifaktorautentisering innebär att användaren bekräftar sin identitet med hjälp av flera identifieringsmetoder, exempelvis genom användarnamn och lösenord tillsammans med en engångskod via e-post.

ut och om det finns något systemstöd som regionen kan implementera för att få stöd för en större samordning av informationssäkerhetsarbetet.

Det är verksamheterna som genomför riskanalys tillsammans med representanter från koncernstab digitalisering. Intervjuade uppger att detta medfört att behov av tekniska säkerhetsåtgärder inkluderas direkt i samband med klassningen. Vid klassningarna finns en metodledare som ska leda arbetet. I vissa fall har metodledaren genomgått utbildning i klassningsmetoden men intervjupersoner beskriver även att det förekommer att metodledare utses på plats, trots att denne saknar utbildning.

Vi har i granskningen tagit del av exempel på genomförda klassningar och noterar att dessa har gjorts i enlighet med regionens beslutade anvisningar.

I dagsläget finns ett attestflöde där chef beslutar och attesterar, men i övrigt saknas en fastställd behörighetshantering inom koncernkontoret. Det finns vissa automatiserade processer vid tilldelning av behörigheter, men det finns behov av att förbättra behörighetshanteringen när det sker förändringar eller avslut av anställning. Intervjupersoner ser även att behörighetsmodellerna tydligare behöver kopplas gentemot informationshantering, informationssäkerhet och dataskydd.

3.3.3 Styrelsen för Regionhälsan

I sitt arbete använder förvaltningen regionala systemtillgångar för att hantera information och det framgår i intervjuer att klassificering av dessa system genomförs på regional nivå. I det fall förvaltningen vid risk- och konsekvensanalyser har behov, efterfrågas stöd från ESB.

I arbetet med informationsklassning deltar informationsägaren, representanter från verksamheten, representant från ESB, chefsläkare, samt jurist vid behov. Informationsklassningarna upprättas i enlighet med vad som anges i myndighetens dokumenthanteringsplan. Det uppges att omprövning av riskanalyser och klassning genomförs i enlighet med de regionövergripande riktlinjerna.

Förvaltningen har utifrån åtgärdsplaner vidtagit vissa åtgärder i syfte att minska risken för att angrepp sker. Bland annat nämns att programvaror som identifierats som osäkra har avinstallerats samt att förvaltningen har genomfört utökade utbildningsinsatser för medarbetarna. Uppföljning av IT-systemens sårbarheter uppges genomföras på regional nivå. Utbildningarna har genomförts och följts upp på arbetsplatsträffar i verksamheterna.

Intervjupersoner uppger att förvaltningen angående behörigheter använder sig av en checklista. Det genomförs i nuläget inga kontroller av tilldelade behörigheter.

3.3.4 Styrelsen för Skaraborgs sjukhus

Av intervjuer framgår att det har pågått ett arbete i syfte att påbörja riskbedömning och informationsklassning, men att detta inte har fullföljts. Det finns ett behov att se över vilka system som förvaltningen själv ansvarar för och vilka som regionen centralt ansvarar för.

Det framgår av intervjuer att behörigheter kopplat till roll samt enhet finns dokumenterat. Det uppges att systemförvaltare gör regelbundna lokala kontroller i syfte att se att behörigheterna stämmer överens med medarbetarens arbetsuppgifter. Linjeansvarig chef tilldelas en lista från systemförvaltaren med samtliga behörigheter som en påminnelse i syfte att se över att behörigheterna stämmer. Det uppges att det finns vissa svårigheter med att kontrollera behörigheterna, då kontrollerna sker manuellt. Det finns de medarbetare som kan ha dubbla behörigheter, där den ena behörigheten avser medarbetarens roll utifrån sin anställning och den andra avser exempelvis ett forskningsprojekt.

Utöver detta genomförs även loggkontroller i journalsystem i syfte att se om den aktivitet som ägt rum i systemet stämmer överens med medarbetarens arbetsuppgifter.

3.3.5 Fastighetsnämnden

Som tidigare nämnts är det informationssäkerhetssamordnaren som genomför risk- och sårbarhetsanalys samt informationsklassning tillsammans med representanter från verksamheten.

Av intervjuer framgår att arbetet har sin utgångspunkt i regionövergripande riktlinjer och rutiner. I syfte att göra modellen applicerbar på Västfastigheters verksamhet justeras modellen något med kompletterande frågeställningar som verksamhet upplever saknas i den gemensamma modellen. Det uppges att de regionala riktlinjerna och rutinerna naturligt har ett större fokus mot området hälso- och sjukvård då det är en övergripande majoritet av regionens verksamhet. Vidare uppges att det även sker justeringar avseende hur dokumentationen av klassningen ser ut i jämförelse med regionala riktlinjer och rutiner, detta i syfte att anpassa utifrån Västfastigheters verksamhet.

Klassning av information sker inom Västfastigheter i samband med större förändringar så som byte av teknisk miljö, förändringar i system eller nya funktionaliteter i befintliga molntjänster. I intervju uppges att det är objektförvaltarrollen som väcker frågan angående behov av ny informationsklassning, som sedan genomförs av informationssäkerhetssamordnaren tillsammans med objektförvaltaren. De klassningar vi tagit del av verifierar arbetssätt i enlighet med riktlinjer och rutiner. Vi ser även att klassningarna är aktuella och att ytterligare riskanalys har upprättats utifrån behov. Vidare finns föreslagna åtgärder för att möta risk till acceptabel nivå.

Intervjupersoner uppger även att det saknas tydlighet angående hur informationsklassningarna ska hanteras avseende diarieföring. Då klassningarna kan innehålla sekretessbelagd information finns det behov av ett IT-stöd där det finns möjlighet att lagra sekretessbelagda dokument.

För hantering av de åtgärder som framkommer i informationsklassning använder sig Västfastigheter vid tiden för granskningen av den tidigare styrmodellen för IS/IT.

Inom Västfastigheter är det funktionen teknisk förvaltare inom verksamhetsområde fastighetsförvaltning som hanterar tilldelning av behörigheter.

3.3.6 Bedömning

Vår bedömning är att regionstyrelsen har beslutat om styrande och stödjande dokument i syfte att det ska finnas etablerade metoder och arbetssätt för att riskbedöma och klassa den information som hanteras i regionen. Vi uppfattar att det i hög grad har bidragit till en tydlighet angående krav på informationsklassning.

Vi gör dock bedömningen att det i dagsläget till viss del saknas ett systematiskt arbete för att identifiera, hantera och åtgärda risker och behov av åtgärder för att säkerställa en robust informationshantering. Vi anser att den riskbedömning och informationsklassning som sker inom regionstyrelsens samt styrelsen för regionhälsans verksamheter behöver systematiseras ytterligare och genomföras vid andra typer av förändringar än enbart vid införande samt större förändringar av system. Nya riskbedömningar bör göras med en viss regelbundenhet för att dessa ska vara uppdaterade utifrån nya omvärldsfaktorer, hot eller exempelvis omorganisationer vilket kan påverka det totala skyddsvärdet för den information som hanteras. Utifrån detta gör vi bedömningen att regionstyrelsen och regionhälsan till viss del brister i efterlevnad av policy för säkerhet och beredskap samt efterlevnad av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster angående att agera proaktivt genom att identifiera och begränsa tänkbara hot, risker och sårbarheter.

Vi noterar att den riskbedömning och informationsklassning som sker inom fastighetsnämnden genomförs i enlighet med upprättade riktlinjer och rutiner. Vidare är vår bedömning att klassningarna är genomförda i syfte att möta nya behov utifrån eventuellt nytillkomna risker.

Vår bedömning är att styrelsen för Skaraborgs sjukhus inte har säkerställt att det finns ett systematiskt arbete för att identifiera, hantera och åtgärda risker och behov av åtgärder för att säkerställa en robust informationshantering, Detta då riskbedömning och informationsklassning inte har genomförts för den information som hanteras inom verksamheten. Det kan därigenom inte fastställas att den information som hanteras

inom sjukhuset och som styrelsen är ansvarig för har det skydd som det finns behov av. Här gör vi bedömningen att styrelsen för Skaraborgs sjukhus brister i efterlevnad av gällande regelverk.

För att ytterligare stärka förutsättningarna för ett systematiskt arbete med risker för en robust informationshantering i regionen anser vi att det bör beslutas om en gemensam hantering av dokumentation av riskbedömningar och informationsklassningar. Styrelser och nämnder bör därefter bedöma om det finns behov av alternativa lagringsytor utifrån en bedömning av informationens skyddsvärde.

Behörighetshantering är en väsentlig process för att säkerställa informationssäkerheten både internt och externt. Vi gör bedömningen att samtliga revisionsobjekt har behov av att stärka sin hantering av behörigheter genom att upprätta förvaltningsspecifika rutiner som kopplar an gentemot de regionövergripande riktlinjerna, då detta saknas. Vi ser även att samtliga objekt behöver säkerställa att uppföljande kontroller av tilldelade behörigheter genomförs i syfte att säkra att medarbetare inte har otillbörlig tillgång till information.

Utifrån Myndigheten för samhällsskydd och beredskaps (MSB) rekommendationer om stärkt cyberförsvarsförmåga bör regionstyrelsen efterfråga underlag för att kunna fatta beslut om regionövergripande införande av multifaktorautentisering. Underlag bör presentera en risk- och konsekvensanalys av införande av stärkta behörighetsrutiner där säkerhetsaspekter ställs mot den problematik med effektivitetsbortfall som uppfattats inom vissa verksamheter.

3.4 Medvetenhet och förståelse

3.4.1 Regionövergripande

Av riktlinjer för informationssäkerhet från 2018 framgår att nämnder och styrelser ansvarar för att medarbetare regelbundet får utbildning om vilka regler som gäller vid hantering av information. Det framgår dock av intervjuer att ansvaret för att utbildningar finns tillgängliga uppfattas ligga centralt på koncernkontoret. Koncernstab HR beslutar om vilka utbildningar i regionens utbildningsplattform som ska vara obligatoriska för alla medarbetare. Vi uppfattar av intervjuade att beslut fattats att utbildningen Digital informationssäkerhetsutbildning för alla (DISA)[13] är obligatorisk. I utbildningsplattformen finns även en säkerhetsskyddsutbildning från försvarshögskolan tillgänglig.

Koncernstab digitalisering arbetar med att komplettera nuvarande utbud med utbildningar inom cybersäkerhet. Som ett första steg erbjuds utbildningarna till chefer och andra ledare, men avsikten är att den ska distribueras ut i större omfattning i hela regionen i ett systemägarperspektiv.

I intervjuer uppges att det fortfarande finns en relativt låg mognadsgrad inom regionen. Det uppges att informationssäkerhet är ett aktuellt ämne på ledningsnivå, men att arbetet som bedrivs saknar systematik.

Intervjupersoner uppger att regionen under MSB:s säkerhetsmånad[14] har för avsikt att informera om informationssäkerhet via bland annat regionens intranät. Det uppges att det finns ett behov av att arbeta bredare med den här typen av frågor än endast genom utbildning i syfte att skapa en god säkerhetskultur och att arbetet under säkerhetsmånaden är en del i det.

[13] En kostnadsfri digital utbildning på grundläggande nivå som tillhandahålls av MSB.

[14] MSB bedriver tillsammans med Polisen en kampanj under temat ”Tänk säkert”. Arbetet har sin utgångspunkt i EU:s informationssäkerhetsmånad (oktober) och syftar till att öka medvetenhet om informations- och cybersäkerhetsfrågor hos allmänhet och företag.

Ansvaret för att följa upp antalet deltagare som genomgått en utbildning åligger förvaltningschef på respektive förvaltning.

3.4.2 Regionstyrelsen

Det uppges i intervjuer att medarbetare inom regionstyrelsens verksamhetsområde har erbjudits de utbildningar som finns på den regionala plattformen. Vidar uppges att det inte genomförs någon uppföljning på vilka medarbetare som genomfört utbildningarna.

3.4.3 Styrelsen för Regionhälsan

Intervjupersoner lyfter att det finns behov av att stärka medvetenheten om informationssäkerhet. Styrelsen behöver hållas informerad angående utveckling inom området.

Medarbetarna inom styrelsen för Regionhälsans verksamheter har erbjudits webbaserad utbildning, däribland DISA. Det uppges även att verksamheterna har delgetts regionalt framtaget material som är anpassat för presentation vid arbetsplatsträffar.

Intervjupersoner uppger även att säkerhet i olika perspektiv är inkluderat i förvaltningens nya utbildning för chefer inom Regionhälsan.

Det uppges att det inom förvaltningen saknas ett bra arbetssätt för att följa upp att medarbetare har genomfört utbildning. Ansvaret att se till att medarbetarna har en fullgod kunskapsnivå ligger på respektive enhetschef.

3.4.4 Styrelsen för Skaraborgs sjukhus

Intervjupersoner lyfter att det upplevs finnas en medvetenhet angående informationssäkerhet bland medarbetare inom Styrelsen för Skaraborgs sjukhus verksamheter. Upplevelsen bygger främst på att medarbetarna är aktiva med att anmäla uppkomna incidenter och risker för att en incident ska ske.

Det har inte genomförts någon särskild utbildningsinsats inom styrelsens verksamhetsområde kopplat till informationssäkerhet. Nyanställda medarbetare

genomgår de utbildningar som finns tillgängliga på regionens läroplattform och de intervjuade lyfter särskilt DISA-utbildningen utifrån granskningsområdet. Intervjupersoner uppger att det är obligatoriskt att genomgå utbildningarna samt att det är verksamhetschefens ansvar att följa upp detta. Det uppges inte har genomförts någon sammanställd uppföljning. Tidigare informationssäkerhetssamordnare har genomfört utbildning utifrån GDPR-lagstiftning vid behov.

Utöver detta uppges det även finnas informationsblad och liknande för medarbetaren att ta del av.

3.4.5 Fastighetsnämnden

Inom Västfastigheter genomgår samtliga nyanställda i samband med introduktion ett antal utbildningar som finns tillgängliga på den regionala läroplattformen. Bland annat finns som tidigare nämnts DISA samt säkerhetsskyddsutbildning tillgängligt på plattformen. Det framgår av intervjuer att det i dagsläget inte genomförs någon uppföljning på förvaltningsnivå över vilka som genomgått utbildningarna. Vidare lyfts att många av utbildningarna som tillhandahålls regionalt har perspektivet hälso- och sjukvård och det finns önskemål att detta kompletteras med utbildningar utifrån andra perspektiv.

Intervjupersoner uppger att det inom regionen har förts diskussioner om att införskaffa licens till ett plattformsverktyg som ger möjligheten att sätta ihop egna utbildningar utifrån verksamhetens behov och som även erbjuder interaktiva utbildningar. Det uppges att en sådan plattform skulle bistå Västfastigheter i de utbildningsbehov som förvaltningen ser.

Informationssäkerhetssamrodnaren medverkar även vid arbetsplatsträffar samt andra arbetsgrupper i syfte att informera om informationssäkerhet utifrån ett mer praktiskt perspektiv utifrån verksamheten.

3.4.6 Bedömning

Vi gör bedömningen att det för samtliga styrelser och nämnd som ingår i granskningen saknas en tillräcklig mognad och medvetenhet i respektive organisation i syfte att skydda information mot interna och externa hot. Det är få utbildningar som är obligatoriska och har endast genomförts i begränsad utsträckning. Vi gör genom det bedömningen att nuvarande insatser inte är tillräckliga för att etablera en medvetenhet och kunskap hos medarbetare.

Vi ser ett behov av att regionstyrelsen inför obligatoriska utbildningar för samtliga medarbetare och förtroendevalda i regionen samt att deltagandet följs upp på respektive förvaltning. Utbildningarna kan med fördel vara återkommande och innehålla interaktiva test. Därtill bör övriga nämnder och styrelser som omfattas av granskningen utvärdera om det finns behov av kompletterande utbildningar för sina medarbetare utifrån specifika verksamhetskrav och de informationstillgångar som hanteras. Detta så att inte information hanteras på ett riskfyllt sätt och kan leda till att incidenter sker.

Vi ser positivt på att regionen under MSB:s säkerhetsmånad har för avsikt att genomföra informationsinsatser angående informationssäkerhet. Vi gör dock bedömningen att arbetet med att informera medarbetarna bör ske återkommande och med tätare periodicitet än en månad om året.

3.5 Cybersäkerhet

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.

Som tidigare nämnts har VGR IT ombildats till Koncernstab digitalisering. Som vi beskrivit under avsnittet organisation finns inom staben Cybersäkerhetsenheten. Enheten etablerades i januari 2021. Bildandet föranleddes av en utredning i vilken övergripande information om krav och förväntningar på enheten framgår. Intervjuade uppger dock att krav på enhetens leveranser förändras kontinuerligt, beroende på aktuell hotbild och de åtgärder som behöver vidtas som ett resultat av dessa.

Arbetet med att etablera funktioner och processer har enligt intervjuade skett i hög takt mot bakgrund av det förändrade säkerhetsläget i omvärlden och en inre hotbild kring bland annat så kallad ransomeware. Det har inneburit att det i ett tekniskt perspektiv har funnits behov av att snabbt etablera viktiga funktioner för att stärka regionens cyberförsvar. Intervjuuppgifter gör gällande att många processer är etablerade men att arbetet i vissa delar behöver formaliseras och dokumentation upprättas.

Regionens förstärkta förmåga att upptäcka och agera på hot anges främst vara i form av etablering av en regelbunden övervakning och kontroll av IT-miljön för att identifiera sårbarheter. I arbetet ingår en regelbunden och rutinlagd sårbarhetscanning.

Enheten har infört en SOC-funktion med tekniska verktyg och organisation för att aktivt kontrollera det faktiska läget och agera om incidenter sker. Därtill har cybersäkerhetsenheten fattat beslut om att etablera funktionen Cyber security response team (CSRT), i vilken SOC är en viktig del. Funktionens huvuduppgifter enligt det beslutsunderlag vi tagit del av är att teamet ska ha kompetens för att ta ansvara för hanteringen vid särskilda säkerhetshändelser samt ha teknisk kompetens för att

analysera och aktivt hantera pågående eller inträffade incidenter. CSRT ska säkerställa förmåga att bevaka händelser och omvärld för att fatta beslut om aktivering av CSRT samt vid behov ta in ytterligare kompetens till dess att händelser är lösta.

Funktionen som etablerats ska agera inom alla typer av incidenter eller problem men aktiveras bara om händelsen bedöms akut påverka cybersäkerheten inom regionen negativt och det därför finns behov av central styrning och ett mycket skyndsamt agerande. Andra händelser som inte bedöms lika akuta åligger Cybersäkerhetscentret att förmedla vidare till berörd ägare. Vid allvarligare incidenter finns en nära dialog med funktionen IT-TIB och TIB (Tjänsteperson i beredskap).

En risk som lyfts från ansvariga inom cybersäkerhetsenheten är den pågående förändringen av IS/IT-styrmodell. Avsaknaden av modell och att tidigare etablerade roller har bytts ut har försvårat för enheten för cybersäkerhet att ställa krav på de som förvaltar verksamhetssystemen. Det medför att kommunicering av sårbarheter eller andra säkerhetshändelser kan sakna mottagare och krav därför inte tas omhand.

Som nämnts genomförs sårbarhetsscanning samt även penetrationstest av regionens system. Penetrationstest sker dock utan särskild periodicitet. Det uppges även att det finns behov av att upprätta former för att förmedla resultat av scanning till berörda systemförvaltare. Vidare uppges att regionen har för avsikt att införa sårbarhetsscanning som en beställartjänst, där systemförvaltaren eller systemägaren själv beställer en scanning av sina verksamhetssystem och applikationer och är mottagare av resultatet för vidare hantering. Enheten för cybersäkerhet behöver vid en sådan tjänst inte agera mellanhand och förmedla resultatet vidare. Det finns en upprättad dialog i syfte att kunna bygga upp processen för detta.

Regionen har vidtagit åtgärder i syfte att säkerställa att säkerhetskopior ska kunna återläsas utan att data förloras. Dock uppges att ansvaret för att data är korrekt åligger respektive system- och informationsägare. De behöver därför som en del i kontinuitetsarbetet verifiera sin information så att den är korrekt. Intervjuade uppger att det inte sker med någon systematik i nuläget.

3.5.1 Bedömning

Vår bedömning är att regionstyrelsen genom etableringen av en cybersäkerhetsenhet har tillsett att det för externa hot och intrångsförsök finns ett systematiskt arbete för att identifiera, hantera och åtgärda risker. Det finns både tekniska funktioner och personella resurser för att i tid upptäcka och agera vid cyberhot eller när andra sårbarheter identifieras. Det arbete som pågår bedömer vi är i enlighet med NIS-direktivets krav och MSB:s rekommendationer. Vår bedömning är även att det genomförs systematiska uppföljningar och kontroller av vidtagna säkerhetsåtgärder för att upptäcka eventuella brister, ex. penetrationstest och sårbarhetsscanning.

3.6 Incidenthantering och kontinuitetshantering

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.

3.6.1 Incidenthantering

Av riktlinjerna för informationssäkerhet framgår att det på varje förvaltning ska finnas ansvar och rutiner för rapportering, eskalering och uppföljning av informationssäkerhetsincidenter. Rutinerna ska även omfatta sårbarheter som kan förverkligas till incident.

Samtliga revisionsobjekt uppger att anmälan av incidenter sker i MedControl, oavsett vilken sorts incident som har inträffat. Intervjupersoner lyfter dock att MedControl inte är utformat i syfte att hantera incidenter avseende informationssäkerhet utan är ett avvikelsehanteringssystem, främst utvecklat för hälso- och sjukvårdsverksamheter. Det uppges därigenom finnas vissa svårigheter att snabbt bilda sig en uppfattning om de incidenter som anmäls. Det uppges finnas ett behov av ett rapporteringssystem som är mer anpassat för informationssäkerhetsincidenter.

Det är närmaste chef som avgör om en incident ska anmälas. Inom ESB finns en beredskap för att bevaka de incidenter som anmäls och som även eskalerar vidare till berörd verksamhet för hantering. Det är den berörda verksamheten som ansvarar för den vidare hanteringen av incidenten. Samtliga förvaltningar ska enligt riktlinjen ha en incidentansvarig och intervjupersoner uppger att rollen är etablerad inom regionen. Tekniska incidenter eskaleras vidare till systemägaren via TIB-organisationen.

I det fall incidenten uppstått i något av de regiongemensamma systemen är det enheten för säkerhet och beredskap som är mottagare. ESB kan även informeras i det fall det är en regionövergripande påverkan om incidenten skett lokalt.

ESB är incidentansvarig för regionstyrelsen, samtidigt som enheten har en samordnade roll för samtliga incidenter som inträffat i regionen. Då ESB har växt under det senaste året med fler antal medarbetare uppges att enheten nu har större möjlighet att utreda inträffade incidenter. Incidenterna dokumenteras i en aktivitetslista som sedan blir en del i det systematiska arbetet med att se över vilka åtgärder som behöver vidtas. Intervjupersoner uppger att ESB utifrån sin roll som samordnande kan ha en god överblick över incidenterna, medan detta är svårare för varje enskild förvaltning.

Intervjupersoner uppger att rutinerna för incidenthantering ska utökas med perspektivet cybersäkerhet.

Vid incidenter utanför kontorstid uppges att chefer tar kontakt med koncernstab digitalisering med frågeställningar angående sin verksamhets reservrutiner, vilket indikerar att verksamheter själva saknar kunskap angående detta. Det uppges finnas ett behov av att genomföra övningar av de upprättade reservrutinerna i syfte att säkerställa att rutinerna leder till förväntat resultat samt att rutinerna kommuniceras ut i verksamheten för kännedom. Intervjupersoner lyfter att det finns goda exempel i regionen där reservrutinerna fungerar väl och uppger att det främst handlar om certifierad verksamhet.

3.6.2 Kontinuitetshantering

Det framgår i policy för säkerhet och beredskap att regionen ska säkerställa kontinuitet genom att förebygga störningar och oönskade händelser i den dagliga verksamheten. Vidare framgår av riktlinjer för informationssäkerhet 2015 att inom ramen för verksamhetens arbete med kontinuitetsplanering ska en konsekvens- och riskanalys genomföras, för identifiera kritiska verksamhetsprocesser och krav på kontinuitet för dessa. Därefter ska organisationen identifiera vilka informationstillgångar, samt nivåer av tillgänglighet, riktighet, sekretess och spårbarhet som krävs för att de verksamhetskritiska processerna ska fungera som avsett. Även beroenden till nyckelpersoner för att upprätthålla verksamheten ska identifieras och dokumenteras i detta arbete.

Intervjupersoner uppger att det inom Enheten för säkerhet och beredskap organiseras en processansvarig som ansvarar för kontinuiteten inom VGR, men det åligger respektive verksamhet att ansvara för kontinuitetsplaneringen.

Samtliga revisionsobjekt saknar dokumenterade kontinuitetsplaner, men intervjupersoner uppger att det finns pågående arbeten inom vissa verksamheter. Det uppges i intervjuer att incidenter vid exempelvis systemuppdateringar har gett förvaltningen inom Styrelsen för Skaraborgs sjukhus kunskap om vilka system som är verksamhetskritiska. Det uppges att det inom förvaltningen finns reservrutiner men att dessa kan tydliggöras och dokumenteras i en kontinuitetsplan. Det saknas därmed dokumenterade anvisningar angående tillgänglighet och kontinuitet för systemen.

Inom Västfastigheter pågår ett kontinuitetsarbete inom driftsorganisationen som syftar till att upprätta reservrutiner. Förvaltningen har gentemot tidigare VGR IT upprättat ett SLA[15] för varje system i syfte att definiera vilken tillgänglighet som Västfastigheter förväntar sig av sina verksamhetssystem.

3.6.3 Bedömning

Av det som framkommer i granskningen gör vi bedömningen att det finns upprättade riktlinjer och rutiner för hur incidenter ska hanteras inom regionen. Av det som beskrivs i intervjuer gör vi bedömningen att riktlinjer och rutiner efterlevs. Vi ser att det kan finnas behov av att utvärdera att nuvarande avvikelsehanteringssystem är funktionellt och anpassat för regionens behov vid hantering av incidenter. Detta så att inträffade incidenter kan bedömas, analyseras och hanteras effektivt och med en tillräcklig dokumentation.

Vi gör även bedömningen att det finns en upprättad organisation i syfte att samordna inträffade incidenter och analysera dessa utifrån eventuella åtgärder som behöver vidtas, i enlighet med gällande regelverk.

[15] Service Level Agreement – serviceavtal som definierar tjänsterna som ska levereras, kvalitetsnivå samt vilken servicenivå som parten har rätt att förvänta sig.

Vi anser att samtliga revisionsobjekt har behov av att upprätta kontinuitetsplaner för att säkerställa verksamhetens fortgående vid en eventuell incident. Dessa bör därtill testas med regelbundenhet. Vi uppfattar att det i vissa delar saknas kunskap och förståelse för ansvar och behov av kontinuitetsplaner, vilket bör emotses med utbildningsinsatser för ansvariga. Vår bedömning blir därför att det till viss del finns brister i efterlevnad av policy för säkerhet och beredskap samt av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

3.7 Uppföljning och rapportering

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.

Av Policy för styrning i Västra Götalandsregionen[16] framgår att intern kontroll är en del av styrningen i regionen och ett redskap för ständiga förbättringar. Den interna kontrollen ska även säkerställa att regler och riktlinjer följs samt att rapportering och information i och om organisationen är tillförlitlig.

3.7.1 Intern kontroll

Regionstyrelsen

I regionstyrelsens internkontrollplan år 2022 saknas kontrollmoment som kan kopplas till granskningsområdet. Den riskanalys som ligger till grund för internkontrollplanen saknar även den risker kopplat till granskningsområdet.

Av regionstyrelsens internkontrollplan år 2021 framgår följande risker:

- VGR IT hanterar information felaktigt då verksamheterna som äger informationen inte har gjort informationsklassning eller risk- och sårbarhetsanalys.
- Information hanteras i molntjänster utan bedömning om det är lämpligt/lagligt. Det finns ingen överblick över vilka molntjänster regionen använder sig av. I många fall ändrar leverantörer sin leveransmodell från drift hos VGR till molntjänst.

[16] Beslutad av: Regionfullmäktige 2019-05-28 §104, dnr RS 2019-02491

- VGR publicerar information mot internet som är dåligt skyddade mot ID-kapning, intrång med mera.
- För att undvika att sprida skadlig kod eller virus från vissa delar av VGR:s IT-system till helheten, har vissa delar separerats från VGR:s normala IT-hantering så kallas nätverkssegmentering.
- Information hanteras felaktigt.
- RS har inte tillräcklig insyn i införandet av FVM[17] för att kunna utöva sin uppsiktsplikt.

Av uppföljningen av internkontrollplanen framgår att styrelsen har upprättat ett systematiskt arbete med informationssäkerhet i en gruppering med representation från IS/IT, chefläkare, säkerhetsansvarig på staben och jurist. Vid användning av journalsystem krävs säker autentisering via SITHS-[18]kort på alla datorer. En handfull större driftsstörningar inom telefoni och IT-system har fått stor verksamhetspåverkan. Behovet av en bättre kontinuitetsplanering samt en robust IT-miljö är tydlig. Arbetet med att genomföra förbättringar utifrån ett regionalt uppdrag gällande reservkraft och redundant IT-försörjning har påbörjats.

Inget av de kontrollmoment som fanns med 2021 är med i 2022 års plan. Intervjupersoner uppger att inför 2022 års plan prioriterades andra områden och kontrollmoment.

[17] Framtidens vårdinformationsmiljö

[18] Står för Säker IT Hälsa och Sjukvård och är en elektronisk identitetshandling som används för inloggning, signering samt säker åtkomst till, och kommunikation mellan, nationella vårdsystem och tjänster.

Styrelsen för Regionhälsan

I regionhälsans internkontroll för 2022 saknas riskområden som kan kopplas till granskningsområdet. I regionhälsans internkontrollplan för 2021 framgår följande riskområden som kan kopplas till granskningsområdet:

- Uppfyller inte kraven i Dataskyddsförordningen (GDPR)

Av uppföljningen framgår att det finns behov av en bättre kontinuitetsplanering samt en robust IT-miljö och att ett arbete har påbörjats med att genomföra förbättringar utifrån ett regionalt uppdrag gällande reservkraft och redundant IT-försörjning.

Styrelsen för Skaraborgs sjukhus

I internkontrollplan för 2022 saknas riskområden samt kontrollmoment som kan kopplas till informationssäkerhet. I internkontrollplan avseende år 2021 finns följande kontrollmoment:

- Svårigheter att säkerställa webbaserad information/integritet, sekretessbrott.

Kontrollen avser ärenden till Datainspektionen och uppföljningen visade att inga eller få avvikelse identifierades och att åtgärder inte behöver vidtas.

Fastighetsnämnden

I internkontrollplan för 2022 saknas riskområden samt kontrollmoment avseende informationssäkerhet. I internkontrollplan avseende år 2021 finns följande kontrollmoment:

- Bristande informationssäkerhet genom att skyddsvärd information ligger kvar hos entreprenörer och konsulter efter avslutade projekt. Kontrollen avser kontroll av entreprenörers informationshantering.

Vi har i granskningen efterfrågat uppföljning av internkontrollplan för 2021 men inte mottagit detta.

3.7.2 Samlad uppföljning av regionens informationssäkerhetsarbete

I samtliga revisionsobjekts reglementen[19] går att finna följande gemensamma bestämmelser för samtliga nämnder och styrelser: Styrelsen/nämnden ska följa upp sin verksamhet kontinuerligt och säkerställa att den får tillräcklig information för att kunna ta sitt ansvar för verksamheten.

Av riktlinjer för informationssäkerhet 2015 framgår att nämnder och styrelser ska genomföra en regelbunden uppföljning av informationssäkerhetsarbetet som ska utgöra underlag till den regionövergripande säkerhetsredovisningen som nämnder, styrelser och bolag årligen ska lämna till regionstyrelsen.

Vidare framgår att koncernsäkerhetschefen, på uppdrag av regiondirektören, ansvarar för sammanställning och analys till regionstyrelsen av förvaltningar och bolags säkerhetsredovisningar. Som tidigare nämnts finns inte rollen koncernsäkerhetschef kvar men motsvarande roll benämns i nuvarande organisation Enhetschef säkerhet och beredskap. Vi har inte tagit del av någon samlad uppföljning av regionens informationssäkerhetsarbete. Intervjupersoner uppger att det för år 2021 inte upprättats någon säkerhetsredovisning och hänvisar till den uppföljning som presenterats i årsredovisning samt patientsäkerhetsberättelse.

Av patientsäkerhetsberättelsen framgår att informationssäkerhetsarbetet följs upp bland annat inom ramen för den intern kontrollen. Av patientsäkerhetsberättelsen framgår vidare att det sker systematisk uppföljning av ledningssystemet för informationssäkerhet och dataskydd i olika delar. Det framgår även att IVO[20] under juni 2021 genomförde en granskning av regionen och programmet FVM:s (Framtidens vårdinformationsmiljö) arbete utifrån NIS-lagstiftningen och kraven på riskhantering. Det framgår att granskningen bidragit till genomlysning och inspel i det fortsatta

[19] Reglemente för styrelsen för regiongemensam hälso- och sjukvård, Reglemente för styrelsen för Skaraborgs sjukhus, Regionfullmäktige, 10–11 juni 2019. Västra Götalandsregionen (2021) *Reglemente för fastighetsnämnden.* https://www.vgregion.se/politik/politisk-organisation/namnder-och-styrelser/fastighetsnamnden/reglemente-for-fastighetsnamnden/ [2022-11-23]

[20] Inspektionen för vård och omsorg

informationssäkerhetsarbetet. Vidare framgår att flertalet riskanalyser har genomförts vid etablering eller förändring av IS/IT-stöd och inom ramen för arbetet med ett nytt journalsystem.

Av Västra Götalandsregionens årsredovisning framgår att det inom informationssäkerhetsområdet har genomförts informationssäkerhetsklassningar, samt att ett utvecklingsarbete har bedrivits på både regional nivå och inom respektive förvaltning och bolag. Vidare uppges att ett antal incidenter har utretts, hanterats och anmälts i enlighet med NIS-direktivet. Vidare uppges att en teknisk sårbarhet kallad ”log4J” som är vanligt förekommande i många system ledde till en stor regiongemensam händelsehantering för att trygga regionens digitala infrastruktur.

I intervjuer uppges att det sker en uppföljning och sammanställning av de ärenden som registreras i MedControl samt de anmälningar som gjorts till Integritetsmyndigheten inom Styrelsen för Regionhälsan. I övrigt uppges att det inom samtliga revisionsobjekt saknas en etablerad uppföljning samt återrapportering av det informationssäkerhetsarbete som genomförts.

Intervjuade uppger att det inte har skett någon kontroll av att ledningssystemet för informationssäkerhet och de styrande dokument som ledningssystemet består av efterlevs. Av den interna kontrollen för styrelser och nämnd kan vi därtill konstatera att efterlevnad av gällande lagar, exempelvis GDPR eller NIS-direktivet inte har kontrollerats.

3.7.3 Bedömning

Vi gör bedömningen att det i riktlinjer för informationssäkerhet finns formaliserade uppföljnings- och rapporteringsrutiner. Vi gör dock bedömningen att riktlinjerna inte efterlevs då det vid tiden för granskningen inte har upprättats någon säkerhetsredovisning i enlighet med riktlinjerna. Den uppföljning som genomförs och som presenteras i årsredovisning och patientsäkerhetsberättelsen bedömer vi inte vara tillräcklig i syfte att utgöra underlag för utvärdering och beslut om åtgärder.

Samtliga revisionsobjekt behöver vidta åtgärder i syfte att stärka sitt uppföljningsarbete. Vidare ser vi behov av att samtliga revisionsobjekt upprättar former för kontinuerlig återrapportering av det informationssäkerhetsarbete som bedrivs i respektive verksamhet. Vår bedömning är att revisionsobjekten inte fullt ut följer bestämmelser om uppföljning och intern kontroll i reglemente, kommunallagens bestämmelser och Policy för styrning.

Vi bedömer att regionstyrelsen brister i sitt övergripande ansvar då styrelsen inte har tillsett att det finns en regelbunden uppföljning och rapportering av det samlade informationssäkerhetsarbetet i regionen i enlighet med krav i regionens riktlinjer för informationssäkerhet. Den saknar därigenom tillräckliga underlag för att besluta om åtgärder eller resurser som det finns behov av för att stärka regionens informations- och cybersäkerhet.

4 Sammanfattande bedömning

Vår sammanfattande bedömning utifrån granskningens syfte är att regionstyrelsen, inom ramen för sitt övergripande ledningsansvar, inte har etablerat en tillräcklig styrning av informations- och cybersäkerhetsarbetet. Det ramverk som utgörs av regionens ledningssystem för informationssäkerhet innehåller riktlinjer, rutiner och instruktioner för hur arbetet ska bedrivas men är i behov av revidering och komplettering för att informationssäkerhetsarbetet ska vara ändamålsenligt.

Vår sammanfattande bedömning är att styrelsen för regionhälsan och fastighetsnämnden i huvudsak har en tillräcklig styrning av informationssäkerhetsarbetet för att säkerställa att det sker på ett ändamålsenligt sätt.

Vår bedömning är att styrelsen för Skaraborgs sjukhus inte har en tillräcklig styrning av informationssäkerhetsarbetet och det i nuläget inte sker på ett ändamålsenligt sätt.

Den interna kontrollen tillsammans med andra uppföljningsrutiner behöver stärkas i samtliga revisionsobjekt. Detta för att utvärdera att det arbete som genomförs är tillräckligt i förhållande till de risker och behov som finns. Informationssäkerhetsrisker är ständigt närvarande, dels vid en bristande intern hantering vilket vi ser en viss risk för då utbildning har erbjudits i relativt liten utsträckning. Dels så finns risker i form av externa hot, som intrångsförsök eller cyberattacker. Vår bedömning är dock att etableringen av Enhet för cybersäkerhet och det uppdrag som enheten har, i hög grad har stärkt regionens förmåga att med tekniska säkerhetsåtgärder identifiera och hantera externa hot och intrångsförsök. Därtill finns en organisation med beredskap för att lösa särskilda säkerhetshändelser med ett tydliggjort uppdrag och mandat.

Avslutningsvis är vår bedömning att regionstyrelsen brister i sitt övergripande ansvar för säkerhetsarbetet i regionen. Styrelsen har inte tillsett att det finns en regelbunden rapportering av informationssäkerhetsarbetet i enlighet med krav i regionens riktlinjer för informationssäkerhet. Den saknar därigenom tillräckliga underlag för att besluta om åtgärder eller resurser som det finns behov av för att stärka regionens informations- och cybersäkerhet.

5 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen inom ramen för sitt övergripande ledningsansvar att:

- Revidera och komplettera LIS i enlighet med granskningens resultat, främst med avseende på:
  - De kompletterande riktlinjer, planer och rutiner som enligt tidigare beslut fattade av regionstyrelsen och regiondirektören upprättas.
  - Gällande lagar, regler och nya krav inom området.
  - Beskrivning av ansvar och roller på både strategisk och operativ nivå så att det överensstämmer med nuvarande organisation.
  - Rutiner för uppföljning och kontroll.
- Säkerställa att det regelbundet genomförs obligatoriska utbildningar i informationssäkerhet för medarbetare.
- Förstärka uppföljning, intern kontroll och uppsikt av informationssäkerhetsarbetet för att säkerställa följsamhet till interna krav och gällande regelverk.
- Etablera en årlig rapportering från samtliga nämnder och styrelser i syfte att ge styrelsen en samlad bild av regionens informationssäkerhet.

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen, styrelsen för regionhälsan, fastighetsnämnden och styrelsen för Skaraborgs sjukhus att:

- Upprätta förvaltningsspecifika rutiner avseende hantering av behörighet som kopplar an mot de regionövergripande riktlinjerna samt säkerställa att kontroller av tilldelade behörigheter genomförs.
- Säkerställa att obligatoriska utbildningar som svarar mot verksamhetens behov genomförs och att deltagandet följs upp.
- Upprätta kontinuitetsplaner för att säkerställa verksamhetens fortgående vid en eventuell incident samt säkerställa att dessa testas med regelbundenhet.
- Vidta åtgärder i syfte att stärka uppföljningsarbetet samt upprätta former för kontinuerlig återrapportering till styrelse/nämnd av det informationssäkerhetsarbete som bedrivs.

Vi rekommenderar Styrelsen för Skaraborgs sjukhus att även:

- Säkerställa att riskbedömning och informationsklassning genomförs av den information som hanteras inom styrelsens verksamhet.

Datum som ovan

KPMG AB

Jenny Thörn
Projektledare
Verksamhetsrevisor

Ida Larson
Verksamhetsrevisor

Veronica Hedlund Lundgren
Kvalitetssäkrare
Certifierad kommunal yrkesrevisor

Bilaga 1 Styrande dokument

Följande styrande och stödjande dokument har ingått i granskningen:

- Policy för styrning
- Policy för säkerhet och beredskap
- Riktlinje för informationssäkerhet – 2015
- Riktlinjer för informationssäkerhet, med tillhörande rutiner – 2018
- ISIT Styrmodell
- Styrande dokument säkerhet
- Exempel på Informationsklassningar
- Verkställighetsbeslut – ”Styrande dokument inom säkerhets- och beredskapsområdet tillämpas tills nya beslutats

Bilaga 2 Intervjupersoner

Följande funktioner har deltagit i intervjuer och avstämningar:

- Regiondirektör
- Avdelningschef, Ärendesamordning och kansli
- Ledningsstöd regiondirektör
- Enhetschef säkerhet och beredskap
- Funktionsansvarig för informationssäkerhet
- Enhetschef för cybersäkerhet
- Enhetschef för IT-infrastruktur
- Arkivchef koncernkontoret
- Chef eHälsa och Säkerhet tillika informationssäkerhetssamordnare samt IT-chef
- Verksamhetschef Skaraborgs sjukhus
- Strateg på kvalitet- och utvecklingsenheten, Skaraborgs sjukhus
- Säkerhetschef/enhetschef, Enheten för Säkerhet, Brand och Risk, Västfastigheter
- IT-chef, Västfastigheter
- Strateg informationssäkerhet, Enheten för Säkerhet, Brand och Risk, Västfastigheter