Uppsala kommun

Brandförsvaret
Tjänsteskrivelse till Räddningsnämnden

Handläggare:
Mikael Lundkvist

Datum:
2025-01-15

Diarienummer:
RÄN-2024-00163

Yttrande om Kommunrevisionen Granskning av krisberedskap och kontinuitetsplanering

Förslag till beslut

Räddningsnämnden beslutar

1. **att** avge yttrande till kommunrevisionen enligt ärendets bilaga 1

Ärendet

Kommunrevisionen har 25 oktober begärt in yttrande från granskade kommunala nämnder och bolag. Granskningen avser krisplanering och kontinuitetsplanering. Granskningen är utförd av kommunrevisionen i Uppsala kommun med stöd av KPMG.

Beredning

Ärendet har beretts av tjänstepersoner vid Uppsala brandförsvar.

Föredragning

Utifrån genomförd granskning är kommunrevisionens samlade bedömning att kommunkoncernens krisberedskapsarbete i allt väsentligt bedrivs på ett sammanhållet och ändamålsenligt vis.
Kommunrevisionens samlade bedömning av arbetet kopplat till kontinuitetsplanering vid kritiska it-säkerhetshändelser är att kommunkoncernen delvis bedriver ett sammanhållet och ändamålsenligt arbete.

Beslutsunderlag

- Tjänsteskrivelse daterad 2025-01-15
- Bilaga 1, Yttrande om Granskning av krisberedskap och kontinuitetsplanering

Postadress: Uppsala kommun, brandförsvaret, 753 75 Uppsala
Besöksadress: Almungevägen 33
Telefon: 018-727 00 00 (Kontaktcenter)
E-post: brandforsvaret@uppsala.se
www.uppsala.se

- Bilaga 2, Revisionsrapport Granskning av krisberedskap och kontinuitetsplanering

Brandförsvaret

Mikael Lundkvist
tillförordnad förvaltningsdirektör

Uppsala kommun

Datum:
2025-01-15

Diarienummer:
RÄN-2024-00163

Räddningsnämnden
Yttrande

Handläggare:
Mikael Lundkvist

Kommunrevisionen
kommunrevisionen@uppsala.se

Yttrande om kommunrevisionens granskning av krisberedskap och kontinuitetsplanering

Räddningsnämnden anser att både krisberedskap och kontinuitetsplanering är viktiga områden och ser positivt på att kommunrevisionen valt att granska dessa områden. Generellt anser räddningsnämnden att granskningen är relevant och belyser viktiga förbättringsområden.
Kommunrevisionen skriver under punkt 3.1.3 att krisledningsnämndens förhållande till gemensamma nämnder bör förtydligas vilket räddningsnämnden håller med om och anser det vara en viktig fråga som bör prioriteras.

Kommunrevisionen rekommenderar räddningsnämnden följande:

- Tillse att SLA (servicenivåöverenskommelser för system) finns för samtliga kritiska verksamhetssystem
- Tillse att informationsklassning sker årligen i enlighet med vad som anges i styrande dokument
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Räddningsnämnder tar till sig dessa rekommendationer och avser att följa dem.

Räddningsnämnden arbetar med att det ska finnas SLA (servicenivåöverenskommelser för system) för samtliga kritiska verksamhetssystem och det beräknas vara klart under 2025. Informationsklassningen beräknas också vara klar 2025 för att därefter uppdateras årligen. En övning med IT-avbrott är planerad att genomföras i mars 2025.

Räddningsnämnden

Tobias Lundblad
Ordförande

Rosalind Göthberg
Nämndsekreterare

Postadress: Uppsala kommun, kommunledningskontoret, 753 75 Uppsala
Besöksadress: Stadshusgatan 2
Telefon: 018-727 00 00 (växel)
E-post: kommunledningskontoret@uppsala.se
www.uppsala.se

Granskning av krisberedskap och kontinuitetsplanering

Rapport

Uppsala kommunkoncern

KPMG AB

2024-10-25

Antal sidor 35

Uppsala kommunkoncern
Granskning av krisberedskap och kontinuitetsplanering

2024-10-25

Innehållsförteckning

1 Sammanfattning

KPMG har av Uppsala kommuns revisorer och lekmannarevisorer fått i uppdrag att granska kommunens och utvalda kommunala bolags arbete med krisberedskap. Granskningen har utifrån förhöjd risk och hot om cyberangrepp ett fokus på kommunens och ett av bolagens förmåga att motstå och hantera kritiska it-säkerhetshändelser för att upprätthålla kontinuitet i verksamheterna.

Granskningen har syftat till att bedöma om kommunkoncernen bedriver ett sammanhållet och ändamålsenligt krisberedskapsarbete med särskilt fokus på kontinuitet vid kritiska it-säkerhetshändelser.

Vår samlade bedömning utifrån granskningens syfte är att kommunkoncernens krisberedskapsarbete i allt väsentligt bedrivs på ett sammanhållet och ändamålsenligt vis.

Vår bedömning grundas i att det finns ett systematiskt arbete i hela kommunkoncernen med risk- och sårbarhetsanalyser och dokumenterade ledningsplaner både på koncernövergripande nivå och för varje enskild nämnd och bolag, vilket är i enlighet med de krav som ställs i lag och interna styrdokument. Kommunfullmäktige har därtill fastställt ett inriktningsprogram för arbetet med krisberedskap samt inkluderat fokusområden och uppdrag inom krisberedskap riktat till samtliga nämnder och bolag vilket vi bedömer ger en tydlig och konkret styrning och förväntan på krisberedskapsarbetet samt en god grund för kontroll och uppföljning att arbetet utvecklas i enlighet med kraven. Vi har däremot identifierat ett utvecklingsbehov vad gäller utbildning och övning av både personal och förtroendevalda vilket i nuläget endast bedrivs i begränsad utsträckning i koncernen och utan en tydlig systematik. Bland annat saknas för flera revisionsobjekt upprättade utbildnings- och övningsplaner och vi har även noterat att den kommunövergripande planen inte inkluderar koncernen som helhet utan en begränsad målgrupp.

Vår samlade bedömning av arbetet kopplat till kontinuitetsplanering vid kritiska it-säkerhetshändelser är att kommunkoncernen delvis bedriver ett sammanhållet och ändamålsenligt arbete.

Vi baserar vår bedömning på att det i huvudsak saknas färdigställda kontinuitetsplaner i berörda nämnder och styrelser. Endast räddningsnämnden, omsorgsnämnden och äldrenämnden har kunnat uppvisa dokumenterade kontinuitetsplaner. Samtidigt kan vi konstatera att arbetet i hög grad är pågående och genomförs i enlighet med det mål som fullmäktige har ställt upp, att dokumenterade kontinuitetsplaner ska finnas på plats senast år 2026. I nuläget noterar vi att det varierar mellan revisionsobjekten hur långt arbetet har kommit men ser positivt på att arbetet sker utifrån gemensam metod och struktur vilket ger förutsättningar till en kontinuitetsplanering som kan samordnas på ett bra sätt inom hela koncernen. Vi bedömer att det är väsentligt att arbetet med kontinuitetsplaner slutförs både generellt för de risker som identifierats, men särskilt kopplat till risken för it-avbrott där hotbilden är stor och konsekvenserna kan bli allvarliga om händelsen drabbar de samhällsviktiga verksamheterna. Mot bakgrund av bristerna kopplat till kontinuitetsplanering samt avsaknaden av en tydlig systematik för

utbildnings- och övningsarbetet ser vi också att övningar utifrån scenariot it-avbrott i begränsad utsträckning har genomförts och utan en tydlig sammanhållen systematik. Vi ser dock positivt på att risken för it-avbrott inkluderats inom ramen för internkontroll i samtliga berörda nämnder och styrelser, vilket möjliggör uppföljning, kontroll och kravställning både på nämnds-/bolagsspecifik nivå så väl som koncernövergripande nivå.

I det följande redovisas samlad bedömning av revisionsfråga per revisionsobjekt för granskning av krisberedskap:

Har krisledningsnämndens sammansättning och ansvar fastställts på ett ändamålsenligt sätt?	
Kommunstyrelsen	Nej
Finns en ändamålsenlig krisledningsorganisation vad gäller förebyggande krisberedskapsarbete samt operativt krisledningsarbete?	
Uppsala Arenor och fastigheter AB	Nej
Uppsala Stadshus AB	Inte tillämpbar
Samtliga övriga revisionsobjekt	Ja
Säkerställs det att förtroendevalda och personal får tillräcklig utbildning och övning avseende krisberedskap?	
Räddningsnämnden och Uppsala Vatten och Avfall AB	I allt väsentligt
Kommunstyrelsen och Uppsalahem AB	Delvis
Omsorgsnämnden, plan- och byggnadsnämnden, socialnämnden, utbildningsnämnden, äldrenämnden, Uppsala Kommun Skolfastigheter AB, Uppsala Arenor och Fastigheter AB	Nej
Uppsala Stadshus AB	Inte tillämpbar
Finns det ett systematiskt arbete med uppföljning och/eller intern kontroll av krisberedskapsarbetet?	
Samtliga nämnder och styrelser	Ja

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

I det följande redovisas samlad bedömning av revisionsfråga per revisionsobjekt för granskning av kontinuitetsplanering för it-avbrott:

Finns dokumenterade kontinuitetsplaner med en tydlig koppling till genomförd risk- och sårbarhetsanalys?	
Omsorgsnämnden, räddningsnämnden och äldrenämnden	Ja
Samtliga övriga nämnder och styrelser	Nej
Har kritiska beroenden till informationssystem beaktats i kontinuitetsplaneringen och har åtgärder identifierats och hanterats?	
Omsorgsnämnden, räddningsnämnden och äldrenämnden	Ja
Samtliga övriga nämnder och styrelser	Nej
Finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem?	
Gatu- och samhällsmiljönämnden	Inte tillämpbart
Räddningsnämnden & Uppsala Vatten och Avfall AB	Nej
Kommunstyrelsen, omsorgsnämnden, plan- och byggnadsnämnden, socialnämnden, utbildningsnämnden & äldrenämnden	Ja
Har övningar genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig?	
Omsorgsnämnden och äldrenämnden	Delvis
Kommunstyrelsen, plan- och byggnadsnämnden, gatu- och samhällsmiljönämnden, socialnämnden Uppsala Vatten och Avfall AB, utbildningsnämnden & räddningsnämnden	Nej
Finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar?	
Samtliga berörda nämnder och styrelser	I allt väsentligt

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

1.1 Rekommendationer

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen att:

- Säkerställa att val av ledamöter till krisledningsnämnden förrättas av kommunfullmäktige
- Föreslå kommunfullmäktige att revidera reglementet för krisledningsnämnden där krisledningsnämndens roll i förhållande till gemensamma nämnder tydliggörs.
- Följ upp arbetet med kontinuitetsplanering i koncernens nämnder och styrelser
- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna slutförs och att planeringen beaktar risken för it-avbrott på verksamhetskritiska system
- Tillse att informationsklassning genomförs för systemet inom kommunikation
- Tillse att arbetet med att ta fram vägledningar och stöd för hur arbetet med utbildning och övningar ska bedrivas slutförs
- Särskilt följa upp att arbetet med utbildning och övning sker enligt tilltänkt systematik i nämnder och bolag
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig

Utifrån våra iakttagelser och bedömningar rekommenderar vi plan- och byggnadsnämnden samt gatu- och samhällsmiljönämnden att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna genomförs och att planeringen beaktar risken för it-avbrott för verksamhetskritiska system
- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur.

Utifrån våra iakttagelser och bedömningar rekommenderar vi omsorgsnämnden och äldrenämnden att:

- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig

- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi räddningsnämnden att:

- Tillse att SLA finns för samtliga kritiska verksamhetssystem
- Tillse att informationsklassning sker årligen i enlighet med vad som anges i styrande dokument
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi socialnämnden att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna slutförs och att planeringen beaktar risken för it-avbrott för verksamhetskritiska system.
- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi utbildningsnämnden att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna slutförs och att planeringen beaktar risken för it-avbrott för verksamhetskritiska system
- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi Uppsala Kommun Skolfastigheter AB att:

- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov

- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi Uppsala Arenor och Fastigheter AB att:

- Säkerställ att aktuell ledningsplan finns beslutad
- Säkerställ att aktuell inventering av risker och sårbarheter, motsvarande risk- och sårbarhetsanalys, finns framtagen
- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur
- Säkerställ att uppdrag 35 i kommunens mål och budget följs upp inom ramen för verksamhetsplan

Utifrån våra iakttagelser och bedömningar rekommenderar vi Uppsala Vatten och Avfall AB att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna slutförs och att planeringen beaktar risken för it-avbrott på verksamhetskritiska system
- Tillse att SLA eller motsvarande it-beredskap etableras och ställs i relation till de behov som identifieras gällande tillgänglighetsaspekten
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur.

Utifrån våra iakttagelser och bedömningar rekommenderar vi Uppsalahem AB att:

- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

2 Bakgrund

KPMG har av Uppsala kommuns revisorer och lekmannarevisorer fått i uppdrag att granska kommunens och utvalda kommunala bolags arbete med krisberedskap. Granskningen har utifrån förhöjd risk och hot om cyberangrepp ett fokus på kommunens och bolagens förmåga att motstå och hantera kritiska it-säkerhetshändelser för att upprätthålla kontinuitet i verksamheterna. Uppdraget ingår i revisionsplanen för år 2024.

En god krisberedskap är en förutsättning för att både kommunens och de kommunala 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 och kriser för informationstillgångar och it baseras på att det finns ett systematiskt informationssäkerhetsarbete som är riskbaserat.

Under de senaste åren med mindre och större händelser har de kommunala verksamheternas krisberedskapsförmåga prövats och testats i skarpt läge. Några exempel är flyktingkrisen 2015, pandemin 2020–2022, den ökade flyktingtillströmningen som en effekt av Rysslands angrepp av Ukraina och en el-kris. Ett flertal kommuner, bolag och regioner har under de senaste åren även utsatts för cyberattacker med stora konsekvenser som följd där skyddsvärd information förlorats eller röjts till obehöriga eller där bristande hantering lett att berörda drabbats av ekonomisk skada eller förtroendeskada.

I inledningen av 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 informationssystem, däribland region Uppsala. För att skydda sig mot externa hot krävs att skyddsåtgärder är anpassade efter skyddsvärde hos informationstillgångar och en analys av de hot och risker som finns.

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 samhällsviktiga funktioner behöver fungera varje dag även om incidenter inträffar och det för verksamheten är ett så kallat onormalt läge. Den digitala transformationen innebär också att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Det ökande beroendet till it- och informationssystem leder också till att ett bortfall av dessa kritiska tillgångar får större konsekvenser än tidigare. Kommunen har ansvar för att verksamheten kan upprätthållas även när externa leverantörer nyttjas varpå det är väsentligt att sådana beroenden har analyserats i kontinuitetsplaneringen.

Det är av största vikt att det bedrivs ett systematiskt och sammanhållet 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 att de negativa konsekvenserna vid en extraordinär händelse eller annan kris som betydande om det inte finns ändamålsenlig

krisberedskap och kontinuitetsplanering. Därtill har de förtroendevalda revisorerna genom tidigare genomförd granskning identifierat brister i informationssäkerhetsarbetet vilket kan föranleda risk för förmågan att hantera kritiska säkerhetshändelser, exempelvis i form av cyberattacker och intrång.

Revisorerna drar därför slutsatsen att både sannolikheten för, och konsekvenserna av kritiska säkerhetshändelse inom it är icke-försumbar och att arbetet med krisberedskap på en övergripande nivå samt tillhörande kontinuitetsplanering och reservrutiner behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen har syftat till att bedöma om kommunkoncernen bedriver ett sammanhållet och ändamålsenligt krisberedskapsarbete med särskilt fokus på kontinuitet vid kritiska it-säkerhetshändelser.

Granskningen har besvarat följande revisionsfrågor:

Revisionsfrågor avseende generell krisberedskap

- Har krisledningsnämndens sammansättning och ansvar fastställts på ett ändamålsenligt sätt?
- Finns en ändamålsenlig krisledningsorganisation vad gäller förebyggande krisberedskapsarbete samt operativt krisledningsarbete?
- Säkerställs det att förtroendevalda och personal får tillräcklig utbildning och övning avseende krisberedskap?
- Finns det ett systematiskt arbete med uppföljning och/eller intern kontroll av krisberedskapsarbetet?

Fördjupning enligt avgränsning

Revisionsfrågor avseende kontinuitetsplanering för kritiska it-säkerhetshändelser

- Finns dokumenterade kontinuitetsplaner med en tydlig koppling till genomförd risk- och sårbarhetsanalys?
- Har kritiska beroenden till informationssystem beaktats i kontinuitetsplaneringen och har åtgärder identifierats och hanterats?
- 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 avser nedan revisionsobjekt i Uppsala kommunkoncern:

Kommunstyrelsen, omsorgsnämnden, plan- och byggnadsnämnden, räddningsnämnden, socialnämnden, utbildningsnämnden, äldrenämnden och krisledningsnämnden. Projektplanen har efter beslut av de förtroendevalda revisorerna även kompletterats med gatu- och samhällsmiljönämnden.

Granskningen avser även de kommunala bolagen Uppsala Stadshus AB, Uppsala Kommun Skolfastigheter AB, Uppsala Arenor och Fastigheter AB, Uppsala Vatten och Avfall AB och Uppsalahem AB.

2.2.1 Generell krisberedskap

Samtliga revisionsobjekt är inkluderade i den fördjupade granskningen av krisberedskap. För kommunstyrelsens del har granskningen avgränsats till ledning, styrning och uppföljning av kommunens krisberedskapsarbete. För nämndernas och bolagens del har granskningen vad gäller generellt krisberedskapsarbete avgränsats till arbete med risk- och sårbarhetsanalys, implementering av kommunens plan för extraordinära händelser samt utbildning och övning.

2.2.2 Fördjupningsdel kontinuitetsplanering för kritiska it-säkerhetshändelser

Granskning som avser kontinuitetsplanering för kritiska it-säkerhetshändelser har baserats på ett urval av revisionsobjekt där verksamheterna bedömt att de har kritiska beroenden till it och informationssystem. Urvalet har sedan utgått från de tre system med högst skyddsbehov i aspekten tillgänglighet, vilket innebär att verksamheten endast klarar sig utan tillgång till informationen i systemet under en mycket begränsad tid. Uppsala Vatten och Avfall AB har valts ut för granskning mot bakgrund av att dricksvattenförsörjning är en samhällsviktig verksamhet som de flesta andra verksamheter har ett beroende till för att kunna fungera på en acceptabel nivå.

2.3 Revisionskriterier

I granskningen har revisionskriterierna utgjorts 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

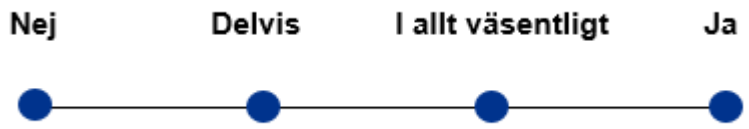
2.4 Metod

Granskningen har genomförts genom:

— Dokumentstudier av: Reglementen, bolagsordningar och ägardirektiv, Instruktion för kommundirektör, Risk- och sårbarhetsanalyser, Planer för hantering av extraordinära händelser, Utbildnings- och övningsplaner (eller motsvarande), Övriga styrdokument gällande för kommunens, nämndernas eller bolagens krisberedskap, Styrdokument inom informationssäkerhet, Kontinuitetsplaner eller motsvarande rutiner och planer, Åtgärdsplaner, SLA (servicenivåöverenskommelser för system)

- Intervjuer har genomförts med tjänstepersoner ansvariga för kommunens övergripande arbete med krisberedskap, kontinuitetsplanering och informations- och it-säkerhet. Ledande tjänstepersoner, verksamhetschefer, funktioner som arbetar med nämndens/bolagets krisberedskap eller system, samt urval av förtroendevalda inom berörda nämnder/styrelser och förvaltningar/bolag.
- Stickprovsvisa kontroller av dokumenterade kontinuitetsplaner och hur kritiska beroenden till informationssystem bedömts. Utifrån bedömning granskade vi för utvalda system de säkerhetsåtgärder som vidtagits samt om det finns avtal om servicenivåer för tillgänglighet och beredskap hos intern it-avdelning eller externa systemleverantörer.

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



Rapporten har skickats på faktakontroll till samtliga intervjupersoner via granskningssamordnare på enheten för krisberedskap och civilt försvar.

3 Resultat av granskningen – Övergripande krisberedskapsarbete

3.1 Organisation

3.1.1 Krisledningsnämnd

Av 2 kap. 2 § i LEH (2006:544) framgår att krisledningsnämnden är obligatorisk nämnd i en kommun och den är därav inte en del av kommunstyrelsen. Även om det kan råda personunion mellan kommunstyrelsen och krisledningsnämnden ska val av ledamöter till krisledningsnämnden förrättas av fullmäktige i egenskap av obligatorisk nämnd[1], antingen i ett eget beslut eller i samband med beslut av ledamöter till kommunstyrelsen där det framgår att val av ledamöter till både kommunstyrelsen och krisledningsnämnden förrättas.

Vid protokollgranskning har vi inte kunnat styrka att kommunfullmäktige beslutat om ledamöter för krisledningsnämnden. Av kommunens ledningsplan för extraordinära händelser [2] framgår att kommunstyrelsen utgör krisledningsnämnd.

Krisledningsnämnden ansvarar enligt reglemente[3] för kommunens uppgifter enligt lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Krisledningsnämnden har rätt att överta beslutanderätt från kommunens övriga nämnder i den utsträckning som nämnden finner nödvändigt i den uppkomna krisen. Enligt lag och krisledningsplan kan ordföranden i krisledningsnämnden bedöma när en extraordinär händelse (samhällsstörning) medför att nämnden ska träda i funktion och beslutar att detta då ska ske. Bedömningen görs i samråd med stadsdirektören. Av reglementet framgår även att krisledningsnämnden kan sammankallas på begäran av en enskild ledamot och nämnden ska då kollegialt ta ställning till om nämnden ska träda i funktion.

I övrigt framgår inget ytterligare av krisledningsnämndens reglemente, exempelvis uppgifter utöver lagstiftade förhållanden, eller särskilda undantag från andra nämnders arbetsformer.

Det framgår även av krisledningsplan att krisledningsnämnden inte har rätt att överta kommunala bolags verksamhet om inte detta särskilt specificeras i bolagsordning. Vad som gäller för gemensamma nämnder framgår ej. I intervju med representanter från räddningsnämndens förvaltning framkommer att den gränsdragningen uppfattas otydlig i dagsläget.

[1] Handbok i civil beredskap, 1. Övergripande processer, MSB2309, s.15
[2] Ledningsplan inför och vid extraordinära händelser. Beslutad av kommunfullmäktige 2023-11-06
[3] Reglemente för kommunstyrelsen och övriga nämnder. Beslutad av kommunfullmäktige 2023-11-06

3.1.2 Krisledningsorganisation

3.1.2.1 Förebyggande

Risk och sårbarhetsanalys

Kommuner ska analysera vilka extraordinära händelser i fredstid som kan inträffa i kommunen och hur dessa händelser kan påverka den egna verksamheten. Resultatet av arbetet ska värderas och sammanställas i en risk- och sårbarhetsanalys.[4]

I Uppsala kommun är det enheten för krisberedskap och civilt försvar under kommunstyrelsen som tillser att kommunen uppfyller lagkravet och tar fram en kommunövergripande risk- och sårbarhetsanalys för varje mandatperiod.

I den senaste risk- och sårbarhetsanalysen[5] har kommunen arbetat enligt FORSA-modellen.[6] Arbetet har bedrivits i flera steg, där första steget var att enheten för krisberedskap och civilt försvar bjöd in berörda samhällsviktiga verksamheter till en workshop. Vid tillfället fick verksamheterna med stöd av enheten identifiera sin verksamhet, sina kritiska beroenden och sina oönskade händelser. Enheten hjälpte till att sammanställa grovmaterialet från den första workshopen, vilket sedermera fick kvalitetssäkras av verksamhetsrepresentanterna och användas som material för det fortsatta arbetet utifrån riskerna. Därefter genomfördes en andra workshop med verksamheterna som var mer inriktad mot händelseanalys och att identifiera behov av åtgärder.

I vår granskning har vi kunnat konstatera att samtliga förvaltningar och bolag som har samhällsviktig verksamhet har deltagit i gemensamma workshops. De har även beslutat om risk- och sårbarhetsanalys för egna förvaltningen eller bolaget. Dessa analyser har utgjort grund för den kommunövergripande risk- och sårbarhetsanalysen som enheten för krisberedskap och civilt försvar beslutat om på kommunövergripande nivå.

Uppsala Stadshus AB har inte en risk- och sårbarhetsanalys då bolaget inte bedriver någon egen operativ verksamhet och saknar anställd personal. Detta innebär att moderbolaget utifrån sin nuvarande organisation och styrning inte är en del i kommunkoncernens arbete med krisberedskap och civilt försvar, vilket vi återkommer till i flera avsnitt i rapporten.

De bolag som ingår i granskningen men inte bedriver samhällsviktig verksamhet (enligt bedömning gjord av enheten för krisberedskap och civilt försvar) har inte ingått i arbetet med risk- och sårbarhetsanalys enligt ovan metod. Vi kan dock konstatera att det finns en förståelse i dessa bolag för risker i den egna verksamheten och att riskanalyser har arbetats fram enligt andra metoder, exempelvis inom ramen för internkontrollarbetet alternativt separat process inom respektive verksamhet. Vi har inte kunnat styrka att så har skett i Uppsala Arenor och Fastigheter AB då vi inte delgivits underlag.

[4] (LEH 2006:544) 2.kap §1
[5] Beslutad 2023-08-21
[6] Modellen är framtagen av Totalförsvarets Forskningsinstitut.

Kontinuitetshantering

I inriktningsdokumentet Program för krisberedskap och civilt försvar [7] anges målsättningen att nämnderna och bolagsstyrelserna ska arbeta för att slutföra ett första utkast av kontinuitetshantering senast 2026, samt att behovet av reservkraft ska inkluderas i kontinuitetshanteringen. Krav om kontinuitetshantering avser samhällsviktiga verksamheter i koncernen.

Arbetet med kontinuitetsplanering följer ansvarsprincipen vilket innebär att respektive verksamhet själva bär ansvaret att kontinuitetsplanera sin verksamhet. Enheten för krisberedskap och civilt försvar är i den meningen en stödjande funktion. Utifrån den rollen har de erbjudit och genomfört utbildning för representanter från förvaltningar och bolag så att dessa ska kunna agera processledare för den kommungemensamma metodiken för kontinuitetsplanering. Metodiken utgår från MSB:s metodstöd för kontinuitetsplanering, men med vissa anpassningar. Genom utbildningen har processledarna lärt sig metodiken samt fått mallar och metodstöd för att kunna arbeta vidare i den egna verksamheten.

Processledarna i verksamheterna är i regel någon i en ledande central befattning i verksamheten eller förvaltningen/bolaget beroende på storleken på förvaltningen/bolaget. Vi har inom ramen för granskningen intervjuat processledarna i berörda verksamheter/förvaltningar och kan konstatera att det finns en samstämmig bild kring hur arbetet har bedrivits och att det finns en förståelse för det egna ansvaret att driva arbetet.

I granskningen har vi kunnat konstatera att arbetet bedrivs i respektive förvaltning och bolag enligt tilltänkt metod för risk- och sårbarhetsanalys och kontinuitetsplanering. Vi kan även konstatera att arbetet med kontinuitetsplanering i granskade nämnder och bolag generellt är i en startfas. Endast ett fåtal av de nämnder och bolag som ingår i granskningen har kommit så pass långt att det finns färdigställda kontinuitetsplaner i de egna verksamheterna (se avsnitt 4.1).

Vissa utmaningar kopplat till det fortsatta arbetet har identifierats kopplat till hur risker ska åtgärdas och samordnas över verksamhetsgränserna. Enligt ansvarsprincipen bär respektive förvaltning och bolag ansvaret att själva samordna sina kritiska beroenden internt i kommunen mot andra förvaltningar eller bolag. Exempelvis skulle omsorgsförvaltningen eller utbildningsförvaltningen och dess underliggande verksamhetsområden självständigt behöva kommunicera sina behov mot ansvarigt bolag för reservvatten eller reservkraft. Arbetet upplevs tidskrävande och utmanande, inte minst för mottagaren av kravställningen som ska kommunicera och tillmötesgå många verksamheter i parallella processer.

Det finns än så länge ingen formaliserad process för hur kritiska beroenden som många förvaltningar eller bolag har av samma sort kan samordnas/omhändertas koncernövergripande. Enligt intervjuer har en sådan dialog initierats i det koncernövergripande nätverket för krisberedskap, som samordnas av enheten för krisberedskap och civilt försvar, men mer i generella termer än att det bestämts hur det

[7] Beslutad av kommunfullmäktige 2023-10-02

ska gå till. Nätverket sammanträder sex gånger per år och utgörs av representanter från samtliga förvaltningar och bolag där tidigare nämnda processledare är vanligen utsetts som representant i nätverket.

3.1.2.2 Operativt

Kommuner ska, med beaktande av risk- och sårbarhetsanalysen, för varje ny mandatperiod fastställa en plan för hur de ska hantera extraordinära händelser[8].

Uppsala kommun har en ledningsplan inför och vid extraordinära händelser[9] som beskriver kommunövergripande krisorganisering. Ledningsplanen är en riktlinje som beskriver former och förhållningssätt för att effektivt hantera akuta och prioriterade händelser på ett kommungemensamt sätt. En allvarlig störning behöver ofta hanteras samordnat av flera förvaltningar och bolag samtidigt. Ledningsplanen ersätter dock inte normala lednings- besluts- och organisationsstrukturer, undantaget då krisledningsnämnd har övertagit annan nämnds ansvarsområde.

Kommunledningskontoret förvaltar ledningsplanen genom att följa upp tillämpningen samt att revidera planen minst varje mandatperiod. Varje förvaltningschef och direktör ansvarar för att riktlinjen är känd inom den egna förvaltningen.

Utöver krisledningsnämnd benämns ett antal centrala funktioner/roller i den centrala krisledningsorganisationen i ledningsplanen.

Inriktningsfunktion säkrar verksamhetsnytta och effektivitet genom inriktande beslut. Inriktningsfunktionen består av interna och vid behov även externa aktörer med mandat att överenskomma inriktning. Internt är inriktningsfunktionen bemannad av berörda förvaltningsdirektörer, vd:ar eller motsvarande med beslutsmandat.

Samordningsfunktion anpassar aktiviteter så att tillgängliga resurser kommer till största möjliga nytta. Samordningsfunktionen prioriterar åtgärder och resurser till de mest angelägna behoven. Samordningsfunktionen består av avdelnings- och enhetschefer och personal med mandat och kunskap. Vid behov finns även externa aktörer representerade på motsvarande nivå. Alla förvaltningar kan initiera samordningsfunktionen. Detta görs genom att kontakta Tjänsteperson i beredskap (TiB). TiB:s mandat och ansvar regleras i en separat TiB-instruktion[10]

Kontaktpunkten i förvaltningar och bolag, förvaltningsledning eller beredskapsjourer har mandat att kontakta TiB. TiB utgör även extern kontaktpunkt för kommunen. TiB har också i uppgift, i syfte att få en samlad lägesbild och samordna resurser, att särskilt verka för samverkan mellan interna och externa aktörer. TiB kan starta upp samordningsfunktion i samråd med säkerhetschef och stadsdirektör.

Samordningsstöd stödjer samordningsfunktionen genom kommungemensamt analys-, kommunikations- och administrativt stöd beroende på vad den särskilda händelsen kräver.

[8] (LEH 2006:544) 2.kap §1
[9] Beslutad av kommunfullmäktige 2023-11-06
[10] Tjänsteperson i beredskap. Beslutad 2024-02-15.

Av ledningsplanen framgår, vilket även styrks av intervjuer, att händelser i möjligaste mån ska hanteras så nära som möjligt där händelsen inträffar, det vill säga *närhetsprincipen*. Det ordinarie verksamhetsansvaret ska också råda så långt som möjligt, det vill säga *ansvarsprincipen.*

Utifrån detta förväntas varje enskild nämnd och bolagsstyrelse enligt ledningsplanen ha egna ledningsplaner som på en behovsanpassad nivå beskriver respektive nämnds- och bolagsstyrelses ledning vid och hantering av allvarliga störningar. Det är förvaltningschef eller VD:s ansvar att säkerställa att ledningsplan finns för den egna förvaltningen/bolaget.

Det kravställs även i den kommunövergripande ledningsplanen att samtliga förvaltningar och bolag som bedriver samhällsviktig verksamhet ska ha en definierad kontaktpunkt i sin ledningsplan, en samordningsfunktion mot andra förvaltningar, bolag och den kommunövergripande nivån. Om inte denna definieras i ledningsplan utgör förvaltningschef eller VD kontaktpunkt.

Ledningsplanerna på nämnds- och bolagsnivå beskriver former för hur eskalering till kommungemensamt agerande i kommunövergripande ledningsplan ska gå till. Det framgår därtill hur ledningsplan på förvaltningsnivå/bolagsnivå kan brytas ned till beredskapsplaner för specifika typer av händelser när det anses relevant för verksamheten.

Utifrån vår granskning kan vi konstatera att samtliga nämnder och bolag har en krisledningsplan bortsett från Uppsala Stadshus AB som inte bedriver operativ verksamhet. Vi kan konstatera att ledningsplaner följer en liknande systematik som korresponderar mot den kommunövergripande ledningsplanen med anpassningar utifrån den egna förvaltningen eller bolagets storlek och typ av verksamhet. Vi har i intervjuer även kunnat konstatera att det finns en förståelse för hur händelser eskaleras internt i kommunen, hur ansvars- och närhetsprincipen fungerar och vilka händelser som är rimligt att den egna förvaltningen/bolaget ska kunna hantera.

En del av ledningsplanerna är under revidering då de anses behöva uppdateras för att fortsatt korrespondera mot kommunövergripande ledningsplan, alternativt med hänsyn till förändrade arbetssätt/organisationer som därigenom behöver dokumenteras.

I intervju uppges att Uppsala Arenor och Fastigheter ha en krisplan, men vi har inte delgivits ledningsplanen inom ramen för granskningen och kan därför inte styrka detta.

3.1.3 Bedömning

Vår bedömning är att krisledningsnämndens sammansättning och ansvar inte fastställts på ett ändamålsenligt sätt.

Vår bedömning baseras på att krisledningsnämnden i egenskap av obligatorisk nämnd ska ha beslutade ledamöter av kommunfullmäktige, antingen i ett eget beslut eller i samband med beslut av ledamöter till kommunstyrelsen där det framgår att val av ledamöter till både kommunstyrelsen och krisledningsnämnden förrättas.

Vi bedömer även att krisledningsnämndens förhållande till gemensamma nämnder bör förtydligas.

Vi bedömer att samtliga revisionsobjekt, med undantag av Uppsala Stadshus AB och Uppsala Arenor och fastigheter AB, har en ändamålsenlig krisorganisation vad gäller både förebyggande krisberedskapsarbete samt operativt krisledningsarbete.

Vår bedömning grundas i att alla nämnder och bolag med samhällsviktig verksamhet har arbetat enligt samma process och metodik med stöd av enheten för krisberedskap och civilt försvar med att framta en förvaltnings-/bolagsspecifik risk- och sårbarhetsanalys. Vi bedömer att detta underlag utgör en god grund för det fortsatta riskarbetet i kommunen. I bolagen som inte omfattas av samhällsviktig verksamhet ser vi också att det bedrivs ett eget riskarbete i olika former som vi bedömer korresponderar mot behovet utifrån den verksamhet som bedrivs.

Vår bedömning grundas vidare i att den övergripande ledningsplanen är tydlig och innehåller relevanta roller med etablerade mandat och eskaleringsvägar. Vi bedömer att samtliga nämnder och bolag har en ledningsplan som i allt väsentligt är aktuell, genomarbetad och följer den koncerngemensamma strukturen vad avser organisation, roller och eskalering internt. Inom ramen för arbetet med kontinuitetsplaner som närmare berörs i avsnitt 4.1 ser vi också att nästa steg i att bygga ett än mer robust operativt krisledningsarbete kan ta form genom beredskapsplaner utifrån särskilda scenarion som finns definierat i den övergripande ledningsplanen.

Vi bedömer att det saknas underlag som styrker att Uppsala Arenor och Fastigheter AB har en ändamålsenlig krisorganisation vad gäller förebyggande krisberedskapsarbetet samt operativt krisledningsarbete.

Vi bedömer att revisionsfrågan inte är tillämpbar på Uppsala Stadshus AB då bolaget inte bedriver någon operativ verksamhet och saknar egen personal.

3.2 Övning och utbildning

Kommuner ansvarar 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 [11].

Kommunfullmäktige har i linje med lagkravet fastställt både i Mål och budget 2024 [12] samt i Program för krisberedskap och civilt försvar vikten av ett systematiskt arbete med utbildning och övning. Ett av målen i programmet är: *Uppsala kommun stärker sin förmåga att upprätthålla samhällsviktig verksamhet vid samhällsstörningar och under höjd beredskap.*

Arbetet ska enligt programmet ske genom att varje nämnd och bolagsstyrelse som bedriver samhällsviktig verksamhet ska ta fram en utbildnings- och övningsplan för perioden 2024–2027. Planen ska redovisa hur nämnd eller bolagsstyrelse avser att utbilda och öva sina medarbetare och verksamheter. Planen ska utgå från så väl specifika verksamhetsbehov och utvecklingsområden som de prioriterade förmågor och scenarier som beskrivs i den kommunövergripande utbildnings- och övningsplanen för mandatperioden.

Uppsala kommun har fastställt en kommunövergripande utbildnings- och övningsplan för mandatperioden [13]. I utbildnings- och övningsplanen anges inriktningen för arbetet. Uppsala kommuns utbildnings- och övningsplan omfattar i huvudsak uppgifter som anges i de nationella överenskommelser som träffats av Myndigheten för samhällsskydd och beredskap (MSB) och Sveriges Kommuner och Regioner (SKR) för kommuners användning av statliga medel från anslag 2:4 krisberedskap samt civilt försvar.

Detta innebär att utbildnings- och övningsplanen omfattar övning av den centrala krisorganisationen, tjänstemannaledningen i kommunen och krisledningsnämnden minst en gång per mandatperiod. Kommunstyrelsen och kommunledning ska också utbildas i höjd beredskap och totalförsvar. Utöver dessa övningar är en inriktning att kommunen ska delta i övningar i extern regi, exempelvis Försvarsmakten, Hemvärnet, Länsstyrelsen och andra statliga myndigheter. Det anges även inriktning på utbildningen utifrån de områden som identifierats som risker i risk- och sårbarhetsanalysen för mandatperioden, exempelvis elbortfall och nödvattenförsörjning.

Av utbildnings- och övningsplanen framgår att vid större övningar där flertalet av kommunens verksamheter och/eller externa aktörer deltar kommer det att finnas behov av att kommunen tillför egna medel för att kunna genomföra sådana övningar. Detta då den statliga finansieringen i dagsläget inte är dimensionerad för att täcka de kostnader som kan uppstå i samband med sådana övningar.

Övrig utbildnings- och övningsverksamhet som sker inom kommunen finansieras av respektive nämnd och bolag självständigt. I vår granskning kan vi konstatera att

[11] (LEH 2006:544) kap 2. §8
[12] Mål och budget 2024 med plan för 2025–2026. Beslutad av kommunfullmäktige 2023-11-06
[13] Beslutad på tjänstemannanivå 2023-08-31

utbildnings- och övningsplaner för innevarande mandatperiod i huvudsak saknas i granskade nämnder och bolag.

Räddningsnämnden har en fastställd utbildnings- och övningsplan för innevarande mandatperiod. Uppsala Vatten och Avfall AB har en övnings- och utbildningsplan för hösten 2024, utifrån vilken det två mindre övningar i krisledningen och två större övningar med stöd av konsult är genomförda/planerade. Dessa övningar är beslutade i kanslisektionens verksamhetsplan för 2024. En formellt upprättad utbildningsplan för 2025 och planåren därefter finns med som aktivitet i kanslisektionen verksamhetsplanering för 2025 samt som huvudåtgärd i bolagets affärsplan.

Enligt program för krisberedskap och civilt försvar ska enhet krisberedskap och civilt försvar ta fram två kommunövergripande rutiner som stöd för övriga verksamheters framtagande utbildnings- och övningsplaner under 2024. Den ena är en kommungemensam rutin för hur nämnder och bolagsstyrelser kan inventera sina behov av utbildning och övning inom krisberedskap och civilt försvar och den andra en kommungemensam rutin för utvärdering och erfarenhetsåterföring av utbildning och övningar. Rutinerna är inte framtagna än.

I intervjuer har vi fått beskrivet att det trots avsaknaden av utbildnings- och övningsplaner delvis bedrivs ett arbete med utbildning och övning i nämnder och bolag. Vi har i granskningen fått nedan exempel på övningar som genomförts:

- I socialförvaltningen, utbildningsförvaltningen och vård- och omsorgsförvaltningen har övningar skett på olika nivåer i verksamheten och utifrån olika scenarios. Exempelvis utifrån scenario el och kyla i socialförvaltningen, skyfall och översvämning i utbildningsförvaltningen och it-bortfall i vård- och omsorgsförvaltningen.
- Stadsbyggnadsförvaltningen har övat sin ledningsplan för föregående mandatperiod vid två olika tillfällen. Utöver detta har inga övningar eller utbildningar genomförts.
- Uppsalahem AB har löpande arbetat med utbildningsinsatser utifrån sina respektive ansvarsområden och utifrån identifierade risker.

Uppsala Skolfastigheter AB har inte bedrivit någon särskild övningsverksamhet senaste tre åren utöver grundläggande årliga övningar i HLR, brandskydd och hjärtstopp. Uppsala Arenor och Fastigheter AB bedriver enligt intervjuuppgift motsvarande övnings- och utbildningsverksamhet som Uppsala Skolfastigheter AB. Uppsala Stadshus AB bedriver ingen övningsverksamhet då bolaget saknar operativ verksamhet.

3.2.1 Bedömning

Vi bedömer att kommunstyrelsen delvis säkerställt att förtroendevalda och personal får tillräcklig utbildning och övning avseende krisberedskap.

Vår bedömning baseras på att kommunstyrelsen uppfyllt grundläggande krav för utbildning och övning av centrala tjänstepersoner och politiker i kommunen. Vi bedömer dock att det finns ett utvecklingsarbete i att stödja och säkerställa att nämnder

och bolag arbetar mer aktivt med utbildning och övning, särskilt då resurserna inte är tillräckliga för att bedriva kommun- eller koncernövergripande utbildningar och övningar i någon större utsträckning. Vi ser därför positivt på de initiativ som finns för innevarande år från kommunledningskontoret med att framta metodstöd och mallar för inventering och utvärdering av utbildningsinsatser på nämnds- och bolagsspecifik nivå.

Vi bedömer att räddningsnämnden och Uppsala Vatten och Avfall AB i allt väsentligt säkerställt att förtroendevalda och personal får tillräcklig utbildning och övning avseende krisberedskap.

Vår bedömning grundas i att räddningsnämnden har en aktuell utbildnings- och övningsplan för mandatperioden. Vi kan konstatera att planen innehåller övningar och utbildningar som både inriktar sig specifikt på insatser enligt Lag (2003:778) om skydd mot olyckor men också bredare utbildningar inom krisberedskapsområdet. Utifrån beroendet till it för nämndens verksamhet ser vi att övningar kopplat till scenariot it-avbrott bör inkluderas (se 4.3). Vi bedömer att Uppsala Vatten och Avfall AB också har tillsett att ett aktivt övningsarbete bedrivs utifrån en tillfällig utbildnings- och övningsplan. Vi bedömer också att det är positivt att bolaget prioriterar framtagandet av en längre utbildnings- och övningsplan kommande år.

Vi bedömer att Uppsalahem AB delvis säkerställt att förtroendevalda och personal får tillräcklig utbildning och övning avseende krisberedskap.

Vi bedömer dock att aktuella utbildnings- och övningsplaner bör tas fram för att systematisera arbetet. Vi bedömer även att det är av betydelse att arbetet med utvärdering av utbildningar och övningar sker systematiskt. Vi ser att arbetet med fördel kan genomföras med stöd i de koncernövergripande rutiner som ska tillhandahållas av kommunledningskontoret.

Vi bedömer att Uppsala Arenor och Fastigheter AB, Uppsala Skolfastigheter AB, socialnämnden, utbildningsnämnden, omsorgsnämnden, plan- och byggnadsnämnden, gatu- och samhällsmiljönämnden, äldrenämnden inte säkerställt att förtroendevalda och personal får tillräcklig utbildning och övning avseende krisberedskap.

Samtliga revisionsobjekt enligt ovan bedömning saknar i nuläget utbildnings- och övningsplan och en övergripande styrning och systematik i arbetet. Vi bedömer att samtliga framgent bör ta fram utbildnings- och övningsplan som utgår från ett inventerat behov av anpassade utbildningar och övningar samt arbeta systematiskt med utvärdering av utbildningar och övningar. Vi ser att arbetet med fördel kan genomföras med stöd i de koncernövergripande rutiner som ska tillhandahållas av kommunledningskontoret.

Vi bedömer att revisionsfrågan inte är tillämpbar på Uppsala Stadshus AB då bolaget saknar operativ verksamhet och egen anställd personal.

3.3 Uppföljning

Genom dokumentgranskning kan vi konstatera att arbetet med krisberedskap och civilt försvar följs upp dels i den ordinarie styrkedjan utifrån Mål och budget 2024, dels med grund i det av fullmäktige beslutade Program för krisberedskap och civilt försvar som har två inriktningsmål och aktiviteter som ska genomföras under mandatperioden.

I Mål och budget 2024 beskrivs att kommunfullmäktiges politiska inriktning för planperioden är formulerad i fyra gemensamma fokusmål. Fokusmålen syftar till att kraftsamla hela kommunkoncernen för att göra de förflyttningar som pekas ut och säkerställer det politiska genomslaget. För att följa koncernens utveckling i förhållande till målbilder så kopplas indikatorer till varje fokusmål.

Till fokusområde fyra *Uppsala ska bli tryggare med jämlika livsvillkor* finns ett tidsbegränsat uppdrag[14] som omfattar samtliga nämnder och bolag:

- Utveckla kommunens krisberedskap och det civila försvaret i syfte att stärka samhällets motståndskraft

I beskrivningen av uppdraget framgår behov av förstärkning i planering för att minska sårbarheter, stärkt kontinuitetshantering med ökad förmåga att hantera samhällsstörningar och behov av planering för civilt försvar i alla verksamheter. I beskrivningen av uppdraget lyfts även beredskap för att kunna arbeta analogt när vardagens tillgängliga teknik inte längre fungerar. Det sistnämnda kommer vi ytterligare att belysa i rapportens avsnitt om kontinuitetshantering för kritiska it-säkerhetshändelser.

De indikatorer som beslutats för att följa utvecklingen är:

Tabell 22. Indikatorer inom krisberedskap och civilt försvar.

Krisberedskap och civilt försvar	Mål
Andel nämnder och bolagsstyrelser som har, utifrån sin risk- och sårbarhetsanalys (RSA), identifierat åtgärdsbehov och arbetar aktivt med dessa	Öka
Andel nämnder och bolagsstyrelser som har en kontinuitetshantering inom sina samhällsviktiga verksamheter	Öka
Andel nämnder och bolagsstyrelser som har en aktuell plan för höjd beredskap	Öka
Andel nämnder och bolagsstyrelser med samhällsviktiga verksamheter som har övat sin krisledningsorganisation inför och vid allvarlig störning och kris	Öka

Vi har utifrån erhållna verksamhetsplaner 2024 för berörda styrelser och nämnder, (utom Uppsala Arenor och Fastigheter AB som inte presenterat några underlag till granskningen) kunnat konstatera att dessa inkluderat ”uppdrag 35” i sin verksamhetsplanering. Muntliga uppgifter har erhållits att även Uppsala Arenor och Fastigheter har inkluderat uppdraget i sin verksamhetsplanering.

[14] Uppdrag 35

Uppdrag och mål bryts ner till åtgärder för den egna nämnden eller bolaget. Det finns även en förankring till Program för krisberedskap och civilt försvar och de inriktningsmål och aktiviteter som samtliga nämnder och bolag ska genomföra under mandatperioden.

Nedan återges ett exempel på hur detta kan konkretiseras och presenteras i verksamhetsplaneringen.

Nämndens åtgärd	Koppling till styrdokument	Förväntade effekter av åtgärden
Fortsätt att utveckla nämndens krisberedskap så att nämndens verksamheter kan säkerställa stöd och insatser till brukare och kommuninvånare även vid samhällsstörningar.	Program för krisberedskap och civilt försvar	Samhällsviktig verksamhet säkerställs vid samhällsstörningar.
Fortsätt arbetet med att utveckla nämndens kontinuitetsplanering för höjd beredskap.	Program för krisberedskap och civilt försvar	Samhällsviktig verksamhet säkerställs vid samhällsstörningar.

Tabell 16. Uppdrag 35. Utveckla kommunens krisberedskap och det civila försvaret i syfte att stärka samhällets motståndskraft.

Nämnderna och styrelserna följer upp målet i samband med delårsrapporten och årsbokslutet. Enhetschef på enhet krisberedskap och civilt försvar har uppdraget att sammanställa samtliga nämnder och bolags rapportering till en aggregerad version till kommunstyrelsen vilket även framgår av kommunstyrelsens verksamhetsplan enligt nedan.

Indikatorer krisberedskap och civilt försvar	2021	2022	2023	Mål	Jämförvärde	Källa
Andel nämnder och bolagsstyrelser som har, utifrån sin risk- och sårbarhetsanalys (RSA), identifierat åtgärdsbehov och arbetar aktivt med dessa.				Öka		Egen uppföljning
Andel nämnder och bolagsstyrelser som har en kontinuitetshantering inom sina samhällsviktiga verksamheter				Öka		Egen uppföljning
Andel nämnder och bolagsstyrelser som har en aktuell plan för höjd beredskap				Öka		Egen uppföljning
Andel nämnder och bolagsstyrelser som har övat sin krisledningsorganisation inför och vid allvarlig störning och kris				Öka		Egen uppföljning

Tabell 27. Kommunstyrelsens indikatorer till uppdrag 35. Utveckla kommunens krisberedskap och det civila försvaret i syfte att stärka samhällets motståndskraft.

Vi har efterfrågat uppföljning vid delårsrapporteringen men fått till svar att den inte kommer vara sammanställd och beslutad inom tidsramen för granskningen. Vi har därför inte haft möjlighet att inom granskningen verifiera hur arbetet inom revisionsobjekten har utvecklats i förhållande till mål och uppdrag under 2024. Samtliga

intervjuade uppfattar att rapporteringsvägarna går direkt till samordnande funktioner inom kommunledningskontoret.

3.3.1 Bedömning

Vi bedömer att det finns ett systematiskt arbete med uppföljning och/eller intern kontroll av krisberedskapsarbetet i samtliga berörda nämnder och styrelser.

Vår bedömning baseras på att det finns en tydlig struktur för uppföljning inom krisberedskapsområdet inom ramen för ordinarie styrning som omfattar samtliga nämnder och bolag och en uppföljning på aggregerad nivå till kommunstyrelsen. Vi bedömer att det är särskilt positivt att det finns en tydlig koppling i uppdraget till inriktningen i styrande dokument och identifierade utvecklingsområden inom beredskapsområdet. Vi saknar dock underlag som styrker intervjuuppgiften att uppdrag 35 är en del av Uppsala Arenor och Fastigheter AB:s verksamhetsplan.

4 Resultat av granskningen – Kontinuitetsplanering för kritiska it-säkerhetshändelser

4.1 Kontinuitetsplanering

4.1.1 Identifierade risker med tillhörande kontinuitetsplanering

I den kommunövergripande risk- och sårbarhetsanalysen som vi beskrivit i tidigare avsnitt finns identifierad risk för it-avbrott. Mot bakgrund av det så behöver förvaltningarnas och bolagens kontinuitetsplanering inkludera detta scenario. Av de risk- och sårbarhetsanalyser vi tagit del av på förvaltnings- och bolagsnivå samt genom muntliga uppgifter kan vi konstatera att en majoritet av revisionsobjekten i sina analyser har identifierat att de har kritiska beroenden till it och informationssystem.

Även vid andra kriser och händelser än cyberangrepp så kan risken för it-bortfall vara påtaglig, exempelvis vid elbortfall eller översvämning som påverkar infrastrukturen.

Som vi tidigare beskrivit så finns krav om att samtliga samhällsviktiga verksamheter ska arbeta vidare med kontinuitetsplanering. Mål och inriktningsområden i Program för krisberedskap och civilt försvar anger att ett första utkast av kontinuitetshantering ska vara klara senast 2026.

Förvaltningarna och bolagen bär själva ansvaret för att bedriva sin kontinuitets-planering utifrån ansvarsprincipen och närhetsprincipen.

I granskningens metod ingick att granska:

1. Finns dokumenterade kontinuitetsplaner?
2. Har risk för it-avbrott inkluderats i kontinuitetsplaneringen?
3. Har kritiska beroenden till informationssystem identifierats?

Vi kan genom dokumentgranskning och muntliga uppgifter konstatera att arbetet med kontinuitetsplaner är pågående men att dokumenterade kontinuitetsplaner saknas förutom i räddningsnämndens verksamhet samt verksamheterna som svarar mot omsorgsnämnden respektive äldrenämnden där vård- och omsorgsförvaltningen genomfört arbetet. Som nämnts ovan så är nuvarande kravställning att ett dokumenterat första utkast av kontinuitetshantering ska finnas senast år 2026.

Då dokumenterade kontinuitetsplaner i stort saknas i nuläget så blir följdeffekten att risk för it-avbrott inte har inkluderats samt att kritiska beroenden till informationssystem inte har identifierats.

Det ska dock samtidigt förtydligas att vi från samtliga intervjuer med verksamhets-representanter har fått både muntliga redogörelser och vissa underlag som ger oss en bild att risk för it-avbrott ingår i de analyser och det arbete som pågår. Samtliga representanter har därtill kunnat redogöra för vilka system som de har ett kritiskt beroende till och därigenom höga krav om tillgänglighet för, så att verksamheten ska kunna fungera på en acceptabel nivå även om det skulle bli ett it-avbrott. Dock lyfter vissa intervjuade att det saknas beslut eller inriktning över hur långt avbrott

verksamheterna ska planera för vilket kan påverka behovet av planering och rutiner kopplat till åtgärder.

4.1.2 Bedömning

Vi bedömer att omsorgsnämnden, räddningsnämnden och äldrenämndens berörda verksamheter har dokumenterade kontinuitetsplaner med en tydlig koppling till risk- och sårbarhetsanalys.

De tre nämnderna har sedan tidigare arbetat fram kontinuitetsplaner som föregår den nu pågående mer koncerngemensamma processen, men det finns en tydlig koppling till de risker och sårbarheter som identifieras inom ramen för risk- och sårbarhetsanalysen. Vi ser det därigenom som väsentligt att nämndernas verksamheter håller sin planering uppdaterad och vid behov reviderar planeringen i förhållande till kommunens gemensamma metodik och mallar samt med grund i uppdaterade behov och analyser.

Vi bedömer att kommunstyrelsen, plan- och byggnadsnämnden, gatu- och samhällsmiljönämnden, socialnämnden, utbildningsnämnden och Uppsala Vatten och Avfall AB inte har dokumenterade kontinuitetsplaner med en tydlig koppling till genomförd risk- och sårbarhetsanalys.

Vi kan konstatera att nämnderna och styrelserna har kommit olika långt i planeringen utifrån målet att färdiga utkast av kontinuitetshanteringen ska finnas senast 2026. Även inom en och samma nämnd eller styrelse förekommer skillnader, där vissa verksamheter har kommit långt medan andra är i en tidigare fas. Gemensamt för samtliga nämnder och bolag ovan är dock att det i nuläget saknas dokumenterade kontinuitetsplaner för samtliga berörda verksamheter. Vår bedömning är att kontinuitetsplanering är en väsentlig del i att säkerställa att en verksamhet kan hantera en störning, oavsett typ av störning. Det är därför väsentligt att planeringen slutförs, senast enligt utstakad tidsplan men vi vill samtidigt framhålla att vi mot bakgrund av den hotbild som råder rekommenderar att prioritera planeringen för it-avbrott för att minska konsekvenserna vid en sådan händelse.

Vi bedömer att kritiska beroenden till informationssystem har beaktats i kontinuitetsplaneringen och att åtgärder har identifierats och hanterats inom omsorgsnämnden, räddningsnämnden och äldrenämnden.

Vår bedömning baseras på att det har funnits en tydlig process för att identifiera risker och åtgärdsbehov i arbetet med risk- och sårbarhetsanalys och kontinuitetsplanering som hanterats genom att dokumentera och medvetandegöra alternativa arbetsrutiner och planer för hantering. Avseende räddningsnämnden bedömer vi dock att det är väsentligt att informationsklassningar genomförs för samtliga kritiska system för att framgent kunna identifiera och hantera ytterligare relevanta åtgärder.

Vi bedömer däremot att kommunstyrelsen, plan- och byggnadsnämnden, gatu- och samhällsmiljönämnden, socialnämnden, utbildningsnämnden och styrelsen för Uppsala Vatten och Avfall AB:s verksamheter inte har beaktat kritiska beroenden till informationssystem i kontinuitetsplaneringen och att åtgärder inte har identifierats och hanterats i tillräcklig utsträckning.

Vår bedömning grundar sig i att det saknas dokumenterade kontinuitetsplaner. Vi kan dock konstatera kritiska beroenden till informationssystem ingår i det pågående arbetet inom samtliga nämnder och styrelser.

4.2 Analys och bedömningar av krav på tillgänglighet för kritiska informationssystem

4.2.1 Bedömning av behov och åtgärder för att ha redundans vid it-avbrott

Det finns olika sätt att göra analyser och bedömningar för att fastställa krav om tillgänglighet för att anpassa säkerhetsåtgärder och identifiera behov av reservrutiner. Ett vedertaget arbetssätt som rekommenderas av Myndigheten för samhällsskydd och beredskap samt regleras i lagkrav för verksamheter som identifieras som samhällsviktiga och digitala tjänster och därigenom står under NIS-direktivets krav är att göra informationsklassningar och riskanalyser för informationstillgångar som nyttjas.

Vi har i granskningen fått uppgift om att det finns ett etablerat arbete med informationsklassning sedan flera år i kommunen. Detta genomförs inom ramen för PM3-modellen[15]. För varje objekt (samling av system) utses en objektledare it respektive objektledare verksamhet med en ansvars- och uppgiftsfördelning. Informationsklassningen sker med stöd i kommunens vägledning för informationssäkerhetsklassning[16]

Enligt intervjuer ska informationsklassning alltid ske i samband med upphandling av nya system och årligen för befintliga system. Till stöd för den årliga uppdateringen finns en instruktion kring vad som behöver genomföras [17]. Utifrån genomförd informationsklassning arbetar IT-staben vidare med de tekniska åtgärder som det finns behov av och gör samtidigt en prioritering av systemet internt i jämförelse med andra system. För system som har extern drift så bistår IT-staben med kravställning mot leverantören i form av SLA (service level agreement) som bland annat reglerar acceptabla avbrottstider, tider för felavhjälpning, eskaleringsvägar mm. Vid intern drift så används inte formella SLA mellan verksamhet och IT-staben, utan är mer av informell karaktär och baseras på underlagen i klassningen och den prioritering som gjorts.

[15] Vedertagen styr- och samverkansmodell för förvaltning av system och applikationer.
[16] Beslutad av CIO 2021-05-17
[17] Instruktioner för Excelarket för årshjulet för säkra it-leveranser, beslutad av CISO

Verksamheten har i ansvar att omhänderta de åtgärder som det identifieras behov av i informationsklassningen som har bäring på verksamhetens rutiner för alternativa arbetssätt vid exempelvis avbrott i systemet.

I intervjuer med den verksamhet som aktivt arbetat med kontinuitetsplanering (vård- och omsorgsförvaltningen) beskrivs att kontinuitetsplanering både fungerar som en ingång i och ett resultat av informationsklassningen. Objektledare från verksamheten tar med sig befintliga identifierade risker och åtgärder från verksamhetens planering in i informationsklassningen för att kunna kommunicera nuläge, risker och behov. Utifrån resultatet av klassningen sammanställs behovet av åtgärder i en gemensam handlingsplan mellan it och verksamheten, i handlingsplanen är vissa av åtgärderna kopplade direkt mot tekniska åtgärder som IT-staben förväntas åtgärda enligt ovan, medan vissa av åtgärderna i handlingsplanen kräver åtgärder i verksamheten. Verksamhetens åtgärder blir en del av att vid behov justera kontinuitetsplaner och tillhörande verksamhetsrutiner.

Detta arbetssätt är enligt intervju den tilltänkta processen för hur verksamheterna tillvaratar informationsklassningen utifrån vår intervju med representanter från IT-staben. Som framgår av tabellen och tillhörande kommentarer nedan är dock inte det tilltänkta arbetssättet fullt ut etablerat i en huvudsak av de berörda verksamheterna. Till stor del beror det på att kontinuitetsplaneringen kopplat mot it-avbrott inte är så pass genomarbetad att det på ett systematiskt går att använda sig av underlaget som en ingång för verksamhetsrepresentanten i informationsklassningen eller tillvarata de åtgärder informationsklassningen renderar i.

Värt att notera är även att verksamheter lyfter att de i sina analyser även identifierat kritiska beroenden till system som de inte själva är ansvariga för, och därigenom inte kan ta ansvar för analys och bedömningar samt tillhörande åtgärder. Exempel som lyfts är kommunövergripande system som ekonomisystem och hr-system där utsedda roller i objektsförvaltningen enligt PM3 bemannas från andra verksamheter inom kommunen.

En annan aspekt som behöver lyftas fram utifrån informationsklassning är att givet att verksamheterna i huvudsak befinner sig i en tidig fas i arbetet med kontinuitetsplanering så kan det finns behov av att omvärdera risker och behov för aspekten tillgänglighet när kontinuitetsarbetet kommit längre mot bakgrund av nya identifierade kritiska beroenden med tillhörande åtgärder.

4.2.2 Presentation av resultat från granskning av kritiska system

Vi redogör översiktligt i tabell på nästa sida de iakttagelser vi gjort avseende analyser och åtgärder för de kritiska systemen med högst behov av tillgänglighet inom respektive verksamhet. En kort förklaring till de bedömningar som redovisas följer nedan.

Aktuell informationsklassning finns
För att få ett ja i kolumnen som redogör för om det finns en *aktuell informationsklassning* så ska uppdatering ha skett årligen, i enlighet med kommunens interna rutin som anger krav på detta. För att få ett ja krävs att informationsklassning har skett för samtliga kritiska system.

Åtgärder har vidtagits utifrån klassning

Bedömningen i kolumnen baseras på intervjuuppgifter där vi har fått beskrivet att det utifrån det tekniska perspektivet och IT-stabens arbete i huvudsak vidtas åtgärder kopplat till resultat i informationsklassningar. I bedömningen har vi tagit i beaktande huruvida verksamheterna har kunnat redogöra för vilka åtgärder man kravställt eller åtgärder som verksamheten själva tagit ansvar för att vidta. Vi har även efterfrågat om det har skett en uppföljning av att åtgärder genomförts. Vi har inte kunnat verifiera detta i tillräcklig grad vilket påverkat bedömningen. Följaktligen har flertalet av nämnderna/bolaget bedömts *delvis* i de fall tekniska åtgärder vidtagits, men åtgärder i verksamhetens rutiner inte vidtagits.

SLA eller motsvarande underlag finns

För bedömningen om *SLA eller motsvarande finns* har vi för de verksamheter som enbart har system där driften finns hos kommunens IT-stab gjort bedömningen att de underlag och den prioritering som görs utifrån klassning är likvärdig de SLA som avtalas med externa leverantörer.

Ansvarig	Aktuell informations-klassning finns	Åtgärder har vidtagits utifrån klassning	SLA eller motsvarande underlag finns
Kommunstyrelsen	Delvis	Delvis	Ja
Omsorgsnämnden	Ja	Ja	Ja
Plan- och byggnadsnämnden	Ja	Delvis	Ja
Gatu- och samhälls-miljönämnden[18]			
Räddningsnämnden	Nej	Nej	Nej
Socialnämnden	Ja	Nej	Ja
Utbildningsnämnden	Ja	Delvis	Ja
Äldrenämnden	Ja	Ja	Ja

[18] Gatu- och samhällsmiljönämndens system är i uppstartsfas och bedömning går inte att göra då objektet inte har gått in i förvaltningsfas än. Vi har delgivits information om att verksamheten kommer att vara en del av objektet inom ramen för PM3-modellen som också omfattar andra verksamheter.

Uppsala Vatten och Avfall AB	Ja	Delvis	Nej

4.2.3 Bedömning

Vi bedömer att det finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem inom kommunstyrelsen, omsorgsnämnden, plan- och byggnadsnämnden, socialnämnden, utbildningsnämnden och äldrenämndens verksamheter.

Bedömningen baseras på att styrelsen och nämndernas verksamhetskritiska informationssystem har en aktuell informationsklassning och en kravställning i form av SLA som bygger på informationsklassningen mot extern leverantör, alternativt har kravställt exempelvis återställningstider och behov av tillgänglighet mot intern it i kommunen.

Vi bedömer att det inte går att bedöma om det finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem inom gatu- och samhällsmiljönämnden.

Vi kan dock konstatera att ambitionen är att objektledare verksamhet ska delta i objektet inom ramen för PM3-modellen för att säkerställa kravställning och ändamålsenliga åtgärder utifrån behov.

Vi bedömer att det inte finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem inom räddningsnämnden och Uppsala Vatten och Avfall AB.

Bedömningen avseende räddningsnämnden baseras på att det saknas aktuell informationsklassning samt SLA för samtliga kritiska system. Bedömningen avseende Uppsala Vatten och Avfall AB baseras på att det i nuläget saknas intern it-beredskap vilket innebär att även om behov av detta identifieras så saknas organisatoriska förutsättningar. I nuläget är detta beroende av en intern bedömning av alltför hög kostnad i förhållande till behovet av att ha ökad beredskap.

4.3 Övning

Det har inte genomförts någon övning utifrån scenariot för kritisk it-säkerhetshändelse eller it-avbrott på koncern- eller kommunövergripande nivå. En anledning som lyfts i intervjuer är det faktum att dokumenterade kontinuitetsplaner ännu saknas varpå övningar inte skulle kunna utvärdera etablerad planering. Flertalet förvaltningar och bolag har uttryckt i intervju att man ser ett behov av att genomföra och/eller har planerat in en övning utifrån scenariot it-avbrott. Den generella hållningen har varit att kontinuitetsplaneringen behöver komma längre innan ställningstagande kan göras kring hur en sådan övning skulle kunna arrangeras i egen regi hos förvaltning eller bolag.

En övning har genomförts under 2023 för krisledningsnämnden kopplat till risken för it-avbrott. Fokus för övningen var hanteringen på den politiska nivån, där även diskussioner om prioritering av samhällsviktiga verksamheter utifrån informationssystem berördes.

De nämnder och bolag vars förvaltningar som i någon form har genomfört en övning på scenariot it-avbrott är kommunstyrelsen, Uppsala Vatten och Avfall AB, utbildningsnämnden, omsorgsnämnden och äldrenämnden. Inom kommunstyrelsen har övningar skett på verksamhetsnivå, exempelvis inom ekonomi kopplat till avbrott i ekonomisystemet. För Uppsala Vatten och Avfall AB genomfördes senaste övningen utifrån scenariot 2019. Inom utbildningsförvaltningen genomfördes en övning inom skolområde gymnasium. För omsorgsnämnden och äldrenämndens verksamheter har också övningar i olika konstellationer genomförts på verksamhetsnivå, men inte förvaltningsövergripande.

Mot bakgrund av iakttagelser i kapitel 3 kan vi se att det generellt på förvaltnings- och bolagsnivå saknas övergripande övnings- och utbildningsplaner, varför de övningar som genomförts sker efter enskilda initiativ i verksamheterna, till exempel per verksamhetsområde eller skolform och inte som del i en övergripande planering och prioritering av övningar för olika målgrupper.

4.3.1 Bedömning

Vi bedömer att omsorgsnämnden och äldrenämnden delvis genomfört övningar i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

Vår bedömning baseras på att nämnderna har kontinuitetsplaner som kan utgöra grund för övningar på scenariot it-avbrott. Vi kan dock inte se en tydlig systematik utifrån en förvaltningsövergripande styrning av utbildnings- och övningsarbetet.

Vi bedömer att det finns ett behov av en förvaltningsövergripande inriktning och styrning av utbildning och övning för att tillse att det finns en systematik i arbetet och ett stöd i hur scenariot kan it-avbrott bör övas och hur erfarenheter kan tillvaratas i ett bredare perspektiv utifrån kontinuitetsplaneringen. Vi ser mot bakgrund av detta positivt på kommunledningskontoret pågående arbete med att bistå med stöd i hur behov av utbildning kan inventeras och utvärderas är nödvändigt för att stärka systematiken och erfarenhetsåterföringen, särskilt mot bakgrund av att risken för it-avbrott utgör en väsentlig risk som bör övas inom många nämnder och styrelser.

Vi bedömer att kommunstyrelsen, plan- och byggnadsnämnden, gatu- och samhällsmiljönämnden, socialnämnden, Uppsala Vatten och Avfall AB utbildningsnämnden och räddningsnämnden inte genomfört övning i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

Vi ser det som väsentligt att pågående kontinuitetsarbete fortgår i enlighet med mål om att detta ska vara färdigställt under 2026 så att övningar för att utvärdera planeringen därefter kan genomföras.

4.4 Intern kontroll

Enligt reglemente för intern kontroll[19] ska kommunstyrelsen utforma den interna kontrollen på kommunövergripande nivå. Kommunstyrelsen kan rekommendera eller besluta om obligatoriska kontrollmoment för enskilda, flera eller samtliga nämnder och bolagsstyrelser att hantera i sina respektive internkontrollplaner. För året finns två obligatoriska kontrollmoment för samtliga nämnder och bolag med bäring på risken för it-avbrott.

Vi kan i granskningen konstatera att samtliga nämnder och bolag har med de obligatoriska kontrollmomenten i sina respektive internkontrollplaner. Vi kan samtidigt konstatera att ingen uppföljning av internkontroll hade genomförts vid tid för granskningen. Samma två kontrollmoment fanns med i samtliga berörda nämnder och bolags internkontrollarbete för 2023. Vid protokollgranskning kan vi utläsa att samtliga berörda nämnder och bolag har följt upp utifrån kontrollmomenten.

Som vi tidigare konstaterat så sker även en uppföljning av krisberedskapsarbetet med tillhörande kontinuitetsplanering i den ordinarie styrkedjan med uppföljning vid delår och årsbokslut i respektive nämnd och sammanställt till kommunstyrelsen utifrån uppdrag 35 i mål och budget.

4.4.1 Bedömning

Vi bedömer att det inom samtliga nämnder och styrelser finns en i allt väsentligt tillräcklig intern kontroll som följer upp verksamheternas status för att säkerställa att kontinuitetsplaneringen fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar.

Samtidigt konstaterar vi att planeringen i många delar inte är färdigställd, vilket även har redovisats i den interna kontrollen för berörda nämnder och styrelser. Vi bedömer att en viktig kontrollmetod för styrelser och nämnder i att säkerställa en tillräcklig planering är att planeringen övas, vilket i mycket begränsad utsträckning har genomförts.

[19] Beslutad av kommunfullmäktige 2022-02-28

5 Samlad bedömning och rekommendationer

Granskningen syftade till att bedöma om kommunkoncernen bedriver ett sammanhållet och ändamålsenligt krisberedskapsarbete med särskilt fokus på kontinuitet vid kritiska it-säkerhetshändelser.

Vår samlade bedömning utifrån granskningens syfte är att kommunkoncernens krisberedskapsarbete i allt väsentligt bedrivs på ett sammanhållet och ändamålsenligt vis.

Vår samlade bedömning av arbetet kopplat till kontinuitetsplanering vid kritiska it-säkerhetshändelser är att kommunkoncernen delvis bedriver ett sammanhållet och ändamålsenligt arbete.

Vi konstaterar dock att arbetet i hög grad är pågående och att dokumenterade kontinuitetsplaner endast finns för tre av nämnderna som ingår i granskningen. Nuvarande kravställning är dock att samtliga samhällsviktiga verksamheter senast år 2026 ska ha dokumenterade kontinuitetsplaner tillgängliga.

Se inledning samt respektive rapportkapitel för en mer detaljerad beskrivning.

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen att:

- Säkerställa att val av ledamöter till krisledningsnämnden förrättas av kommunfullmäktige
- Föreslå kommunfullmäktige att revidera reglementet för krisledningsnämnden där krisledningsnämndens roll i förhållande till gemensamma nämnder tydliggörs.
- Följ upp arbetet med kontinuitetsplanering i koncernens nämnder och styrelser
- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna slutförs och att planeringen beaktar risken för it-avbrott på verksamhetskritiska system
- Tillse att arbetet med att ta fram vägledningar och stöd för hur arbetet med utbildning och övningar ska bedrivas slutförs
- Särskilt följa upp att arbetet med utbildning och övning sker enligt tilltänkt systematik i nämnder och bolag
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig

Utifrån våra iakttagelser och bedömningar rekommenderar vi plan- och byggnadsnämnden samt gatu- och samhällsmiljönämnden att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna genomförs och att planeringen beaktar risken för it-avbrott för verksamhetskritiska system
- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi omsorgsnämnden och äldrenämnden att:

- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi räddningsnämnden att:

- Tillse att SLA finns för samtliga kritiska verksamhetssystem
- Tillse att informationsklassning sker årligen i enlighet med vad som anges i styrande dokument
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi socialnämnden att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna slutförs och att planeringen beaktar risken för it-avbrott för verksamhetskritiska system.
- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig

- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi utbildningsnämnden att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna slutförs och att planeringen beaktar risken för it-avbrott för verksamhetskritiska system
- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi Uppsala Kommun Skolfastigheter AB att:

- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur

Utifrån våra iakttagelser och bedömningar rekommenderar vi Uppsala Arenor och Fastigheter AB att:

- Säkerställ att aktuell ledningsplan finns beslutad
- Säkerställ att aktuell inventering av risker och sårbarheter, motsvarande risk- och sårbarhetsanalys, finns framtagen
- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur
- Säkerställ att uppdrag 35 i kommunens mål och budget följs upp inom ramen för verksamhetsplan

Utifrån våra iakttagelser och bedömningar rekommenderar vi Uppsala Vatten och Avfall AB att:

- Tillse att arbetet med kontinuitetsplanering i de egna verksamheterna slutförs och att planeringen beaktar risken för it-avbrott på verksamhetskritiska system

- Tillse att SLA eller motsvarande it-beredskap etableras och ställs i relation till de behov som identifieras gällande tillgänglighetsaspekten
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur.

Utifrån våra iakttagelser och bedömningar rekommenderar vi Uppsalahem AB att:

- Tillse att arbetet med utbildning och övning sker i tillräcklig omfattning utifrån inventering av behov
- Tillse att övningar och utbildningar utvärderas och att erfarenheter tillvaratas i enlighet med tilltänkt koncernövergripande struktur.

Datum som ovan

KPMG AB

Jenny Thörn	Simon Homander	Alfred Tilly
Verksamhetsrevisor	*Verksamhetsrevisor*	*Verksamhetsrevisor*