IT- och eHälsoavdelningen
Marit Nilsson
Tfn: 063-147677 (ank 27677)
E-post: marit.nilsson@regionjh.se

2024-08-27

RS/237/2024

Regionens revisorer

Svar på granskning av IT-säkerhet_2024

Granskningsrapporten

Regionens revisorer granskade 2020 regionens IT-säkerhet (RS/338/2021). Granskningen genomfördes av KPMG. I granskningen framkom bland annat att det fanns en bristande efterlevnad av de styrande dokumenten då delar av det ansvar som pekades ut i dokumenterad ansvarsfördelning inte uppfylldes av avdelnings-och områdeschefer. Vidare framkom att det vilade ett stort ansvar för både det strategiska och operativa arbetet på nyckelpersoner inom informationssäkerhet och IT-säkerhet. Granskningen visade även att medarbetare inte fått tillräcklig utbildning och därigenom den kunskap och medvetenhet som krävs för att efterleva de lagkrav och interna regler som finns för hantering av känslig information och informationstillgångar.

Det noterades att det saknades ett systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar samt att det saknades ändamålsenliga rutiner för behörigheter och lösenord. Det saknades också en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter och befintlig kontinuitetsplan avseende IT-drift var inte uppdaterad. I granskningen noterades att det inte fanns kontrollområden avseende information-eller IT-säkerhet i internkontrollplaner.

Regionens revisorer har genomfört en uppföljande granskning av IT-säkerheten (RS/237/2024). Denna granskning genomfördes av PwC. Syftet var att bedöma om regionstyrelsen vidtagit åtgärder för att åtgärda de brister som framkom vid den tidigare granskningen. Syftet var också att bedöma om regionens arbete med IT-säkerhet är ändamålsenligt.

Revisorernas övergripande bedömningen är att regionstyrelsen i Region Jämtland Härjedalen delvis har åtgärdat de brister som framkom vid den tidigare granskningen, och delvis bedriver ett ändamålsenligt IT-säkerhetsarbete.

Under granskningen noterades ett antal brister och utvecklingsområden:

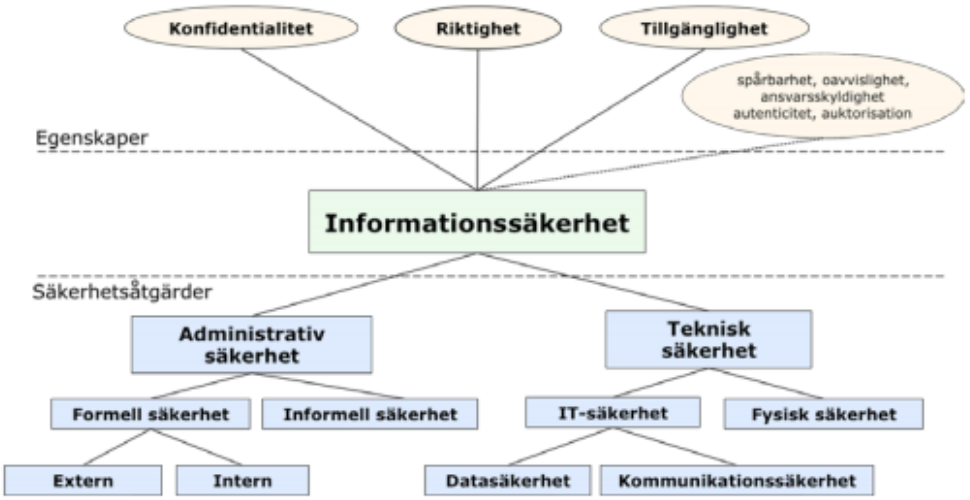
- Behov av att utveckla internkontrollplanens riskbaserade ansats.
- En manuell behörighetshantering.
- Avsaknad av kontroll eller säkerställande av medarbetares kunskapsnivå.
- Avsaknad av ändamålsenlig informationsklassning.
- Avsaknad av systematik kopplat till identifiering av verksamhetskritiska system.

Granskningen har genomförts genom studier av styrdokument, beslut och beslutsunderlag samt intervjuer med nyckelpersoner. Primärt har granskningen genomförts genom tillämpning av det så kallade NIST-ramverket.

Regionstyrelsens svar

Titeln på rapporten är Uppföljande granskning av IT-säkerhet. Liksom vid den tidigare granskningen speglar det inte helt rapportens innehåll. Informationssäkerhet är en kombination av administrativ och teknisk säkerhet, där fysisk och IT-säkerhet ingår i den tekniska säkerheten.

Bilden nedan från Teknisk rapport SIS-TR 50:2015 Terminologi för informationssäkerhet, illustrerar vad som omfattas av begreppet informationssäkerhet.



Figur 1 – Informationssäkerhetsmodell

Informationssäkerhet handlar om att förhindra att information läcker ut, förvanskas eller förstörs. Det handlar också om att göra information lättillgänglig när den behövs och för rätt person. Begreppet omfattar information tryckt på papper, lagrad elektroniskt, som överförs per mejl eller post, visas på film eller yttras i en konversation.

Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk så som policys och riktlinjer, men även tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd.

IT-säkerhet handlar om skydd av IT-system och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid

databehandling samt dator- och telekommunikation. En viktig del av arbetet med IT-säkerhet handlar om att förstå olika hotbilder, hantera sannolikheter för att utsättas för skada samt att balansera kostnader för motmedel för skydd mot värdet av det man skyddar.

Rapporten innehåller 8 revisionsfrågor med revisorernas bedömning och rekommendationer till respektive fråga.

Revisionsfråga 1: Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?

Revisorerna rekommenderar Regionstyrelsen att: Fullfölja arbetet med att utveckla internkontrollarbetets riskbaserade ansats, vilket innebär att etablerade kontrollaktiviteter bör stå i proportion till verksamhetens befintliga risker. Ett riskbaserat förhållningssätt syftar till att bidra till att regionens resurser och medel utnyttjas effektivt, vilket i sin tur möjliggör värdeskapande för regionens medborgare.

Regionstyrelsens svar: Politisk nivå**:** Internkontrollarbetet är indelat i nivåer där Politikens riskarbete finns i internkontrollplanen i Stratsys (i enlighet med kommunallagen). Här har målområde, nyckeltal och uppdrag riskbaserats. Det sker på styrelse och nämndnivå

Verksamhetsnivå**:** Arbetsmiljöarbetet i RISK hanteras i Stratsys där allt annat arbetsmiljöansvar också dokumenteras. Nytt sedan i maj är att HS också adderades till samma riskmodell med nya säkerhetsområden (miljö, informationssäkerhet, patientsäkerhet)

I höst kommer även arbetet starta med att sammanföra alla risker för att styra på risker. Regionen har då tillräckligt med material för att kunna göra ett bra arbete och också avgöra om det ska hanteras i Stratsys eller ej eftersom klassningen blir en annan.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att det arbete som påbörjats för att göra den interna kontrollen mer riskbaserad slutförs.

Regionstyrelsens svar: Föräldraledighet för medarbetare vid säkerhet och beredskap medför att arbetet inte kunnat starta.

Intern kontroll sker i Stratsys

1. Internrevisionen utvalda frågor att ställa till chefer och specialister.
2. Kontrollmoment lagefterlevnad med påståenden till chefer– Idag utför verksamheterna kontrollmoment på miljö, läkemedel och patientsäkerhet.
3. Checklistor – används framför allt i Arbetsgivaransvaret tex. skyddsrond.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att planerade aktiviteter och åtgärder inom området slutförs. Flera olika IT-säkerhetsrelaterade åtgärder tas upp i verksamhetsplan både för 2022 och 2023, exempelvis säkerheten i nätverksansluten hårdvara. Samtidigt noterar vi att aktiviteterna återkommande inte når den eftersträvade måluppfyllelsen.

Regionstyrelsens svar: IT-säkerhetsfunktionen genomför två gånger per år en övergripande analys baserade på CIS ramverket. De aktiviteter och åtgärder som hänvisas ovan är brister som identifierats i analyserna och ålagts IT-enheten och dess leverantörer att åtgärda. Planering och genomförande ligger utanför IT-säkerhetsfunktionens kontroll.

Revisorerna rekommenderar Regionstyrelsen att: Fortsätta prioritera området IT-säkerhet och följa upp att önskade resultat och effekter uppnås. Större delen av en regions verksamhet är i dag beroende av IT-system och digitala verktyg. Det innebär i sin tur att funktionalitet, kontinuitet och säkerhet i dessa system och verktyg utgör en grundläggande förmåga för att regionen ska kunna leva upp till sitt lagstadgade åtagande (exempelvis hälso- och sjukvård).

Regionstyrelsens svar: Säkerhetsläget har försämrats till följd av krig i världen och hotbilden i form av cyberattacker har ökat. Åtgärder för att stärka regionens IT-säkerhet är därför ett prioriterat område. Regionstyrelsen verksamhetsplan innehåller mål och uppdrag för att stärka regionens skydd och robusthet.

Security Operations Center (SOC) är i drift sedan juni 2022, för övervakning, analys och skydd från cyberattacker. Ett antal tekniska åtgärder har genomförts, pågår och planeras genomföras. Vad dessa åtgärder innebär kan av naturliga skäl inte beskrivas i detta dokument.

Revisionsfråga 2: Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?

Revisorerna rekommenderar Regionstyrelsen att: Utvärdera om den bristande måluppfyllelsen av relevanta aktiviteter i verksamhetsplanen beror på bristande resurser, och i så fall åtgärda den bristen.

Regionstyrelsens svar: Det är IT-enheten och dess leverantörer som ansvarar för att åtgärda de brister som identifierats av IT-säkerhetsfunktionen. Att identifiera brister är oftast den enkla biten. Det som tar tid och resurser är att åtgärda bristerna. En utvärdering bör därför riktas mot IT-enheten i stort och inte begränsas till IT-säkerhetsfunktionen.

Revisorerna rekommenderar Regionstyrelsen att: Fortsätta utvärdera och vara uppmärksam på behov av eventuella ytterligare resurser. Eventuella risker som ännu inte har identifierats kan medföra ett ökat behov av nya resurser och kompetenser .

Regionstyrelsens svar: Regionen instämmer med revisorernas rekommendation.

Revisionsfråga 3: Sker säkerhetsklassning av funktioner och tjänster?

Revisorerna rekommenderar Regionstyrelsen att: Regelbundet utvärdera och uppdatera rutiner i linje med identifierade risker och förändrade lagkrav, för att säkerställa en anpassningsbar och effektiv hantering av säkerhetsskyddet.

Regionstyrelsens svar: Utvärdering och uppdatering av rutiner görs fortlöpande genom regionens riktlinje för säkerhetsskydd och tillhörande rutiner, checklistor samt planer

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa en korrekt hantering av säkerhetsklassning av leverantörer. Vid identifiering av eventuella nya risker bör regionen upprätthålla en korrekt hantering av säkerhetsklassning för funktioner och tjänster relaterade till leverantörer..

Regionstyrelsens svar: Regionen löser detta genom att teckna säkerhetsskyddsavtal med de entreprenörer som vistas eller kommer kontakt med våra säkerhetsklassade anläggningar och lokaler samt säkerhetskänsliga uppgifter och handlingar. Dessutom finns det en fastställd befattningsanalys över klassade befattning i regionen

Revisionsfråga 4: Finns ändamålsenliga rutiner för behörigheter och lösenord? Med inriktning på den interna hanteringen.

Revisorerna rekommenderar Regionstyrelsen att: Fullfölja den planerade revideringen av lösenordskraven.

Regionstyrelsens svar: Uppdraget är utlagt på driftleverantör och pågående.

Revisorerna rekommenderar Regionstyrelsen att: Effektivisera behörighetsstyrningen genom införandet av ett automatiserat verktyg. Ett verktyg såsom ett Identity and Access Management system (IAM) gör det enklare att hålla behörigheter aktuella, bevilja och begränsa åtkomst baserat på roll och upptäckta avvikelser.

Regionstyrelsens svar: Region Jämtland Härjedalen har sedan flera år ett IAM-system i drift. Vi ställer oss därför frågande till denna rekommendation.

Revisorerna rekommenderar Regionstyrelsen att: Upprätta en systematisk uppföljning för att kontinuerligt utvärdera efterlevnaden av lösenordskraven, i syfte att säkerställa att dessa upprätthålls över tiden.

Regionstyrelsens svar: Tekniska funktioner för att säkerställa att domänlösenord minst håller avsedd lägstanivå är redan införda. Under 2024 skall samtliga domänlösenord som inte bytts sedan de nya lösenordskraven infördes få ett tvingande lösenordsbyte för att säkerställa att samtliga domänlösenord uppfyller kraven. Funktionen för IT-säkerhet genomför återkommande säkerhetstester för att identifiera svaga lösenord.

Revisionsfråga 5: Har regionen en ändamålsenlig incidenthanteringsprocess?

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa en hög rapporteringsfrekvens till ledningen avseende uppkomna incidenter och tillhörande lessons-learned dokumentation

Regionstyrelsens svar: Regionens incidentprocess är utformad efter bästa praxis rekommendationer i ITILv4-ramverket, då incidenter med hög prioritet inträffar upprättas en incidentrapport till tjänsteägaren där bland annat ”lessons learned” dokumenteras.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa tillgänglighet av rapporteringsformulär och rutiner. Formulär ska vara utformade så att samtliga anställda utan alltför stor tidsåtgång kan notera en avvikelse.

Regionstyrelsens svar: I den mån avvikelse används som synonym till incident så finns en länk till rapporteringsformulär lätt tillgänglig direkt från skrivbordet i Citrix som är utformad för att vara så enkel som möjligt och ändå tillhandahålla relevant information för felsökning. Om begreppet avvikelse avser brister i processer etcetera så hanteras dessa i systemet Centuri.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa effektiv informationsspridning kopplat till uppkomna och hanterade incidenter. Samtliga berörda av en incident bör erhålla information om denna, från att den hänt till beslut och genomförande av åtgärder.

Regionstyrelsens svar: Vid incidenter som berör enskilda medarbetare kan denne enkelt följa dessa via självbetjäningsdelen av regionens ärendehanteringssystem. Incidenter med högre påverkan kommuniceras dessutom via driftinformation på regionens intranät och talsvarsmeddelande vid samtal till regionens helpdesk. Om intranätet och/eller telefonin skulle vara utslagna har helpdesk också möjlighet att skicka sms-meddelanden till berörda verksamheter via systemet Everbridge.

Revisionsfråga 6: Är medborgarnas integritet säkerställd och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att riktlinjerna för IT-säkerhet efterlevs i praktiken.

Regionstyrelsens svar: Regionstyrelsen instämmer i revisorernas rekommendation.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att övriga rekommendationer i denna rapport implementeras, särskilt avseende uppföljning av behörigheter samt avseende utbildning inom området, eftersom dessa är två centrala aspekter för att säkerställa en adekvat hantering av patientinformation. En noggrann och regelbunden uppföljning av behörigheter är avgörande för att undvika obehörig åtkomst till känslig information. Kunskap och utbildning är även avgörande för dem som hanterar patientinformation. Bristande utbildning kan leda till felaktig hantering av information och att etablerade rutiner inte efterlevs.

Regionstyrelsens svar: Informations- och IT-säkerhet är prioriterade områden i regionen. I Regionstyrelsen verksamhetsplan finns målen - “Hög säkerhet hos mjukvara som körs i regionens IT-miljö genom inventering och kontroll” samt “Hög säkerhet i nätverksansluten hårdvara"

Planen innehåller även uppdraget - “Vidta åtgärder för att öka Region Jämtland Härjedalens robusthet i händelse av olyckor, samhällsstörningar samt krig. Uppdraget omfattar försörjningsberedskap, cybersäkerhet, informationspåverkan och ett fortsatt arbete inom kontinuitetshantering”. I verksamhetsplan för IT- och eHälsoavdelningen finns flera aktiviteter kopplade till detta uppdrag.

Behörigheter till system hanteras i Plexus, med ett gränssnitt för chefer att beställa och följa upp medarbetare behörigheter. Enligt krav från IT-säkerhetsansvarig får ansvariga chefer i Plexus en uppmaning i Behörighetsportalen att revidera anställningsuppgifter när en anställd bytt arbetsplats eller fått ny befattning. Dessutom har chef alltid en möjlighet att enkelt få en överblick över alla anställdas verksamhetsroller genom menyvalet ’Mina medarbetare’ i Plexus. Alla aktiviteter i Plexus loggas i audit-logg.

Revisionsfråga 7: Är det säkerställt att personal som hanterar lagring och hantering av känsliga uppgifter om enskilda patienter har den utbildning i informationssäkerhet som behövs utifrån tilldelade arbetsuppgifter?

Revisorerna rekommenderar Regionstyrelsen att: Införa ett obligatoriskt krav för medarbetare att fullfölja utbildningen inom en given tidsram för att på så sätt öka deltagandet och stärka informationssäkerheten..

Regionstyrelsens svar: Hösten 2024 inför regionen en ny årlig informationssäkerhets-utbildning som alla förväntas ta del av. Genomförande kommer att följas upp och återkopplas till respektive medarbetares chef vid ej genomförd utbildning.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa en adekvat kunskapsnivå genom att relevant personal kunskapstestas på regelbunden basis.

Regionstyrelsens svar: Hösten 2024 inför regionen en ny årlig informations-säkerhetsutbildning som alla förväntas ta del av. Genomförande kommer att följas upp och återkopplas till respektive medarbetares chef vid ej genomförd utbildning.

Att uppnå en bra säkerhetskultur där alla medarbetare förstår sitt informations-säkerhetsansvar baseras ej på kunskapstester utan på regelbunden utbildning inom sakområdet, tillsammans med annan löpande information, riskarbete, etcetera. Rekommendationen är inte baserad på evidensbaserad forskning och regionen anser därmed att revisorernas rekommendation ej är ändamålsenlig.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att medarbetarna utbildas inom området kontinuerligt. Detta är viktigt både för att repetera kunskaperna men också för att kunskapskraven ändras relativt snabbt inom detta område..

Regionstyrelsens svar: Hösten 2024 inför regionen en ny årlig informationssäkerhets-utbildning som alla förväntas ta del av. Genomförande kommer att följas upp och återkopplas till respektive medarbetares chef vid ej genomförd utbildning.

Revisorerna rekommenderar Regionstyrelsen att: Utvärdera möjligheten att införa en specifik IT-säkerhetsutbildning, särskilt riktad till medarbetare som arbetar med känsliga uppgifter.

Regionstyrelsens svar: Regionen instämmer med revisorernas rekommendation och skall utvärdera möjligheten.

Revisorerna rekommenderar Regionstyrelsen att: S. Säkerställa att det systematiskt utvärderas vilka kunskaper som medarbetarna behöver besitta, samt hur det aktuella kunskapsläget inklusive eventuella brister kan åtgärdas. Förändrade behov och identifierade brister bör därefter åtgärdas genom exempelvis utbildning, informationsinsatser och övningar.

Regionstyrelsens svar: Hösten 2024 inför regionen en ny årlig informationssäkerhets-utbildning som alla förväntas ta del av. Genomförande kommer att följas upp och återkopplas till respektive medarbetares chef vid ej genomförd utbildning.

Utöver detta får redan specifika roller såsom registerkoordinatorer regelbunden utbildning av regionens dataskyddsombud, riskombud regelbunden utbildning av brandansvarig, etcetera.

Rekommendationen bör formuleras så att samtliga roller med ett informationssäkerhets-ansvar är medvetna om det delegerade ansvaret för informationssäkerheten.

Revisionsfråga 8: Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att en systematisk och fullständig process för informationsklassning etableras.

Regionstyrelsens svar: En risk består av sannolikhet + konsekvens = risk. I en informationsklassning värderas informationen endast utifrån konsekvensen. Då sannolikheten inte tas i beaktande är detta inte en riskanalys.

Regionen har en dokumenterad regel med tillhörande rutiner och mallar för att kunna genomföra informationsklassningar. Det som saknas är den sista delen i att värderingen omsätts till organisatoriska och tekniska säkerhetsåtgärder där samma värdering genererar samma krav på åtgärder. Detta kommer att åtgärdas under hösten 2024.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att informationsklassningen hålls aktuell och systematiskt omprövas.

Regionstyrelsens svar: Regionen saknar en enhetligt implementerad styr- och förvaltningsmodell för IT och digitalisering. En extern genomlysning av IT-funktionen genomfördes 2019, som bl a resulterade i reviderad styr- och förvaltningsmodell för regionens informationssystem. Modellen baseras på tillämpbara delar av pm3. Förvaltningsdelarna har implementerats i ett fåtal system t ex vårdinformationsystemet

COSMIC. Förvaltningsstyrning enligt modell har inte påbörjats, vilket bl a innebär att inte samtliga informationssystem är identifierade eller identifierade med ägare.

Det saknas även en fullständig processkartläggning eller informationskartläggning så förutsättningarna för att uppfylla kravet att informationsklassa antingen genom informationsmängder eller informationssystem finns inte på plats.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att arbetet med att fastställa och etablera en systemförvaltningsmodell färdigställs.

Regionstyrelsens svar: Etablering av systemförvaltningsmodell enligt rekommendationer i ”Genomlysning av IT-funktionen”, behöver prioriteras och kommer att hanteras i någon form inom ramen för den nya organisationen för Utveckling och digitalisering.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att en strukturerad och formell process för riskanalyser etableras. Den bör vara anpassad utifrån verksamhetens behov, krav och förutsättningar och innehålla en tydlig struktur för löpande styrning och uppföljning för att säkerställa att processen hålls uppdaterad efter förändrade behov. Det är även rekommenderat att verksamheten involverar samtliga relevanta intressenter i processen i syfte att bidra till ökad förståelse och samarbete kring riskanalysen.

Regionstyrelsens svar: Regionens verksamheter ska samtliga arbeta strukturerat med analys och hantering av risker. I utvecklingsprojekt inom IT och digitalisering görs riskanalyser inför initiering och planering av aktiviteter. Omfattning och modell varierar beroende på projektets art. Projektil Riskanalys med handlingsplan är en modell som tillämpas.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att arbetet med ett mer proaktivt riskarbete, som påbörjats, färdigställs.

Regionstyrelsens svar: Proaktivt riskarbetet sker inom en rad olika områden t ex patientsäkerhet, arbetsmiljö, IT och digitalisering. Regionen saknar ett enhetligt riskramverk, som kan vara tillämpbart för samtliga behov. Det finns inte heller en utpekad roll/ funktion som ansvarar för utforming av ramverk och verktyg för identifiering och hantering av risker. I Stratsys ISK Internkontroll finns identifierade processer kartlagda och stöd för riskhantering, dock har modulen inte ännu börjat tillämpas i någon större utsträckning.

Revisorerna rekommenderar Regionstyrelsen att: Införa en strukturerad metod för att identifiera och klassificera verksamhetskritiska system. Detta skapar en tydlig grund för att avgöra vilka system som kräver kontinuitetsplaner, förbättrar hanteringen och prioriteringen av risker samt säkerställer en effektiv beredskap.

Regionstyrelsens svar: I kontinuitetsplan för oplanerade avbrott i regionens IT-miljö, finns verksamhetskritiska system identifierade med en fastställd prioriteringsordning vid återstart.

REGIONSTYRELSEN

Bengt Bergqvist (S)
Regionstyrelsens ordförande

Sara Lewerentz
Regiondirektör

Yttrandet är fastställt av regionstyrelsen 2024-08-27 § 130