Granskning av kontinuitetsplanering för it-avbrott

Rapport

Växjö kommun

KPMG AB

2024-08-12

Antal sidor 22

Växjö kommun
Granskning av kontinuitetsplanering för it-avbrott

2024-08-12

Innehållsförteckning

1	Sammanfattning	2
2	Bakgrund	5
2.1	Syfte och revisionsfrågor	6
2.2	Avgränsning	6
2.3	Revisionskriterier	7
2.4	Metod	7
3	Regelverk för kontinuitetsplanering	9
4	Resultat av granskningen	10
4.1	Process för riskbedömning och planering för it-avbrott	10
4.2	Tillgänglighet till informationssystem och redundans	14
4.3	Intern kontroll	18
5	Samlad bedömning och rekommendationer	20

1 Sammanfattning

Granskningen syftar till att bedöma om kommunstyrelsen och nämnderna har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

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

Vår samlade bedömning utifrån granskningens syfte är att servicenämnden och omsorgsnämnden i allt väsentligt har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser

Vår bedömning baseras på att vi i granskningen har tagit del av styrdokument, rutiner och processer som beskriver hur arbetet med kontinuitetsplanering är tänkt att bedrivas i kommunen. Vi kan i vissa verksamheter se att arbetet bedrivs i linje med detta, men kan också konstatera att det finns tydliga skillnader i hur långt de olika samhällsviktiga verksamheterna har kommit i sin kontinuitetsplanering för it-avbrott. Det skiljer sig även i vilken utsträckning verksamheterna arbetar enligt tänkta strukturer för att identifiera och vidta relevanta åtgärder.

Det saknas idag en tillräcklig kontroll och uppföljning av de verksamheter som inte bedriver ett arbete enligt den struktur som beskrivs i styrdokument och den kravnivå för planering inför it-avbrott som fastställts i risk- och sårbarhetsanalys. Vi bedömer att det är av stor vikt att det finns en tydlig ansvarsfördelning mellan nämnder och styrelsen vad gäller uppföljning av att koninuitetsarbetet i berörda verksamheter sker i enlighet med den kravställning som finns i styrdokument.

I det följande redovisas våra bedömningar och rekommendationer kopplat till revisionsfrågorna.

Revisionsfråga	**Bedömning: Ja**	**Rekommendationer**
Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?	Det finns dokumenterade kontinuitetsplaner eller motsvarande underlag i samtliga granskade verksamheter.	
Revisionsfråga	**Bedömning: I allt väsentligt**	**Rekommendationer**
Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?	Kritiska beroenden till informationssystem har beaktats i kontinuitetsplaneringen för kommunstyrelsen, servicenämnden och omsorgsnämndens verksamheter. Kritiska beroenden till informationssystem har inte beaktats i kontinuitetsplaneringen	**Samhällsbyggnadsnämnden:** Säkerställ att kritiska beroenden till informationssystem beaktas i VA-verksamhetens kontinuitetsplanering.

	för samhällsbyggnadsnämndens VA-verksamhet.	

Revisionsfråga	Bedömning: I allt väsentligt	Rekommendationer
Har åtgärder för att säkerställa kontinuiteten identifierats och vidtagits?	Omsorgsnämnden och servicenämndens verksamheter har identifierat och vidtagit åtgärder för informationssystemen i enlighet med den process som finns i kommunen för informationssäkerhetanalys samt identifierat och vidtagit åtgärder för att säkerställa kontinuiteten i verksamhetens rutiner. Motsvarande systematiska arbete finns inte för granskade verksamheter och system inom kommunstyrelsen och samhällsbyggnadsnämnden. Vi konstaterar att det finns vidtagna åtgärder men baserar vår bedömning på att arbetet inte i tillräcklig nivå följer den kommungemensamma processen för att identifiera relevanta åtgärder varken för informationssystemen eller verksamhetens rutiner.	**Kommunstyrelsen och samhällsbyggnadsnämnden:** Tillse att den egna verksamheten följer kommunens process för informationssäkerhetsanalys i syfte att identifiera och vidta relevanta åtgärder som säkerställer kontinuiteten.
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem?	SLA finns för omsorgsnämnden och servicenämnden granskade verksamheters kritiska system. SLA finns även för samhällsbyggnadsnämndens verksamhet, men den baseras inte på identifierat skyddsvärde och behov av tillgänglighet för det verksamhetskritiska informationssystemet då aktuell informationssäkerhetsanalys saknas. SLA finns inte för kommunstyrelsens granskade verksamhetskritiska system.	**Kommunstyrelsen:** Säkerställ att SLA finns för verksamhetskritiska system inom den egna verksamheten.

Revisionsfråga	Bedömning: Nej	Rekommendationer
Har övningar genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig?	Övningar har inte genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig. Vi kan dock konstatera att övningar är planerade och bedömer att det är positivt och viktigt i syfte att säkerställa en tillräcklig kontinuitetsplanering för it-avbrott.	**Kommunstyrelsen och samtliga nämnder:** Tillse att övningar genomförs i syfte att säkerställa att kontinuitets-planeringen 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-säkerhets-händelser inträffar?	Det finns inte en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar. Det finns krav i styrande dokument avseende kontinuitetsplanering, men arbetet har för flera verksamheter inte genomförts i tillräcklig utsträckning vilket vare sig kommunstyrelsen eller nämnderna har uppmärksammat.	**Kommunstyrelsen:** Tydliggöra ansvar för uppföljning och kontroll av att kommunens samhällsviktiga verksamheter har en kontinuitetsplanering i enlighet med lagar, regler och interna styrdokument samt dokumentera hur kontrollen ska genomföras. **Kommunstyrelsen och samtliga nämnder:** Följ upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad kommunövergripande systematik.

2 Bakgrund

KPMG har av de förtroendevalda revisorerna i Växjö kommun fått i uppdrag att granska kommunens 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 kommunens verksamheter ska stå väl rustade inför olika former av samhällsstörningar och för att klara av att hantera olika former av krissituationer. Förmåga att hantera it-säkerhetshändelser baseras även på att det finns ett systematiskt informationssäkerhetsarbete där hot och risker analyserats för att säkerhetsåtgärder ska anpassas efter dessa och skydda kommunens information och verksamhet.

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 av it- och informationssystem leder till att ett bortfall av dessa kritiska tillgångar får större konsekvenser än tidigare. I det arbetet krävs väl genomarbetade, förankrade och testade kontinuitetsplaner för att upprätthålla verksamheterna vid sådana händelser.

Revisorerna 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 it-säkerhetshändelser är icke-försumbar och att arbetet med kontinuitetsplanering och reservrutiner behöver granskas.

2.1 Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om kommunstyrelsen 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

Granskningen har inte tagit del av underlag eller information som är säkerhetsskyddsklassade.

Granskningen avgränsas till kommunstyrelsen, omsorgsnämnden, servicenämnden och samhällsbyggnadsnämnden.

- Granskningen av kommunstyrelsen har omfattat dels övergripande styrning och uppföljning, dels verksamhet inom ekonomifunktionen.
- Granskningen av omsorgsnämnden har omfattat verksamheterna inom ordinärt boende samt kommunal hälso- och sjukvård med tillhörande informationsöverföring med regionen.
- Granskningen av servicenämnden avser måltidsverksamheten och i tillämpliga delar även it.
- Granskningen av samhällsbyggnadsnämnden avser verksamheten inom vatten och avlopp.

För samtliga revisionsobjekt avgränsas stickprov av kontinuitetsplanering att omfatta kritiska processer med stort beroende av informationssystem.

2.3 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

- Kommunallagen (2017:725)
- Aktiebolagslagen
- 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 och tillhörande rutiner för berörda verksamheter
- SLA:er (servicenivåöverenskommelser för informationssystem)

Intervjuer

Intervjuer har genomförts med:

- Presidier i berörda nämnder och styrelse
- Kommundirektör
- Ekonomidirektör
- It-chef
- Informationssäkerhetssamordnare
- Säkerhetschef

- Förvaltningschefer inom berörda nämnder och styrelse
- Säkerhetshetssamordnare inom berörda nämnder och styrelse
- Verksamhetschefer inom måltidsverksamheten, ordinärt boende, hälso- och sjukvården och VA.

Stickprov

Stickprov har gjorts av upprättade kontinuitetsplaner inom berörda revisionsobjekt och mot bakgrund av given avgränsning.

Samtliga intervjupersoner har givits möjlighet att faktakontrollera rapporten.

3 Regelverk för kontinuitetsplanering

Kommunens ansvar för krisberedskap och civilt försvar regleras i Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH) med tillhörande förordning och föreskrifter från MSB.

Kommunen har ansvar att upprätthålla samhällsviktig verksamhet och ha förmåga att hantera störningar och krishändelser inom dessa. Myndigheten för samhällsskydd och beredskap, MSB, har definierat samhällsviktiga verksamheter som ”*Verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet*”.

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 att informationssystem och it-miljön inte är tillgänglig för de samhällsviktiga verksamheterna avgränsas denna granskning till kontinuitetsplanering och reservrutiner vid it-bortfall.

4 Resultat av granskningen

4.1 Process för riskbedömning och planering för it-avbrott

I *Policy för säkerhet och beredskap*[1] uttrycks målsättningen att Växjö kommun ska kunna motstå och hantera allvarliga störningar. *Koncernövergripande krishanteringsplan*[2] beskriver hur kommunen ska hantera en extraordinär händelse. Det framgår dock att planen även kan utgöra stöd vid allvarlig händelse som utsätter kommunens organisation, eller delar av den, för stor påfrestning.

Enligt policyn ansvarar nämnderna, genom förvaltningscheferna, för att säkerhets- och beredskapsarbetet inom eget verksamhetsområde bedrivs i enlighet med lagar, förordningar, policy och instruktioner. Nämnderna ska enligt policyn fastställa verksamhetsspecifika rutiner och instruktioner.

Vi har i granskningen tagit del av kommunens *Risk- och sårbarhetsanalys (RSA) 2023* (version som är publik och inte innehåller sekretessbelagda delar). Risk- och sårbarhetsarbetet uppges enligt dokumentet vara en viktig grund för arbetet med skydd av samhällsviktig verksamhet samt för ett systematiskt säkerhetsarbete.

I riskmatrisen för Växjö kommun inkluderas ***”risk för it-bortfall i en vecka”*.**

Det är således denna risk som nämnder och förvaltningar behöver inkludera i sin kontinuitetshantering. Riskvärdet har bedömts till 3 (förekommande intervall 5-20 år) med bedömd konsekvens 4 (förödande samhällsstörning). Detta leder till den sammantagna bedömningen hög risk (orange).

Av RSA 2023 framgår vidare att kommunens samhällsviktiga verksamhet vid tiden för upprättande av RSA kartlagts och arbetet med kontinuitetshantering för dessa var pågående. I intervjuerna i denna granskning beskrivs delvis att arbetet sedan 2023 har skett enligt en angiven struktur där det finns olika steg från risk- och sårbarhetsanalysen ned till kontinuitetsplanering.

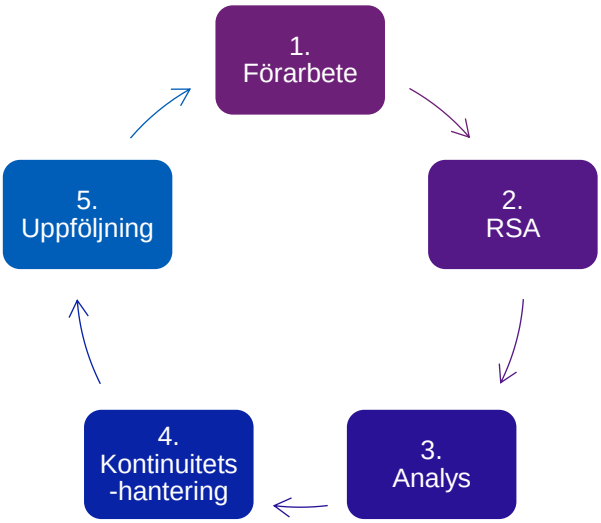
Detta arbete är i kommunen tänkt att ske långt ut i verksamheterna som berörs, där samtliga förvaltningar har en egen säkerhetssamordnare som leder arbetet och utgör förvaltningarnas språkrör i det kommunövergripande säkerhetssamordnarforumet som leds av kommunens övergripande säkerhetssamordnare. I de olika stegen finns kommungemensamma mallar och beskrivningar över hur arbetet bör gå till. Vissa verksamheter, exempelvis omsorgsförvaltningen har arbetat enligt denna struktur, om än delvis med stöd av egna strukturer och rutiner utifrån den egna verksamhetens särskilda behov. Vi kan dock konstatera utifrån de underlag vi tilldelats och de uppgifter som har lämnats vid intervju att verksamheterna i olika utsträckning arbetar enligt angivna kommungemensamma mallar och strukturer. Detta medför i sin tur att verksamheterna har kommit olika långt i att planera för den i RSA identifierade risken ”***risk för it-bortfall i en vecka”,*** för närmare beskrivning se stickprovsresultat.

[1] Kommunfullmäktige 2017-06-13 § 132
[2] Kommunstyrelsen 2024-01-09 § 16

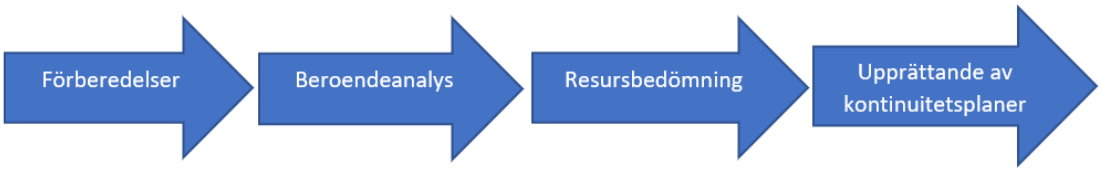
4.1.1 Kontinuitetsplaner och kritiska beroenden till informationssystem

I RSA 2023 finns processen för RSA-arbetet beskriven av vilken det framgår att kontinuitetshantering är en del.

Förvaltningarna ska enligt beskrivning i dokumentet analysera hur den egna verksamheten påverkas av de händelser som inkluderats i den övergripande RSA:n. Efter genomförda analyser ska de sedan ta fram åtgärder för att minska påverkan samt kontinuitetshantera de samhällsviktiga verksamheterna.



I RSA-dokumentet finns även nedan process för kontinuitetshantering. Av den framgår att dokumenterade kontinuitetsplaner är sista steget i processen.



I granskningen har ingått att göra stickprov av dokumenterade kontinuitetsplaner för att kontrollera om kritiska beroenden till informationssystem har ingått i analys och planering.

Resultat av stickproven presenteras i tabellen nedan.

Ansvarig nämnd	Verksamhet	Kontinuitets-plan finns	Risk för it-avbrott har inkluderats	Kritiska informations-system är identifierade
Kommunstyrelsen	Ekonomiavdelningen	Ja	Ja	Ja
Servicenämnden	Måltidsverksamheten	Ja	Ja	Ja
Omsorgsnämnden	Hemtjänst	Ja	Ja	Ja
	Kommunal hälso- och sjukvård	Ja	Ja	Ja
Samhällsbyggnads-nämnden	VA-verksamheten	Ja	Nej	Nej

Kommentar till resultat av stickprov

Samtliga verksamheter som ingår i granskningen har kunnat uppvisa kontinuitetsplaner eller motsvarande planer. Det förekommer dock en del olika begrepp i hur dessa benämns i de olika verksamheterna, men i en bredare tolkning av begreppet som inkluderar planering för händelser kan vi konstatera att detta finns i samtliga verksamheter. Utformningen och aktualiteten av kontinuitetsplanerna skiljer sig också åt. Omsorgsförvaltningen har en uppdaterad kontinuitetsplan som aktualiserats innevarande mandatperiod, vilket innebär att bedömningar utgår från nuvarande risk- och sårbarhetsanalys och risken för it-bortfall i en vecka. Andra verksamheter har kontinuitetsplanering som inkluderar risken för it-avbrott men där planerna inte fullt ut är färdigställda och uppdaterade för innevarande mandatperiod (servicenämnden och kommunstyrelsens verksamheter). VA-verksamheten har inte inkluderat risken för it-avbrott och den kontinuitetsplanering som är gjord är inte aktualiserad i närtid.

Samtliga verksamheter uppger dock i intervjuer att ett arbete med uppdatering, aktualisering eller utveckling av kontinuitetsplaneringen är pågående.

Samtliga verksamheter utom VA-verksamheten har i sin dokumenterade planering identifierat vilka informationssystem som är kritiska för verksamheten. Denna bild bekräftas också vid intervjuer där samtliga funktioner som arbetat med kontinuitetsplanering inom respektive verksamhet och inkluderat risk för it-avbrott vet vilka system som är särskilt kritiska och varför. Även VA-verksamheten har vid intervju bekräftat att man vet vilket system som är kritiskt, men det är inte dokumenterat i kontinuitetsplaneringen.

I avsnitt 4.2 fördjupas iakttagelser om åtgärder och planering för de kritiska beroenden till informationssystem som har gjorts i kontinuitetsplaneringen.

4.1.2 Övning

Det har enligt de intervjuade inte skett någon övning med specifikt fokus på it-avbrott i kommunen. Kommunledningsförvaltningens chef har dock gett säkerhetschef och it-chef i uppdrag att tillse att en sådan övning ska genomföras för kommunledningsförvaltningen ledningsgrupp. Därtill planeras en motsvarande skrivbordsövning med omsorgsförvaltningen genomföras under maj månad 2024.

4.1.3 Bedömning

Vår bedömning är att det finns dokumenterade kontinuitetsplaner eller motsvarande underlag i samtliga granskade verksamheter.

Kontinuitetshantering beskrivs i kommunens Risk- och sårbarhetsanalys (RSA) där det framgår att det ska upprättas kontinuitetsplaner för de risker som fastställts i analysen. Vi kan dock konstatera att arbetet kommit olika långt och att det i viss utsträckning inte sker på samma sätt i enlighet med kommungemensamma processbeskrivningar och mallar. Vi kan därigenom även konstatera att det varierar i om risken för it-bortfall i en vecka har inkluderats i kontinuitetsplaneringen. Det finns ett värde i att säkerställa att arbetet i så stor utsträckning som möjligt sker enligt gemensam systematik och enligt kravställd nivå för att skapa en förutsägbarhet, följsamhet och fungerande intern samverkan i kommunen för kritiska beroenden med påverkan över förvaltningsgränserna.

Vår bedömning är att kritiska beroenden till informationssystem har beaktats i kontinuitetsplaneringen för kommunstyrelsen, servicenämnden och omsorgsnämndens verksamheter. Vår bedömning är att kritiska beroenden till informationssystem inte har beaktats i kontinuitetsplaneringen för samhällsbyggnadsnämndens VA-verksamhet.

Vår bedömning är att övningar inte har genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

Vi kan dock konstatera att övningar är planerade och bedömer att det är positivt och viktigt i syfte att säkerställa en tillräcklig kontinuitetsplanering för it-avbrott.

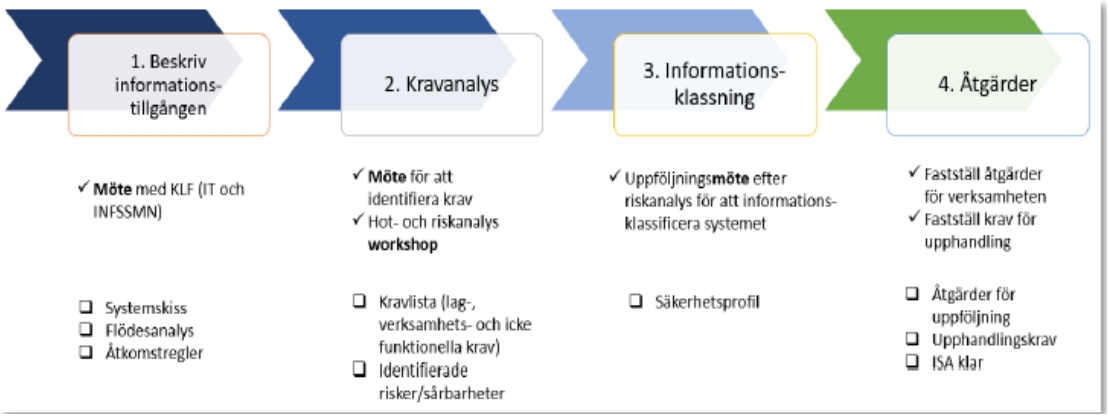
4.2 Tillgänglighet till informationssystem och redundans

Enligt ISO27001[3] innebär aspekten tillgänglighet ”*möjlighet att utnyttja tillgångar efter behov i förväntad utsträckning inom önskad tid*”. Med andra ord hur stort behovet av tillgänglighet till information och system är, utan att det ska uppstå alltför stora konsekvenser. Denna bedömning är i sin tur vägledande för vilka reservrutiner och lösningar som behöver finnas för att verksamhetens kontinuitet ska upprätthållas, vilket kallas redundans. Redundans kan ske genom exempelvis digitala kopior som speglar information i systemen eller rutiner för att utföra processer och verksamhet utan tillgång till systemen och informationen som hanteras i dessa. Det kan exempelvis vara manuella arbetssätt, utskrivna listor/externa lagringsmedier där information om tidigare utförda insatser, beställningar osv. har lagrats. Det kan även vara krispärmar och andra beskrivningar som stöd för verksamheterna i händelse av it-störning eller avbrott.

4.2.1 Analys och bedömningar av skyddsbehov och krav på tillgänglighet

I *Informationssäkerhet instruktion förvaltning och bolag*[4] beskrivs informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet. I instruktionen framgår att verksamhetskrav rörande tillgänglighet för informationssystem ska identifieras. Detta uppges ingå i ordinarie process för informationssäkerhetsanalys, vilket det finns en upprättad rutin för.

Vi har i granskningen tagit del av rutinen [5] av vilken det framgår att processen ser ut som följer:



Denna process ska genomföras årligen för systemen som en del av det systematiska informationssäkerhetsarbetet, alternativt ska ny informationssäkerhetsanalys upprättas i samband med betydande förändringar i systemet. Verksamhetens behov ska vara i centrum för analysen, och representanter från verksamheten förväntas driva arbetet i samråd med centrala it- och informationssäkerhetsfunktioner. Bland verksamhetens centrala funktioner i arbetet finns analysledare som leder arbetet med informationssäkerhetsanalysen, systemägare som initierar analysen och säkerställer

[3] ISO27001 är en etablerad standard för ledningssystem för informationssäkerhet som beskriver hur ett systematiskt informationssäkerhetsarbete bör genomföras för att skydda verksamhetens information.
[4] Säkerhets- och beredskapsavdelningen, senaste revidering 2023-09-01.
[5] Instruktion för genomförande av informationssäkerhetsanalys

att lagstiftning inom området följs, att användarna har rätt kompetens och att systemet ger avsedd nytta i verksamheten.

Som ett sista led i arbetet med informationssäkerhetsanalysen ingår att fastställa åtgärder för verksamheten men också direkt kopplat till informationssystemen i form av krav för upphandling av leverantör.

Vi har mot bakgrund av de bedömningar som gjorts i verksamheternas analyser och kontinuitetshantering efterfrågat om informationssäkerhetsanalyser för de system som identifierats som kritiska för att upprätthålla verksamheterna genomförts.

I intervjuer har vi fått beskrivet för oss att det inom it-avdelningen (organiserad under servicenämnden) sker ett arbete med informationssäkerhetsanalys (ISA) och framtagande av så kallade SLA (Service Level Agreement) som baseras på resultat i analysen. Arbetet med ISA sker tillsammans med berörd verksamhet och it-chef uppger i intervju att ISA och SLA ska finnas för samtliga system.

Vi har i samband med intervjuer med verksamheten efterfrågat om ISA och SLA finns för de system som bedömts som verksamhetskritiska. Svaren sammanställs i tabellen nedan.

Ansvarig nämnd	Verksamhet och antal verksamhetskritiska system	Informations-säkerhetsanalys finns och är aktuell	Åtgärder har vidtagits utifrån analys	Aktuell SLA finns
Kommunstyrelsen	Ekonomiavdelningen 2 system	Nej	Nej	Nej
Servicenämnden	Måltidsverksamheten 2 system	Ja	Ja	Ja
Omsorgsnämnden	Hemtjänst 4 system[6]	Ja	Ja	Ja
	Kommunal hälso- och sjukvård 4 system[7]	Ja	Ja	Ja
Samhällsbyggnads-nämnden	VA-verksamheten 1 system	Nej	Nej	Ja

[6] Ett av systemen ägs av regionen, där kommunen är användare. I dessa fall har vi tittat på att ändamålsenliga beredskapsrutiner för hantering av den information som kommunen har i systemet finns. Se 4.2.2.1
[7] Se ovan fotnot.

Kommentar till granskning av systemdokumentation

Då alltför detaljerade uppgifter om system tillsammans med bedömningar av risker och sårbarheter kan utsätta kommunen för risk väljer vi att i rapporten endast redogöra för iakttagelser på en övergripande nivå.

För ekonomiavdelningens system finns enligt intervjuer idag inte informationssäkerhetsanalyser och tillhörande SLA. För ekonomiavdelningens två system ska detta ske i närtid då nya system behöver upphandlas under året och informationssäkerhetsanalys är ett internt krav i upphandlingsprocessen.

Vad avser VA-verksamhetens system uppges att ett arbete med informationssäkerhetsanalys har skett vid ett tidigare tillfälle för aktuellt system. Denna process ska dock ske årligen, och en uppdatering har inte skett på flertalet år enligt uppgift. Däremot har en SLA framtagits för det verksamhetskritiska systemet tillsammans med kommunens it-avdelning och gentemot leverantören av systemet.

I intervjuer har det framkommit att det finns en intern prioriteringslista på it-avdelningen mellan olika system, i händelse av ett större avbrott/störning som påverkar flera system i kommunen samtidigt. Denna prioritering baseras på resultatet av ISA och SLA. Även de system som det inte finns aktuell ISA eller SLA för finns prioriterade i denna lista, men prioriteringen baseras då mer på en generell bedömning av systemets betydelse även om den inte är fastställd genom de processer som ska leda fram till dessa bedömningar, det vill säga ISA och SLA.

4.2.2 Reservrutiner

Avseende reservrutiner finns det rutiner som är kopplade till de krav som kommunens verksamheter ställt mot externa leverantörer eller interna it-avdelningen på exempelvis underhåll, beredskap och svarstid på incidenter. Med extern leverantör är detta ett formellt avtal, kallat SLA. För de system som it-avdelningen hanterar internt i kommunen är dessa avtal liknande utformade men inte formellt påskrivna avtal. De krav som finns i SLA eller motsvarande är en del av att säkerställa kontinuiteten. Av tabellen framgår vilka verksamheter som, enligt intervjuuppgift med verksamhetsrepresentanter, har aktuella SLA.

En annan del i att säkerställa verksamhetens kontinuitet är de delar som rör verksamhetens planering för att upprätthålla sin verksamhet vid ett it-avbrott. Detta kan vara exempelvis manuella instruktioner eller rutiner som medarbetare ska utgå från vid bortfall av kritiska system eller funktioner i system. Det kan också vara genom olika tekniska reservåtgärder i verksamheten, exempelvis att ha redundans med parallella system, tillgång till externa nätverk mm. För samtliga verksamheter har vi kunnat identifiera att vissa rutiner finns för de verksamhetskritiska systemen. Verksamheterna har dock kommit olika långt i detaljnivån av planeringen för att upprätthålla verksamheten och vi kan även genom dokumentgranskning konstatera att rutinerna i vissa fall endast är avsedda att fungera vid relativt kort tid av bortfall. Som framgår av tabellen avseende stickprov så har arbetet inom servicenämnden och omsorgsnämnden kommit längre medan VA-verksamheten och ekonomikontorets arbete med rutiner och åtgärder är pågående. Vi kan dock genom dokumentgranskning konstatera att vissa rutiner finns för samtliga system som ingått i granskningen.

En annan övergripande iakttagelse i granskningen är att reservrutinerna är olika utformade och att det används olika begrepp för att beskriva planerna/rutinerna. Detta kan bero på flera olika saker, en orsak som har lyfts fram i intervjuer är att det delvis råder en begreppsförvirring kring vad som är en kontinuitetsplan, vad den innehåller, hur en kontinuitetsplan skiljer från en krisplan eller annan form av rutin. En annan orsak beskrivs vara att verksamheterna i olika utsträckning har arbetat i enlighet med de metodstöd och den process som finns för exempelvis informationssäkerhetsanalyser och processen för risk- och sårbarhetsanalys och efterföljande kontinuitetsplanering.

4.2.2.1 Digital informationsöverföring med externa parter

Omsorgsnämndens verksamheter har på olika sätt kritiska beroenden kopplat till regionen. Samtliga dessa informationssystem ägs och förvaltas av regionen som därigenom har ansvar för säkerhet och åtgärder för systemet även om de till viss del används även av kommunen. För systemen har dock kommunen ansvar för den egna informationen i systemet, men inte själva systemet i sig. I händelse av avbrott krävs följaktligen en samverkan och dialog mellan parterna. För aktuellt system har kommunen driftsstoppsrutiner för att kunna hantera situationen i sina egna verksamheter. I intervjuer beskrivs att det finns en god samverkan med regionen kring dessa frågor. I samband med ett avbrott i närtid fick samverkan och rutiner testas i skarpt läge vilket upplevs ha fungerat väl utifrån upparbetade kontaktvägar med regionen och befintliga rutiner i verksamheten.

4.2.3 Bedömning

Vår bedömning är att åtgärder har identifierats och vidtagits för att säkerställa kontinuiteten inom servicenämndens och omsorgsnämndens granskade verksamheter. Vi bedömer att åtgärder delvis finns identifierats inom kommunstyrelsens och samhällsbyggnadsnämndens verksamheter.

Vi baserar vår bedömning på att det inom servicenämnden och omsorgsnämndens verksamheter har identifierats och vidtagits åtgärder kopplat till informationssystemen i enlighet med den process som finns reglerad i styrdokument i kommunen för informationssäkerhetsanalys. Därtill har båda nämndernas vidtagit åtgärder i verksamhetens rutiner för att säkerställa kontinuiteten, också i enlighet med vad kommunens process för informationssäkerhetsanalys anger. Vi bedömer också att riskerna kopplat till digital informationsöverföring med regionen i gemensamma system beaktas inom ramen för omsorgsnämndens riskarbete och driftstoppsrutiner.

Inom samhällsbyggnadsnämndens och kommunstyrelsens granskade verksamheter och tillhörande system ser vi inte att det finns åtgärder vidtagna baserade på identifierade åtgärdsbehov för informationssystemen i enlighet med kommunens process för informationssäkerhetsanalys. Då åtgärder inte finns identifierade enligt denna process kan vi inte heller se att vidtagna åtgärder i verksamhetens kontinuitet baseras på ett strukturerat arbete med ISA. Vi gör dock bedömningen delvis baserat på att olika åtgärder trots detta har vidtagits för att säkerställa kontinuiteten i verksamheten i form av dokumenterade rutiner för hur stopp/avbrott i systemen ska hanteras i verksamheterna. Det är positivt att dessa rutiner finns framtagna men vi bedömer att arbetet bör systematiseras i enlighet med kommunens process för

informationssäkerhetsanalys för att på ett systematiskt sätt identifiera relevanta åtgärder både kopplat till åtgärder för beredskapen för informationssystemen och åtgärder i verksamheten.

Vår bedömning är att det finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem inom servicenämndens och omsorgsnämndens granskade verksamheter. Vår bedömning är att det finns avtalade servicenivåer och beredskap inom samhällsbyggnadsnämndens verksamhet, men vi bedömer att det bara delvis baseras på identifierat skyddsvärde och behov av tillgänglighet då aktuell informationssäkerhetsanalys saknas. Vi bedömer att avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem saknas inom kommunstyrelsen granskade verksamhet.

4.3 Intern kontroll

4.3.1 Kommunstyrelsens och nämndernas kontroll avseende kontinuitetsplaneringen

I granskningen har det framkommit att det idag inte finns någon strukturerad, formell eller på annat sätt systematisk politisk uppföljning av kontinuitetsplaneringen i kommunen. Den rapportering som skett har varit genom informationsärenden eller kopplat till budgetpåverkande åtgärder.

Olika förklaringar har framkommit till varför uppföljningen av kontinuitetsplaneringen i kommunen brister. Det har bland annat framförts att det saknas tydliga politiska uppdrag och kravställning att följa upp utifrån, att det saknas ett fungerande systemstöd för uppföljning generellt i kommunen, att kontinuitetsplanering inte har inkluderats i ordinarie ledningssystem fullt ut och att det i viss mån förefaller otydligt var ansvaret för politisk uppföljning är placerat både vad gäller kommunstyrelsen och nämnderna.

Vid genomgång av reglemente för kommunstyrelsen noterar vi att detta inte innehåller beskrivning av ansvar för säkerhets- eller beredskapsfrågor utöver säkerhetsskyddslagen. Policy för säkerhet och beredskap reglerar inte ansvar för uppföljning och kontroll av arbetet. Dock framgår att kommunstyrelsen har ansvar för samordning av säkerhets- och beredskapsarbetet och som vi skrivit inledningsvis i rapporten, att nämnderna, genom förvaltningscheferna, ansvarar för att säkerhets- och beredskapsarbetet inom eget verksamhetsområde bedrivs i enlighet med lagar, förordningar, policy och instruktioner. Från centrala säkerhetsfunktioner bekräftas att det är nämndernas uppdrag att följa upp de egna verksamheterna enligt ordinarie ansvarsprinciper.

I intervjuer har det framkommit att uppföljning sker i begränsad utsträckning och att det saknas en samlad uppföljning av kontinuitetsarbetet från centralt håll i kommunen, vilket innebär att det saknas en kontroll över att kontinuitetsplaneringen sker enligt avsedd struktur och på en tillräcklig nivå.

I granskningen har vi dock kunnat se olika spår för uppföljning på tjänstemannanivå. Exempelvis bedrivs inom kommunledningsförvaltningen ett arbete med uppföljning för servicenämndens och kommunstyrelsens verksamheter genom Stratsys där det finns ett beslutat uppdrag från förvaltningschef på kommunledningsförvaltningen kopplat till uppföljning av kontinuitetsplaneringen. Frågan har också varit uppe i koncernledningen där respektive förvaltningschef har fått beskriva nuläge i arbetet.

Det finns därtill ett pågående uppdrag från kommundirektör till den centrala säkerhetsfunktionen att identifiera kritiska processer för kontinuitetsplaneringen som faller under flera förvaltningar eller bolag samt att bistå i samordningen i dessa kritiska beroenden.

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 bedömer att ansvar för säkerhetsfrågor inte är tillräckligt tydliggjort i reglementen och konstaterar att policyns reglering att nämnderna har ansvar att tillse att lagar, förordningar och interna styrdokument för krisberedskap efterlevs inte har kontrollerats av vare sig kommunstyrelsen eller nämnderna.

Vi konstaterar därtill att det finns krav i styrande dokument avseende samtliga verksamheters kontinuitetsplanering, till exempel kopplat till strukturen för informationssäkerhetsanalys och tillhörande åtgärder. Vi kan samtidigt konstatera att arbetet på flera håll inte har genomförts i tillräcklig utsträckning, vilket varken kommunstyrelsen eller nämnderna har uppmärksammat genom intern kontroll eller annan uppföljning.

Vi ser därför att uppföljningen är i behov av att stärkas avseende efterlevnad av styrande dokument samt för att säkerställa att kommunens 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 kommunstyrelsen och nämnderna har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

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

Vår samlade bedömning utifrån granskningens syfte är att servicenämnden och omsorgsnämnden i allt väsentligt har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser

Vår bedömning baseras på att vi i granskningen har tagit del av styrdokument, rutiner och processer som beskriver hur arbetet med kontinuitetsplanering är tänkt att bedrivas i kommunen. Vi kan i vissa verksamheter se att arbetet bedrivs i linje med detta, men kan också konstatera att det finns tydliga skillnader i hur långt de olika samhällsviktiga verksamheterna har kommit i sin kontinuitetsplanering för it-avbrott och i vilken utsträckning man arbetar enligt tänkta strukturer för att identifiera och vidta relevanta åtgärder.

Det saknas idag en tillräcklig kontroll och uppföljning av de verksamheter som inte bedriver ett arbete enligt den struktur som beskrivs i styrdokument och den kravnivå för planering inför it-avbrott som fastställs i risk- och sårbarhetsanalys.

Vi bedömer att det är väsentligt att det finns en tydlig ansvarsfördelning mellan nämnder och styrelsen vad gäller uppföljning av att koninuitetsarbetet i berörda verksamheter sker i enlighet med de krav som fastställts i styrdokument.

Utifrån resultatet av vår granskning rekommenderar vi **kommunstyrelsen** att:

- Tydliggöra ansvar för uppföljning och kontroll av att kommunens samhällsviktiga verksamheter har en kontinuitetsplanering i enlighet med lagar, regler och interna styrdokument samt dokumentera hur kontrollen ska genomföras.
- Tillse att den egna verksamheten följer kommunens process för informationssäkerhetsanalys i syfte att identifiera och vidta relevanta åtgärder som säkerställer kontinuiteten.
- Säkerställ att SLA finns för verksamhetskritiska system inom den egna verksamheten.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Följ upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt beslutad kommunövergripande systematik.

Utifrån resultatet av vår granskning rekommenderar vi **samhällsbyggnadsnämnden** att:

- Säkerställ att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Tillse att den egna verksamheten följer kommunens process för informationssäkerhetsanalys i syfte att identifiera och vidta relevanta åtgärder som säkerställer kontinuiteten.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Följ upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad kommunövergripande systematik.

Utifrån resultatet av vår granskning rekommenderar vi **omsorgsnämnden** att:

- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Följ upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad kommunövergripande systematik.

Utifrån resultatet av vår granskning rekommenderar vi **servicenämnden** att:

- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Följ upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad kommunövergripande systematik.

Datum som ovan

KPMG AB

Jenny Thörn

Verksamhetsrevisor

Simon Homander

Verksamhetsrevisor

Alfred Tilly

Verksamhetsrevisor