MISSIV

DNR:23RV10
Fastställt 2024-01-24
Revisorerna Region Kronoberg

TILL REGIONFULLMÄKTIGE

Granskning av Region Kronobergs informationssäkerhet

Region Kronobergs revisorer har låtit genomföra en granskning av Region Kronobergs informationssäkerhet. Granskningen har utförts av konsulter från Helseplan Consulting Group AB och utgått från syfte och revisionsfrågor som revisorerna har fastställt.

Granskningens syfte och övergripande revisionsfråga

Syftet med granskningen är att ge revisorerna ett underlag för att bedöma om Regionstyrelsen har säkerställt att:

- Det finns en tillräcklig intern styrning (exempelvis genom beslut och riktlinjer, budgetmedel), uppföljning och kontroll som säkerställer ett ändamålsenligt systematiskt arbetssätt med informationssäkerheten i regionen?

- Den interna kontrollen avseende regionens cybersäkerhet är tillräcklig?

- Region Kronobergs nuvarande tekniska IT-säkerhet är tillräcklig och tillfredställande för att reducera risker för obehörigt intrång till en acceptabel nivå? Granskningen syftar även till att kontrollera om regionstyrelsen utifrån tidigare noterade brister vidtagit åtgärder.

Sammanfattande bedömning

Den samlade bedömningen är att Regionstyrelsen har säkerställt att

- **Det finns en tillräcklig intern styrning, uppföljning och kontroll som säkerställer ett ändamålsenligt systematiskt arbetssätt med informationssäkerheten i regionen.** Detta sker framför allt genom den utvecklade och beslutade styr- och samverkansmodellen, som skapar förutsättningar för ett effektivt arbete och god relation mellan de enheter som äger sakfrågorna och verksamheterna som ska följa beslutade riktlinjer. Region Kronoberg arbetar också enligt ISO 27000 vilket medför att det finns en struktur för utförande men också för regelbundna översyner som gynnar regionens arbete.

- **Den interna kontrollen avseende regionens cybersäkerhet är tillräcklig.** Region Kronoberg uppvisar ett aktivt arbete och samtidigt en medvetenhet kring att det finns krav på ständiga förbättringar. De framtagna utbildningarna kommer att stärka enskilda medarbetare och verksamheterna som helhet i att arbeta med informationssäkerhet.

- **Region Kronobergs nuvarande (med vilket avses tidpunkten november 2023) tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå.** Även här finns det kompetens och kunskap om sakfrågorna i regionen och det pågår ett ständigt arbete med att försöka minska riskerna som uppstår genom den mänskliga faktorn.

I granskningen framgår även

I granskningen framgår även följande:

- Det systematiska informationssäkerhetsarbetet i Region Kronoberg följer standarden för ISO 27000, men det är inte ett mål för Region Kronoberg att bli certifierade.

- Bedömningen görs i granskningen att Regionstyrelsen delvis säkerställt att det finns rutiner för kontroll av systembehörigheter som är ändamålsenliga.

- I granskningen noteras att uppföljningen på en övergripande politisk nivå är svag givet resultatet från protokollgranskningen.

Identifierade förbättringsområden

Granskningen har identifierat förbättringsområden. Regionstyrelsen rekommenderas att:

- Trots tydliga förbättringar fortsätta följa upp Region Kronobergs arbete med informationssäkerhet.

- Skapa förutsättningar för att beslutade riktlinjer och rutiner är välkända i organisationen genom att hålla frågorna aktuella och relevanta så att informationssäkerhetsperspektivet finns med i alla delar av verksamheten.

Svar önskas från Regionstyrelsen

Mot bakgrund av vad som framkommit i granskningen önskar revisorerna ett svar från Regionstyrelsen med uppgift om tidsplan för eventuella planerade åtgärder samt redovisning av hittills vidtagna åtgärder som tillvaratar de förbättringsmöjligheter som föreslagits.
För varje rekommendation som förslagits ska följande framgå:

- Hittills vidtagna åtgärder
- Eventuella planerade åtgärder
- Tidplan för eventuella planerade åtgärder
- Eventuella andra synpunkter

Revisorerna kommer i ett senare skede vilja ha en avstämning från styrelsen på hur arbetet har fortskridit avseende planerade åtgärder.

Ulf Engqvist
Ordförande Revisionen

Ingrid Hugosson
Vice ordförande Revisionen

Bilaga: Granskningsrapport från Helseplan Consulting Group AB

NETPUBLICATOR® VERIFIED

Detta dokument är elektroniskt signerat och juridiskt bindande.

Signed by: ULF ENGQVIST
Date: 2024-01-26 10:08:37
BankID refno: 7fdea165-1ee7-4797-ab56-12ccf437b787

Ordförande: Ulf Engqvist

Signed by: INGRID HUGOSSON
Date: 2024-01-25 15:03:26
BankID refno: db85adc7-aa07-445f-af68-512248394b31

Vice ordförande: Ingrid Hugosson

Granskning av Region Kronobergs informationssäkerhet

Helseplan Consulting Group AB

Januari 2024

Ulrike Deppert
Emma Pettersson
Erik Blandin

Helseplan Drottninggatan 97 113 60 Stockholm tel 08-410 408 00 helseplan.se

Innehåll

2024-01-25

X

Ulrike Deppert
Projektledare, Helseplan Consulting Group AB
Signerat av: 4a83dc0d-14a6-4001-adbb-d0211d97188f

1. Sammanfattning och slutlig bedömning

Revisorerna i Region Kronoberg har uppdragit åt Helseplan Consulting Group AB (Helseplan) att genomföra *Granskning av Region Kronobergs informationssäkerhet*. Granskningens revisionsfrågor har besvarats genom dokumentgranskning, 10 semistrukturerade intervjuer samt en avstämning mot NIST Cybersäkerhetsramverk. Granskningen har genomförts under perioden juni 2023 till januari 2024.

Den samlade bedömningen är att Regionstyrelsen har säkerställt att

- **det finns en tillräcklig intern styrning, uppföljning och kontroll som säkerställer ett ändamålsenligt systematiskt arbetssätt med informationssäkerheten i regionen.** Detta sker framför allt genom den utvecklade och beslutade styr- och samverkansmodellen, som skapar förutsättningar för ett effektivt arbete och god relation mellan de enheter som äger sakfrågorna och verksamheterna som ska följa beslutade riktlinjer. Region Kronoberg arbetar också enligt ISO 27000 vilket medför att det finns en struktur för utförande men också för regelbundna översyner som gynnar regionens arbete.
- **den interna kontrollen avseende regionens cybersäkerhet är tillräcklig.** Region Kronoberg uppvisar ett aktivt arbete och samtidigt en medvetenhet kring att det finns krav på ständiga förbättringar. De framtagna utbildningarna kommer att stärka enskilda medarbetare och verksamheterna som helhet i att arbeta med informationssäkerhet.
- **Region Kronobergs nuvarande** (med vilket avses tidpunkten november 2023) **tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå.** Även här finns det kompetens och kunskap om sakfrågorna i regionen och det pågår ett ständigt arbete med att försöka minska riskerna som uppstår genom den mänskliga faktorn.

Helseplan rekommenderar Regionstyrelsen att

- trots tydliga förbättringar fortsätta följa upp Region Kronobergs arbete med informationssäkerhet.
- skapa förutsättningar för att beslutade riktlinjer och rutiner är välkända i organisationen genom att hålla frågorna aktuella och relevanta så att informationssäkerhetsperspektivet finns med i alla delar av verksamheten.

2. Inledning

2.1. Bakgrund

Sveriges regioner behandlar känslig och viktig information. Om informationen hamnar i fel händer finns det risk för allvarliga konsekvenser både för medborgarna och för landet.

Informationssäkerhet är det arbete som görs för att hindra att information läcker ut, förvanskas eller förstörs, men det ingår även att se till att information är tillgänglig när den behövs.[1]

IT-säkerhet är den del av informationssäkerhet som avgränsas till it-resurser.[2] Revisorerna genomförde 2016 en uppföljande granskning av IT-säkerhetsarbetet som identifierade ett flertal avvikelser/förbättringsområden.

I årsredovisningen för Region Kronoberg för räkenskapsår 2022 framgår under händelser av väsentlig betydelse att det finns en ökad hotbild gällande **cybersäkerhet**[3], där hotbildsnivån eskalerades ytterligare genom utvecklingen i Östereuropa och Ukraina.[4] Cybersäkerhet är informationssäkerhet avseende indirekta och direkta, externa beroenden och hot som finns i ett större och mer komplext digitalt ekosystem än (enbart) inom den egna organisationen eller samhället.

Med anledning av ovanstående och utifrån en bedömning av risk- och väsentlighet har revisorerna beslutat att genomföra en granskning av Region Kronobergs informationssäkerhet. Granskningen omfattas av revisionens långsiktiga planering för fördjupade granskningar och är ett identifierat riskområde i revisionsplanen 2023.

---

[1] Sveriges Kommuner och Region (2021) *En guide för tillräckligt god informationssäkerhet vid införande av välfärdsteknik och digitala tjänster*. Sida Inledning.

[2] Myndigheten för samhällsskydd och beredskap. Termbank för informationssäkerhet: Sökord ”Informationssäkerhet”. [https://termbanken.informationssakerhet.se/], hämtad 2023-05-05.

[3] Myndigheten för samhällsskydd och beredskap. Termbank för informationssäkerhet: Sökord ”IT-säkerhet”. [https://termbanken.informationssakerhet.se/], hämtad 2023-05-05.

[4] Årsredovisning Region Kronoberg 2022. Sida 12.

Uppföljande granskning av IT-säkerhetsarbetet genomförd 2016

Granskningen identifierade bland annat följande avvikelser/förbättringsområden;

- Formella regler saknas för informationsklassning
- Uppföljning av tilldelade behörigheter
- Granskning av efterlevnad av rutiner och kontroller
- Behörigheter i Cosmic[5]
- Loggkontroll av patientinformation
- Kraftfulla behörigheter i Aplus[6]
- Dataöverföring till Aplus
- Förstärkning av process för programförändringar
- Utbildning
- Extern kommunikation

2.2. Syfte

Granskningen syftar till att ge revisorerna ett underlag för att bedöma om Regionstyrelsen har säkerställt att:

- Det finns en tillräcklig intern styrning (exempelvis genom beslut och riktlinjer, budgetmedel), uppföljning och kontroll som säkerställer ett ändamålsenligt systematiskt arbetssätt med informationssäkerheten i regionen?
- Den interna kontrollen avseende regionens cybersäkerhet är tillräcklig?
- Region Kronobergs nuvarande tekniska IT-säkerhet är tillräcklig och tillfredställande för att reducera risker för obehörigt intrång till en acceptabel nivå?

Granskningen syftar även till att kontrollera om regionstyrelsen utifrån tidigare noterade brister vidtagit åtgärder.

[5] Vårdinformationssystem.
[6] Redovisningssystem.

2.3. Revisionsfrågor

Har Regionstyrelsen säkerställt att:

Informationssäkerhet

- Det finns ändamålsenliga styrande dokument, riktlinjer för informationssäkerhet?
- Det finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i region?
- Regionens verksamheter arbetar systematiskt med att identifiera och analysera risker för informationssäkerheten?
- Det finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?
- Är regionens incidenthanteringsprocess ändamålsenlig?

IT-säkerhet - intrångsskydd

- Det finns styrande dokument, såsom policy, riktlinjer för IT-säkerhet?
- Roller och ansvar för informationssäkerheten är tydliggjord och uppfattad mellan verksamheten och IT-organisation?
- Eventuella attacker upptäcks och icke önskvärda incidenter hanteras på ett ändamålsenligt sätt?
- Säkerheten avseende intrång av extern och intern aktör är ändamålsenlig?
- Det finns rutiner för kontroll av systembehörigheter som är ändamålsenliga?
- Åtgärder har vidtagits med anledning av de brister samt de förbättringsförslag som framfördes i den uppföljande granskningen från 2016?

2.4. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för granskningens analyser, slutsatser och bedömningar. Dessa har bland annat varit:

- Kommunallag (2017:725) 6 kapitlet 6§
- Säkerhetsskyddslag (2018:585)
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- Offentlighets- och sekretesslagen (2009:400)

Helseplan följer SKYREV:s riktlinjer för god redovisningssed.

2.5. Avgränsningar

Viss uppföljning av uppföljande granskning av IT-säkerhetsarbetet ska också ingå men då det är länge sedan granskningen genomfördes sker uppföljningen något mer översiktligt utifrån aktualitet. Avgränsningar kan komma att göras under pågående granskningsarbete.

2.6. Metod

2.6.1. Dokumentgranskning

En förteckning över styrande och redovisade dokument som Helseplan har granskat finns i *Bilaga 1*.

2.6.2. Intervjuer

Semistrukturerade djupintervjuer har genomförts enligt en i förväg fastställd intervjumall. Intervjuer har genomförts med förtroendevalda politiker för regionstyrelsen samt med regiondirektör och sakkunniga, som till exempel säkerhetschef och informationssäkerhetsstrateg, inom förvaltningen. Totalt har 10 personer intervjuats, se *Bilaga 2*.

2.6.3. NIST Cybersäkerhetsramverk

Granskningen har stöttat sig på NIST Cybersäkerhetsramverk (NIST) för att besvara den övergripande revisionsfrågan om den interna kontrollen avseende regionens cybersäkerhet är tillräcklig. Ramverket används inte i Region Kronoberg, som istället arbetar efter ISO 27000-standarden som är vedertagen i Sverige. NIST bygger på fem områden: Identifiera, Skydda, Upptäcka, Respondera och Återställa. Dessa har inom ramen för granskningen nyttjats för att pröva Region Kronobergs interna kontroll avseende cybersäkerhet.

- Identifiera: Region Kronobergs förmåga att identifiera kritiska informationstillgångar och data, det nuvarande läget för styrning och övergripande riskhantering när det kommer till cybersäkerhet.

- Skydda: Region Kronobergs nuvarande tillstånd när det kommer till att skydda regionens information samt avskräcka från hot. Denna kategori inbegriper även förmågan att hantera behörigheter och konton samt säkerhet och skyddsåtgärder kopplad till data som lagras, transporteras och bearbetas.
- Upptäcka: Region Kronobergs förmåga att övervaka IT- och säkerhetsrelaterade händelser. Detta medför bland annat möjlighet till nätverksövervakning, sökning efter skadlig kod och sårbarheter.
- Respondera: Region Kronobergs rutiner för åtgärdsplanering och aktiviteter kopplade till interna och externa intressenter vid en eventuell incident. Denna förmåga inkluderar bland annat incidenthantering.
- Återställa: Region Kronobergs processer för kontinuitetshantering och förmågor relaterade till resiliens och återhämtning efter hantering av incidenter.

2.7. Projektorganisation

Uppdragsgivare har varit Region Kronobergs revisorer med Gunilla Jerklind Platzer som kontaktperson. Från Helseplan har Ulrike Deppert varit projektledare och Emma Pettersson konsult. Erik Blandin har varit expert. Pär Ahlborg har varit kvalitetsgranskare. Rapporten har sakgranskats av företrädare för politiken samt verksamheten. Granskningen genomfördes mellan juni 2023 och januari 2024.

3. Definitioner

Region Kronoberg har tagit fram nedan definitioner som rapporten kommer att nyttja.

Informationssäkerhet är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder för att skydda informationen mot de hot den kan utsättas för.[7]

IT-säkerhet är de delar av begreppet informationssäkerhet som avser säkerheten i den tekniska hanteringen av information som bearbetas, lagras och kommuniceras elektroniskt samt administrationen kring detta.[8]

[7] *Plan för informationssäkerhet och skydd av personuppgifter* (giltig från och med 2021-01-26). Sida 1.
[8] *Plan för informationssäkerhet och skydd av personuppgifter* (giltig från och med 2021-01-26). Sida 3.

4. Iakttagelser, bedömningar och rekommendationer

4.1. Informationssäkerhet

*I detta avsnitt besvaras revisionsfrågorna ”*Har Regionstyrelsen säkerställt att det finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i region?*”, ”*Har Regionstyrelsen säkerställt att regionens verksamheter arbetar systematiskt med att identifiera och analysera risker för informationssäkerheten?*”, ”*Har Regionstyrelsen säkerställt att det finns ändamålsenliga styrande dokument, riktlinjer för informationssäkerhet?*”, ”*Har Regionstyrelsen säkerställt att det finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?*” *samt* ”Är regionens incidenthanteringsprocess ändamålsenlig?*”.*

4.1.1. Organisation

I *Arbetsordningar och reglementen för den politiska organisationen i Region Kronoberg 2023-2026* framgår att Regionstyrelsen ansvarar för den övergripande strategiska IT-utvecklingen samt ansvarar för övergripande säkerhetsfrågor och informationssäkerhet. I *Delegationsordning för regionstyrelsen 2023-2026 inklusive vidaredelegering* finns ett särskilt avsnitt om säkerhet och informationssäkerhet som tydliggör hur Regionstyrelsen har delegerat vissa uppgifter. Det handlar framför allt om hantering av personuppgifter, dataskyddsombud och registerutdrag men det beskrivs också att regiondirektör och säkerhetschefen ansvarar för säkerhetsskyddsklassning av funktioner och har rätt att säkerhetspröva den som ska delta i säkerhetskänslig verksamhet.

Ansvaret för informationssäkerhet i förvaltningen är strukturerat under säkerhetsenheten. Säkerhetsenheten är placerad under kansliet i regionstaben. Enheten arbetar nära regionens ledning men även med övriga verksamheter och har löpande kontakt med andra samverkansparter på nationell, regional och lokal nivå. Uppdraget omfattar bland annat strategiska och operativa frågor inom ett brett område, till exempel med avvikelsehantering i säkerhetsrelaterade situationer eller med hantering av och ledning vid allvarliga händelser.

Informationsteknik (IT) har ansvaret för IT-säkerheten, som är en delmängd av informationssäkerheten. Under 2023 flyttade IT från att vara en servicefunktiontill att organiseras under regionövergripande. Syftet med omorganisationen var att belysa att IT inte enbart är en serviceleverantör. I *Verksamhetsförändring Informationsteknik* (2023) beskrivs detta som att informationsteknik har förflyttats som verksamhet från en

linjelevererande serviceorganisation till en regionövergripande och värdeskapande partner i regionens omställningsarbete. Nu ligger funktionen direkt under regiondirektören, vilket också tydliggör styrningen. Intervjuade uppger att framtida förändringar kan komma att ske för att säkerställa att IT får ett tydligt uppdrag och skapar förutsättningar för organisationen att arbeta ändamålsenligt.

År 2019 skapades en målbild och vision kring en gemensam styr- och samverkansmodell som reglerar hur samtliga organisatoriska delar inom Region Kronoberg ska struktureras och samverka kring utveckling av verksamheten med hjälp av IT-stöd. I intervjuer beskrivs hur modellen har utvecklats över tid med tydliga, årliga målsättningar om till exempel antal objekt som har anslutits till modellen och hur kompetensen ska byggas. Det övergripande syftet med modellen är att skapa hög förmåga, takt och effekt av verksamhetsutveckling med IT-stöd, uppger intervjuade. Enligt dokument *Sammanfattning av styrstruktur för verksamhetsutveckling med hjälp av IT-stöd* (odaterad) har regionen utvecklat en egen styr- och samverkansmodell som är inspirerad av pm3[9]. Kortfattat grupperas regionens IT-stöd samtliga objekt i fyra objektfamiljer. *Dokumentet* beskriver att indelningen utgår från ett verksamhetsperspektiv där process och görande är i fokus, inte organisation eller teknik. Det ger en verksamhetsorienterad struktur för styrning och leverans av IT-stöd menar intervjuade. De fyra objektfamiljerna är enligt *dokumentet*:

- Hälso- och sjukvård. Här samlas objekt som har i uppdrag att säkra stabilitet och utveckling för kärnverksamheten hälso- och sjukvård.
- Trafik. Objekten här avser att stödja aktiviteter inom allmän kollektivtrafik, skoltrafik och särskild kollektivtrafik samt ärendehantering och inventariehantering för trafikverksamheten.
- Stödverksamhet. Här finns objekt som har i uppdrag att säkra stabilitet och utveckling av IT-stöd för stödverksamheter, till exempel ekonomi, fastighet, HR och utbildning.
- IT-verksamhet. Här ingår objekt som har i uppdrag att säkra stabilitet och utveckla förutsättningsteknik, bland annat digital arbetsplats, identitet och skydd samt leverans.

[9] pm³ är en styr- och samverkansmodell som möjliggör för en organisation att skapa balans mellan stabil leverans och effektiv verksamhetsutveckling. pm3: pm3-modellen. https://pm3.se/pm3-modellen/. [hämtad 2023-11-07]

Dokumentet beskriver vidare att verksamhetsutveckling med IT-stöd organiseras i en tydlig styrstruktur:

- På strategisk nivå finns Styrgrupp IT och digitalisering samt objektfamiljstyrgrupper.
- På operativ nivå behövs specialister för att utföra aktiviteter. Objektspecialister med verksamhetskompetens och IT-specialister med teknisk kompetens. Strukturen för operativa roller utformas utifrån respektive objekts struktur och behov.

I *Plan för informationssäkerhet och skydd av personuppgifter* (2021) framgår vilka funktioner som bär ansvar för informationssäkerheten. Detta skapar tydlighet i organisationen, menar intervjuade, särskilt som det också omfattar samtliga nivåer. Till exempel beskrivs att regiondirektören har det övergripande ansvaret till att verksamhetschefen ansvarar för att medarbetare känner till och följer gällande riktlinjer och rutiner. Vidare redogör *planen* för att särskilda funktioner inom organisationen är ansvariga för den grundläggande strukturen, som att säkerhetschefen ansvarar för kravställning, informationssäkerhetsstrategen förvaltar och utvecklar ledningssystemet för informationssäkerhet (LIS) samt att objektägare har det övergripande ansvaret för att informationen och systemen uppfyller informationssäkerhetskraven.

4.1.2. Riskidentifiering och analys

Förutom ansvaret som åligger varje chef eller specialistfunktion är en del av det systematiska arbetet med att identifiera och hantera risker att följsamhet och efterlevnad ska ske inom linjeorganisationen. *Plan för informationssäkerhet och skydd av personuppgifter* tydliggör att varje medarbetare ansvarar för att följa uppställda regler och rapportera funktionsstörningar och fel i informationssystem, utrustningar och informationsinnehåll enligt rutin. Intervjuade menar att det finns variationer i hur väl medarbetare utövar ansvaret men att det är en viktig del för att regionen ska ges förutsättningar för att arbeta strukturerat och förebyggande med informationssäkerhet.

Vidare noteras att Inera AB i sin *revisionsrapport* (2019), som omfattar SITHS Tillitsramverk[10], konstaterar övergripande att Region Kronoberg har ett gott klimat och

[10] SITHS är benämning för konceptet Identifieringstjänsten SITHS. Tillitsramverket fastställer gemensamma krav för utfärdare inom SITHS. Tillämpningen av tillitsramverket beskrivs i de rutiner som

en god samarbetskultur. Bland de styrkor som har identifierats, i relation till SITHS Tillitsramverk, finns bland annat en proaktiv och förbättringsorienterad organisation samt en aktiv verksamhetsutveckling för att göra IT-stöd användbart.

Dokument *Rutin för risk- och sårbarhetsanalyser* (2020, giltig till och med 2022-05-02) beskriver hur det analysarbetet sker generellt i Region Kronoberg. Det är således ingen rutin som enbart avser informationssäkerheten utan som gäller för all verksamhet inom regionen. Av *rutinen* framgår att riskanalyser följer Sveriges Kommuner och Regioners (SKR) metodik för genomförande av riskanalys samt att en mall har tagits fram som innehåller stödtexter, analysschema samt fastställda bedömningsskalor och definitioner. Vidare beskrivs i *rutinen* att riskanalyser ska genomföras vid ett antal situationer. För denna granskning är bland annat följande centralt:

- Regionövergripande risk- och sårbarhetsanalyser inom arbetet med den nationella krisberedskapen och civilt försvar samt för att förmedla övergripande riskbilder till beslutsorgan inom organisationen. Säkerhetsenheten ansvarar för analys och sammanställning.
- Vid en upprepad iakttagelse av risker i system, verksamhet och processer.
- Inför planerade driftstopp med möjlig påverkan på organisationen och dess verksamheter.
- Inför beslut om förändringar i drifts- och/eller IT-system samt inför implementering av förändringar (till exempel uppdateringar och införande).
- Årligen i det informationssäkerhetsarbete som syftar till att upprätthålla en hög säkerhet i nätverk och informationssystem, enligt Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Som *rutinen* tydliggör finns det särskilda situationer när informationssäkerheten är i fokus men det ska också genomföras generella riskanalyser där informationssäkerheten kan vara en delmängd uppger intervjuade. I intervjuer framgår att riskanalyser där informationssäkerhet behandlas varierar mellan verksamheterna men att detta inte är en utmaning enbart för informationssäkerhetsfrågor utan omfattar samtliga verksamhetsaspekter.

---

fastställs av SITHS Policy Authority, den grupp som äger, definierar och följer upp regelverket för SITHS. Inera AB: Termer och Begrepp. https://inera.atlassian.net/wiki/spaces/IAM/pages/538870657/Termer+och+Begrepp. [hämtad 2023-11-05]

Som exempel på hur verksamheter arbetar med att identifiera och analysera risker för informationssäkerheten nämner intervjuade bland annat den information som skrivs i *Patientsäkerhetsberättelsen* (2022). I ett eget avsnitt rörande informationssäkerhet framgår att uppdraget är att säkerställa att verksamhetsstödet följer kraven som anges i *Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården* (HSLF-FS 2016:40). I *föreskrifterna* beskrivs bland annat att det åligger vårdgivaren, det vill säga Region Kronoberg, att löpande bedöma om det finns risker för händelser som medför att kraven i föreskrifterna inte uppfylls. Sådana riskanalyser ska uppskatta sannolikhet för att händelser inträffar, bedöma negativa konsekvenser samt dokumentera analysen. I *patientsäkerhetsberättelsen* redogörs för Region Kronobergs arbete med att förbättra informationssäkerheten och att åtgärder, till exempel skydd mot olovlig åtkomst och utbildning, vidtas.

4.1.3. Styrande dokument och uppföljning

I Region Kronoberg sker nedbrytningen av regionplanen till nämndplanen som i sin tur ligger till grund för verksamhetsplanen inom förvaltningen och för enskilda enheter. Regionen har också beslutade årshjul för planering, uppföljning och rapportering. Detta ger enligt intervjuade en tydlig röd tråd för styrningen av sakfrågorna samt utrymme att skapa tätare uppföljningar om behov finns.

Regionens verksamhetsplaneringssystem är Stratsys och intervjuade uppger att vissa aktiviteters innehåll inte kan dokumenteras i systemet. Stratsys är ett transparent och molnbaserat IT-stöd och saknar funktion för att arbeta med sekretessbelagt information. Det gör att detaljplaneringen sköts separat, att status inte syns i Stratsys men att övergripande aktiviteter klarmarkeras när de är utförda, uppger intervjuade. I *Plan för informationssäkerhet och skydd av personuppgifter* (2021) tydliggörs också att efterlevnaden av fastställda mätetal rapporteras till Stratsys. Det är informationssäkerhetsstrategen som ansvarar för att sammanställa efterlevnad på aggregerad nivå för att kunna jobba systematiskt med informationssäkerhet.

Plan för informationssäkerhet och skydd av personuppgifter styr arbetet inom regionen. I den beskrivs målsättningen med regionens informationssäkerhetsarbete, som övergripande handlar det om att invånarna ska vara förvissade om att information hanteras korrekt och har tillräckligt skydd. Det betyder, enligt *planen*, att informationen skyddas så att enbart behöriga får tillgång till den (konfidentialitet), att den är korrekt och inte är manipulerad eller förstörd (riktighet) och att den finns när den behövs (tillgänglighet). Det beskrivs vidare i *planen* att skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för regionens verksamheter att

uppnå sina mål. I intervjuer påpekas att det kan finnas motsatsförhållanden mellan att bedriva verksamhet och att arbeta enligt skyddande principer. Intervjuade uppger att det handlar om att tillsammans med verksamheten diskutera vilka behov som finns och sedan tillsammans se över lösningar för att verksamheternas funktionalitet, kvalitet och effektivitet kan ske i samklang med en god informationssäkerhet.

En del av styrningen inom informationssäkerhet inkluderar också planer för de olika IT-objekten som förvaltas inom regionen. Enligt presentationen *Styrochsamverkan_översikt* (2023) pekar objektplanen ut fokus och sätter ramarna för uppdraget att utveckla och säkra stabilitet i IT-stöd. Regionens inriktningar, verksamhetsplaner, lagkrav och tekniska förutsättningar är exempel på input till objektplanen, vilket gör att den har hög följsamhet till politiska viljeinriktningar och beslutade verksamhetsplaner på regionövergripande nivå menar intervjuade.

Det systematiska informationssäkerhetsarbetet följer standarden för ISO 27000. Enligt Svenska Institutet för Standarder ger ISO 27000 förutsättningarna för att applicera säkerhetsåtgärder utifrån ett riskbaserat angreppssätt samt följa upp och förbättra[11]. Region Kronoberg är inte certifierad enligt standarden men nyttjar den som en tydlig utgångspunkt för att skapa struktur och ledningssystem uppger intervjuade. Intervjuade uppger att det eventuellt finns någon kommun eller region som är certifierad och att detta inte är ett mål för Region Kronoberg. ISO 27000 utgör basen för det LIS som gäller för regionen och regionen följer standarden även om verksamheten inte officiellt är certifierad. I ledningssystemet beskrivs regionens samlade säkerhetskrav vilket omfattar bland annat organisation, personalsäkerhet, styrning av åtkomst, fysisk och miljörelaterad säkerhet, driftsäkerhet och kommunikationssäkerhet[12]. På Region Kronobergs intranät under rubriken *Informationssäkerhet* är det tydligt beskrivet för samtliga medarbetare vilka riktlinjer och rutiner som gäller, vilka stöddokument och -system som finns samt vilket ansvar olika funktioner har.

I *Plan för informationssäkerhet och skydd av personuppgifter* framgår också hur arbetet med uppföljning och efterlevnad ska ske. Förutom ovan beskrivna process som involverar Stratsys ska uppföljning av arbetet med informationssäkerhet ske årligen i

[11] Svenska Institutet för Standarder: Säkerhetsåtgärder enligt ISO 27000 – konkreta åtgärder för dataskydd, cyber- och informationssäkerhet. https://www.sis.se/iso27001/dettariso27001/sakerhetsatgarder-enligt-iso-27000/ [hämtad 2023-10-17]
[12] Observation av Region Kronobergs interna webbsida under rubriken ”Informationssäkerhet” [2023-09-06]

Regionstyrelsens internkontrollplan. Till exempel visar *Uppföljning av regionstyrelsens internkontrollplan 2022* att Efterlevnad av GDPR (ingen avvikande nivå noterades för 2022) och Informationsklassning (projektet löper enligt plan och övergår i förvaltning vid årsskiftet 2022/2023) har följts upp. Uppföljning av efterlevnaden av LIS sker också årligen och rapporteras till regionledningen, enligt *Plan för informationssäkerhet och skydd av personuppgifter*. Dokumentgranskningen visar att stabsdirektörena vid flera tillfällen har delgetts information om informationssäkerhet och dataskydd.

Det bör noteras att protokollsgenomgången av Regionstyrelsen protokoll från januari 2021 till och med juni 2023 omnämner informationssäkerhet vid två tillfällen. Enligt *protokoll* för sammanträdet 2021-01-26 fastställer Regionstyrelsen plan för informationssäkerhet och skydd av personuppgifter. I *protokoll* för sammanträdet 2021-05-19 framgår att Regionstyrelsen behandlar remissyttrande för informationsöverföring inom vård och omsorg (SOU 2021:4), men detta har ingen bäring på styrning, ledning eller uppföljning av regionens egna processer.

4.1.4. Incidenthanteringsprocess

I *Plan för informationssäkerhet och skydd av personuppgifter* (2021) beskrivs hur incidenter ska hanteras på ett övergripande sätt. Här framgår till exempel att inträffade incidenter ska hanteras effektivt för att minimera skadorna för verksamheten, identifierade sårbarheter ska åtgärdas så att incidenter kan undvikas samt att vid incidenter där anmälningsskyldighet finns enligt lag eller förordning ska anmälan göras till ansvarig myndighet. I intervjuer framkommer också att en viktig del av incidenthanteringen är att dra lärdomar av det inträffade samt proaktivt arbeta med att åtgärda sårbarheter.

Intervjuade beskriver att varje incident hanteras enligt rutin och att den bland annat omfattar en orsaksanalys (root cause analysis) och att samtliga involverade deltar i att mildra konsekvenserna för att sedan, när incidenten är hanterad, tillsammans definiera vilka förbättringar som behöver genomföras. Enligt intervjuade finns det en styrka i att detta sker över förvaltningsgränser och att det därmed ges förutsättningar för att stärka förutsättningarna genom såväl verksamhet som teknik.

Inom ramen för LIS, som finns på Region Kronobergs intranät under rubriken *Informationssäkerhet*, beskrivs också hantering av informationssäkerhetsincidenter. Under avsnittet för *Dataintrång* redogörs bland annat för åtgärder vid otillåten

användning. Här kan medarbetare ta del av aktuella rutiner och åtgärder.[13] Det kan till exempel handla om stickprovskontroller som ska göras eller om patient misstänker att obehörig person har varit inne i vårdinformationssystemet[14]. Ett exempel på rutiner är *Rutin och åtgärder vid misstanke om dataintrång* (2020, giltig till och med 2022-02-05). *Dokumentet* ger en steg-för-steg-instruktion om hur samtalet med medarbetare ska struktureras, vilka ytterligare funktioner som behöver informeras samt hur det disciplinära förfarandet ser ut när misstanken om dataintrång har bekräftats. *Rutinen* betonar också vikten av dokumentation och att nödvändiga anmälningar ska göras till berörd/a myndighet/er.

4.1.5. Bedömning och rekommendation

Helseplan bedömer att Regionstyrelsen har säkerställt att det finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i regionen. Organisationsstrukturen för informationssäkerhet är tydliggjord och enheternas placering, under regiondirektören respektive som en del av kansliavdelningen, visar att Region Kronoberg tilldelar sakfrågorna en central betydelse. Den införda styr- och samverkansmodellen skapar förutsättningar för de tekniska och verksamhetsnära delarna att samverkan i en tydlig organisation i syfte att främja arbetet med informationssäkerhet.

Helseplan bedömer att Regionstyrelsen har säkerställt att regionens verksamheter arbetar systematiskt med att identifiera och analysera risker för informationssäkerheten. Det finns utarbetade styrdokument som tydligt beskriver risker och hur dessa ska identifieras, hanteras samt analyseras. Arbetet har systematiserats över tid och det finns tydliga kontrollpunkter och ansvarsfördelning för hur enskilda verksamheter samt regionen övergripande ska arbeta med modeller och verktyg för att förebygga, identifiera och analysera risker. Det bör noteras att den mänskliga faktorn kan vara en utmaning som medför att riskbedömningar och -analyser trots strukturerade arbetssätt och tydliga styrdokument uteblir.

[13] Observation av Region Kronobergs interna webbsida under rubriken ”Informationssäkerhet” [2023-09-06]
[14] Observation av Region Kronobergs interna webbsida under rubriken ”Informationssäkerhet” [2023-09-06]

Helseplan bedömer att Regionstyrelsen har säkerställt att det finns ändamålsenliga styrande dokument, riktlinjer för informationssäkerhet. Det finns tydliga rutiner och riktlinjer som strukturerat beskriver hur arbetet med informationssäkerhet ska ske inom Region Kronoberg. Dokumenten omfattar de punkter som krävs för att styrningen av sakfrågan ska kunna ske ändamålsenligt, till exempel tydliggörs ansvarsfördelningen mellan den tekniska och verksamhetsnära organisationen, samtidigt som verksamhetsplaneringssystemet Stratsys skapar struktur för planering, uppföljning och rapportering av aktiviteter. Det bör noteras att styrdokumenten både omfattar det övergripande arbetet som planer för hur enskilda objekt ska hanteras med avseende på informationssäkerhet.

Helseplan bedömer att Regionstyrelsen har säkerställt att det finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs. Styrdokumenten beskriver hur uppföljning och revideringar ska ske. Verksamhetsplaneringssystemet Stratsys har också en roll att skapa struktur och system för uppföljning och efterlevnad av regelverk och planer. Det bör samtidigt noteras att uppföljningen på en övergripande politisk nivå är svag givet resultatet från protokollgranskningen.

Helseplan bedömer att regionens incidenthanteringsprocess är ändamålsenlig. Processen bygger på tydliga styrdokument som beskriver olika funktioners ansvar och som efter hanteringen säkerställer lärande inom organisationen. Vidare inkluderar processen samverkan mellan den tekniska och den verksamhetsnära organisationen vilket skapar förutsättningar för att identifiera, hantera och åtgärda incidenter oavsett var de inträffar.

Helseplan rekommenderar Regionstyrelsen att

- trots tydliga förbättringar fortsätta följa upp Region Kronobergs arbete med informationssäkerhet.

4.2. IT-säkerhet

*I detta avsnitt besvaras revisionsfrågorna ”*Har Regionstyrelsen säkerställt att det finns styrande dokument, såsom policy, riktlinjer för IT-säkerhet?*”, ”*Har Regionstyrelsen säkerställt att det finns rutiner för kontroll av systembehörigheter som är ändamålsenliga?*” samt ”*Har Regionstyrelsen säkerställt att roller och ansvar för informationssäkerheten är tydliggjord och uppfattad mellan verksamheten och IT-organisation?*”.*

4.2.1. Styrande dokument och kontroll

I *Avsnitt 4.1.3 Styrande dokument och uppföljning* beskrivs de styrande dokument som rör informationssäkerheten. Då IT-säkerhet är en del av informationssäkerheten enligt gällande definition omfattas även denna av ovan beskrivna riktlinjer och rutiner.

Därtill finns det inom Region Kronoberg styrdokument som beskriver hur verksamheten genom kontinuitetshantering kan minska konsekvenser och minska avbrottstiden vid störningar i till exempel IT-stöd. På Region Kronobergs intranät framgår under rubriken *Kontinuitetshantering* hur verksamheten systematisk kan arbeta med att förebygga händelser och arbeta med tydliga reservrutiner för att stärka IT-säkerheten. Där finns också tydliga mallar och vägledningar som stöd för verksamhetens arbete.[15]

I *Avsnitt 4.1.4 Incidenthanteringsprocess* beskrivs hur intrånghantering hanteras och bland annat hur kontroller av behörigheter går till. Styrande dokument omfattar till exempel hur loggkontroller utförs, som är ett verktyg för att säkerställa att ingen obehörig tar del av patientinformation.[16] Relaterat till behörighetskontroll görs också externa revisioner. Inera AB beskriver i sin *revisionsrapport* mindre avvikelser som har identifierats utifrån SITHS Tillitsramverk. Det handlar om IT-säkerhetsfrågor i form av att det finns brister i lokala rutiner för utgivning av reservkort och vid utfärdande av funktionscertifikat samt det saknas kvittenser för ordinarie kort. Region Kronoberg har identifierat rotorsaker till dessa avvikelser och det beskrivs i *rapporten* att dessa till största del grundar sig på manuell hantering som avviker från beslutade rutiner, till exempel att administratörer öppnar förslutna kuvert med reservkort och pinkod vid utlämnade av dessa. Enligt *rapporten* handlar detta om att individer vill ge god service och att de inte reflekterar kring att de frångår gällande rutiner för IT-säkerhet. I de åtgärdsplaner som har tagits fram har inkluderas att rutiner ska ses över, ökad kommunikation och information kring rutiner samt att kontroller på plats ska genomföras för att säkerställa följsamhet.

I intervjuer framkommer att det finns styrdokument för hur behörigheter beställs, avslutas och slumpvisa kontroller utförs. När avvikelser sker är den mänskliga faktorn oftast orsaken, det vill säga att framställan om behörighetsändring inte sker. Detta kan

[15] Observation av Region Kronobergs interna webbsida under rubriken ”Kontinuitetshantering” [2023-09-06]
[16] Observation av Region Kronobergs interna webbsida under rubriken ”Informationssäkerhet” [2023-09-06]

avse såväl tillgång till system som fysiskt till lokaler. När en medarbetare ändrar anställningsform/funktion kanske inte behörigheten revideras för att hen fortsatt ska kunna utföra sina arbetsuppgifter. Samtidigt kan regelverket föreskriva ändringar i behörigheten. Den manuella hanteringen i kombination med att restriktioner kan försvåra utförandet av uppgifter kan leda till att enskilda chefer inte meddelar förändringar. För att arbeta mer proaktiv med dessa frågor och systematisera hanteringen av framför allt behörighetsåterkallning har säkerhetsenheten tagit fram ett antal nyckeltal som följs kvartalsvis. Bland dem finns antal aktiva interna och externa användarkonton som inte har använts på sex månader. Genom att arbeta med uppföljning av dessa nyckeltal kan IT identifiera riskområden och aktivt arbeta med att påminna chefer om att avsluta behörigheter.

4.2.2. Roll- och ansvarsfördelning

Som tidigare beskrivit under *Avsnitt 4.1.1. Organisation* finns det en etablerad styr- och samverkansmodell som beskriver ansvars- och rollfördelningen samt samarbetsformer mellan verksamheten och IT-organisationen. Kortfattat beskriver *Sammanfattning av styrstruktur för verksamhetsutveckling med hjälp av it-stöd* de olika objekten, deras ansvar samt de obligatoriska rollerna som finns i organisationen. Det finns också kompletterande information på Region Kronobergs intranät under rubriken *Styr- och samverkansmodell för IT-stöd* vilken roll och ansvar som respektive funktion har. Exempelvis beskrivs att verksamhetsnära IT, det vill säga funktioner som befinner sig i verksamheten och har verksamhetens perspektiv, ska utbilda och informera användare samt fånga nya behov och följa upp hur befintligt stöd fungerar för verksamheten. Motparten, tekniknära IT, ansvarar bland annat för att ta fram och utvärdera IT-tjänsters tekniska krav samt att övervaka IT-miljön och agera på larm för teknisk plattform och applikationstjänst[17]. På samma sida på intranätet beskrivs också hur personer som har fått nya funktioner, till exempel är ny som objektspecialist, ska förstå sin roll och ska erhålla kunskap för att kunna utöva sitt ansvar på ett ändamålsenligt sätt[18].

I intervjuer beskrivs att roller och ansvar är tydliga och att den centrala IT-organisationen gärna vägleder till dokument där medarbetaren kan läsa med om sin funktion och det

[17] Observation av Region Kronobergs interna webbsida under rubriken ”Styr- och samverkansmodell” [2023-09-06]
[18] Observation av Region Kronobergs interna webbsida under rubriken ”Styr- och samverkansmodell” [2023-09-06]

ansvar som ligger i rollen. Däremot menar intervjuade att det förekommer att enskilda personer behöver tid för att lära sig strukturerna och att det kan finnas en otydlighet längre ut i verksamheten. Den vanligaste förekommande avvikelsen i sammanhanget är att medarbetaren i verksamheten inte har kunskap om beslutade funktioner och vänder sig direkt till IT trots att hen egentligen skulle sökt stöd hos den verksamhetsnära IT-funktionen. Intervjuade menar att detta på sikt åtgärdas genom utbildning och att tekniknära IT i högre grad avvisar sådana ärenden och hänvisar till rätt funktion.

4.2.3. Bedömning och rekommendation

Helseplan bedömer att Regionstyrelsen har säkerställt att det finns styrande dokument, såsom policy, riktlinjer för IT-säkerhet. Det finns tydliga rutiner och riktlinjer som strukturerat beskriver hur arbetet med informationssäkerhet, och därigenom med IT-säkerhet ska ske inom Region Kronoberg. Dokumenten tydliggör exempelvis ansvarsfördelningen mellan den tekniska och verksamhetsnära organisationen och verksamhetsplaneringssystemet Stratsys skapar struktur för planering, uppföljning och rapportering av aktiviteter. Det bör noteras att styrdokumenten både omfattar det övergripande arbetet som planer för hur enskilda objekt ska hanteras med avseende på informationssäkerhet.

Helseplan bedömer att Regionstyrelsen delvis har säkerställt att det finns rutiner för kontroll av systembehörigheter som är ändamålsenliga. Det finns tydliga styrdokument, som beskriver hur behörigheter beställs, hanteras och avslutas. Dessa rutiner inkluderar också hur kontroll ska ske. Däremot kan den mänskliga faktorn vara avgörande för att rutinerna efterlevs. Region Kronoberg har börjat skapa systematiska kontroller av behörigheter som borde ha avslutats och genom att utveckla denna struktur kan fler behörighetsavvikelser upptäckas och hanteras tidigare.

Helseplan bedömer att Regionstyrelsen säkerställt att roller och ansvar för informationssäkerheten är tydliggjord och uppfattad mellan verksamheten och IT-organisation. Den införda styr- och samverkansmodellen beskriver tydligt funktions-, roll- och ansvarsfördelningen mellan de tekniska och de verksamhetsnära delarna i organisationen. Det finns därtill tydliga beskrivningar för vilka uppdrag olika roller innehar. Däremot kan den mänskliga faktorn även här vara avgörande för om etablerade kommunikationsstrukturer, och därmed den beslutade ansvarsfördelningen, följs.

Helseplan rekommenderar Regionstyrelsen att

- skapa förutsättningar för att beslutade riktlinjer och rutiner är välkända i organisationen genom att hålla frågorna aktuella och relevanta så att informationssäkerhetsperspektivet finns med i alla delar av verksamheten.

4.3. Cybersäkerhet

*I detta avsnitt besvaras revisionsfrågorna "*Har Regionstyrelsen säkerställt att eventuella attacker upptäcks och icke önskvärda incidenter hanteras på ett ändamålsenligt sätt?*"* *samt "*Har Regionstyrelsen säkerställt att säkerheten avseende intrång av extern och intern aktör är ändamålsenlig?*".*

4.3.1. Hantering av intrång

I *Avsnitt 4.1.4 Incidenthanteringsprocess* beskrivs hur intrånghantering hanteras och bland annat hur kontroller av behörigheter går till. Processen beskriver hur en redan skedd händelse hanteras och intervjuade menar att det förebyggande arbetet är desto viktigare för att hindra att attacker och incidenter sker. I detta arbete ligger till exempel ett tätt samarbete med systemleverantörerna, som enligt avtal måste informera regionen om säkerhetsluckor eller när andra sårbarheter upptäcks. Detta omfattar även leverantörer eller kunder som har tillgång till information via personuppgiftsbiträdesavtal. Den här formen av kravställan och uppföljning är del av ett aktivt arbete med ISO 27000, uppger intervjuade.

Intervjuade beskriver vidare att det finns olika nationella, regionala och lokala samverkansytor kring hantering av interna eller externa informationssäkerhetshot. Det finns bland annat forum som leds av Myndigheten för samhällsskydd och beredskap, SKR eller som riktar sig till regionala aktörer som Länsstyrelse, Polismyndigheten eller kommunerna i länet. Här delas information om händelser, i syfte att bygga förmåga att hantera och praktiska förbereda sig för attacker eller incidenter, menar intervjuade.

Syftet med alla förberedelser och med att arbeta med lärdomar från inträffade incidenter är att ständigt stärka säkerheten avseende intrång av externa eller interna aktörer. Kommunikation och informationsspridning är en viktig del i detta arbete. Intervjuade menar att det kan vara små beteendeförändringar som leder till att skyddet blir högre. Som exempel beskrivs vikten av att öppet visa sina passerkort och att våga efterfråga någons passerkort när det inte bärs synligt. Detta är ett sätt att stärka kunskapen och samtidigt minskar det risken för att obehöriga får fysisk tillgång till lokaler. Analyser av intrångsskyddet omfattar därför också mjuka värden i form av personal likväl som av tekniska verktyg.

Det finns också skydd som Region Kronoberg har upphandlat. Det kan till exempel röra sig om teknisk mjukvara vars syfte är att stoppa attacker långt utanför regionens och även Sveriges fysiska gränser. Här är det viktigt, uppger intervjuade, att det ställs rätt krav i upphandlingen och att det sker ett samarbete med leverantören för att säkerställa att skyddet hela tiden är uppdaterat och anpassar sig efter nya hot som upptäcks.

För att bedöma hur Region Kronoberg arbetar med cybersäkerhet använder granskningen sig av de fem centrala begrepp som finns i NIST Cybersäkerhetsramverket: Identifiera, Skydda, Upptäcka, Respondera och Återställa.

- **Identifiera:** Intervjuade beskriver att Region Kronoberg har ett strukturerat arbete kring informationssäkerhet, som speglas av ett tydligt LIS som också baserar sig på ISO 27000. Dokumentgranskningen visar att det finns en tydlig styr- och samverkansmodell som möjliggör att regionen kan hantera behov, delge information och skapa god samverkan mellan verksamhetsnära och tekniknära funktioner. Det finns vidare en tydlig beskrivning av funktion, roll och ansvar samt tydliga styrdokument för informationssäkerhet, inklusive IT-säkerhet, på Region Kronobergs intranät. Verksamheten kan ha utmaningar, enligt intervjuade, med att ha hög följsamhet till beslutade dokument och styrprocesser. Det leder till att säkerhetsenheten arbetar med att systematiskt och löpande kommunicerar i olika kanaler för att öka medvetenheten, uppger intervjuade.
- **Skydda:** Enligt intervjuade finns det ett omfattande förebyggande arbete som syftar till att på olika nivåer och inom olika områden skydda Region Kronoberg. Det handlar om ändamålsenlig mjukvara som förhindrar attacker och om att stärka behörigheter för att minska intrång i fysiska lokaler eller vid stöld. Dokumentgranskningen visar att det finns tydliga roll- och ansvarsfördelningar, som även omfattar den enskilde medarbetaren, och därmed finns det ett teoretiskt högt skydd. Intervjuade menar vidare att den svaga länken är det mänskliga beteenden och att även här behövs det utbildning för att öka skyddet. Det finns utbildningar i informationssäkerhet tillgängliga för regionens medarbetare. Dessa är inte obligatoriska utan det är upp till verksamheterna och funktioner som berörs att delta.
- **Upptäcka:** Dokumentgranskningen visar att det finns rutiner för att arbeta med till exempel loggkontroll för att säkerställa att intrång upptäcks. I rutinerna beskrivs det också vilket ansvar chefer respektive medarbetare för att förhindra missbruk samt för att tidigt upptäcka avvikelser. Intervjuade beskriver att det finns olika upphandlade tjänster som ska larma vid obehörigt intrång i IT-stöd. Återigen kan fler upptäckter göras eller intrång förhindras om samtliga medarbetare följer rutinerna, vilket aktualiserar frågan huruvida befintliga utbildningar borde vara obligatoriska utbildningar, menar intervjuade.

- **Respondera:** Region Kronoberg har utsedda resurser och en kontaktkedja för hantering av incidenter. Dokumentgranskningen visar att incidenter hanteras tillsammans med samtliga berörda aktörer, vilket även kan inkludera externa parter, och att verksamhet och teknik samarbetar för att mildra konsekvenserna och dra lärdomar. Vidare finns det också riktlinjer för rapportering av incidenter och för hur förbättringsarbeten med grund i lärdomar dragna från incidenter kan genomföras.
- **Återställa:** Region Kronoberg har tydliga styrande dokument för kontinuitetshantering, vilket inte syftar till att återställa data utan att hantera data när en incident inträffar. Samtidigt handlar en god kontinuitetshantering om att minska avbrottstiden och att en återställning av tillgång till data kan ske tidigare. Vad avser att återställa till exempel data görs enligt intervjuade back-up av alla system enligt beslutade intervall. Detta skapar förutsättningar för att data kan vara tillgänglig men beroende på vilket system som är hotat kan åtgärden dröja. Intervjuade uppger att det görs regelbundna teståterställningar för att testa systemet samt att Region Kronobergs vårdinformationssystem Cosmic har hög prioritet i detta arbete.

4.3.2. Bedömning och rekommendation

Helseplan bedömer att Regionstyrelsen säkerställt att eventuella attacker upptäcks och icke önskvärda incidenter hanteras på ett ändamålsenligt sätt. Det finns i Region Kronoberg fysiska och tekniska förutsättningar för att upptäcka eventuella attacker. Arbetet utvecklas ständigt och så gör också regionens skydd mot nya attacker. Region Kronoberg ingår i flera samverkansforum samt har ett systematiskt arbete för att till exempel tillsammans med leverantörer arbeta med att upphandlade tjänster och produkter ständigt upprätthåller ett högt skydd. Därtill beskriver styrdokument utförligt hur incidenter hanteras samt hur arbetet med att utifrån lärdomar genomföra förbättringar ska utföras.

Helseplan bedömer att Regionstyrelsen har säkerställt att säkerheten avseende intrång av extern och intern aktör är ändamålsenlig. Förutom redan beskrivna faktorer som strukturer för att systematiskt upptäcka attacker och styrdokument för incidenthantering är det tydligt att arbetet för att förhindra intrång är ständigt pågående. Detta inkluderar att utbilda och medvetandegöra medarbetare inom Region Kronoberg som är viktiga spelare i att förhindra intrång.

Helseplan rekommenderar Regionstyrelsen att

- skapa förutsättningar för att beslutade riktlinjer och rutiner är välkända i organisationen genom att hålla frågorna aktuella och relevanta så att informationssäkerhetsperspektivet finns med i alla delar av verksamheten.

5. Uppföljning av rekommendationer från 2016

*Följande avsnitt behandlar revisionsfråga "*Har åtgärder vidtagits med anledning av de brister samt de förbättringsförslag som framfördes i den uppföljande granskningen från 2016?*".*

Tabell 1 visar en uppföljning av de rekommendationer som gavs i *Granskning av IT-säkerhetsarbetet* (2016). Grön färgmarkering i tabellen innebär att rekommendationer åtgärdats, gul färgmarkering de delvis åtgärdats och röd färgmarkering att de inte har åtgärdats. Vit färgmarkering innebär att rekommendationen inte är aktuell längre och därmed inte kan bedömas.

Tabell 1 Bedömning av rekommendationerna från tidigare genomförd granskning.

Rekommendation	Bedömning	
Formella regler saknas för informationsklassning	Sedan 2016 har projekt med fokus på informationsklassning genomförts. Projekten har syftat till att ta fram en modell för informationsklassning samt att påbörja implementation och utbilda organisationen. Den valda modellen är Sveriges Kommuner och Regioners verktyg KLASSA. Därtill görs kontinuerlig uppföljning kring objektens arbete med informationsklassning. *Rutin för informationsklassning* (2022, giltig till och med 2024-01-05) beskriver syfte, ansvar och arbetssätt för att genomföra en klassning samt hur det löpande arbetet ska ske.	
Uppföljning av tilldelade behörigheter	Region Kronoberg har tydliga rutiner för hur behörigheter tilldelas och avbeställs. Därtill har regionen ett antal nyckeltal som följs och som syftar till att identifiera behörighetsområden där eftersläpning kan finnas.	
Granskning av efterlevnad av rutiner och kontroller	Granskning sker bland annat genom att ett aktivt arbete utifrån ISO 27000 samt genom externa aktörer som Inera AB, Integritetsskyddsmyndigheten och Myndigheten för samhällsskydd och beredskap.	
Behörigheter i Cosmic	Region Kronoberg har tydliga rutiner för hur behörigheter tilldelas och avbeställs. Därtill har regionen ett antal nyckeltal som följs och som syftar	

	till att identifiera behörighetsområden där eftersläpning kan finnas.	
Loggkontroll av patientinformation	Loggkontroll sker enligt rutin och det finns tydligt beskrivet vilket ansvar chef respektive medarbetare har.	
Kraftfulla behörigheter i Aplus	Aplus har ersatts av ekonomisystemet Raindance. Denna rekommendation är därmed inte längre aktuell.[19]	
Dataöverföring till Aplus	Aplus har ersatts av ekonomisystemet Raindance. Denna rekommendation är därmed inte längre aktuell.[20]	
Förstärkning av process för programförändringar	År 2019 skapades en målbild och vision kring en gemensam styr- och samverkansmodell som reglerar hur samtliga organisatoriska delar inom Region Kronoberg ska struktureras och samverka kring utveckling av verksamheten med hjälp av IT-stöd. Eftersom modellen är förändrad sedan föregående granskning är denna rekommendation inte längre aktuell.	
Utbildning	Det finns utbildningar i informationssäkerhet tillgängliga för regionens medarbetare. Dessa är inte obligatoriska utan det är upp till verksamheterna och funktioner som berörs att delta.	
Extern kommunikation	Skydd mot extern påverkan sker i flera lager. Innan ett intrång skulle nå en brandvägg finns skydd mot överbelastningsattacker och det genomförs automatiska trafikanalyser. *Rutin för administration av brandvägg och extern åtkomst* (2018, giltig till och med 2023-08-11) beskriver hanteringen av extern åtkomst.	

[19] Inom ramen för sakgranskningen framkommer följande information: Efter den förra granskningen infördes Raindance som ersatte Aplus. I samband med införandet gjordes en översyn av behörigheter och åtgärder vidtogs för att minimera antalet kraftfulla behörigheter och risker förknippade med detta. Då det är några år sedan Raindance infördes nu står det i objektplanen för 2024 att en systemöversyn kring behörighet ska ske för att säkerställa att hanteringen är fortsatt korrekt och att eventuella avvikelser ska korrigeras.

[20] Inom ramen för sakgranskningen framkommer följande information: I och med införandet av Raindance har de dagliga överföringarna automatiserats och det finns även larm som utlöses om överföringar inte sker eller inte sker korrekt. De överföringar som sker månadsvis är också automatiserade och kontrolleras därutöver manuellt utifrån en checklista för att säkerställa att överföringen har varit korrekt. Checklistan signeras av ansvarig kontrollant. Sedan införandet av Raindance har det inte förekommit några incidenter där verksamheten i efterhand (efter att kontroller genomförts och eventuella larm har hanterats) har upptäckt att filöverföringen inte har skett korrekt.

	I intervjuer beskrivs att samtliga förändringar i regionens IT-miljö hanteras spårbart. Brandväggar, det vill säga fysiska eller digitala tekniker som nyttjas för att hindra dataintrång, är bland de högst klassade tillgångarna med begränsat åtkomst. Brandväggar hanteras systematiskt i tillhörande objekt och vid större förändring i objektet sker en extern verifiering av säkerheten. Därtill genomförs sårbarhetsanalyser av extern åtkomst minst årligen av extern part.	

Sammanfattande visar tabellen att rekommendationer till stor del är åtgärdade. Det handlar framför allt om att Region Kronoberg har skapat en struktur för att arbeta med informationssäkerhet och det finns rutiner och riktlinjer som styr verksamheterna. En del av rekommendationerna är inte aktuella längre eftersom förutsättningarna i form av teknik eller verksamhetsmässiga förändringar har ändrats.

5.1.1. Bedömning och rekommendation

Helseplan bedömer att åtgärder har vidtagits med anledning av de brister samt de förbättringsförslag som framfördes i den uppföljande granskningen från 2016. En del av rekommendationerna bedöms inte längre vara aktuella eftersom tekniska och verksamhetsmässiga förändringar har skett vilket bland annat medför att IT-stöd har bytts ut. Uppföljningen visar att det finns en tydlig struktur för hur samverkan inom ramen för informationssäkerhet och IT-säkerhet ska ske samt tydliga riktlinjer och rutiner som verksamheterna utbildas i och förhåller sig till.

6. Övergripande revisionsfråga

I *Tabell 2* illustreras bedömning för revisionsfrågorna. Den enskilda bedömningen har graderats utifrån skalan uppfyllt (grön markering), delvis uppfyllt (gul markering) samt ej uppfyllt (röd markering).

Tabell 2 Svar och bedömning för de enskilda revisionsfrågorna.

Revisionsfråga	Bedömning	
Informationssäkerhet		
Det finns ändamålsenliga styrande dokument, riktlinjer för informationssäkerhet?	Helseplan bedömer att Regionstyrelsen har säkerställt att det finns ändamålsenliga styrande dokument, riktlinjer för informationssäkerhet. Det finns tydliga rutiner och riktlinjer som strukturerat beskriver hur arbetet med	

	informationssäkerhet ska ske inom Region Kronoberg. Dokumenten omfattar de punkter som krävs för att styrningen av sakfrågan ska kunna ske ändamålsenligt, till exempel tydliggörs ansvarsfördelningen mellan den tekniska och verksamhetsnära organisationen, samtidigt som verksamhetsplaneringssystemet Stratsys skapar struktur för planering, uppföljning och rapportering av aktiviteter. Det bör noteras att styrdokumenten både omfattar det övergripande arbetet som planer för hur enskilda objekt ska hanteras med avseende på informationssäkerhet.	
Det finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i region?	Helseplan bedömer att Regionstyrelsen har säkerställt att det finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i regionen. Organisationsstrukturen för informationssäkerhet är tydliggjord och enheternas placering, under regiondirektören respektive som en del av kansliavdelningen, visar att Region Kronoberg tilldelar sakfrågorna en central betydelse. Den införda styr- och samverkansmodellen skapar förutsättningar för de tekniska och verksamhetsnära delarna att samverkan i en tydlig organisation i syfte att främja arbetet med informationssäkerhet.	
Regionens verksamheter arbetar systematiskt med att identifiera och analysera risker för informationssäkerheten?	Helseplan bedömer att Regionstyrelsen har säkerställt att regionens verksamheter arbetar systematiskt med att identifiera och analysera risker för informationssäkerheten. Det finns utarbetade styrdokument som tydligt beskriver risker och hur dessa ska identifieras, hanteras samt analyseras. Arbetet har systematiserats över tid och det finns tydliga kontrollpunkter och ansvarsfördelning för hur enskilda verksamheter samt regionen övergripande ska arbeta med modeller och verktyg för att förebygga, identifiera och analysera risker. Det bör noteras att den mänskliga faktorn kan vara en utmaning som medför att	

	riskbedömningar och -analyser trots strukturerade arbetssätt och tydliga styrdokument uteblir.	
Det finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?	Helseplan bedömer att Regionstyrelsen har säkerställt att det finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs. Styrdokumenten beskriver hur uppföljning och revideringar ska ske. Verksamhetsplaneringssystemet Stratsys har också en roll att skapa struktur och system för uppföljning och efterlevnad av regelverk och planer. Det bör samtidigt noteras att uppföljningen på en övergripande politisk nivå är svag givet resultatet från protokollgranskningen.	
Är regionens incidenthanteringsprocess ändamålsenlig?	Helseplan bedömer att regionens incidenthanteringsprocess är ändamålsenlig. Processen bygger på tydliga styrdokument som beskriver olika funktioners ansvar och som efter hanteringen säkerställer lärande inom organisationen. Vidare inkluderar processen samverkan mellan den tekniska och den verksamhetsnära organisationen vilket skapar förutsättningar för att identifiera, hantera och åtgärda incidenter oavsett var de inträffar.	
IT-säkerhet - intrångsskydd		
Det finns styrande dokument, såsom policy, riktlinjer för IT-säkerhet?	Helseplan bedömer att Regionstyrelsen har säkerställt att det finns styrande dokument, såsom policy, riktlinjer för IT-säkerhet. Det finns tydliga rutiner och riktlinjer som strukturerat beskriver hur arbetet med informationssäkerhet, och därigenom med IT-säkerhet ska ske inom Region Kronoberg. Dokumenten tydliggör exempelvis ansvarsfördelningen mellan den tekniska och verksamhetsnära organisationen och verksamhetsplaneringssystemet Stratsys skapar struktur för planering, uppföljning och rapportering av aktiviteter. Det bör noteras att styrdokumenten både omfattar	

	det övergripande arbetet som planer för hur enskilda objekt ska hanteras med avseende på informationssäkerhet.	
Roller och ansvar för informationssäkerheten är tydliggjord och uppfattad mellan verksamheten och IT-organisation?	Helseplan bedömer att Regionstyrelsen säkerställt att roller och ansvar för informationssäkerheten är tydliggjord och uppfattad mellan verksamheten och IT-organisation. Den införda styr- och samverkansmodellen beskriver tydligt funktions-, roll- och ansvarsfördelningen mellan de tekniska och de verksamhetsnära delarna i organisationen. Det finns därtill tydliga beskrivningar för vilka uppdrag olika roller innehar. Däremot kan den mänskliga faktorn även här vara avgörande för om etablerade kommunikationsstrukturer, och därmed den beslutade ansvarsfördelningen, följs.	
Eventuella attacker upptäcks och icke önskvärda incidenter hanteras på ett ändamålsenligt sätt?	Helseplan bedömer att Regionstyrelsen säkerställt att eventuella attacker upptäcks och icke önskvärda incidenter hanteras på ett ändamålsenligt sätt. Det finns i Region Kronoberg fysiska och tekniska förutsättningar för att upptäcka eventuella attacker. Arbetet utvecklas ständigt och så gör också regionens skydd mot nya attacker. Region Kronoberg ingår i flera samverkansforum samt har ett systematiskt arbete för att till exempel tillsammans med leverantörer arbeta med att upphandlade tjänster och produkter ständigt upprätthåller ett högt skydd. Därtill beskriver styrdokument utförligt hur incidenter hanteras samt hur arbetet med att utifrån lärdomar genomföra förbättringar ska utföras.	
Säkerheten avseende intrång av extern och intern aktör är ändamålsenlig?	Helseplan bedömer att Regionstyrelsen har säkerställt att säkerheten avseende intrång av extern och intern aktör är ändamålsenlig. Förutom redan beskrivna faktorer som strukturer för att systematiskt upptäcka attacker och styrdokument för incidenthantering är det tydligt att arbetet för att förhindra intrång är ständigt pågående. Detta inkluderar att utbilda och	

	medvetandegöra medarbetare inom Region Kronoberg som är viktiga spelare i att förhindra intrång.	
Det finns rutiner för kontroll av systembehörigheter som är ändamålsenliga?	Helseplan bedömer att Regionstyrelsen delvis har säkerställt att det finns rutiner för kontroll av systembehörigheter som är ändamålsenliga. Det finns tydliga styrdokument, som beskriver hur behörigheter beställs, hanteras och avslutas. Dessa rutiner inkluderar också hur kontroll ska ske. Däremot kan den mänskliga faktorn vara avgörande för att rutinerna efterlevs. Region Kronoberg har börjat skapa systematiska kontroller av behörigheter som borde ha avslutats och genom att utveckla denna struktur kan fler behörighetsavvikelser upptäckas och hanteras tidigare.	
Åtgärder har vidtagits med anledning av de brister samt de förbättringsförslag som framfördes i den uppföljande granskningen från 2016?	Helseplan bedömer att åtgärder har vidtagits med anledning av de brister samt de förbättringsförslag som framfördes i den uppföljande granskningen från 2016. En del av rekommendationerna bedöms inte längre vara aktuella eftersom tekniska och verksamhetsmässiga förändringar har skett vilket bland annat medför att IT-stöd har bytts ut. Uppföljningen visar att det finns en tydlig struktur för hur samverkan inom ramen för informationssäkerhet och IT-säkerhet ska ske samt tydliga riktlinjer och rutiner som verksamheterna utbildas i och förhåller sig till.	

Förutom ovan svar på de enskilda revisionsfrågorna bedöms också de övergripande revisionsfrågorna, vilket illustreras i *Tabell 3*. Den enskilda bedömningen har graderats utifrån skalan uppfyllt (grön markering), delvis uppfyllt (gul markering) samt ej uppfyllt (röd markering).

Tabell 3 Svar och bedömning för de övergripande revisionsfrågorna.

Revisionsfråga	Bedömning	
Det finns en tillräcklig intern styrning (exempelvis genom beslut och riktlinjer, budgetmedel), uppföljning och kontroll som	Helseplan bedömer att Regionstyrelsen säkerställt att det finns en tillräcklig intern styrning, uppföljning och kontroll som säkerställer ett ändamålsenligt systematiskt	

säkerställer ett ändamålsenligt systematiskt arbetssätt med informationssäkerheten i regionen?	arbetssätt med informationssäkerheten i regionen. Detta sker framför allt genom den utvecklade och beslutade styr- och samverkansmodellen, som skapar förutsättningar för ett effektivt arbete och god relation mellan de enheter som äger sakfrågorna och verksamheterna som ska följa beslutade riktlinjer. Region Kronoberg arbetar också enligt ISO 27000 vilket medför att det finns en struktur för utförande men också för regelbundna översyner som gynnar regionens arbete.	
Den interna kontrollen avseende regionens cybersäkerhet är tillräcklig?	Helseplan bedömer att Regionstyrelsen säkerställt att den interna kontrollen avseende regionens cybersäkerhet är tillräcklig. Region Kronoberg uppvisar ett aktivt arbete och samtidigt en medvetenhet kring att det finns krav på ständiga förbättringar. De framtagna utbildningarna kommer att stärka enskilda medarbetare och verksamheterna som helhet i att arbeta med informationssäkerhet.	
Region Kronobergs nuvarande tekniska IT-säkerhet är tillräcklig och tillfredställande för att reducera risker för obehörigt intrång till en acceptabel nivå?	Helseplan bedömer att Regionstyrelsen säkerställt att Region Kronobergs nuvarande (med vilket avses tidpunkten november 2023) tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå. Även här finns det kompetens och kunskap om sakfrågorna i regionen och det pågår ett ständigt arbete med att försöka minska riskerna som uppstår genom den mänskliga faktorn.	

7. Bilagor

Bilaga 1 – Dokumentgenomgång

Följande dokument har ingått i dokumentgranskningen:

- Arbetsordningar och reglementen för den politiska organisationen i Region Kronoberg 2023-2026
- Delegationsordning för regionstyrelsen 2023-2026 inklusive vidaredelegering
- Inera AB: Revisionsrapport (2019)
- Patientsäkerhetsberättelsen (2022)
- Plan för informationssäkerhet och skydd av personuppgifter (2021)
- Regionstyrelsens protokoll för sammanträden januari 2021 till och med juni 2023
- Rutin för administration av brandvägg och extern åtkomst (2018, giltig till och med 2023-08-11)
- Rutin för informationsklassning (2022, giltig till och med 2024-01-05)
- Rutin för risk- och sårbarhetsanalyser (2020, giltig till och med 2022-05-02)
- Rutin och åtgärder vid misstanke om dataintrång (2020, giltig till och med 2022-02-05)
- Sammanfattning av styrstruktur för verksamhetsutveckling med hjälp av IT-stöd (odaterad)
- Styrochsamverkan_översikt (2023)
- Uppföljning av regionstyrelsens internkontrollplan 2022
- Verksamhetsförändring Informationsteknik (2023)

Bilaga 2 – Intervjuförteckning

Följande funktioner har intervjuats, se *Tabell 4*.

Tabell 4 Förteckning över intervjuade funktioner.

Funktion, Organisation
Ordförande, Regionstyrelsen
2:e vice ordförande, Regionstyrelsen
Regiondirektör
Säkerhetschef/Säkerhetsskyddschef, Säkerhetsenheten, Regionstaben
Objektägare Cosmic
Objektägare Trafikobjekt
Facklig representant
Chief technology officer (CTO)
Informationssäkerhetsstrateg, Säkerhetsenheten
Avdelningschef, IT-drift