Granskning av kontinuitetsplanering för it-avbrott

Rapport

Region Gotland

KPMG AB

2024-10-30

Antal sidor 21

Region Gotland
Granskning av kontinuitetsplanering för it-avbrott

2024-10-30

Innehållsförteckning

1	Sammanfattning	2
2	Bakgrund	6
2.1	Syfte och revisionsfrågor	7
2.2	Avgränsning	7
2.3	Revisionskriterier	8
2.4	Metod	8
3	Inledning	10
4	Resultat av granskningen	11
4.1	Riskbedömning och planering för it-avbrott	11
4.2	Tillgänglighet till informationssystem och redundans	15
4.3	Intern kontroll	17
5	Samlad bedömning och rekommendationer	19

1 Sammanfattning

KPMG har av Region Gotlands förtroendevalda revisorer fått i uppdrag att granska regionen arbete med beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa. Uppdraget ingår i revisionsplanen för år 2024.

Granskningen syftade till att bedöma om regionstyrelsen, hälso- och sjukvårdsnämnden och socialnämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen och nämnderna delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser.

Vi baserar vår bedömning på att det finns ett aktivt arbete med att säkerställa ändamålsenliga åtgärder, servicenivåer och beredskap utifrån regionens process för informationsklassning. I huvudsak efterlevs dessa processer. Granskningen har dock kunnat identifiera att ett verksamhetskritiskt system saknar slutförd informationsklassning, beslutade servicenivåer och beredskap.

Vi bedömer vidare att det pågår ett utvecklingsarbete vad gäller arbetet att säkerställa verksamheternas kontinuitet vid it-avbrott men konstaterar samtidigt att arbetet i hög grad skiljer sig mellan de olika verksamheterna. Detta avseende både mognadsgrad, hur arbetet genomförs samt hur dokumentationen utformas.

Vi bedömer att detta är en konsekvens av en bristande regionövergripande styrning där det idag inte är tydligt vilka krav som ställs på verksamheternas kontinuitetsplanering, enligt vilka metoder och processer planeringen bör ske och hur detta ska följas upp i nämnderna och på en regionövergripande nivå.

Det har inte heller genomförts krisövningar avseende scenario för it-avbrott. Vi bedömer att det medför att det inte finns någon utvärdering eller kontroll över att befintliga underlag och rutiner skulle vara tillräckliga för att upprätthålla verksamheternas kontinuitet på en acceptabel nivå. Vi ser därför övningar som en väsentlig del för att bedöma planeringen samt för att identifiera eventuella förbättringsbehov.

På följande sida redovisas våra bedömningar och rekommendationer kopplat till revisionsfrågorna.

Revisionsfråga	Bedömning: Delvis	Rekommendationer
Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?	I två av fem granskade verksamheter kan vi se ett fullt ut strukturerat arbete med underlag som motsvarar kontinuitetsplaner och vi kan delvis se ett sådant arbete i ytterligare två verksamheter. Vår bedömning är att det idag inte är tydligt hur kontinuitetsarbete generellt ska bedrivas utifrån befintliga riskprocesser i regionen. Följaktligen skiljer sig kontinuitetsarbetet åt både vad avser metodik, dokumentation och mognadsgrad.	**Regionstyrelsen:** Säkerställa att arbetet med kontinuitetsplanering ska bedrivs i enlighet med beslutade styrdokument och med grund i befintliga riskprocesser i regionen. **Regionstyrelsen och hälso- och sjukvårdsnämnden:** Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna sker enligt en av regionstyrelsen beslutad systematik. **Socialnämnden:** Även om nämnden har en god planering i nuläget kan det finnas behov av att anpassa denna om regionstyrelsen fattar beslut om krav och gemensamma arbetssätt.
Revisionsfråga	**Bedömning: I allt väsentligt**	**Rekommendationer**
Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?	För de fyra granskade verksamheter som har kontinuitetsplaner eller motsvarande underlag, fullt ut eller delvis, beaktas kritiska beroenden till informationssystem. Ekonomiavdelningen saknar kontinuitetsplan eller motsvarande underlag och således beaktas inte kritiska beroenden till informationssystem. På en regionövergripande nivå behöver det definieras varför, hur och vad verksamheterna ska planera för kopplat till risken för it-avbrott inom ramen för en generell styrning av kontinuitetsarbetet. Idag är det inte tydligt för verksamheterna hur risken för it-avbrott identifierats på en övergripande nivå. Det är heller inte definierat på vilken nivå eller utifrån vilken kravställning det förväntas att verksamheterna ska planera för ett it-avbrott eller enligt vilken struktur, metod och i vilken process detta arbete ska ske. Följaktligen finns det stora skillnader i hur verksamheterna	**Regionstyrelsen:** - Tillse att det är tydligt på vilket sätt kritiska beroenden till informationssystem ska beaktas i verksamheternas kontinuitetsplanering. - Säkerställ att de egna verksamheterna beaktar kritiska beroenden till informationssystem i sin kontinuitetsplanering.

	har planerat för risken för it-avbrott, även om kritiska beroenden till informationssystem i allt väsentligt beaktas i den planering som finns. Vi ser därför positivt på att det finns ett pågående arbete att tydliggöra styrningen för kontinuitetsplanering.	
Revisionsfråga	**Bedömning: I allt väsentligt**	**Rekommendationer**
Har åtgärder för att säkerställa kontinuiteten identifierats och vidtagits?	Åtgärder har identifierats och vidtagits för att säkerställa kontinuiteten i hälso- och sjukvårdsnämndens och socialnämndens verksamheter och system. Åtgärder har delvis identifierats och vidtagits för att säkerställa kontinuiteten i regionstyrelsens verksamheter och system. Det verksamhetskritiska systemet för måltidsverksamheten har idag inte en slutförd informationsklassning eller tillhörande åtgärder. Däremot kan vi konstatera att detta är genomfört för ekonomiavdelningens system.	**Regionstyrelsen:** Tillse att informationsklassningen för måltidsverksamhetens kritiska system slutförs samt att erforderliga åtgärder vidtas
Revisionsfråga	**Bedömning: I allt väsentligt**	**Rekommendationer**
Finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem?	Det finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem inom hälso- och sjukvårdsnämndens och socialnämndens verksamheter. Det finns delvis avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem inom regionstyrelsens verksamheter. Det verksamhetskritiska systemet för måltidsverksamheten har idag inte avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet, i avsaknad av en slutförd informationsklassning av systemet.	**Regionstyrelsen:** Säkerställ att avtalad servicenivå och beredskap baserad på skyddsvärde och behov av tillgänglighet tas fram för måltidsverksamheten verksamhetskritiska informationssystem.

	Vi kan dock konstatera att ekonomiavdelningens system har avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för sina verksamhetskritiska informationssystem.	
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Har övningar genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig?	Vår bedömning är att övningar inte har genomförts inom regionstyrelsen eller berörda nämnder i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.	**Regionstyrelsen och samtliga nämnder:** Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar?	Det finns inte en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.	**Regionstyrelsen:** Säkerställ att det är tydligt på vilket sätt kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar. **Regionstyrelsen och samtliga nämnder:** Följ upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad regionövergripande systematik.

2 Bakgrund

KPMG har av Region Gotlands förtroendevalda revisorer fått i uppdrag att granska regionens arbete med beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa. Uppdraget ingår i revisionsplanen för år 2024.

En god krisberedskap är en förutsättning för att både regionen och de regionala bolagens verksamheter ska stå väl rustade inför olika former av samhällsstörningar och för att klara av att hantera olika former av krissituationer. Förmåga att hantera säkerhetshändelser för informationstillgångar och it baseras på att det även finns ett systematiskt informationssäkerhetsarbete.

Ett flertal offentliga organisationer har under de senaste åren utsatts för cyberattacker med stora konsekvenser som följd. Exempelvis har skyddsvärd information förlorats eller röjts till obehöriga eller så har den bristande hanteringen lett till att organisationer drabbats av ekonomisk skada eller förtroendeskada. Inledningsvis 2024 utsattes en större leverantör av serverdrift och molntjänster för en ransomware-attack vilken fått en allvarlig påverkan på ett stort antal statliga myndigheters, kommuners och regioners tillgång till sina informationssystem.

Inom ramen för det kommunala åtagandet finns en rad samhällsviktiga funktioner, vilka om de inte fungerar kan leda till skada för såväl enskilda individer som samhället i stort. Dessa funktioner behöver fungera varje dag även om incidenter inträffar och det för verksamheten är ett så kallat onormalt läge. Det ökande beroendet till it- och informationssystem leder till att ett bortfall av dessa kritiska tillgångar får större konsekvenser än tidigare. Det är därför av största vikt att det bedrivs ett systematiskt och sammanhållet informationssäkerhetsarbete samt krisberedskapsarbete för att undvika allvarlig påverkan på samhället. I det arbetet krävs väl genomarbetade, förankrade och testade kontinuitetsplaner för att upprätthålla verksamheterna.

Revisorerna och lekmannarevisorerna bedömer de negativa konsekvenserna vid en extraordinär händelse eller annan kris som betydande om det inte finns ändamålsenlig kontinuitetsplanering. Revisorerna drar därför slutsatsen att både sannolikheten för, och konsekvenserna av kritiska säkerhetshändelse inom it är icke-försumbara och att arbetet med kontinuitetsplanering och reservrutiner behöver granskas.

2.1 Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om regionstyrelsen och nämnderna har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Granskningen har besvarat följande revisionsfrågor:

- Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?
- Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?
- Har åtgärder för att säkerställa kontinuiteten identifierats och vidtagits?
- Finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem?
- Har övningar genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig?
- Finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar?

2.2 Avgränsning

Vi har i granskningen inte tagit del av underlag eller information som är säkerhetsskyddsklassad.

Granskningen avser regionstyrelsen, dels utifrån övergripande styrning och uppföljning, dels verksamhet inom ekonomifunktionen och måltidsverksamheten. Stickprov för granskning av kontinuitetsplanering avser kritiska processer med stort beroende av digital information.

Granskningen avser socialnämnden. Stickprov för granskning av kontinuitetsplanering avser kritiska processer inom ordinärt boende samt kommunal hälso- och sjukvård med stort beroende av digital information.

Granskningen avser hälso- och sjukvårdsnämnden. Stickprov för granskning av kontinuitetsplanering avser kritiska processer inom regional hälso- och sjukvård med stort beroende av digital information.

2.3 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

- Kommunallagen (2017:725)
- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och beredskap.
- Myndigheten för samhällsskydd och beredskaps vägledning för Risk- och sårbarhetsanalyser, MSB245
- MSBFS 2015:5
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (där detta är tillämpbart)
- MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (där detta är tillämpbart)
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- Tillämpbara interna regelverk, policys och beslut

2.4 Metod

Granskningen har genomförts genom dokumentgranskning, intervjuer och stickprov.

Dokumentgranskning

Följande dokument har ingått i granskningen:

- Reglemente för styrelsen och nämnder
- Styrande dokument inom krisberedskap och informationssäkerhet
- Risk- och sårbarhetsanalys (informationsklass under säkerhetsskydd)
- Kontinuitetsplaner eller motsvarande underlag och tillhörande rutiner
- SLA:er (servicenivåöverenskommelser för informationssystem)

Intervjuer

Intervjuer har genomförts med:

- Presidier i samtliga berörda nämnder och regionstyrelsen
- Regiondirektör
- Digitaliseringsdirektör
- Digitaliseringsstrateg
- Säkerhetschef
- Beredskapssamordnare
- Avdelningschefer inom demokrati och kvalitet, hemtjänst, hemsjukvård, ekonomi och måltidsverksamhet

- Förvaltningsdirektörer inom samtliga berörda förvaltningar
- Beredskapsläkare hälso- och sjukvårdsförvaltningen
- Verksamhetsarkitekt och informationssäkerhetssamordnare inom hälso- och sjukvårdsförvaltningen
- Enhetschef för ehälsa/MIT
- Administrativ chef socialförvaltningen

Stickprov

Stickprov av upprättade kontinuitetsplaner och SLA:er inom berörda revisionsobjekt och system har granskats mot bakgrund av given avgränsning.

Rapporten har via beredskapschef skickats på faktakontroll.

3 Inledning

Arbetet med krisberedskap och extraordinära händelser tar sin utgångspunkt i en övergripande Risk- och sårbarhetsanalys (RSA) som kommuner och regioner enligt lagkrav ska genomföra vid varje ny mandatperiod. En del i RSA-processen är att identifiera vilka samhällsviktiga verksamheter som kommunen bedriver samt att kontinuitetsplanera för dessa.

MSB har även gett ut råd för att säkra tillgången till organisationens information. I den framgår att kontinuitetshantering handlar om att planera för att verksamheten ska kunna bedrivas på en acceptabel nivå oavsett vilken störning den utsätts för.

Ofta är organisationens information nödvändig för att verksamheten ska kunna fungera. Information hanteras idag till stor del digitalt. Kontinuitetshanteringen behöver därför säkerställa tillgång till information och därmed it-resurser. Det kan exempelvis handla om verksamhetsspecifika och administrativa system, e-post, filer, molntjänster och hårdvara som PC, servrar, telefoner och nätverk.

Exempel på arbetssätt som kan behöva planeras är chatt- och videoverktyg för möten, e-post för kommunikation och för att förmedla information samt interna nätverk för att spara eller sprida information. Därtill kan det behövas alternativa arbetssätt i form av utskrivna kontaktlistor, lokala kopior av nödvändig information samt beskrivna rutiner för att övergå till alternativa sätt att bedriva den dagliga verksamheten om tillgång till it saknas.

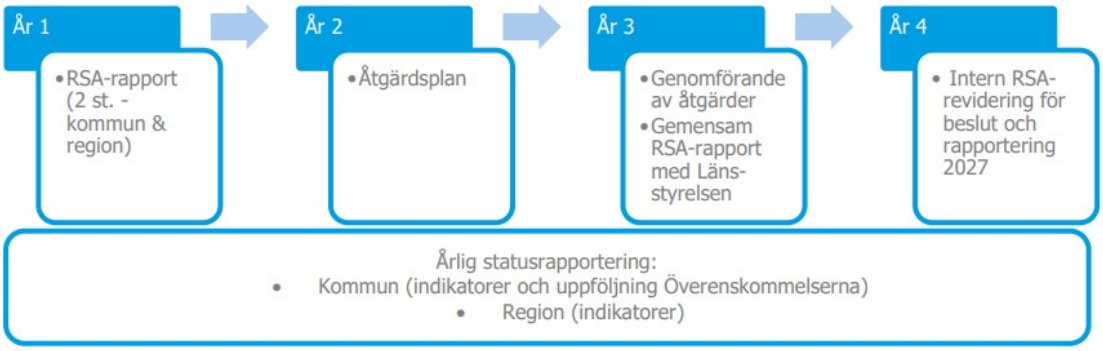
Mot bakgrund av den ökande hotbilden för cyberattacker med risk för att informationssystem och it-miljön inte är tillgängliga för de samhällsviktiga verksamheterna avgränsas denna granskning till kontinuitetsplanering och reservrutiner vid it-bortfall.

4 Resultat av granskningen

4.1 Riskbedömning och planering för it-avbrott

I den regionala utvecklingsstrategin ”Vårt Gotland 2040” finns effektmålet ”Gotland har god beredskap och förmåga att hantera samhällsstörningar”. Effektmålet fastställdes av regionfullmäktige i februari 2021. I policy för civil beredskap[1] beskrivs att utifrån effektmålet och *lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap* ska Region Gotland bland annat genomföra risk- och sårbarhetsanalyser (RSA) inklusive kontinuitetshantering, det vill säga minska risker och sårbarheter samt ha förmåga att upprätthålla och skydda verksamhet mot/vid samhällsstörningar.

I policy för civil beredskap beskrivs också processen för risk- och sårbarhetsanalys och kontinuitetshantering enligt nedan:



Enligt policyn har regionstyrelsen det övergripande ansvaret för att fastställa Region Gotlands arbete med civil beredskap. Arbetet ska ske koncernövergripande samt inom respektive förvaltning. Utifrån en sammanställning av förvaltningarnas underlag skapas en aggregerad bild av Region Gotlands hot- och riskbild, samhällsviktig och kritisk verksamhet, konsekvenser för Region Gotland vid avbrott i verksamheter samt vad Region Gotland har för kritiska beroenden och kritiska resurser, både inom organisationen och till andra aktörer. På koncernövergripande nivå ska kompletterande RSA och kontinuitetsarbete ske, både inom särskilda områden såväl som övergripande strategiarbete.

I riktlinjen för informationssäkerhet [2] framgår också att kontinuiteten för informationssäkerheten ska planeras, implementeras och revideras som en integrerad del av hela organisationens system för kontinuitetshantering. Vi har inom ramen för granskningen också tagit del av underlag som styrker att risken för it-avbrott utgör en risk i den regionövergripande risk- och sårbarhetsanalysen.

I granskningen har vi inte kunnat spåra att arbetet därefter sker enligt en systematisk process. Berörda verksamheter har i liten utsträckning kunskaper om de risker som

[1] Fastställd av regionfullmäktige 2023-02-20
[2] Fastställd av regionstyrelsen 2023-04-26

definieras i den regionövergripande risk- och sårbarhetsanalysen, och kopplat till risken för it-avbrott har inte verksamheterna någon kännedom om ett tydligt uppdrag utifrån risk- och sårbarhetsanalysen som fastställer vad arbetet ska utmynna i, hur det ska bedrivas eller utifrån vilken riskbedömning. Vi kan utifrån detta inte se att det funnits någon gemensam systematisk process för riskidentifiering och kontinuitetsplanering kopplat till risken för it-avbrott i regionen

Vi har i granskningen fått presenterat för oss att ett konkret uppdrag för planering inför ett it-avbrott kommunicerades ut under en begränsad period i samband med Sveriges Nato-inträde. Verksamheterna skulle enligt uppdraget vidta robusthöjande åtgärder i syfte att tillse att de skulle kunna fortsätta bedrivas vid ett it-avbrott omfattande två veckor. Uppdraget var tillfälligt, ingick inte i någon annan process för kontinuitetsplanering och ingen systematisk uppföljning av resultatet ingick som en del av uppdraget. Däremot har det framförts i intervjuer att uppdraget hade positiva bieffekter i syfte att få i gång ett aktivt kontinuitetsarbete kopplat till risken för it-avbrott vilket av de intervjuade bedöms generellt ha höjt beredskapen i verksamheterna.

Mot bakgrund av att det hos de intervjuade finns en upplevelse av bristande styrning och uppföljning av bland annat risken för it-avbrott har det i granskningen lyfts fram att det pågår ett arbete med att inom ramen för den nya styrmodellen i regionen styra beredskapsfrågor på ett tydligare sätt. Den tilltänkta strukturen, som vid granskningens tidpunkt inte är fastställd, bygger på att beredskap ska vara ett prioriterat område som ska brytas ned till konkreta mål till respektive nämnd. Utifrån målen ska respektive nämnd fastställa ett antal insatser med bäring på målen i sin verksamhetsplan. I detta arbete ska regionstyrelseförvaltningen processleda och ha en tydligt uttalat stöttande och uppföljande roll gentemot respektive förvaltning för att säkerställa att arbetet sker i enlighet med tilltänkt struktur.

4.1.1 Kontinuitetsplaner och kritiska beroenden till informationssystem

I granskningen har ingått att granska stickprov av dokumenterade kontinuitetsplaner för att kontrollera om kritiska beroenden till informationssystem har ingått i analys och planering. Resultat av stickprovsgranskningen presenteras i tabell på nästa sida.

Ansvarig	Verksamhet	Kontinuitets-plan finns	Risk för it-avbrott har inkluderats	Kritiska informations-system är identifierade
Regionstyrelsen	Ekonomi	Nej	Nej	Ja
	Måltid	Delvis	Ja	Ja
Hälso- och sjukvårdsnämnden	Regional hälso- och sjukvård	Delvis	Ja	Ja
Socialnämnden	Hemtjänst	Ja	Ja	Ja
	Kommunal hälso- och sjukvård	Ja	Ja	Ja

4.1.1.1 Kommentar till resultat av stickprovsgranskning

Det finns idag nyligen framtagna regiongemensamma mallar och metodstöd för hur verksamheterna ska arbeta med kontinuitetsplanering, men kännedomen om dessa i verksamheterna är enligt intervjuer låg och har inte varit vägledande för arbetet. Det arbete som gjorts har inte en tydlig spårbarhet till definierad risk för it-avbrott eller motsvarande risk i den regionövergripande risk- och sårbarhetsanalysen eller annan systematik i regionen. Detta uppges i intervju innebära att det är otydligt hur nämnder och verksamheter förväntas jobba med sin samhällsviktiga verksamhet utifrån risken för it-avbrott. Vi har i analysen av kontinuitetsplaner eller motsvarande underlag gått igenom de underlag verksamheterna använder för att planera för att upprätthålla kontinuiteten i sina verksamheter och gjort en bedömning huruvida detta underlag motsvarar en kontinuitetsplanering eller inte. Ingen av verksamheterna använder idag begreppet kontinuitetsplanering för att beskriva det arbete man gör med att planera för att upprätthålla verksamheten i händelse av exempelvis it-avbrott. Enligt intervjuer beror detta på att man inte konsekvent använder det här begreppet, eller angränsande begrepp, på ett gemensamt sätt i styrningen av frågorna i regionen.

I socialnämndens verksamheter finns en kontinuitetsplanering bestående av en struktur med riskbedömningsmatriser, beredskapsplaner och verksamhetsspecifika rutiner för hantering av avbrott i de kritiska system som verksamheten arbetar med. Motsvarande struktur ser vi inte i underlagen från övriga förvaltningar, men både hälso- och sjukvården och måltidsverksamheten har olika former av rutiner för att hantera bland annat it-avbrott, exempelvis i form av beredskapsrutiner vid it-avbrott och krispärmar. Vad avser ekonomiavdelningen finns inget motsvarande underlag.

Samtliga verksamheter har däremot identifierat sina kritiska verksamhetssystem. Detta har inte dokumenterats på ett spårbart sätt inom ramen för ett strukturerat arbete med kontinuitetsplanering. Däremot finns ett strukturerat arbete i regionen med informationsklassning av system, inom vilket verksamheterna, i samverkan med regionens interna digitaliseringsavdelning, har informationsklassat sina system och därmed definierat vilka system som är särskilt kritiska (se 4.2).

4.1.2 Övning

I intervjuer har det framkommit att inga planerade övningsinsatser kopplat till it-avbrott har genomförts i regionen i närtid. Inom vissa verksamheter finns det planer på att genomföra en övning med personal i den egna verksamheten. Det uppges i intervjuer att man i skarpa situationer som har skett i olika verksamheter har försökt betrakta dessa som övning och tillvarata och utvärdera händelserna.

4.1.3 Bedömning

Vår bedömning är att det delvis finns dokumenterade kontinuitetsplaner eller motsvarande underlag. Vi bedömer att kritiska beroenden till informationssystem i allt väsentligt beaktats i verksamheternas kontinuitetsplanering.

Vår bedömning baseras på att vi i två av fem granskade verksamheter kan se ett fullt ut strukturerat arbete med att planera för verksamhetens kontinuitet och att vi delvis kan se ett sådant arbete i ytterligare två verksamheter. Vi bedömer att det på en regionövergripande nivå behöver definieras varför, hur och vad verksamheterna ska planera för kopplat till risken för it-avbrott inom ramen för en generell styrning av kontinuitetsarbetet. Idag är det inte tydligt definierat för verksamheterna hur risken för it-avbrott identifierats på en övergripande nivå, på vilken nivå eller utifrån vilken kravställning det förväntas att verksamheterna ska planera för ett it-avbrott eller enligt vilken struktur, metod och i vilken process detta arbete ska ske. Följaktligen finns det stora skillnader i hur verksamheterna har planerat för risken för it-avbrott, även om kritiska beroenden till informationssystem i allt väsentligt beaktas i den planering som finns. Vi ser därför positivt på att det finns ett pågående arbete med att tydliggöra styrningen för kontinuitetsplanering. Vi ser även positivt på de initiativ som tidigare tagits för att stärka beredskapen i verksamheterna.

Vår bedömning är att övningar inte har genomförts inom regionstyrelsen eller berörda nämnder i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

Då övningar inte har genomförts går det inte att fastställa att nuvarande planering skulle vara tillräcklig i händelse av allvarligare it-avbrott. Detta bör således planeras som del i kontinuitetshanteringen.

4.2 Tillgänglighet till informationssystem och redundans

4.2.1 Analys och bedömningar av skyddsbehov och krav på tillgänglighet

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

Det framgår i guiden att objektsförvaltaren praktiskt har hand om förvaltningen av informationsmängden och informationssystemet. Klassningen ska ske utifrån perspektiven konfidentialitet, tillgänglighet, riktighet och spårbarhet samt följande konsekvensnivåer: försumbar skada, måttlig skada, betydande skada och allvarlig skada. Genomförd klassning ska dokumenteras i *verktyget*[3]. I guiden finns en tydlig beskrivning av vad som ska ingå i dokumentationen. Det framgår vidare att klassning och riskanalys ska genomföras innan upphandling av nya verksamhetssystem.

Av objektsförvaltningsmodellen framgår att det finns ett årshjul med aktiviteter som objektsförvaltaren ansvarar för. Objektsförvaltaren ska årligen genomföra:

- Informationsklassningar
- Risk och sårbarhetsanalyser
- Förvaltningsplaner
- Återkommande revision

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

Som en del i granskningen har vi fått en genomgång av verktyget och den dokumentation som lagras där. på nästa sida presenteras resultatet av vår genomgång.

[3] Internt utvecklat systemstöd som utgör regionens ledningssystem för informationssäkerhet.

Ansvarig nämnd	Verksamhet och antal verksamhetskritiska system	Informations-klassning finns och är aktuell	Åtgärder har vidtagits utifrån klassning	SLA finns
Regionstyrelsen	Ekonomiavdelningen 3 system	Ja	Ja	Ja
	Måltidsverksamheten 1 system	Nej	Nej	Nej
Hälso- och sjukvårdsnämnden	Regional hälso- och sjukvård 3 system	Ja	Ja	Ja
Socialnämnden	Ordinärt boende 3 system	Ja	Ja	Ja
	Kommunal hälso- och sjukvård 3 system	Ja	Ja	Ja

4.2.1.1 Kommentar till granskning av systemdokumentation

Vid vår genomgång av *verktyget* kan vi konstatera att det generellt sett finns ett systematiskt arbete med informationsklassning, i enlighet med styrande dokument. Vi kunde dock notera att måltidsverksamhetens kritiska system inte hade en slutförd informationsklassning och därmed inte heller en SLA för aktuellt system. Vad avser kolumnen att åtgärder har vidtagits utifrån klassning åsyftas de åtgärder som ska definieras och vidtas inom ramen för processen för informationsklassning, varför samtliga revisionsobjekt som följt processen för informationsklassning har bedömts som ett ja.

Vi vill dock framhålla att kontinuitetsplanering även omfattar den planering som sker genom att arbeta med mer verksamhetsnära reservrutiner, vilket beskrivs och bedöms i avsnitt 4.1. Detta för att inte riskera att missa åtgärder som inte är systemnära eller av teknisk karaktär utan mer avser alternativa arbetssätt och manuella rutiner som behövs för att upprätthålla verksamheten i de perioder som verksamheten är utan it.

4.2.2 Bedömning

Vår bedömning är att hälso- och sjukvårdsnämnden och socialnämnden för sina verksamhetskritiska system har identifierat och vidtagit åtgärder för att säkerställa kontinuiteten. Vår bedömning är att regionstyrelsen delvis har identifierat och vidtagit åtgärder för att säkerställa kontinuiteten i sina verksamhetskritiska system.

Vi baserar vår bedömning på att det verksamhetskritiska systemet för måltidsverksamheten idag inte har en slutförd informationsklassning med tillhörande åtgärder. Däremot kan vi konstatera att detta är genomfört för ekonomiavdelningens system.

Vår bedömning är att det finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem inom hälso- och sjukvårdsnämndens och socialnämndens verksamheter. Vår bedömning är att det delvis finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem inom regionstyrelsens verksamheter.

Det verksamhetskritiska systemet för måltidsverksamheten har idag inte avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet i avsaknad av en slutförd informationsklassning av systemet. Vi kan konstatera att ekonomiavdelningens system har avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för sina verksamhetskritiska informationssystem.

4.3 Intern kontroll

4.3.1 Regionstyrelsens och nämndernas kontroll avseende kontinuitetsplaneringen

Vi har i granskningen inte kunnat spåra någon systematisk uppföljning inom ramen för intern kontroll eller annan form av uppföljning från styrelse och nämnder som omfattar kontinuitetsplanering. I intervjuer beskrivs att det idag inte finns någon formell struktur för hur uppföljning av kontinuitetsarbetet ska ske på en övergripande regionstyrelsenivå eller för respektive nämnd. I intervjuer uppges att information ges vid behov utifrån budgetpåverkande åtgärder och allmänna informationspunkter kopplat till exempelvis risk- och sårbarhetsanalys till resplektive nämnd och styrelse. I skarpt läge hålls styrelsen och i synnerhet regionstyrelsens ordförande mer löpande informerad om händelseutvecklingen.

Det har också beskrivits för oss i intervjuer att det framgent finns ett arbete planerat kopplat till den nya styrmodellen där beredskapsarbetet generellt kommer vara en prioritering/inriktning med tilldelat ansvar till ansvarig tjänsteperson (säkerhetschef) att följa upp utifrån uppdraget. Dessutom avses att införa en ordning där nämnderna ska fastställa insatser kopplat till beredskapsfrågor i verksamhetsplanen i syfte att få en tydligare uppföljning.

4.3.2 Bedömning

Vår bedömning är att det inte finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

Vi kan konstatera att arbetet i vissa delar inte har genomförts i tillräcklig utsträckning vilket vare sig regionstyrelsen eller nämnderna har uppmärksammat genom sin interna kontroll. Vi ser därför att den interna kontrollen behöver stärkas för att säkerställa att regionens kontinuitet i kritiska verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser.

5 Samlad bedömning och rekommendationer

Granskningen har syftat till att bedöma om regionstyrelsen, hälso- och sjukvårdsnämnden och socialnämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen och nämnderna delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser.

Vi baserar vår bedömning på att det finns ett aktivt arbete med att säkerställa ändamålsenliga åtgärder, servicenivåer och beredskap utifrån regionens process för informationsklassning. I huvudsak efterlevs dessa processer. Granskningen har dock kunnat identifiera att ett verksamhetskritiskt system saknar slutförd informationsklassning, beslutade servicenivåer och beredskap.

Vi bedömer vidare att det pågår ett utvecklingsarbete vad gäller arbetet att säkerställa verksamheternas kontinuitet vid it-avbrott men konstaterar samtidigt att arbetet i hög grad skiljer sig mellan de olika verksamheterna. Detta avseende både mognadsgrad, hur arbetet genomförs samt hur dokumentationen utformas.

Vi bedömer att detta är en konsekvens av en bristande regionövergripande styrning där det idag inte är tydligt vilka krav som ställs på verksamheternas kontinuitetsplanering, enligt vilka metoder och processer planeringen bör ske och hur detta ska följas upp i nämnderna och på en regionövergripande nivå.

Det har inte heller genomförts krisövningar avseende scenario för it-avbrott. Vi bedömer att det medför att det inte finns någon utvärdering eller kontroll över att befintliga underlag och rutiner skulle vara tillräckliga för att upprätthålla verksamheternas kontinuitet på en acceptabel nivå. Vi ser därför övningar som en väsentlig del för att bedöma planeringen samt för att identifiera eventuella förbättringsbehov.

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen att:

- Förtydliga hur arbetet med kontinuitetsplanering är tänkt att bedrivas utifrån befintliga riskprocesser i regionen.
- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna sker enligt en av regionstyrelsen beslutad systematik.
- Tillse att det är tydligt på vilket sätt kritiska beroenden till informationssystem ska beaktas i verksamheternas kontinuitetsplanering.
- Säkerställa att de egna verksamheterna beaktar kritiska beroenden till informationssystem i sin kontinuitetsplanering.
- Tillse att informationsklassningen för måltidsverksamhetens kritiska system slutförs.
- Säkerställa att avtalad servicenivå och beredskap baserad på skyddsvärde och behov av tillgänglighet framtas för måltidsverksamheten verksamhetskritiska informationssystem.

- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Säkerställa att det är tydligt på vilket sätt kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar.
- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad regionövergripande systematik.

Utifrån resultatet av vår granskning rekommenderar vi hälso- och sjukvårdsnämnden att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna sker enligt en av regionstyrelsen beslutad systematik.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad regionövergripande systematik.

Utifrån resultatet av vår granskning rekommenderar vi socialnämnden att:

- Även om nämnden har en god planering i nuläget kan det finnas behov av att anpassa denna om beslut fattas av regionstyrelsen över krav och gemensamma arbetssätt.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad regionövergripande systematik.

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Simon Homander
Verksamhetsrevisor