A decorative graphic on the left side of the page consists of a large blue triangle pointing right, and a cluster of smaller triangles in shades of grey, green, and blue, some pointing right and some pointing left, creating a sense of movement and depth.

Granskning av kontinuitetshantering i händelse av it-avbrott

Rapport

Solna stad

2025-12-11

Antal sidor 15

INNEHÅLLSFÖRTECKNING

1	Sammanfattning	3
2	Bakgrund	6
2.1	<i>Syfte, revisionsfrågor och avgränsning</i>	6
2.1.1	Avgränsning	7
2.2	<i>Revisionskriterier</i>	7
2.3	<i>Metod</i>	7
3	Resultat av granskningen	9
3.1	<i>Krav på arbetet med kontinuitetshandling</i>	9
3.1.1	Bedömning	10
3.2	<i>Arbetet med kontinuitetshandling</i>	10
3.2.1	Stöd och samordning av arbetet	10
3.2.2	Metod och genomförande av kontinuitetshandling	11
3.2.3	IT-kontinuitetsplaner	11
3.2.4	Åtgärder och reservrutiner	12
3.2.5	Bedömning	12
3.3	<i>Övning för att utvärdera kontinuitetsplaneringen</i>	13
3.3.1	Bedömning	14
3.4	<i>Uppföljning</i>	14
3.4.1	Bedömning	14
4	Samlad bedömning och rekommendationer	15

1 SAMMANFATTNING

Azets Revision & Rådgivning har av Solna stads förtroendevalda revisorer fått i uppdrag att granska stadens beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa som leder till it-avbrott. Uppdraget ingår i revisionsplanen för år 2025. Granskningen har även genomförts hos de kommunala bolagen Solna Vatten AB, Norrenergi AB och stiftelsen Signalisten. Resultatet för dessa presenteras i separata rapporter.

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


Vår samlade bedömning utifrån granskningens syfte är att såväl kommunstyrelsen som omvårdnadsnämnden endast delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Bakgrunden till vår samlade bedömning är att granskningen visat att det finns en styrning genom Säkerhetspolicy och Handlingsplan för krisberedskap. Dessa ställer krav på verksamheternas genomförande av kontinuitetshandling. Arbetet är dock i en uppstartsfas och genomförandet, enligt fastställd modell, är inte slutfört vilket innebär att dokumenterade och implementerade kontinuitetsplaner saknas i hög grad. Däremot finns dokumenterade IT-kontinuitetsplaner för samtliga verksamhetskritiska system som nyttjas inom kommunstyrelsen och omvårdnadsnämndens verksamheter. IT-kontinuitetsplanerna innehåller väsentliga delar för backup och redundans som kan utgöra underlag i verksamheternas kontinuitetsplaner. Vi bedömer dock att planerna i nuläget främst är tillämpliga som stöd för IT-verksamheten. Planering för att säkerställa att verksamheterna kan fungera på en acceptabel nivå vid kritiska it-säkerhetshändelser saknas dock då arbetet med den sortens planering inte är slutfört.

Till det visar granskningen att det inte har genomförts övningar för att utvärdera att nuvarande planer och rutiner är tillräckliga vid kriser eller händelser som en följd av att kontinuitetsplanerna ännu inte är färdigställda. Utöver det har det inte genomförts någon strukturerat uppföljning i enlighet med de krav som ställs i säkerhetspolicy och handlingsplan. Det innebär att kommunstyrelsen och omvårdnadsnämnden inte säkerställt att de har insyn i nuläget vad gäller stadens förmåga att hantera kriser och händelser. Kommunstyrelsen har inte gett något uppdrag eller riktlinje kring hur rapportering av krisberedskapsarbetet ska göras, vilket i sin tur lett till att varken nämnder, bolag eller stiftelser har återkopplat detta i enlighet med krav som kommunfullmäktige fastställt om årlig rapportering till kommunstyrelsen.

Uppföljningsrutiner uppges dock vara planerade att införas innan årsskiftet 2025 där arbetet är initierat av stadsledningsförvaltningen.

I det följande redovisas våra samlade bedömningar av respektive revisionsfråga.

<div style="display: flex; justify-content: space-around; align-items: center;"> Nej Endast delvis I allt väsentligt Ja </div> 	
Revisionsfråga	Bedömning
Finns tydliggjorda krav avseende kontinuitetshantering och hur arbetet ska genomföras?	Endast delvis
Finns dokumenterade kontinuitetsplaner eller motsvarande underlag som beskriver hantering om it-avbrott skulle inträffa?	Endast delvis
Har de samhällsviktiga verksamheterna analyserat sina kritiska beroenden till informationssystem och identifierat behov av åtgärder för att hantera it-avbrott?	I allt väsentligt
Har åtgärder vidtagits som stärkt förmågan att upprätthålla verksamheten på en tolererbar nivå i händelse av it-avbrott (exempelvis reservrutiner, analoga arbetssätt eller redundanta lösningar)?	Endast delvis
Har övningar genomförts för att utvärdera kontinuitetsplaner och tillhörande rutiner?	Nej
Finns en etablerad uppföljning och kontroll av arbetet med kontinuitetshantering?	Nej

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen i deras övergripande ansvar för ledning och samordning av krisberedskapsarbetet att:

- Tillse att reglementen för kommunstyrelsen och nämnderna revideras i syfte att tydliggöra ansvarsfördelning för krisberedskap.
- Besluta om styrande dokument inom krisberedskap och kontinuitetshantering som konkretiserar kommunfullmäktiges viljeriktning i handlingsplanen för krisberedskap.
- Utvärdera om nuvarande organisation och resurser för genomförande av kontinuitetshantering är tillräcklig så att det finns förutsättningar att nå upp till kommunfullmäktiges förväntningar i handlingsplan för krisberedskap.
- Besluta om rutin och uppdrag för årlig uppföljning av arbetet med krisberedskap i enlighet med reglering i säkerhetspolicy och handlingsplan för krisberedskap.

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen och omvårdnadsnämnden att inom sina respektive ansvarsområden:

- Tillse att arbetet med kontinuitetsplaner slutförs och fastställs för att sedan implementeras inom respektive verksamhet.
- Tillse att identifierade åtgärder vidtas som syftar till att stärka redundans och kontinuitet för verksamheterna.
- Genom övning utvärdera kontinuitetshandlingen och tillhörande rutiner.
- Tillse att arbetet löpande följs upp och rapporteras till kommunstyrelsen i enlighet med reglering i säkerhetspolicy och handlingsplan för krisberedskap.

2 BAKGRUND

Azets Revision & Rådgivning har av Solna stads förtroendevalda revisorer och lekmannarevisorer fått i uppdrag att granska stadens och bolagens beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetskändelser skulle inträffa som leder till it-avbrott. Uppdraget ingår i revisionsplanen för år 2025.

En god krisberedskap är en förutsättning för att verksamheterna ska stå väl rustade inför olika former av samhällsstörningar och för att klara av att hantera olika former av krissituationer. En väsentlig del i arbetet är kontinuitetshandling för kritiska processer utifrån olika kriser som kommunen kan drabbas av.

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.

Under 2026 förväntas två nya lagar träda i kraft i Sverige:

Lag om motståndskraft hos kritiska verksamhetsutövare

Med utgångspunkt från CER¹-direktivet beslutat av EU. Direktivet ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet.

Cybersäkerhetslagen

Med utgångspunkt från NIS²-direktivet beslutat av EU. Direktivet syftar till att uppnå en hög gemensam cybersäkerhetsnivå i hela unionen. Jämfört med nuvarande NIS-reglering kommer tydligare krav ställas på bland annat riskanalyser och olika säkerhetsåtgärder.

Ett flertal offentliga organisationer har under de senaste åren utsatts för cyberattacker med stora konsekvenser som följd. Exempelvis har skyddsvärd information förlorats, verksamhetsprocesser stoppats eller så har den bristande säkerheten och beredskapen lett till att organisationer drabbats av ekonomisk skada eller förtroendeskada. Det ökande beroendet till it- och informationssystem leder till att ett bortfall av dessa kritiska tillgångar får större konsekvenser än tidigare. Kontinuitetshandling är en väsentlig del för att kunna upprätthålla verksamheter på en tolererbar nivå vid sådana händelser.

Revisorerna bedömer att de negativa konsekvenserna vid en extraordinär händelse eller annan kris som betydande om det inte finns ändamålsenlig kontinuitetsplanering. Revisorerna drar därför slutsatsen att arbetet med kontinuitetshandling och rutiner behöver granskas.

2.1 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

Syftet med granskningen har varit att bedöma om kommunstyrelsen och omvårdnadsnämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetskändelser.

Granskningen har omfattat följande revisionsfrågor:

- Finns tydliggjorda krav avseende kontinuitetshandling och hur arbetet ska genomföras?

¹ Directive on the resilience of critical entities

² The Directive on Security of Network and Information Systems

- Finns dokumenterade kontinuitetsplaner eller motsvarande underlag som beskriver hantering om it-avbrott skulle inträffa?
- Har de samhällsviktiga verksamheterna analyserat sina kritiska beroenden till informationssystem och identifierat behov av åtgärder för att hantera it-avbrott?
- Har åtgärder vidtagits som stärkt förmågan att upprätthålla verksamheten på en tolererbar nivå i händelse av it-avbrott (exempelvis reservrutiner, analoga arbetsätt eller redundanta lösningar)?
- Har övningar genomförts för att utvärdera kontinuitetsplaner och tillhörande rutiner?
- Finns en etablerad uppföljning och kontroll av arbetet med kontinuitetshantering?

2.1.1 Avgränsning

Granskningen har avgränsats till att omfatta kommunstyrelsen och omvårdnadsnämnden.

Granskningen avser år 2025.

Granskningen har inte omfattat underlag eller information som är säkerhetsskyddsklassad.

2.2 REVISIONSKRITERIER

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen 6 kap § 6
- Lag om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och beredskap.
- Myndigheten för samhällsskydd och beredskaps vägledning för Risk- och sårbarhetsanalyser, MSB245
- MSBFS 2015:5
- Handlingsplan för krisberedskap 2024–2026
- Reglemente för kommunstyrelsen och omvårdnadsnämnden

2.3 METOD

Granskningen har genomförts genom studium och analys av för granskningen relevanta styrande dokument. De dokument vi tagit del av är Handlingsplan för krisberedskap 2024–2026, reglemente för kommunstyrelsen och omvårdnadsnämnden samt IT-kontinuitetsplaner för granskade verksamhetens system.

Intervjuer har genomförts med representanter från stadsledningsförvaltningen: säkerhetschef, säkerhetssamordnare, ekonomichef och redovisningschef.

Intervjuer har genomförts med representanter från omvårdnadsförvaltningen: tf stabschef, konsult med uppdrag att utveckla säkerhetsarbetet, samordnare och systemspecialist och systemspecialist.

Vidare ingick i granskningens metod att göra en aktgranskning i form av stickprovvis kontroll av dokumenterade kontinuitetsplaner. I dessa skulle en bedömning göras huruvida kritiska beroenden till informationssystem beaktats.

Detta har endast delvis kunnat genomföras då underlag i hög grad saknades vid tid för granskningen vilket framgår under iakttagelse-avsnitten.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.



Samtliga intervjuade har getts möjlighet att sakgranska rapportens innehåll.

3 RESULTAT AV GRANSKNINGEN

3.1 KRAV PÅ ARBETET MED KONTINUITETSHANDLING

Kommunfullmäktige har beslutat om en Säkerhetspolicy³. Policyn reglerar Solna stads inriktning för säkerhetsarbetet. Syftet med säkerhetsarbetet uppges vara att förebygga och begränsa negativa effekter av oönskade händelser som kan drabba de människor som bor, arbetar eller vistas i Solna, stadens egna verksamheter och egendom eller miljön. Säkerhetsarbetet ska även ligga till grund för stadens förberedelser för och förmåga att hantera samhällskriser i fredstid och säkerställa stadens förmåga vid höjd beredskap.

Policyn anger att kommunstyrelsen har det övergripande ansvaret för säkerhetsarbetets ledning, styrning och uppföljning. Respektive nämnd ansvarar för säkerhetsarbetet inom sin verksamhet där krav ställs på att nämnderna genomför risk- och sårbarhetsanalyser och kontinuitetsplanering för sina verksamheter. På stadsövergripande nivå sammanställs dessa av kommunstyrelsen.

Ansvaret för säkerhetsfrågor följer verksamhetsansvaret på alla nivåer i hela staden. En chefsbefattning innebär ett utökat säkerhetsansvar och ansvar för att medarbetarna är informerade om policy och tillhörande styrande dokument och att dessa följs i verksamheten.

Kommunfullmäktige har beslutat om Handlingsplan för krisberedskapsarbetet 2024–2026⁴. Handlingsplanen syftar till att skapa en övergripande strategisk inriktning för stadens arbete med krisberedskap och civilt försvar. Handlingsplanen omfattar alla nämnder, stiftelse- och bolagsstyrelser och ska användas som ett inriktande stöd för mer detaljerad och verksamhetsspecifik planering.

Ett av målen med arbetet som framgår av handlingsplanen är att verksamheterna ska ha en förmåga att förebygga, motstå och hantera kriser så att samhällsviktig verksamhet kan upprätthållas.

Inriktning för perioden uppges vara indelad i fem övergripande områden:

- Stärkt förmåga att hantera samhällsstörningar.
- Ökad förmåga genom övningsverksamhet.
- Utvecklad kontinuitetsplaneringen i samhällsviktiga verksamheter.
- Förbättrad samordning.
- Beredskapsförberedelser.

Handlingsplanen innehåller ett antal uppdrag för perioden 2024–2026 där genomföra kontinuitetsplanering är ett av dessa. Samtliga nämnder, stiftelser och bolag förväntas arbeta förebyggande med kontinuitetsplanering. Arbetet ska utgå från nämndens eller bolagets genomförda risk- och sårbarhetsanalys.

Enligt uppgift så pågår en översyn av styrdokument inom krisberedskap. Ett av de dokument som planeras att ta fram är Anvisning för kontinuitetshandling som förväntas bli klar och beslutad under hösten 2025. I praktiken så finns en vald metod för arbetet som även består av

³ Beslutad 2025-04-28

⁴ Beslutad 2023-12-18 KS/2023:262

en tydlig process och krav för analyser och avvägningar som behöver göras för att upprätta kontinuitetsplaner för de samhällsviktiga verksamheterna.

Kommunstyrelsens reglemente⁵ och omvårdnadsnämndens reglemente⁶ saknar reglering av ansvar för krisberedskapsarbetet i staden. Av den ansvarsfördelning som framgår av Handlingsplan för krisberedskap 2024 - 2026 har kommunstyrelsen ansvar för övergripande styrning, samordning och uppföljning av stadens arbete med krisberedskap och civilt försvar. Varje nämnd, stiftelse och bolagsstyrelse är inom sitt ansvarsområde ansvarig för planering och organisering av krisberedskap och civilt försvar. Det åligger varje nämnd och styrelse att årligen planera och löpande följa upp arbetet.

Kommunstyrelsen, genom Stadsledningsförvaltningen ansvarar för samordningen och framtagande av centrala direktiv och inriktning.

3.1.1 Bedömning

Vår bedömning är att det endast delvis finns tydliggjorda krav avseende kontinuitetshantering och hur arbetet ska genomföras.

Reglementen för kommunstyrelsen och omvårdnadsnämnden saknar reglering av ansvar för krisberedskapsarbetet. Kommunfullmäktige har dock genom beslut om säkerhetspolicy och handlingsplan för krisberedskapsarbetet fastställt ansvarsfördelning samt krav om inriktning och uppdrag till samtliga nämnder och styrelser. I handlingsplanen ingår uppdrag att genomföra kontinuitetshantering.

Det saknas dock tydlighet över vilken omfattning eller inriktning arbetet med kontinuitetshantering ska ha, exempelvis avseende metod samt planeringsförutsättningar för den beredskap som krävs från kommunfullmäktige. Vi bedömer därför att det finns behov av att kommunstyrelsen i sitt övergripande ansvar för krisberedskap och civilt försvar tydliggör styrningen och inriktningen för arbetet.

3.2 ARBETET MED KONTINUITETSHANTERING

3.2.1 Stöd och samordning av arbetet

Som vi nämnt ovan så anger handlingsplanen att stadsledningsförvaltningen ansvarar för samordning och inriktning inom området.

Inom stadsledningsförvaltningen finns enheten för trygghet och säkerhet som är organiserad inom administrativa avdelningen. På enheten arbetar sju personer där en säkerhetssamordnare ansvarar för arbetet med kontinuitetshantering. Samordnaren håller ihop och leder arbetet med kontinuitetsplanering för samtliga verksamheter utom omvårdnadsförvaltningen. I verksamheterna under omvårdnadsnämnden finns en extern konsult som leder och samordnar omvårdnadsförvaltningen och socialförvaltningens krisberedskapsarbete och kontinuitetshantering. Detta har möjliggjorts genom extern finansiering från Socialstyrelsen.

⁵ Beslutat av kommunfullmäktige 2022-12-19 § 239

⁶ Beslutat av kommunfullmäktige 2022-12-19 § 239

Säkerhetssamordnaren inom stadsledningsförvaltningen och konsulten inom omvårdnads- och socialförvaltningen har ett nära samarbete och samverkar kring arbetet med utveckling, exempelvis styrande dokument och mallar mm.

Intervjuade uppger att det finns ett stort engagemang och delaktighet hos både ledning och andra företrädare i verksamheterna i arbetet med kontinuitetshandling. Då säkerhetssamordnaren och konsulten är de som har kunskap om metoden för kontinuitetshandling så utgör det i nuläget en begränsad faktor över hur snabb framdrift arbetet kan ha.

3.2.2 Metod och genomförande av kontinuitetshandling

Staden utgår från metod som Myndigheten för samhällsskydd och beredskap (MSB) erhåller som i sin tur baseras på ISO-standard⁷. Det finns bland annat utbildning, stödmaterial och mallar att tillgå i genomförandet. Säkerhetssamordnaren har genomfört utbildning och är processledare i det arbete som genomförs inom respektive verksamhet.

Under våren uppges fokus ha varit på stadsledningsförvaltningens verksamheter. Då arbetet på omvårdnadsförvaltningen har egen resurs för genomförandet har arbetet enligt uppgift kunnat prioriteras på ett annat sätt och därigenom kommit lite längre än många andra verksamheter. Intervjuade beskriver att nästa steg är utbildningsförvaltningen och sedan tekniska förvaltningen. Det finns vilja att även inkludera bolagen i koncernen men detta har inte kunnat prioriteras ännu med hänvisning till att tiden inte räcker till och att arbetssätt ska kunna sätta sig innan fler inkluderas.

Av intervjuade beskrivs omvårdnadsförvaltningen ha utkast till dokumenterade kontinuitetsplaner som inom kort ska fastställas. I verksamheterna under kommunstyrelsen har endast de inledande analyserna och avvägningarna genomförts men resultatet av dessa har ännu inte dokumenterats i verksamheternas kontinuitetsplaner. Säkerhetssamordnaren som lett arbetet har planerat att följa upp framdriften under hösten samt stödja de som har behov för att komma vidare med arbetet.

Då det saknas fastställda kontinuitetsplaner vid tid för granskningen har ingen aktgranskning kunnat genomföras för att verifiera dess innehåll och omfattning. Muntliga uppgifter bekräftar att planeringen tar sin utgångspunkt i stadens övergripande Risk- och sårbarhetsanalys där risk för it-avbrott är en identifierad risk att planera för. Metoden som sådan inkluderar bedömning av kritiska beroenden inom flera områden, där beroende till digitala informationssystem, telefoni osv. är obligatoriska delar att analysera och bedöma behov av reservrutiner för.

3.2.3 IT-kontinuitetsplaner

Vi har i granskningen tagit del av dokumenterade IT-kontinuitetsplaner. Av planerna framgår att IT-kontinuitetsplanen är ett underlag för beredskap att hantera planerade och oplanerade avbrott i systemet från en teknisk synvinkel.

Arbetet med dessa har inte gjorts enligt MSB:s metod utan är ett krav som ställs i stadens arbete med systemförvaltning. Dessa planer har funnits på plats sedan några år och revideras årligen som del i systemförvaltningsarbetet. Intervjuade beskriver att dessa tas i beaktande i det nu startade arbetet med kontinuitetshandling. Uppfattningen är att IT-kontinuitetsplanerna i stora

⁷ Ledningssystem för kontinuitetshandling ISO 22301:2019

delar beskriver rutiner i ett IT-perspektiv. Ett undantag som finns i planerna är om en större cyberattack eller ett mer omfattande säkerhetsavbrott inträffar. Då kan Solnas övergripande plan för säkerhetsarbete gå före kontinuitetsplanens genomförande.

De planer vi tagit del av beskriver krav och behov för specifika system inom respektive förvaltningsobjekt⁸. Vi har i granskningen kunnat verifiera att de system som beskrivs i planeringen i hög grad samstämmer med de system som verksamheterna identifierat som verksamhetskritiska, där tillgängligheten är betydande för att verksamheten ska fungera på en acceptabel nivå. IT-kontinuitetsplanerna beskriver exempelvis krav om tillgänglighet, säkerhetskopiering samt acceptabla avbrottstider. Av planen framgår även kontakt- och eskaleringsvägar om systemen inte är tillgängliga.

3.2.4 Åtgärder och reservrutiner

Intervjuade beskriver att åtgärder inom informationssäkerhet och tekniska skydd för it och system genomförs löpande som del i IT-avdelningen och externa leverantörers ansvar och uppdrag.

I granskningen har vi fokuserat frågeställningen på åtgärder som identifierats i arbetet med kontinuitetshandling som därigenom syftar till att stärka förmågan för verksamheterna att fortsätta fungera oavsett vilken kris eller händelse som inträffar.

Inom omvårdnadsförvaltningen så har arbetet med utgångspunkt från IT-kontinuitetsplanen resulterat i ett antal åtgärder och rutiner som kommunicerats till verksamheterna. Det finns även krisberedskapsutrustning som testas enligt rutin årligen samt ett antal lathundar inom kritiska processer, exempelvis trygghetslarm, digitala lås och redundanta lösningar för tillgång till information i det fall nätverket eller vissa system skulle vara påverkade.

Inom kommunstyrelsens verksamheter så har granskningen inriktats till ekonomifunktionen som har vissa processer som identifieras som samhällsviktiga. Intervjuade har beskrivit ett antal reservrutiner som finns på plats samt åtgärder för att stärka redundans om systemen är otillgängliga. Företrädare från verksamheten har dock själva identifierat behov av ytterligare rutiner och åtgärder för att hantera mer omfattande störningar och avbrott, exempelvis vid en cyberattack.

3.2.5 Bedömning

Vår bedömning är att det endast delvis finns dokumenterade kontinuitetsplaner eller motsvarande underlag som beskriver hantering om it-avbrott skulle inträffa.

Vi baserar vår bedömning på att dokumenterade kontinuitetsplaner saknas. Det finns en metod för genomförande och arbetet är i hög grad pågående utifrån en fastställd planering. Vi bedömer att det finns risk att nuvarande tillgång till stöd för verksamheternas genomförande påverkar framdriften i arbetet då endast två funktioner finns som kan vara processledare i metoden.

⁸ Staden har organiserat arbetet med system i ett antal objekt för vilka det årligen tas fram systemförvaltningsplaner. En del i detta arbete är även upprättande av kontinuitetsplaner.

Vi noterar att de IT-kontinuitetsplaner som finns innehåller väsentliga delar för backup och redundans som kan utgöra underlag i verksamheternas kontinuitetsplaner. Vi bedömer dock att planerna i nuläget främst är tillämpliga som stöd för IT-verksamheten vid störningar eller avbrott. Vi uppfattar därigenom att det i nuläget saknas kontinuitetshandlingsrutiner för verksamhetens processer och arbetssätt vid kritiska it-säkerhetshändelser som beskriver hur verksamheten ska fortsätta fungera utan tillgång till system som de är beroende av.

Vår bedömning är att de samhällsviktiga verksamheterna inom kommunstyrelsen och omvårdnadsnämnden i allt väsentligt har analyserat sina kritiska beroenden till informationssystem och identifierat behov av åtgärder för att hantera it-avbrott.

Vi bedömer att arbetet med åtgärder baserat på analyserna endast delvis har vidtagits inom omvårdnadsnämnden och kommunstyrelsen.

Den metod som valts inkluderar analyser av kritiska beroenden till informationssystem varpå detta har gjorts för de verksamheter som ingår i granskningen. Då arbetet inte är slutfört är vår bedömning att åtgärder endast delvis vidtagits.

3.3 ÖVNING FÖR ATT UTVÄRDERA KONTINUITETSPLANERINGEN

Enligt Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap ska kommuner ansvara för att förtroendevalda och anställd personal får den utbildning och övning som behövs för att de ska kunna lösa sina uppgifter vid extraordinära händelser i fredstid.

Som vi nämnt inledningsvis i rapporten så är en av inriktningarna i handlingsplanen övningsverksamhet för ökad förmåga att hantera allvarlig störning. Bland annat anges att ledningsplanerna för styrelser och nämnder behöver övas.

Intervjuade från kommunstyrelsens verksamheter beskriver att det har genomförts övning under året med krisledningsfokus där både tjänstepersoner och representanter från kommunstyrelsen deltog. Detsamma gäller inom omvårdnadsnämndens verksamheter som också har övat krisledning. Representanter från omvårdnadsförvaltningen har även genomfört utbildning i stabsmetodik, lägesbilder mm.

Dessa har dock inte haft scenariot it-säkerhetshändelse eller digitalt bortfall. Då kontinuitetshandlingarna inte är genomförda så har inte några dokumenterade kontinuitetsplaner och tillhörande rutiner kunnat utvärderas.

Vi har fått uppgift om att övningar har genomförts inom två förvaltningar efter att våra intervjuer genomfördes, dessa utgick från scenario att staden tappar både internet och mobiltelefoni. Ytterligare övningar var under planering.

3.3.1 Bedömning

Vår bedömning är att det inte har genomförts övningar för att utvärdera kontinuitetsplaner och tillhörande rutiner.

Vi baserar vår bedömning på att kontinuitetsplaner saknas varpå övningar för att utvärdera dessa och tillhörande rutiner inte har genomförts. Krisledningsövning har genomförts vilket vi bedömer som positivt då ledningsförmågan är en väsentlig del som behöver fungera oavsett vilken händelse eller kris som inträffar.

3.4 UPPFÖLJNING

Enligt säkerhetspolicyn ska uppföljning av säkerhetsarbetet ske kontinuerligt. Respektive nämnd ansvarar för uppföljning av säkerhetsarbetet inom sin verksamhet. Kommunstyrelsen ansvarar för den stadsövergripande uppföljningen.

Enligt handlingsplan för krisberedskapsarbetet 2024 – 2026 är kommunstyrelsen ansvarig för uppföljning och utvärdering av denna. Alla nämnder, stiftelse och bolagsstyrelser ska årligen till kommunstyrelsen redovisa resultatet av sitt arbete med att uppfylla målen. Kommunstyrelsen ska följa upp detta genom uppdrag. Arbetet ska även följas upp och redovisas till Länsstyrelsen.

Enligt intervjuade har ingen strukturerad uppföljning genomförts ännu varken inom nämnderna eller av kommunstyrelsen. I slutskedet av granskningen har vi dock fått uppgift om att uppföljningsarbetet är planerat att påbörjas under november eller december 2025.

Ledningsgrupperna i förvaltningarna ska då besvara en enkät som baseras på målen i Handlingsplan för krisberedskapsarbetet 2024 – 2026. Resultatet ska sammanställas och presenteras för stadsledningen. Intervjuade uppger att denna utvärdering är tänkt som ett startskott för en mer systematisk uppföljning inom området krisberedskap och civilt försvar. I utvärdering framgent är tanken att kontinuitetshandlingarna ska ingå.

Det har under året skapats en beredskapsgrupp med bred representation från förvaltningarna. Gruppen samordnas av säkerhetssamordnaren från enhet trygghet och säkerhet. I gruppen sker en mer informell uppföljning. Genom att de två säkerhets- och beredskapssamordnarna deltar i samtliga verksamheters arbete finns en god kännedom om nuläge och status för arbetet.

3.4.1 Bedömning

Vår bedömning är att det inte finns en etablerad uppföljning och kontroll av arbetet med kontinuitetshandlingarna.

Vi baserar vår bedömning på att det saknas strukturerad uppföljning i enlighet med krav i säkerhetspolicyn samt beskrivning i stadens handlingsplan för krisberedskapsarbetet. En viss uppföljning av informell karaktär sker i det löpande arbetet samt när beredskapsgruppen träffas. Då nämnder och styrelser är ansvariga för krisberedskaps- och kontinuitetshandlingsarbetet så bedömer vi att det är väsentligt att rutiner för uppföljning och rapportering etableras.

4 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

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

Vår samlade bedömning utifrån granskningens syfte är att såväl kommunstyrelsen som omvårdnadsnämnden endast delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen i deras övergripande ansvar för ledning och samordning av krisberedskapsarbetet att:

- Tillse att reglementen för kommunstyrelsen och nämnderna revideras i syfte att tydliggöra ansvarsfördelning för krisberedskap.
- Besluta om styrande dokument inom krisberedskap och kontinuitetshandling som konkretiserar kommunfullmäktiges viljeriktning i säkerhetspolicy och handlingsplan för krisberedskap.
- Utvärdera om nuvarande organisation och resurser för genomförande av kontinuitetshandling är tillräcklig så att det finns förutsättningar att nå upp till kommunfullmäktiges förväntningar i handlingsplan för krisberedskap.
- Säkerställa att årlig uppföljning av arbetet med krisberedskap i enlighet med reglering i säkerhetspolicy och handlingsplan för krisberedskap.

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen och omvårdnadsnämnden att inom respektive styrelsen/nämnden:

- Tillse att arbetet med kontinuitetsplaner slutförs och fastställs för att sedan implementeras inom respektive verksamhet.
- Tillse att identifierade åtgärder vidtas som syftar till att stärka redundans och kontinuitet för verksamheterna.
- Genom övning utvärdera kontinuitetshandlingen och tillhörande rutiner.
- Tillse att arbetet löpande följs upp och rapporteras till kommunstyrelsen i enlighet med reglering i säkerhetspolicy och handlingsplan för krisberedskap.

Datum som ovan

Azets Revision & Rådgivning AB

Mikael Lind

Certifierad kommunal revisor

Jenny Thörn

Verksamhetsrevisor