Uppföljande granskning av informations- och cybersäkerhet

Region Gävleborg

September 2021

Linus Owman
Patrik Bauer

pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Gävleborg genomfört en uppföljande granskning av informations- och cybersäkerhetsarbetet i regionen. Denna granskning har innefattat intervjuer med intressenter inom regionen samt dokumentgranskning.

Dokumentgranskningen har omfattat relevanta styrande dokument som berör områdena informations- och cybersäkerhet. Inom ramen för granskningen har intervjuer genomförts med tjänstemän inom huvudsakligen IT-säkerhet, IT-stödsystem, IT-teknik och IT-förvaltningen.

Då granskningen är en uppföljning av tidigare genomförd granskning (2019) är den övergripande frågeställningen: *"Har ändamålsenliga åtgärder vidtagits med anledning av 2019 års granskning?"*. För att besvara denna fråga har ett antal ytterligare revisionsfrågor ställts.

Revisionsfrågorna lyder:

- Har regionen fastställt styrande dokument inom både informations- och cybersäkerhet?
- Har regionen fastställt dokumenterade processer för arbetet med informations- och cybersäkerhet?
- Har regionen formaliserat och systematiserat arbetet med informationssäkerhetsrisker?
- Har regionen en incidenthanteringsprocess som samordnas genom samverkan mellan informationssäkerhetsavdelningen och IT-avdelningen?
- Har regionen säkerställt att funktionen för informationssäkerhet har tillräckligt med mandat för att bedriva sitt uppdrag och att de förvaltar sin egen budget?
- Har regionen genomfört, samt fortsätter att genomföra, utbildningar och kompetenshöjande aktiviteter inom området cybersäkerhet?

Revisionsfråga	Bedömningar
Revisionsfråga 1: Har regionen fastställt styrande dokument inom både informations- och cybersäkerhet?	**Helt uppfylld** - Regionen har vidtagit en mängd åtgärder för att förtydliga och systematisera styrningen av regionens arbete med informations- och cybersäkerhet inom ramen för regionens dokumentation för området. Alla dokument som blivit fastställda härrör från år 2019 eller senare, vilket indikerar att arbetet varit intensivt och genomgripande på flera nivåer. Dokumentationen rör både övergripande styrning, incident- och kontinuitetshantering, behörighetshantering, informationsklassning och risk, samt ytterligare områden kring användning av specifika tekniska lösningar (molntjänster, dataskydd, lagring och kommunikation).

Revisionsfråga 2: Har regionen fastställt dokumenterade processer för arbetet med informations och cybersäkerhet?	**Till övervägande del uppfylld -** Regionen har påbörjat ett arbete med processkartläggning av samtlig information som regionen behandlar och hur/var den bör lagras, där enligt uppgift bortåt 200 processer är kartlagda, även om några kärnprocesser kvarstår. Arbetet har dock försenats på grund av pandemin. Det finns idag ett systematiskt och dokumenterat informationssäkerhetsarbete relaterat till risker med en normskala (konsekvensskala) baserad på MSB:s metodstöd vilket bygger på standarden ISO 27001 som innebär att riskägarskapet inom organisationen förtydligats. Inrättandet av ett informationssäkerhetsråd har ytterligare förtydligat samverkan mellan IT och informationssäkerhet inom organisationen, vilket ytterligare stärker bilden av en region som aktivt arbetar med att förtydliga och förbättra processerna inom informationssäkerhets- och cyberområdet.
Revisionsfråga 3: Har regionen formaliserat och systematiserat arbetet med informationssäkerhets-risker?	**Till övervägande del uppfylld -** Regionen har nu tillsett att alla incidenter i slutändan rapporteras till enheten för informationssäkerhet. Det finns ett utbyggt samarbete mellan enheten för informationssäkerhet och IT-avdelningen som innebär att informationen når enheten för informationssäkerhet, oavsett om rapporteringsvägen för incidenten sker via IT-support eller på annat sätt. Vidare har inrättandet av ett informationssäkerhetsråd ytterligare bidragit till att organisationen stärkt sin förmåga till överblick avseende incidenter. Det finns i dagsläget även ett fastställt direktiv för hantering av informationssäkerhetsincidenter med tillhörande rutiner. Vi konstaterar dock att arbetet med kontinuitetsfrågor fortfarande ännu ej är fullt ut genomfört och att det saknas en övergripande kontinuitetsplan för regionens IT-infrastruktur, även om en sådan är under utarbetande. Direktiv kring kontinuitet samt mall för arbetssätt finns att tillgå för verksamheterna, men arbetet och uppföljningen av dessa har ännu inte nått fullt genomslag.
Revisionsfråga 4: Har regionen en incidenthanteringsprocess som samordnas genom samverkan mellan informationssäkerhets-avdelningen och IT-avdelningen?	**Till övervägande del uppfylld -** Bedömningen grundar sig till stor del på att regionen nu tillsett att alla incidenter i slutändan rapporteras till enheten för informationssäkerhet. Det finns ett utbyggt samarbete mellan enheten för informationssäkerhet och IT-avdelningen som innebär att informationen når enheten för informationssäkerhet, oavsett om rapporteringsvägen för incidenten sker via IT-support eller på annat sätt. Vidare har inrättandet av ett informationssäkerhetsråd ytterligare bidragit till att organisationen stärkt sin förmåga till överblick avseende incidenter. Vi konstaterar dock att arbetet med kontinuitetsfrågor fortfarande ännu ej är fullt ut genomfört.

Revisionsfråga 5: Har regionen säkerställt att funktionen för informationssäkerhet har tillräckligt med mandat för att bedriva sitt uppdrag och att de förvaltar sin egen budget?	**Till övervägande del uppfylld -** Sedan föregående granskning har regionen vidtagit en rad åtgärder som sammantaget syftar till att stärka styrningen och genomslaget för frågor kring informationssäkerhet och IT-säkerhet. Att informationssäkerhet numera utgör en egen enhet kan betraktas som ett steg i denna riktning, liksom det faktum att IT numera utgör en egen förvaltning. Dessa åtgärder sammantaget visar att regionen uppgraderat synen på dessa frågors verksamhetskritiska vikt.
Revisionsfråga 6: Har regionen genomfört, samt fortsätter att genomföra, utbildningar och kompetenshöjande aktiviteter inom området cybersäkerhet?	**Till övervägande del uppfylld -** Regionen tillhandahåller introduktionsutbildningar i informationssäkerhet och i dataskydd till alla anställda, och utöver detta utbildas chefer vid behov ytterligare bland annat med hjälp av MSB:s utbildningsmaterial. Genom informationssäkerhetsmånaden söker regionen höja medvetenheten hos medarbetarna. Vår bedömning är dock att utbildningsinsatserna kan höjas (se rekommendationerna nedan).

Rekommendationer baserade på denna granskning följer efter varje granskningsavsnitt nedan.

1. Inledning

1.1 Bakgrund

Kommuner och regioner har ett av det svenska samhällets mest komplexa uppdrag. Detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. Förtroendet för en organisation tar lång tid att bygga upp, men kan snabbt raseras av en enskild säkerhetsincident.

Med dagens snabba digitalisering blir informationssäkerhet allt viktigare. Ett gott informations- och cybersäkerhetsarbete är beroende av en god styrning. Ledningen ska vara engagerad och ha kunskap om informations- och cybersäkerhetsarbetet. Ledningen ska ge den strategiska inriktningen och säkerställa att det finns tillräckligt med resurser och mandat i organisationen för att kunna utföra arbetet. Det är ledningens kravställning som styr verksamheten och det är därmed ledningen som ska säkerställa att det bedrivs ett cyber- och informationssäkerhetsarbete som är i linje med externa och interna krav.

Bristande informationssäkerhet innebär en stor risk för samhället och med dagens snabba digitalisering blir informationssäkerhetsområdet allt viktigare. Information är värdefull och behöver många gånger skyddas. Ett proaktivt cyber- och informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering. Detta skapar i sin tur förtroende både inom och utanför organisationen.

PwC genomförde 2019 en granskning av Region Gävleborgs arbete med informations- och cybersäkerhet. Revisorerna har utifrån sin riskbedömning valt att genomföra en uppföljande granskning av området utifrån perspektiven ändamålsenlighet och tillräcklig intern kontroll. Detta för att det finns en risk att regionstyrelsen inte har säkerställt att det finns en god informationssäkerhet inom regionen och har därför gett PwC ett uppdrag att granska området.

1.2 Syfte och revisionsfrågor

Granskningens syfte är att följa upp de rekommendationer som gavs vid granskningen som genomfördes 2019 och därmed bedöma huruvida regionstyrelsen säkerställer ett ändamålsenligt cyber- och informationssäkerhetsarbete. Den övergripande frågeställningen för granskningen är således: *Har ändamålsenliga åtgärder vidtagits med anledning av 2019 års granskning?*

Följande revisionsfrågor används för att svara mot syftet:

- Har regionen fastställt styrande dokument inom både informations- och cybersäkerhet?
- Har regionen fastställt dokumenterade processer för arbetet med informations- och cybersäkerhet?
- Har regionen formaliserat och systematiserat arbetet med informationssäkerhetsrisker?
- Har regionen en incidenthanteringsprocess som samordnas genom samverkan mellan informationssäkerhetsavdelningen och IT-avdelningen?
- Har regionen säkerställt att funktionen för informationssäkerhet har tillräckligt med mandat för att bedriva sitt uppdrag och att de förvaltar sin egen budget?

- Har regionen genomfört, samt fortsätter att genomföra, utbildning och kompetenshöjande aktiviteter inom området cybersäkerhet?

1.3 Revisionskriterier

- Regionens relevanta styrande dokument
- God redovisningssed

1.4 Avgränsning

I tid avgränsas granskningen i huvudsak till år 2021. I övrigt se syfte, revisionsfrågor och metod.

1.5 Metod

Granskningen genomförs genom:

1. Analys av för granskningen relevant dokumentation
2. En gruppintervju med representanter från ledningsbefattningar (regionchef, verksamhetsansvariga) och en gruppintervju med personer från avdelningarna för IT- och informationssäkerhet
3. Resultat från dokumentgranskning och intervjuer sammanställs i en rapport där iakttagelser och rekommendationer listas i förhållande till revisionskriterierna.

Vissa delar i rapporten är sekretessbelagd och texten svartmarkerad.

2. Iakttagelser och bedömningar

2.1 Revisionsfråga 1: Har regionen fastställt styrande dokument inom både informations- och cybersäkerhet?

2.1.1 Iakttagelser

Av föregående granskning (2019) framgick att regionen inte hade någon antagen informationssäkerhetspolicy eller annan form av övergripande styrande dokument för hur regionen ska arbeta med informationssäkerhetsrisker. Det fanns inte heller dokumenterat hur risker ska bedömas, vilken risktolerans som organisationen har eller hur risker ska prioriteras och hanteras.

Dokument för övergripande styrning

Regionen arbetar enligt principen med direktiv som högsta styrande dokument och med rutiner och checklistor för lägre instanser. Således är ett direktiv att likställa med en policy. Regionens ansats, utifrån vad som framkommer under intervjuer, är vidare att inrymma så mycket styrande information som möjligt i centrala direktiv, i syfte att minimera risken för feltolkningar inom verksamheten. Det finns ett övergripande direktiv inom informationssäkerhet som fastställdes 2018 och reviderades 2020-12-09. Direktivet fungerar som hörnsten i regionens ledningssystem för informationssäkerhet (LIS).

Relaterat till regionens dokumentation inom informationssäkerhetsområdet finns idag ett flertal ytterligare dokument. Följande nyligen fastställda dokument förtjänar att nämnas:

- "*Direktiv för styrande dokument i LIS"*, (2021-03-08). Tidigare fanns endast dokumentet "*Informationssäkerhet - Direktiv för ansvar och roller*", (2018-03-29) avseende regionens styrning och organisation fanns vid föregående granskning.
- "*Informationssäkerhetsråd"*, (2020-11-25), vilket beskriver informationssäkerhetsrådets uppdrag i Region Gävleborg.
- "*Direktiv för systematiskt och riskbaserat informationssäkerhetsarbete*", (2020-09-16).
- "*Arbetsfördelning för Systemförvaltning, IT-avdelningen*" och "*Informations- och IT-säkerhet vid distansarbete*", (2019-03-21 respektive 2020-10-21), bidrar ytterligare till styrningen av regionens IT och informationssäkerhet.
- "*Grundläggande regler för IT-säkerhet - Direktiv Region Gävleborg*" (2020-02-24), tydliggör grundläggande krav för hur IT-lösningar skall hanteras.

Dokument för behörighetshantering, informationsklassning och risk

Beträffande områdena behörighetstilldelning (IAM), informationsklassning och risk har ett flertal dokument upprättats och fastställts sedan föregående granskning. Dessa innefattar direktiven

- *"Behovs och riskanalys för behörighetstilldelning - Direktiv, Hälso och sjukvård, Region Gävleborg"* (2021-05-05) samt
- *"Informationssäkerhet - Direktiv för systematiskt och riskbaserat informationssäkerhetsarbete"* (2020-09-16), vilket bland annat berör informationsklassning.

Utöver dessa direktiv finns idag även ett flertal dokument på mer detaljerad nivå. Bland dessa återfinns

- *"Informationssäkerhet - Rutin för systematiskt och riskbaserat informationssäkerhetsarbete*" (2021-06-22),
- "*Övergripande riskanalys avseende informationssäkerhet för Hälso- och sjukvården*" (2021-06-14) för att uppfylla de krav på systematiskt och riskbaserat informationssäkerhetsarbete som framkommer i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, samt
- "*Behovs och riskanalys för behörighetstilldelning - Rutin. Hälso- och sjukvård Region Gävleborg"* (2021-05-05).

Angående behörighet så har även två rutiner fastställts relaterat till registrering av multifaktorautentisering för interna respektive externa parter, "*MFA-registrering - rutin. Region Gävleborg"* (2021-01-04) och "*MFA-registrering - rutin. Externa Företag med RG användarkonton*" (2021-01-04). Det finns även ett upprättat dokument för att möjliggöra framförhållning av livscykelhantering gällande system, servrar och andra IT-infrastrukturkomponenter, vilket dock ej är ett fastställt dokument.

Dokument för incident- och kontinuitetshantering
Vid tiden för de föregående granskningen fanns dokumentet "*Incidenthantering IT-avdelningen*", (2016-10-07). Det finns idag en större flora av dokumentation beträffande regionens kontinuitetsoch incidenthantering, exempelvis:

- "*Direktiv för hantering av informationssäkerhetsincidenter*" (2020-09-16),
- "*Rutin för hantering av personuppgiftsincidenter*" (2021-06-22),
- "*Rutin för hantering av informationssäkerhetsincidenter*" (2021-06-02),
- "*Direktiv för kontinuitetshantering*" (2021-01-13) ● *"Rutin för kontinuitetshantering"* (2020-09-23), samt ● *"Mall för kontinuitetsplanering*" (2020-09-30).

Övrig relevant dokumentation
Andra relevanta dokument fastställda sedan den föregående granskningen kring styrning, arbetssätt, processbeskrivningar och krav inom IT- och informationssäkerhetsområdet är bland annat följande:

- *"Direktiv för lagring och kommunikation i digitala kanaler"* (2021-04-22)
- *"Direktiv för molntjänster. Region Gävleborg"* (2019-09-02)
- *"Molntjänster Regler för Införande och Hantering - Rutin Region Gävleborg"* (2019-10-14)
- *"Digital kommunikation - videosamtal, telefonsamtal, chatt, delning av skrivbord och videomöte - Rutin"* (2021-01-27)
- *"Personuppgiftsbiträdesavtal - Rutin för upprättande"* (2021-04-22)
- *"Inbyggt dataskydd och dataskydd som standard rutin"* (2021-04-30)
- *"Generell rutin för personuppgiftsbehandling"* (2021-04-22)
- *"Regler för hantering databaser och SQL server"* (2020-10-16)

2.1.2 Bedömning

PwC bedömer revisionsfrågan som **helt uppfylld.**

Regionen har vidtagit en mängd åtgärder för att förtydliga och systematisera styrningen av regionens arbete med informations- och cybersäkerhet inom ramen för regionens dokumentation för området. Alla dokument som listats ovan härrör från år 2019 eller senare, vilket indikerar att arbetet varit intensivt och genomgripande på flera nivåer. Dokumentationen rör både övergripande styrning, incident- och kontinuitetshantering, behörighetshantering, informationsklassning och risk, samt ytterligare områden kring användning av specifika tekniska lösningar (exempelvis molntjänster, dataskydd, lagring och kommunikation).

Granskningen svarar endast på frågan kring huruvida styrande dokument fastställts, och inte huruvida dessa i praktiken efterlevs.

Baserat på bedömningen ovan *rekommenderar* PwC följande:

- Fastställ dokumentet (rutinen) “Livscykelhantering i Region Gävleborg”.

2.2 Revisionsfråga 2: Har regionen fastställt dokumenterade processer för arbetet med informations- och cybersäkerhet?

2.2.1 Iakttagelser

Pågående processkartläggning

Sedan föregående granskning har det genomförts en omorganisation från en beställar- och utförarmodell till en regionsförvaltning med flertalet underförvaltningar som arbetar med styrning och förvaltning. Det finns enligt uppgift ett arbete kvar att göra för att få fram en formell tydlig styrning, men det som finns på plats idag upplevs som en reell förbättring jämfört med tiden för den föregående granskningen 2019. Enligt intervjuer med stabschef och IT-direktör ligger fokus i dagsläget på att tillse att styrningen av IT- och informationssäkerhetsområdet fungerar på ett fullödigt sätt, framförallt mellan Regionstaben och övrig verksamhet. Det genomgripande arbetet med styrande dokumentation har berörts i föregående revisionsfråga. I nuläget anses det därför inte föreligga något större behov av att ta fram ytterligare detaljerade styrdokument.

I föregående granskning framkom att funktionen för informationssäkerhet vid tidpunkten för granskningen höll på att genomföra en processkartläggning av samtlig information som regionen behandlar och även var den bör lagras. Vid tidpunkten för föregående granskning beräknades detta vara klart om ca 2,5 år. Tanken var att arbetet skulle utgöra en grund för informationsklassning och riskanalys. Detta arbete gick enligt uppgift framåt men har beräknas ha försenats c:a ett år på grund av pandemin, eftersom arbetet pausades då fysiska workshops ej längre var möjliga att genomföra. Enligt informationssäkerhetsansvarig så är i dagsläget ca 200 processer kartlagda och arbetet bedöms fortsätta under hösten 2021. Kartläggningen har skett via SharePoint och Visio (för kartor över informationen i processer) där informationsflöde, informationsmängder, lagring etc samlats med metadata kring sekretessbestämmelser etc. Enligt uppgift så är stödprocesser och ledningsprocesser till stor del kartlagda men kärnprocesser kvarstår. Samtlig information har inte informationsklassificerats än.

Kravställning och uppföljning av leverantörer

I dagsläget sker numera enligt intervjuer en informationsklassning inför varje upphandling av IT-tjänster. Enligt vad som framkommit under intervjuer finns även upphandlingskrav och

upphandlingsnivåer baserade på SKRs metodstöd för informationsklassificering “KLASSA”. Dessa är dock i behov av uppdatering och ytterligare utveckling.

Vid den tidigare granskningen framkom det att det fanns en plan att upprätta en mall för användning vid upprättandet av informationssäkerhetskrav samt vid kontakt med leverantörer. Denna mall var dock ej ännu på plats. Det fanns dock en rutin för genomförande av granskning av personuppgiftsbiträden. Det fanns planer på att ta fram en liknande rutin för att möjliggöra granskning av samtliga leverantörer och de informationssäkerhetskrav som föreligger mot dessa, men detta dokument var ej fastställt vid tiden för den föregående granskningen.

Enligt uppgift finns numera en fastställd checklista som informationsavdelningen arbetar efter avseende informationskrav på leverantörer. Enligt uppgift finns idag således tydliga krav kring informationssäkerhet gentemot leverantörer, men dessa följs inte upp systematiskt. Den uppföljning som sker av leverantörer sker främst inom ramen för dataskydd (GDPR), och ytterligare systematisk uppföljning saknas. Den uppföljning som sker inom ramen för dataskydd sker idag utifrån en prioritering baserat på antal registrerade, typ av uppgifter och liknande. Inköpsavdelningen anses inte ha förmåga att följa upp tekniska delar i dagsläget. Den uppföljning som sker utöver detta består i att leverantören får besvara self assessment-frågor. Enligt informationssäkerhetsansvarig är ansvaret för uppföljning något oklart, men där det gäller personuppgiftsbiträden så har verksamheterna utsedda personer med ansvar som sedan kan söka stöd från IT-avdelningen och enheten för informationssäkerhet. Det finns en uttalad önskan om att utöka uppföljning av kravställningen gentemot leverantörer genom exempelvis slumpmässig uppföljning av ett antal leverantörer för att synliggöra hur de uppfyller informationssäkerhetskrav. Enligt uppgift pågår ett arbete med att konkretisera ambitionerna inom området, det så kallade “It-säkerhetspaketet”.

Måluppföljning

I föregående granskning framgick det att funktionen för informationssäkerhet inte hade en måluppföljning eller en detaljerad plan för hur informationssäkerhetsarbetet ska följas upp. Det fanns vid tidpunkten ett antal mål listade i det övergripande direktivet för informationssäkerhet, men ingen plan för hur dessa skulle uppnås eller mätas.

Enligt stabschefen så var den tidigare ambitionen att den dåvarande funktionen för informationssäkerhet skulle sätta målen. I dagsläget har denna process nu ändrats så att informationsägare sätter sina egna mål. Detta då det tidigare tillvägagångssättet ansågs vara alltför detaljstyrt. För att säkerställa samma riktning och ambitionsnivå sätts övergripande mål i direktiv som sedan följs upp centralt, enligt IT-direktören. Enligt uppgift är måluppfyllnaden inom ITochinformationssäkerhetsområdet nu en del av verksamhetsplanering och måluppföljning. Enligt svar från intervju har krav som ställts från politiken implementerats ute i verksamheten, bland annat att incidenter skall behandlas inom en viss tidsfrist, och att informationsklassningar skall genomföras, vilket även kan följas upp. Uppföljning och mätning kan ske via regionens verktyg för måluppföljning. Enligt uppgift från intervju sätts i nuläget även tydliga krav på vad som skall levereras från organisationens olika delar och ut i verksamheten, exempelvis för enheten för informationssäkerhet, men även mål för hela regionen.

Utökad samverkan

Vid tiden för föregående granskning (2018-2019), framkom att det ej var utarbetat hur den IT-ansvariga och den informationssäkerhetsansvariga skulle samverka, relaterat till att öka medvetenheten om dataläckor och klassning av information i regionens system. Det finns idag ett

informationssäkerhetsråd, grundat på ett direktörsbeslut. Rådet träffas åtta gånger per år, eller mer vid behov. Informationssäkerhetsrådets uppdrag och sammansättning, där samtliga förvaltningar är representerade, framgår i dokumentet *"Informationssäkerhetsråd"* (2020-11-25).
Informationssäkerhetsrådets uppdrag är att:

- verka för att en god informationssäkerhet upprätthålls i Region Gävleborg,
- samordna och hantera frågor gällande informationssäkerhet och dataskydd,
- agera styrgrupp vid regionövergripande projekt gällande informationssäkerhet, och
- säkerställa beredningsgruppens funktion i systemförvaltningsprocessen.

Ansvariga för IT-säkerhet respektive informationssäkerhet har enligt uppgift även avstämningar regelbundet, ofta veckovis, och arbetar tillsammans med det övergripande arbetet för att se hur långt de kommit och vad de bör fokusera på framåt. Enligt ansvarig för informationssäkerhet sker klassning med verksamheten, ärendet lämnas sedan över till IT där "hur"-nivån upprättas, d.v.s. praktiska lösningar. Efter varje beslutsunderlag producerats relaterat till systemförändringar så kopplas informationssäkerhet och beskriver risker och ger förslag på förutsättningar, vilket enligt uppgift är formaliserat.

2.2.2 Bedömning

PwC bedömer revisionsfrågan som **till övervägande del uppfylld.**

Regionen har påbörjat ett arbete med processkartläggning av samtlig information som regionen behandlar och hur/var den bör lagras, där enligt uppgift bortåt 200 processer är kartlagda, även om några kärnprocesser kvarstår. Arbetet har dock försenats på grund av pandemin och är ännu inte färdigställt.

Uppföljning av den kravställning som sker gentemot leverantörer fokuserar framförallt på uppföljning kring dataskydd, troligen beroende på den starka regleringen inom området.

Det finns ett pågående arbete med att förtydliga målsättningar inom området för informationssäkerhet. Det finns övergripande mål och aktiviteter som informationssäkerhetsenheten gör som en del av sin verksamhetsplanering, vilka följs upp årligen. Eftersom mål även sätts av informationsägare som i flera fall opererar ute i verksamheterna blir det viktigt att följa upp att både målsättningarna som sådana och deras uppfyllnad följs upp centralt för att säkerställa att hela organisationen arbetar enhetligt.

Inrättandet av ett informationssäkerhetsråd har ytterligare förtydligat samverkan mellan IT och informationssäkerhet inom organisationen, vilket ytterligare stärker bilden av en region som aktivt arbetar med att förtydliga och förbättra processerna inom informationssäkerhets- och cyberområdet.

Baserat på bedömningen ovan *rekommenderar* PwC följande:

- Slutför och dokumentera den påbörjade processkartläggningen, med fokus på de återstående kärnprocesserna, då dessa torde ha högre prioritet än resterande stöd- och ledningsprocesser. Sammanställ processkartläggningen på ett sätt som skapar överblick och som underlättar uppföljning och styrning.

- Stärk arbetet med uppföljning av tidigare upphandlingar genom tydligt utpekat ansvar och genom stickprov samt ett dokumenterat systematiskt arbete relaterat till uppföljning.

- Förtydliga hur arbetet med området för informationssäkerhet ska följas upp, med tydliga mål och planer för hur detta ska ske.

2.3 Revisionsfråga 3: Har regionen formaliserat och systematiserat arbetet med informationssäkerhetsrisker?

2.3.1 Iakttagelser

Regionen har arbetat aktivt med systematisk processkartläggning (se föregående revisionsfråga). I föregående granskning behandlades ett antal riskrelaterade områden där regionens förmåga bedömdes, och som ett led i att besvara frågan kring regionens nuvarande arbete med systematik och formalisering inom IT- och informationssäkerhetsområdet ska dessa återbesökas.

Riskbedömning och risktolerans

Vid föregående granskning framgick det att det ej fanns ett systematiskt och dokumenterat arbetssätt för hur risker ska bedömas. Det fanns inte heller tydligt definierat vilken risktolerans som fanns inom organisationen eller hur risker skulle prioriteras och hanteras. Identifiering och bedömning av informationssäkerhetsrisker genomfördes i praktiken men det saknades ett systematiskt och dokumenterat tillvägagångssätt.

Det finns idag ett systematiskt och dokumenterat informationssäkerhetsarbete relaterat till risker med en normskala (konsekvensskala) baserad på Myndigheten för samhällsskydd och beredskaps (MSB:s) metodstöd för systematiskt informationssäkerhetsarbete (LIS), vilket bygger på standarden ISO27001. Detta arbetssätt finns dokumenterat i *"Direktiv för systematiskt och riskbaserat informationssäkerhetsarbete"*, vilket fastställdes 2019 (med senaste revidering 2020-09-16) och som vid tidpunkten för denna granskning (augusti 2021) håller på att revideras ytterligare. Arbetssättet finns även beskrivet i mer detalj i "*Rutin för systematiskt och riskbaserat informationssäkerhetsarbete*", (2021-06-22). Riskbedömningarna sker enligt uppgifter från intervjuer i möjligaste mån direkt relaterat till informationsmängden, vilken alltid är kopplad till en informationsägare. Eftersom informationsägare även har ansvar för riskbedömningen så leder detta till ett klargörande kring ägandeskap även i frågan om vem som är riskägare. Enligt vad som framkommit under intervjuer sker även viss stöttning från centralt håll för att möjliggöra konsekventa bedömningar i samband med informationsklassning. Enligt uppgift från intervju så har informationssäkerhetsrisker och relaterade frågor erhållit ett ökat intresse från regionledningen, och det finns idag en ökad medvetenhet jämfört med tidigare för dessa frågor.

Förmåga att identifiera och analysera cyberhot (inkl. logghantering)

[redacted]

[redacted]

[redacted]

Enligt föregående granskning skedde ingen systematisk analys enligt någon dokumenterad rutin av upptäckta, fullbordade angrepp. Enligt uppgift lämnad av informationssäkerhetsansvarig sker detta idag, inte minst då det finns specificerade regulatoriska krav beträffande informationssäkerhetsincidenter som medför anmälningsplikt till berörd tillsynsmyndighet, exempelvis personuppgiftsincidenter (GDPR) eller incidenter som rör samhällsviktig verksamhet (NIS-direktivet). I dessa exempel finns utfärdade direktiv från tillsynsmyndigheterna (exempelvis IMY och MSB) för hur incidentrapportering ska ske och inom vilka tidsfrister. De ökade kraven på incidentrapportering från tillsynsmyndigheterna har enligt intervjuad IT-personal bidragit till att arbetet med incidenthantering förbättrats, även om förbättringsmöjligheter fortfarande anses föreligga. Enligt uppgift från informationssäkerhetsansvarig analyseras och dokumenteras även de incidenter som inte omfattas av regulatoriska krav. Frågan om incidenthantering behandlas mer utförligt under revisionsfråga 4 (avsnitt 2.4).

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Behörighetshantering

[redacted] Enligt uppgift kan regionen även komma att ta stöd av de riktlinjer myndigheten för digital förvaltning kommunicerat.

Avseende behörighetshantering, förmedlade IT-säkerhetsansvarig vid intervju att regionen önskar nå ett tillstånd där det finns en matris att arbeta efter beroende på om användaren som ska få behörighet kommer internt eller externt. Enligt uppgift från intervju finns denna systematisk till viss del på plats redan idag om användaren kommer till regionen externt, men det beskrivs samtidigt som ett område som kräver ytterligare insatser framåt.

I den tidigare granskningen framkom det att ingen kontinuerlig, automatiserad uppföljning som ser till att behörigheter tas bort när de ej längre behövs existerade inom regionen. Vid intervju med Enhetschefen för IT-stöd framkommer att det idag finns rutiner för när en medarbetare börjar på en annan enhet eller slutar arbeta vid regionen, vilket även framgår av arbetsdokumentet *“Livscykelhantering - användaridentitet”*. Enligt uppgift från intervju och av dokumentet framgår att borttagande av behörigheter sker per automatik när personen i fråga markeras som avslutad i HR-systemet samt manuellt i de fall där personen ska erhålla fortsatt lön under en period. I dokumentet framgår även vilka ändringar som är planerade för hösten Q2/Q3 2021, där även externa användare skall omfattas av en liknande automatiserad rutin.

Förekomsten av lokala administratörer

[redacted] Detta grundade sig bland annat i att vissa program kräver att användare måste kunna agera lokal administratör för att kunna fungera. Granskningen rekommenderade att personal som behövde kunna agera lokal administratör enligt rutin skall använda separata konton för detta ändamål, och enbart vid behov. [redacted]

Övrig systematik

Vid den tidigare granskningen framkom att det fanns ett litet antal gamla system i IT-miljön som inte längre stöddes av leverantören Microsoft, vilket utgjorde en viss säkerhetsrisk. Personalen menade att detta kompenserades genom att begränsa deras exponering. Det fanns inga rutiner för att snabbt adressera plötsligt offentliggjorde sårbarheter i programvara. Enhetschefen för IT-teknik uppger att de arbetar hårt med att hitta livscykeln på även servrar och system och att de tidigare varit mer reaktiva. [redacted]

2.3.2 Bedömning

PwC bedömer revisionsfrågan som **till övervägande del uppfylld**.

Sedan föregående granskning har regionen utvecklat ett systematiskt riskarbete för informationssäkerhet. Det finns idag ett systematiskt och dokumenterat informationssäkerhetsarbete relaterat till risker med en normskala (konsekvensskala) baserad på MSB:s metodstöd vilket bygger på standarden ISO 27001 som innebär att riskägarskapet inom organisationen förtydligats. Arbetet finns dokumenterat i direktiv och styrande dokument.

Förmågan att upptäcka pågående cyberangrepp beskrivs som fortfarande alltför låg. [redacted]

[redacted]

Behörighetshanteringen inom regionen har förbättrats och viss automatik avseende avslutande av användarkonton förekommer i samband med att personal slutar, även om situationer med manuell hantering fortfarande förekommer.

[redacted]

2.4 Revisionsfråga 4: Har regionen en incidenthanteringsprocess som samordnas genom samverkan mellan informationssäkerhetsavdelningen och IT-avdelningen?

2.4.1 Iakttagelser

Regionens IT driftar enligt uppgift ca 80-90% av IT-miljön, men merparten av de driftade systemen är inköpta.

Den föregående granskningen konstaterade att IT-incidenter och informationssäkerhetsincidenter rapporterades och hanterades i två olika strömmar. Informationssäkerhetsincidenter anmäldes genom att medarbetare mailade till olika funktionsbrevlådor (beroende på typ av informationssäkerhetsincident) och IT-incidenter anmäldes genom att medarbetare kontaktade IT-support. I granskningen framkom även att funktionen för informationssäkerhet upplevde att de inte fick löpande och tillräcklig information om samtliga informationssäkerhetsrelaterade incidenter. Det fanns, enligt uppgift, inte en översikt över regionens informationssäkerhetsincidenter då de inte registrerades i ett samlat system.

[redacted]

Vid tidpunkten för den föregående granskningen fanns ett utkast till nytt direktiv för incidenthantering med förslag till gemensam rapportering av samtliga säkerhetsincidenter i regionen. Detta var framtaget av Funktionen för informationssäkerhet. Enligt uppgift från informationssäkerhetsansvarig är detta i dagsläget implementerat och arbetet är slutfört. Regionen har idag *"Direktiv för hantering av informationssäkerhetsincidenter"* (2020-09-16). Utöver detta så har två ytterligare dokument relaterade till incidenthanteringsprocessen fastställts efter det att den tidigare granskningen genomfördes. Detta gäller *"Rutin för hantering av personuppgiftsincidenter"* (2021-06-22) samt *"Rutin för hantering av informationssäkerhetsincidenter"* (2021-06-02).

Tidigare granskning visade även att funktionen för informationssäkerhet planerade att tillhandahålla en övergripande kontinuitetsplan som verksamheten sedan skulle bryta ned till anpassade planer för respektive verksamhet. Detta fanns vid tidpunkten för föregående granskning ej på plats och det bedömdes därför att det fanns en brist gällande kontinuitetsplanering.

Det finns idag en mall för kontinuitetsplanering (2020-09-30), samt ett direktiv för kontinuitetshantering (2021-01-13). Arbetet med att bryta ner direktivet i anpassade kontinuitetsplaner för respektive verksamhet är dock ännu ej i mål, och har blivit försenat. Arbetssätt och mall finns dock att tillgå. [redacted] Regionens IT-säkerhetsansvarig uppger att de arbetat i ungefär sex månader med att ta fram kontinuitetsplan för centralt levererade IT-tjänster. [redacted]

Regionen har enligt uppgift från intervju beredskapsplaner, men dessa är dock till sitt innehåll skilda från informationssäkerhet och ingår i regionens generella katastrofplan, vilken planeras fastställas inom närtid.

Regionen har utöver detta inrättat ett informationssäkerhetsråd som har till uppgift att ge en samlad bild på regionövergripande nivå. Detta råd kan användas som ett forum för informationsdelning kring incidenter och incidentmönster.

2.4.2 Bedömning

PwC bedömer revisionsfrågan som **till övervägande del uppfylld**.

Bedömningen grundar sig till stor del på att regionen nu tillsett att alla incidenter i slutändan rapporteras till enheten för informationssäkerhet. Det finns ett utbyggt samarbete mellan enheten för informationssäkerhet och IT-avdelningen som innebär att informationen når enheten för informationssäkerhet, oavsett om rapporteringsvägen för incidenten sker via IT-support eller på annat sätt. Vidare har inrättandet av ett informationssäkerhetsråd ytterligare bidragit till att organisationen stärkt sin förmåga till överblick avseende incidenter.

Det finns i dagsläget även ett fastställt direktiv för hantering av informationssäkerhetsincidenter med tillhörande rutiner. Detta är en klar förbättring.

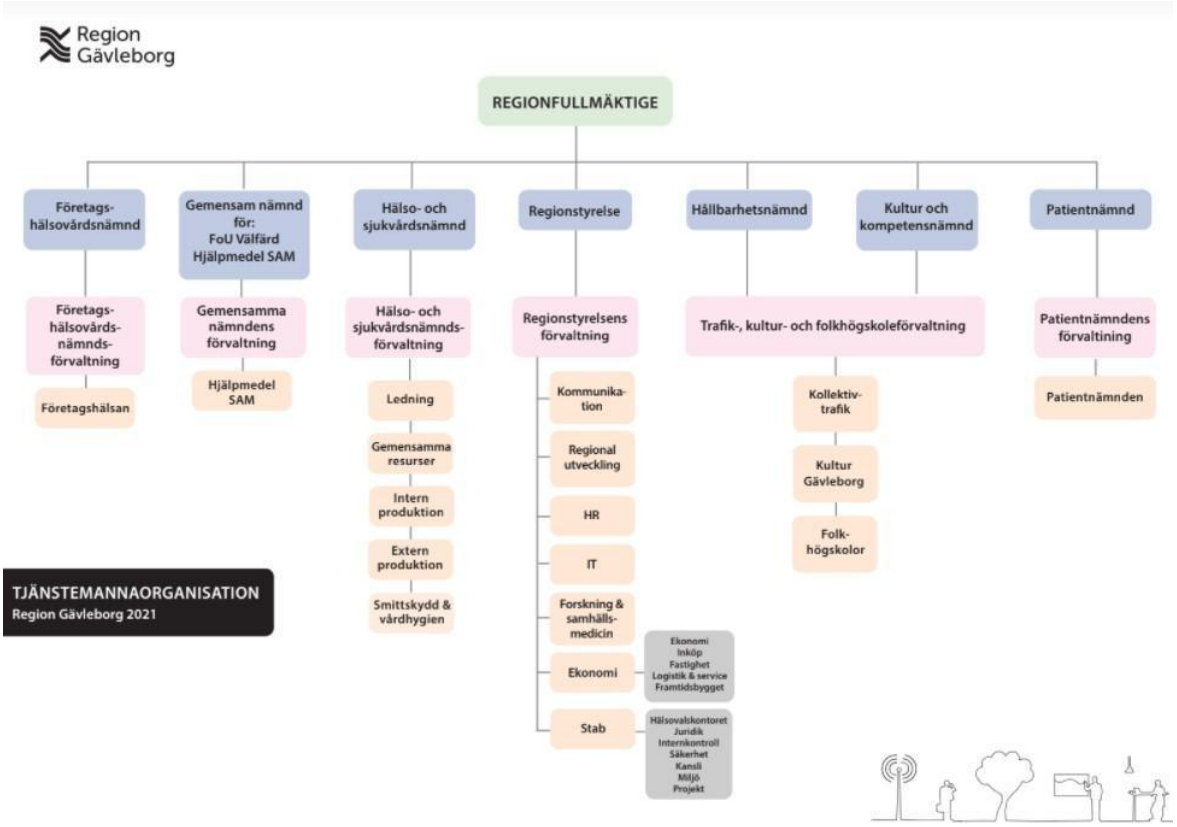
[redacted] Direktiv kring kontinuitet samt mall för arbetssätt finns att tillgå för verksamheterna, men arbetet och uppföljningen av dessa har ännu inte nått fullt genomslag.

Baserat på bedömningen ovan *rekommenderar* PwC följande:

- Slutför arbetet med utformandet av en övergripande kontinuitetsplan och säkerställ att arbetet med nedbrutna och anpassade planer för verksamheterna slutförs.

2.5 Revisionsfråga 5: Har regionen säkerställt att funktionen för informationssäkerhet har tillräckligt med mandat för att bedriva sitt uppdrag och att de förvaltar sin egen budget?

2.5.1 Iakttagelser



Vid föregående granskning hade den dåvarande funktionen för informationssäkerhet det övergripande ansvaret för att styra arbetet med informationssäkerhet i regionen. Funktionen hade det strategiska ansvaret och skötte framtagandet av styrande dokument samt den övergripande övervakningen av området. Det hade (2019) nyligen skett en organisationsförändring i regionen vilket inneburit att funktionen blivit placerad under enheten för informationsförvaltning, vilken i sin tur var placerad under kansliavdelningen på stabsförvaltningen. Funktionen för informationssäkerhet hade ingen egen budget. Granskningen konstaterade att det fanns en risk för att informationssäkerheten blir för beroende av andra delar av organisationen och att de fanns en risk för att det kontinuerliga arbetet inte skulle kunna upprätthållas. Detta ansågs även i praktiken utgöra en verksamhetsrisk. Avståndet till högsta ledning ansågs vidare medföra svårigheter att på ett effektivt sätt ha möjlighet att styra arbetet med informationssäkerhet i regionen.

Enligt uppgift från intervju i denna granskning har två organisationsförändringar genomförts sedan 2019 och informationssäkerhet har flyttats organisatoriskt. Idag är avdelningarna för säkerhet, juridik (där enheten för informationssäkerhet ingår) direkt underställda stabschefen (se bild ovan). Argumentet för den nya placeringen är att informationssäkerhet ofta tangerar rättsliga frågeställningar och att den nuvarande strukturen förenklar samarbete inom området. Fokus ligger, enligt IT-direktör och stabschef, snarare på att få ihop verksamheten bättre än på organisatorisk placering. Det centrala arbetet med informationssäkerhet består av att ta fram lämpliga mål och aktiviteter, tillämpningen sker sedan ute i verksamheterna. Mandatmässigt innebär inrättandet av

enheten för informationssäkerhet att enheten på sikt kommer att få eget budgetansvar. Då enheten är nybildad har den saknat budget för 2021. För 2022 kommer enheten dock att ha eget budgetansvar. Enligt intervjuer anses det faktum att enheten för informationssäkerhet nu har ett tydligt utpekat ansvar för frågorna vara en viktigare grund för mandat än frågan om huruvida enheten som sådan för tillfället disponerar över egen budget.

IT ligger numera under egen förvaltning. Enligt IT-säkerhetsansvarig låg IT tidigare under en gemensam förvaltning med flera olika stödjande funktioner, vilken numera är upplöst. IT är nu en egen förvaltning, där bland annat IT-säkerhet återfinns. Förvaltningen leds av en IT-direktör som lyder direkt under Regiondirektören.

Synen från den intervjuade IT-personalen är att verksamheterna tar ansvaret och att enheten för informationssäkerhet och IT-avdelningen agerar stödjande. Verksamhetens chefer beslutar om medelstilldelning för att upprätthålla de krav på informationssäkerhet som direktiv anger. Enligt uppgift finns idag spårbarhet och chefer är ansvariga för sina prioriteringar.

2.5.2 Bedömning

PwC bedömer revisionsfrågan som **till övervägande del uppfylld**.

Revisionsfrågan är ställd som att ett eget budgetansvar utgör en förutsättning för att revisionsfrågan ska kunna betraktas som uppfylld. Sedan föregående granskning har emellertid regionen vidtagit en rad åtgärder som sammantaget syftar till att stärka styrningen och genomslaget för frågor kring informationssäkerhet och IT-säkerhet. Att informationssäkerhet numera utgör en egen enhet kan betraktas som ett steg i denna riktning, liksom det faktum att IT numera utgör en egen förvaltning. Dessa åtgärder sammantaget visar att regionen uppgraderat synen på dessa frågors verksamhetskritiska vikt. Vår bedömning är därför att revisionsfrågan är till övervägande del uppfylld, eftersom organisationsförändringen inneburit att enheten för informationssäkerhet numera får anses ha tillräckligt med mandat för att bedriva sitt uppdrag. Eget budgetansvar är i detta sammanhang möjligen önskvärt, men utgör inget krav som sådant för att frågorna ska kunna drivas inom organisationen på ett tillfredsställande sätt. Regionstyrelsens krav på att verksamheterna prioriterar informationssäkerhetsfrågorna och genomför påtalade förändringar är viktigt.

2.6 Revisionsfråga 6: Har regionen genomfört, samt fortsätter att genomföra, utbildningar och kompetenshöjande aktiviteter inom området cybersäkerhet?

2.6.1 Iakttagelser

Det fanns vid tiden för den föregående granskningen ett initiativ att utbilda personal inom informationssäkerhet och genomföra medvetandehöjande åtgärder. Gällande informationssäkerhet fanns en obligatorisk introduktionsutbildning för samtliga medarbetare inom regionen. Detta var en e-learning och utgjorde ett minimikrav för alla medarbetare. På det gemensamma intranätet fanns även listor att tillgå kring vilka styrande dokument som varje roll måste ha kännedom om. Medarbetare utbildades inte specifikt i cybersäkerhet. De IT-säkerhetsansvariga hade inte som uttalad uppgift att utbilda medarbetare. Det utbildningsmaterial som medarbetare enligt rutin tog del av var systemintroducerande, utan särskilt fokus på säkerhet.

Vid tidpunkten för föregående granskning höll funktionen för informationssäkerhet på att ta fram ett material för att öka kunskapen kring vad en informationssäkerhetsincident är. Det fanns enligt

uppgift en brist på kunskap kring vad en informationssäkerhetsincident är och det behövdes därför utbildning kring vad olika typer av incidenter är (exempelvis vad en NIS-incident är och vad en personuppgiftsincident är).

Enligt uppgift finns idag två obligatoriska utbildningar; dataskydd och informationssäkerhet. De är på en grundläggande nivå och beskriver bland annat vad en incident är. Dessa två utbildningar genomförs en gång per år för nyanställda, och sedan vartannat år för alla medarbetare. Regionen försöker även sprida kunskap under en informationssäkerhetsmånad, särskilt för att öka medvetenhet kring phishing och vad som skall göras vid en incident och liknande. Utbildningarna sker enligt uppgift ibland via e-portal och ibland via Plexus (regionens portal). Regionen genomför rollbaserade utbildningar, primärt gentemot informationsägare, och de utpekade personerna i samtliga verksamheter som har ett operativt ansvar för att utföra informationssäkerhets- och dataskyddsrelaterade aktiviteter. I början av 2021 genomfördes även en riktad incidentutbildning till hela IT-förvaltningen. Enligt information från intervju så arbetar regionen även med enhetlig information till samtliga medarbetare angående hur de bör agera med hänsyn till ransomware.

Enligt uppgift från intervju med regionens IT-direktör har det utöver detta genomförts kompetensutveckling bland annat med hjälp av MSB:s generella utbildningsmaterial som vänder sig till chefer inom offentlig verksamhet, och samtliga informationsägare fick under hösten 2020 genomgå MSBs nanolearning utbildning avseende operativ informationssäkerhet. Den egna bedömningen bland de intervjuade är att medarbetarna får en systematisk utbildning. IT-direktören påtalar att det är viktigt att se till sammanhang och att det sker kompetenshöjande insatser avseende exempelvis vissa typer av incidenter och att detta inom ramen för ordinarie daglig verksamhet och löpande.

Det finns dock enligt uppgift från intervju ingen dokumenterad utbildningsplan för varje medarbetare, eller en rollbaserad d:o. Det genomförs inga tester för att säkerställa att kompetensen är tillräcklig.

2.6.2 Bedömning

PwC bedömer revisionsfrågan som **till övervägande del uppfylld.**

Regionen tillhandahåller introduktionsutbildningar i informationssäkerhet och i dataskydd till alla anställda, och utöver detta utbildas chefer vid behov ytterligare bland annat med hjälp av MSB:s utbildningsmaterial. Genom informationssäkerhetsmånaden söker regionen höja medvetenheten hos medarbetarna genom punktinsatser under denna månad en gång per år.

Vi konstaterar att medvetandehöjande åtgärder utgör en fundamental del i det löpande arbetet med informations- och IT-säkerhet. Kunskap om pågående attacker och exempelvis förekomsten av ransomware är mycket viktiga beståndsdelar i en organisation, då det är människors beteende och agerande som oftast utgör den svagaste länken i säkerhetsarbetet, oavsett övriga tekniska skydd. Vår bedömning är dock att utbildningsinsatserna kan höjas (se rekommendationerna nedan).

Baserat på bedömningen ovan *rekommenderar* PwC följande:

- Överväg att skapa ett dokumenterat rollbaserat utbildningspaket för olika personalgrupper inom organisationen.

- Överväg att utveckla dokumenterade rollbaserade eller individuella utbildningsplaner, vilka följs upp för att säkerställa att obligatoriska moment verkligen genomförts.
- Överväg att genomföra ytterligare medvetandehöjande kampanjer kring ransomware, phishing eller lösenordsbyte, gärna vid olika tidpunkter varje år.

3. Revisionell bedömning

PwC bedömer att regionstyrelsen **till övervägande del** vidtagit ändamålsenliga åtgärder med anledning av 2019 års granskning. Exempel på hur arbetet med frågorna utvecklats inom organisationen har åskådliggjorts under respektive revisionsfråga, med rekommendationer till ytterligare förbättringar.

3.1 Bedömningar mot revisionsfrågor

Revisionsfråga	Kommentar
Revisionsfråga 1: Har regionen fastställt styrande dokument inom både informations- och cybersäkerhet?	**Helt uppfylld**
Revisionsfråga 2: Har regionen fastställt dokumenterade processer för arbetet med informations- och cybersäkerhet?	**Till övervägande del uppfylld**
Revisionsfråga 3: Har regionen formaliserat och systematiserat arbetet med informationssäkerhetsrisker?	**Till övervägande del uppfylld**
Revisionsfråga 4: Har regionen en incidenthanteringsprocess som samordnas genom samverkan mellan informationssäkerhetsavdelningen och IT-avdelningen?	**Till övervägande del uppfylld**
Revisionsfråga 5: Har regionen säkerställt att funktionen för informationssäkerhet har tillräckligt med mandat för att bedriva sitt uppdrag och att de förvaltar sin egen budget?	**Till övervägande del uppfylld**
Revisionsfråga 6: Har regionen genomfört, samt fortsätter att genomföra, utbildningar och kompetenshöjande aktiviteter inom området cybersäkerhet?	**Till övervägande del uppfylld**

Bilaga 1 - Granskad dokumentation

Namn på dokumentet	Fastställandedatum (alt. senaste revisionsdatum)
Arbetsfördelning för Systemförvaltning, IT-avdelningen	2019-03-21
Behovs och riskanalys för behörighetstilldelning - Direktiv, Hälso och sjukvård, Region Gävleborg	2021-05-05
Behovs och riskanalys för behörighetstilldelning - Rutin. Hälsooch sjukvård Region Gävleborg	2021-05-05
Grundläggande regler för IT-säkerhet - Direktiv Region Gävleborg	2020-02-24
Incidenthantering IT-avdelningen	2016-10-07
Informations- och IT-säkerhet vid distansarbete	2020-10-21
Informationssäkerhet - Digital kommunikation - videosamtal, telefonsamtal, chatt, delning av skrivbord och videomöte - Rutin	2021-01-27
Informationssäkerhet - Direktiv för ansvar och roller	2018-03-29
Informationssäkerhet - Direktiv för hantering av informationssäkerhetsincidenter	2020-09-16
Informationssäkerhet - Direktiv för kontinuitetshantering	2021-01-13
Informationssäkerhet - Direktiv för lagring och kommunikation i digitala kanaler	2021-04-22
Informationssäkerhet - Direktiv för molntjänster. Region Gävleborg	2019-09-02
Informationssäkerhet - Direktiv för styrande dokument i LIS. Region Gävleborg	2021-03-08
Informationssäkerhet - Direktiv för systematiskt och riskbaserat informationssäkerhetsarbete	2020-09-16
Informationssäkerhet - Direktiv för systematiskt och riskbaserat informationssäkerhetsarbete - Region Gävleborg	2020-09-16
Informationssäkerhet - Generell rutin för personuppgiftsbehandling. Region Gävleborg	2021-04-22
Informationssäkerhet - Inbyggt dataskydd och dataskydd som standard rutin. Region Gävleborg	2021-04-30
Informationssäkerhet - Mall för kontinuitetsplanering	2020-09-30
Informationssäkerhet - Personuppgiftsbiträdesavtal - Rutin för upprättande. Region Gävleborg	2021-04-22

Informationssäkerhet - Rutin för hantering av informationssäkerhetsincidenter	2021-06-02
Informationssäkerhet - Rutin för hantering av personuppgiftsincidenter	2021-06-22
Informationssäkerhet - Rutin för kontinuitetshantering	2020-09-23
Informationssäkerhet - rutin för systematiskt och riskbaserat informationssäkerhetsarbete - Region Gävleborg	2021-06-22
Informationssäkerhetsråd	2020-11-25
MFA-registrering - rutin. Region Gävleborg	2021-01-04
MFA-registrering -rutin. Externa Företag med RG användarkonton	2021-01-04
Molntjänster Regler för Införande och Hantering - Rutin Region Gävleborg	2019-10-14
Övergripande riskanalys avseende informationssäkerhet för Hälso- och sjukvården	2021-06-14
Regler för hantering databaser och SQL server	2020-10-16

Bilaga 2 - Intervjuade personer

Funktion
IT-säkerhetsansvarig
Enhetschef IT-stödsystem
Enhetschef IT-teknik
Informationssäkerhetsansvarig och DSO för Region Gävleborg
IT-direktör
Stabschef

Karin Magnusson	**Linus Owman**
Uppdragsledare	*Projektledare*
2021-09-24	

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Region Gävleborgs revisorer enligt de villkor och under de förutsättningar som framgår av projektplan från den 16 april 2021. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.