Socialnämnden
Socialförvaltningen
Kvalitetsenheten
Johanna Lood

Datum
2023-11-22

Diarienummer
SOCN/2023:99

Handlingsnummer
2023:4351

Socialnämnden

Svar på kommunrevisionens granskning av kontinuitetsplanering avseende IT-avbrott

Förslag till beslut

Socialförvaltningens förslag antas som socialnämndens svar på kommunrevisionens granskning av kontinuitetsplanering av IT-avbrott.

Ärendebeskrivning

Revisionen har haft i uppdrag att granska kommunens kontinuitetsplanering i händelse av it-avbrott. Revisionens sammanfattande bedömning är att kommunstyrelsen och de nämnder som ingår i granskningen inte har tillsett en tillräckning styrning och uppföljning av kontinuitetsplaneringen. Revisionen ser därigenom en risk att de underlag som i nuläget finns tillgängliga inte skulle vara tillräckliga som planering i händelse av it-avbrott.

Socialnämnden har fått möjlighet att yttra sig kring revisionens granskning av kommunens kontinuitetsplanering. Granskningen har resulterat i flera rekommendationer som socialnämnden ska yttra sig kring senast 31 december 2023. Revisionens rekommendationer till nämnden är:

- Tillse att det finns dokumenterade kontinuitetsplaner för samhällsviktig verksamhet och att dessa inkluderar planering vid it-avbrott
- Säkerställ att övningar genomförs för att testa verksamheternas kontinuitetsplaner och rutiner.
- Stärka uppföljningen, antingen genom internkontroll eller annat systematiskt arbetssätt, för att säkerställa att kontinuitetsplaner finns framtagna för samtliga samhällsviktiga verksamheter.

Socialförvaltningens förslag till yttrande

Socialtjänsten är en samhällsviktig verksamhet som har till uppgift att upprätthålla samhällets stöd och hjälp till människor som är långvarigt utsatta eller i mer tillfälliga svårigheter, och ska säkerställa människors ekonomiska och sociala trygghet, jämlikhet i levnadsvillkor och aktiva deltagande i samhällslivet.[1] Utvecklingen i samhället gör att det är än mer viktigt att säkerställa att nämnden har möjlighet att upprätthålla en social

[1] https://www.msb.se/sv/publikationer/identifiering-av-samhallsviktig-verksamhet--lista-med-viktiga-samhallsfunktioner/

service till medborgare som har behov av socialtjänsten. Samtidigt pågår en digital transformation inom nämndens verksamheter för att på sikt kunna bli en alltmer datadriven socialtjänst. Detta gör att det ställs högre krav på att det finns en tydlig förvaltningsorganisation för IT-system och digitala stöd i kommunen. Socialförvaltningen anser därför att det behöver etableras en tydligare förvaltningsorganisation, där det blir tydligt vilket stöd som nämndens verksamheter kan få av kommunledningskontoret och serviceförvaltningen i arbetet med bland annat kontinuitetsplanering. Sedan konsolideringen av administrativt stöd genomfördes har detta inte blivit tydliggjort.

Socialförvaltningen har inga invändningar mot de rekommendationer som följer med granskningen, rekommendationerna är både rimliga och relevanta. Socialförvaltningen har tillsammans med kommunledningskontoret gjort en risk- och sårbarhetsanalys under 2023 och behöver arbeta vidare med de identifierade sårbarheterna. Förvaltningens objektledare önskar att samarbeta och få stöd i arbetet av kommunledningskontoret och serviceförvaltningen för att upprätta behövliga kontinuitetsplaner och därefter kunna genomföra övningar. Socialförvaltningen tar till sig av rekommendationen gällande att stärka uppföljningar för att säkerställa att kontinuitetsplaner finns framtagna.

SOCIALFÖRVALTNINGEN

Elisabeth Kántor
Förvaltningschef

———

Beslutet skickas till:
Kommunrevisionen
Kommunstyrelsen

Eskilstuna kommun

Kommunrevisionen

Till:
Kommunstyrelsen, servicenämnden, socialnämnden, vård- och omsorgsnämnden, arbetsmarknads- och vuxenutbildningsnämnden

För kännedom:
Kommunfullmäktige

Revisorernas granskning av kontinuitetsplanering avseende it-avbrott

Vi har med stöd av KPMG genomfört en granskning av kommunens kontinuitetsplanering i händelse av it-avbrott.

Kontinuitetshantering/planering handlar om att systematiskt skapa en förmåga att fortsätta bedriva sin verksamhet på en tolerabel nivå, oavsett vilken typ av störning som organisationen utsätts för. Målet är att organisationen ska ha en förmåga att hantera störningar och avbrott i verksamheten så att dessa får en så liten påverkan som möjligt på verksamheten. Kontinuitetshantering/planering är därtill en fortlöpande process och ska säkerställa att återkommande arbete med krisberedskap sker inom respektive verksamhet. I vår riskanalys har vi bedömt att det kan finnas risk för brister inom ovan nämnda områden.

Vår övergripande bedömning är att kommunstyrelsen och de nämnder som ingått i granskningen inte har tillsett en tillräcklig styrning och uppföljning av kontinuitetsplanering. Vi ser därigenom en risk att de underlag som i nuläget finns tillgängliga inte skulle vara tillräckliga som planering i händelse av it-avbrott.

Ansvar och processen för risk- och sårbarhetsanalys inklusive kontinuitetsplanering är tydliggjord genom styrande dokument men de aktiviteter som det ställs krav om har inte genomförts. Det saknas därför i stora delar underlag i form av riskanalyser, åtgärder samt kontinuitetsplanering i händelse av it-avbrott. Verksamheternas kontinuitet vid it-avbrott har inte beaktats i tillräcklig utsträckning vare sig i risk- och sårbarhetsanalyser eller i tillhörande kontinuitetsplanering. Vi bedömer att både kommunstyrelsen och nämnderna brustit i sitt ansvar då de inte har säkerställt att kontinuitetsplaner finns för kommunens samhällsviktiga verksamheter i enlighet med kommunens egna styrdokument och MSB:s föreskrifter. Vi bedömer att detta är förenat med risker, så som att samhällsviktiga verksamheter inte kan upprätthållas till en tillfredsställande nivå vid it-avbrott.

Vår granskning har samtidigt visat att kommunen i sitt pågående arbete med risk- och sårbarhetsanalys har gjort förstärkningar med stödresurser som bistår som processledare i verksamheternas arbete. I den tydliggjorda processen ingår att utifrån risk- och sårbarhetsanalyser fortsätta processen med en tillhörande kontinuitetsplanering. Förutsatt att den nya processen förankras i kommunens samtliga verksamheter och arbetet slutförs finns förutsättningar att kontinuitetsplaneringen kan stärkas.

Utifrån vår granskning rekommenderar vi kommunstyrelsen, i deras övergripande ansvar, att:

- Tillse att styrande dokument med bäring på krisberedskapsarbetet är förankrade i kommunens verksamheter
- Stärka uppföljning eller kontroll att de styrande dokumenten efterlevs avseende processen för risk- och sårbarhetsanalyser med tillhörande kontinuitetsplanering

Vi rekommenderar vidare kommunstyrelsen och nämnderna att:

- Tillse att det finns dokumenterade kontinuitetsplaner för samhällsviktig verksamhet och att dessa inkluderar planering vid it-avbrott
- Säkerställ att övningar genomförs för att testa verksamheternas kontinuitetsplaner och rutiner.
- Stärka uppföljningen, antingen genom internkontroll eller annat systematiskt arbetssätt, för att säkerställa att kontinuitetsplaner finns framtagna för samtliga samhällsviktiga verksamheter.

Granskningens samlade resultat presenteras i bifogad rapport.

Utöver det rapporten redovisar vill vi från kommunrevisionen även påtala vikten av att kommunstyrelsen tydliggör krav för kontinuitetsplanering eller motsvarande underlag i syfte att kunna hantera avbrott och störningar även för verksamheter som inte är identifierade som samhällsviktiga. Dessutom påpekar vi vikten av att ge kommunledningskontoret i uppdrag att utvärdera hur samordning inom koncernen kan ske för att fånga kritiska beroenden mellan verksamheter inom kommunen samt mellan kommunen och de kommunala bolagen.

Vi emotser kommunstyrelsens och granskade nämnders yttrande till våra iakttagelser och rekommendationer i bifogad rapport **senast 2023-12-31.**

Eskilstuna 2023-09-04

För revisorerna i Eskilstuna kommun

Tommy Kvarsell
Ordförande

Majvor Gyllhamn
Vice ordförande

Granskning av kontinuitetsplanering avseende it-avbrott

Revisionsrapport

Eskilstuna kommun

KPMG AB

2023-06-14

Antal sidor: 13

Eskilstuna kommun
Granskning av kontinuitetsplanering avseende it-avbrott

2023-06-14

Innehållsförteckning

Eskilstuna kommun
Granskning av kontinuitetsplanering avseende it-avbrott

2023-06-14

1 Sammanfattning

KPMG har av Eskilstuna kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunens kontinuitetsplanering i händelse av it-avbrott. Uppdraget ingår i revisionsplanen för år 2023.

Vår sammanfattande bedömning är att kommunstyrelsen och de nämnder som ingår i granskningen inte har tillsett en tillräckning styrning och uppföljning av kontinuitetsplaneringen. Vi ser därigenom en risk att de underlag som i nuläget finns tillgängliga inte skulle vara tillräckliga som planering i händelse av it-avbrott.

1.1 Revisionsfrågor och bedömningar

Revisionsfråga	Bedömning: Ja	Rekommendationer
Är organisation och ansvarsfördelning tydlig avseende kontinuitetsplanering inom respektive verksamhet?	Organisation- och ansvarsfördelning är tydliggjord i styrande dokument. Upprättande av kontinuitetsplaner tillhör verksamhetsansvaret och vi uppfattar att ansvaret är känt och etablerat.	-
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Har kommunstyrelsen etablerat arbetssätt och en tydlig process för arbetet med den kommunövergripande risk- och sårbarhetsanalysen?	Processen för risk- och sårbarhetsanalys inklusive kontinuitetsplanering är tydliggjord genom styrande dokument. Dock är inte styrande dokument tillräckligt förankrade i kommunens verksamheter så att de krav som ställs efterlevs.	Vi rekommenderar att kommunstyrelsen tillser att styrdokument förankras i samtliga verksamheter. Vi rekommenderar kommunstyrelsen att stärka uppföljning eller kontroll att de styrande dokumenten efterlevs avseende processen för risk- och sårbarhetsanalyser med tillhörande kontinuitetsplanering.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Har nämnder fastställt kontinuitetsplaner och är dessa tillräckliga som underlag i händelse av störning eller avbrott?	Våra stickprov visar att kontinuitetsplaner saknas. Vår bedömning är att de underlag som i nuläget finns inte skulle vara tillräckliga som planering i händelse av it-avbrott.	Vi rekommenderar kommunstyrelsen och nämnderna att tillse att det finns dokumenterade kontinuitetsplaner för samhällsviktig verksamhet och att dessa inkluderar planering vid it-avbrott.

Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Har nämndernas kontinuitetsplaner en tydlig koppling till genomförd risk- och sårbarhetsanalys?	Den risk- och sårbarhetsanalys som är gällande (från 2019) har inte utgjort underlag för verksamheternas kontinuitetsplanering.	Vi rekommenderar kommunstyrelsen och nämnderna att tillse att den pågående processen med risk- och sårbarhetsanalyser slutförs och inkluderar kontinuitetsplanering.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Har övning och tester genomförts för att kontrollera att planerna fungerar ändamålsenligt i händelse av störning eller avbrott?	Det har inte genomförts några tester eller övningar för att se att de underlag som finns skulle fungera ändamålsenligt i händelse av it-avbrott.	Vi rekommenderar kommunstyrelsen och nämnderna att säkerställa att övningar genomförs för att testa verksamheternas kontinuitetsplaner och rutiner med regelbundenhet.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Har styrelser och nämnder ett systematiskt arbetssätt genom internkontroll eller annan uppföljning att nödvändiga kontinuitetsplaner samt rutiner för att upprätthålla verksamhet finns och är aktuella?	Vi bedömer att kommunstyrelsen och nämnderna har brustit i sitt ansvar då ingen uppföljning eller kontroll har gjorts över att det för kommunens samhällsviktiga verksamheter finns kontinuitetsplaner i enlighet med krav i styrdokument och MSB:s föreskrifter. Vår bedömning är att det därigenom finns risk att verksamheter inte skulle kunna upprätthållas utan allvarlig påverkan eller på en tillräcklig nivå i händelse av it-avbrott.	Vi rekommenderar kommunstyrelsen och nämnderna att stärka uppföljningen, antingen genom internkontroll eller annat systematiskt arbetssätt, för att säkerställa att kontinuitetsplaner finns framtagna för samtliga samhällsviktiga verksamheter. Därtill bör uppföljning och kontroll inkludera att tester genomförs i enlighet med ovan lämnade rekommendation.

2 Bakgrund

KPMG har av Eskilstuna kommuns förtroendevalda revisorer och lekmannarevisorer fått i uppdrag att genomföra en granskning av kommunens kontinuitetsplanering i händelse av it-avbrott. Uppdraget ingår i revisionsplanen för år 2023.

Lagstiftning[1] gör gällande att kommuner är skyldiga att genomföra risk- och sårbarhetsanalyser, RSA. Arbetet med RSA ska ses som en ständigt pågående process och bör samordnas med övrigt förebyggande arbete i kommunen. Vidare ska kommuner enligt lagstiftningen se till att förtroendevalda och anställda regelbundet får den utbildning och övning som behövs för att de ska kunna lösa sina uppgifter vid extraordinära händelser.

Enligt den standard[2] som finns på området handlar kontinuitetshantering/planering om att systematiskt skapa en förmåga att fortsätta bedriva sin verksamhet på en tolerabel nivå, oavsett vilken typ av störning som organisationen utsätts för. Målet är att organisationen ska ha en förmåga att hantera störningar och avbrott i verksamheten så att dessa får en så liten påverkan som möjligt på verksamheten.

Eskilstuna kommun har en beslutad Plan för krisberedskap 2020–2023. Planen gäller för samtliga nämnder och bolag. I den framgår att RSA är en fortlöpande process och det fortsatta arbetet med kontinuitetsplaneringen ska säkerställa ett återkommande arbete med krisberedskap inom respektive verksamhet. Ett av målen är att ta fram kontinuitetsplaner för samhällsviktig verksamhet. I Eskilstuna kommun finns även en beslutad Plan för hantering av händelser, allvarliga händelser och extraordinära händelser. Den gäller för samtliga nämnder och bolag och reglerar att händelser och allvarliga händelser ska hanteras enligt likhets- och ansvarsprincipen och i enlighet med beslutad kontinuitetsplan eller med andra lokala åtgärder.

I Eskilstuna kommuns riktlinjer för informationssäkerhet framgår att informationssäkerhet inom kommunkoncernen ska vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa.

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 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. För att undvika allvarlig påverkan på samhället krävs därför väl genomarbetade, förankrade och testade kontinuitetsplaner.

Med anledning av ovanstående drar kommunens revisorer och lekmannarevisorer slutsatsen i sin riskanalys, att arbetet med kontinuitetsplanering behöver granskas.

[1] 2 Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
[2] SS 22304:2014 Samhällssäkerhet – Ledningssystem för kontinuitet

2.1 Syfte och revisionsfråga

Syftet med granskningen är att bedöma om kommunstyrelsen och nämnderna har tillsett en tillräckning styrning och uppföljning av kontinuitetsplaneringen, för säkerställa att verksamheter kan upprätthållas vid begränsad tillgång till it.

Granskningen besvaras med följande revisionsfrågor:

- Är organisation och ansvarsfördelning tydlig avseende kontinuitetsplanering inom respektive verksamhet?
- Har kommunstyrelsen etablerat arbetssätt och en tydlig process för arbetet med den kommunövergripande risk- och sårbarhetsanalysen?
- Har nämnder och bolag fastställt kontinuitetsplaner och är dessa tillräckliga som underlag i händelse av störning eller avbrott?
- Har nämndernas och bolagens kontinuitetsplaner en tydlig koppling till genomförd risk- och sårbarhetsanalys?
- Har övning och tester genomförts för att kontrollera att planerna fungerar ändamålsenligt i händelse av störning eller avbrott?
- Har styrelser och nämnder ett systematiskt arbetssätt genom internkontroll eller annan uppföljning att nödvändiga kontinuitetsplaner samt rutiner för att upprätthålla verksamhet finns och är aktuella?

2.2 Avgränsning

Granskningen tar sin utgångspunkt i it-störningar som har påverkan på den dagliga verksamheten och som ställer krav på att det finns en beredskap för att kunna upprätthålla verksamheten även under onormala förhållanden. I detta fall avses it-störningar som påverkar nämndernas och bolagens förmåga att genomföra sitt uppdrag och att it-störningen får betydelse för nämndernas och bolagens relation eller leverans till medborgarna.

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

Kommunstyrelsen

- För kommunstyrelsens del har granskningen avgränsats till ledning, styrning och uppföljning av processen för risk- och sårbarhetsanalys och kontinuitetsarbetet. Det har inte skett någon granskning av kommunstyrelsens kontinuitetsplaner.

Nämnderna

- Arbetet med risk- och sårbarhetsanalys i sin helhet är inte föremål för granskningen, dock omfattar detta arbete viktiga komponenter som utgör underlag för nämndernas arbete i framtagandet av kontinuitetsplaner eller andra lokala åtgärder.
- Granskningen omfattar kontinuitetsplaner som granskade nämnder har upprättat för att säkerställa att verksamheten ska kunna bedrivas även under onormala förhållanden.

2.3 Revisionskriterier

Vi kommer att utgå från följande revisionskriterier:

- Kommunallagen 6 kap. 6 §
- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och beredskap.
- Tillämpbara interna regelverk, policys och beslut:
  - Plan för Krisberedskap 2020–2023 (KFKS/2019:193)
  - Plan för hantering av händelser, allvarliga händelser och extraordinära händelser (KSKF/2021:8)
  - Riktlinje för Informationssäkerhet (KSKF/2020:360)

2.4 Ansvarig nämnd/styrelse

Granskningen avser kommunstyrelsen, servicenämnden, socialnämnden, vård- och omsorgsnämnden samt arbetsmarknads- och vuxenutbildningsnämnden (endast verksamhet egen försörjning).

2.5 Metod

Granskningen kommer att genomföras genom dokumentstudier, stickprov och intervjuer/avstämningar med berörda tjänstemän och politiker.

Stickprov kommer att genomföras genom granskning av kontinuitetsplaner av de utvalda nämndernas verksamheter. Kontinuitetsplanerna och annat underlag kan omfattas av sekretess enligt Offentlighets- och sekretesslag (2009:400) 18 kap §13. Vi kommer således inte beskriva kontinuitetsplaner eller motsvarande underlag på detaljnivå i rapporten.

3 Resultat av granskningen

3.1 Styrning och ansvarsfördelning

I Plan för krisberedskap 2020–2023 beskrivs mål och inriktning för krisberedskapsarbetet. Det anges att kommunen ska ha god kunskap om sådana risker och sårbarheter som kan påverka den egna verksamheten; en god förmåga att bedriva verksamhet vid extraordinär händelse samt en god förmåga att vid extraordinär händelse kunna samverka med andra aktörer, gällande information och resurser.

I Plan för krisberedskap 2020–2023[3] finns beskrivning av koncernens övergripande styrning och ansvarsfördelning för arbetet med krisberedskap. Kommunen har ett verksamhetsansvar som innebär att den ansvarar för att den samhällsviktiga verksamhet som kommunen bedriver även ska fungera vid samhällsstörningar, extraordinära händelser och höjd beredskap.

Säkerhetsarbetet följer linjeansvaret vilket innebär att den som är ansvarig för en verksamhet även är ansvarig för säkerhetsarbetet inom den verksamheten. Verksamhetsansvaret inbegriper enligt planen även ansvar för att samhällsviktig verksamhet inom kommunen ska fungera tillfredsställande, även vid samhällsstörningar, extraordinär händelse och höjd beredskap. Detta innebär att även ansvar för kontinuitetsplaneringen, exempelvis över hur verksamheten ska upprätthållas vid ett allvarligare it-avbrott, åligger respektive verksamhetsansvarig.

Av planen framgår att krisberedskapsarbetet leds och samordnas av kommunledningskontoret. Intervjupersoner beskriver att säkerhetsarbetet leds av en säkerhetschef, som är underställd den administrativa direktören, vilken i sin tur rapporterar till kommundirektören. Det har skett en förstärkning av resurser för kommunens säkerhetsarbete och på kommunledningskontorets säkerhetsenhet finns i nuläget fyra personer som arbetar med beredskapsfrågor. Detta beskrivs i intervjuer ha bidragit till att kommunledningskontoret har fått bättre förutsättningar att samordna arbetet samt finnas med som processtöd i verksamheternas arbete med risk- och sårbarhetsanalyser och tillhörande kontinuitetsplanering. Det finns även en beredskapssamordnare anställd inom serviceförvaltningen som har ett nära samarbete med kommunledningskontorets tjänstepersoner.

Förutom kommunens ordinarie nämndorganisation finns enligt Plan för krisberedskap även en organisering utifrån processer. Varje område leds av en så kallad processutvecklingsgrupp (PUG) med representanter från förvaltningarna, bolagen och kommunledningen. De har som uppgift att underlätta samarbetet, utveckla arbetet inom områdena och att se till att förvaltningar och bolag arbetar mot samma mål. Det finns en särskild processutvecklingsgrupp för bland annat krisberedskap som heter ”Bedriva samhällsskydd och beredskap”. Av intervjuer framgår att ovan beskrivna PUG inte är aktiv i nuläget, dels på grund av att nyckelpersoner inom gruppen slutat, dels då en omorganisation av gruppen ska göras.

Intervjupersoner uppger att kommunen för ca fem år sedan genomförde en omorganisation. Vid denna omorganisation har funktioner som tidigare funnits lokaliserade i förvaltningarna konsoliderats centralt till serviceförvaltningen. Exempelvis

[3] Beslutad av fullmäktige. Beslutsdatum och §§ framgår ej.

hade förvaltningarna egna säkerhetssamordnare, vilka inte längre finns kvar inom respektive förvaltning. Dessa hade till viss del uppdrag inom krisberedskap och det har funnits ett glapp att ersätta dessa resurser med nya funktioner i förvaltningarna. Ett undantag är serviceförvaltningen, där ledningsgruppen prioriterat att ha en beredskapssamordnare inom förvaltningen som stöd i säkerhetsarbetet.

Intervjupersoner menar att avsaknad av säkerhetssamordnare har påverkat förutsättningarna i förvaltningarnas säkerhetsarbete. Exempelvis har vissa förvaltningar haft svårt att möta upp med resurser för olika processer som behöver genomföras, bland annat kring åtgärder för att stärka kontinuiteten samt uppföljning av det arbete som genomförts utifrån tidigare risk- och sårbarhetsanalys.

Serviceförvaltningens prioritering att ha en egen beredskapssamordnare uppges ha medfört att serviceförvaltningens verksamheter haft ett nära och tillgängligt stöd i arbetet. Detta har bidragit till att de kommit längre i sitt arbete med kontinuitetsplanering jämfört med resterande förvaltningar. Beredskapssamordnaren vid serviceförvaltningen har inom sitt uppdrag möjlighet att stötta andra förvaltningar i deras säkerhetsarbete. Stödet kan vid behov avropas av de andra förvaltningarna, exempelvis för risk- och sårbarhetsanalysarbetet.

Att förvaltningarna haft olika förutsättningar att bedriva säkerhetsarbetet har enligt intervjupersoner medfört vissa samordningssvårigheter, exempelvis för kontinuitetsplaneringen, vilket beskrivs i avsnitt 3.2.2.

Av intervjuer framgår att efterlevnad av styrande dokument inte upplevs som tillräcklig i kommunens verksamheter då dessa inte är tillräckligt förankrade. Det innebär att vissa processer och aktiviteter inte har genomförts i enlighet med de krav som ställs. Intervjupersoner menar dock att det inför det arbete som pågår 2023 med risk- och sårbarhetsanalyser har tydliggjorts vad som förväntas av respektive verksamhet samt att processtöd funnits från kommunledningskontoret vilket lyfts som positivt.

3.1.1 Bedömning

Vi bedömer att kommunstyrelsen genom styrande dokument har tillsett en tydlig organisation- och ansvarsfördelning för krisberedskapsarbetet och tillhörande kontinuitetsplanering. Vi bedömer dock att de styrande dokumenten inte är tillräckligt förankrade så att ansvar och aktiviteter i arbetet genomförts fullt ut i enlighet med de krav som ställs.

Vi ser positivt på de förstärkningar som gjorts inom kommunledningskontorets säkerhetsfunktion. Vi uppfattar att detta kan bidra till att krisberedskapsarbetet och framför allt arbetet med risk- och sårbarhetsanalyser och tillhörande kontinuitetsplanering stärks med en tydligare process och sker med större delaktighet från respektive verksamhet. Det nya arbetssättet medför därtill förutsättningar att arbetet kan samordnas på ett mer effektivt sätt.

Vi bedömer dock, baserat på konsolideringen av säkerhetsfunktioner under kommunens omorganisation, att kommunstyrelsen bör tillse att förvaltningarna har tillräckliga resurser och kompetens för att bedriva kontinuitetsplanering.

3.2 Risk- och sårbarhetsanalys samt kontinuitetsplanering

3.2.1 Process för risk- och sårbarhetsanalys

Enligt MSB:s föreskrifter för kommuners risk- och sårbarhetsanalyser[4] ska kommunen senast den 31 oktober under det första kalenderåret efter ordinarie val till kommunfullmäktige ställa samman och rapportera resultatet av sitt arbete med risk- och sårbarhetsanalys. Rapportering görs till Länsstyrelsen.

I kommunens Plan för krisberedskap 2020–2023[5] beskrivs processen för risk- och sårbarhetsanalys. Här framgår att kommunens risk- och sårbarhetsanalysarbete ska utgå från FORSA-modellen.[6] Länsstyrelsen i Södermanlands län har tagit fram en reviderad modell av FORSA, vilken kommunen använder för att ha ett gemensamt arbetssätt med andra kommuner i närområdet.

Kommunen ska använda samma struktur, bedömningsskalor och matriser som framgår av FORSA samt Myndigheten för samhällsskydds och beredskaps (MSB:s) vägledning för risk- och sårbarhetsanalys. Risk- och sårbarhetsanalyserna ska vara strukturerade enligt nedan:

- Metod
- Riskidentifiering
- Riskanalys
- Riskutvärdering
- Förmågebedömning
- Sårbarhetsanalys
- Resultat
- Fortsatt arbete

Risk- och sårbarhetsanalyser ska vara en fortlöpande process och arbetet med kontinuitetsplaneringen avser säkerställa ett återkommande arbete med krisberedskap inom samtliga verksamheter inom kommunen.

I arbetet som genomfördes med risk- och sårbarhetsanalys under 2019 beskrivs av intervjuade att arbetet i hög grad genomfördes på ledningsnivå vilket innebar att de olika verksamheterna inte var involverade i analyser och riskvärdering. Det ledde i sin tur till att krisberedskapsarbetet inte genomfördes med en tillräcklig förankring i samtliga verksamheter och de underlag som togs fram inte utgjort en operativ styrning av det fortsatta arbetet utom för vissa särskilda åtgärder.

[4] MSBFS 2015:5
[5] Beslutad av kommunfullmäktige. Beslutsdatum eller §§ framgår ej.
[6] FOI:s modell för Risk- och sårbarhetsanalyser – FORSA,

Kommunen beslutar årligen om en årsplan för krisberedskapsarbetet. Vi har tagit del av årsplan för 2023.[7] I årsplanen anges fokusområden för arbetet, i årets plan anges bland annat nedan fokusområden:

- Revidera risk- och sårbarhetsanalyser samt uppdatera kontinuitetsplaner
- Minska sårbarheter gällande informationssäkerhetsfrågor och i synnerhet cybersäkerhet

Intervjuade beskriver att det vid tiden för granskningen pågår ett arbete inom samtliga verksamheter med risk-och sårbarhetsanalyser som sedan ska sammanställas till den kommungemensamma risk- och sårbarhetsanalysen. Förvaltningarna har kommit olika långt i sitt arbete där vissa har slutfört sitt arbete medan det pågår för andra förvaltningar. Vi har tagit del av exempel och utdrag av vissa nämnders risk- och sårbarhetsanalyser. Vi konstaterar att beroenden av robust it-infrastruktur och tillgång till digitala informationssystem och information är väsentliga delar som beaktas i riskbedömning och tillhörande konsekvensbeskrivningar.

Som stöd i förvaltningarnas process med risk- och sårbarhetsanalyser deltar utsedd funktion från kommunledningskontoret som har ett uttalat ansvar för arbetet med risk- och sårbarhetsanalyser. Serviceförvaltningens beredskapssamordnare leder och samordnar säkerhetsarbetet inom serviceförvaltningen och bistår också till viss del i andra förvaltningars arbete utifrån behov.

Det stöd som tillhandahållits för risk- och sårbarhetsanalyser upplevs som positivt och beskrivs ha bidragit till att tydliggöra arbetssätt och metoder i krisberedskapsarbetet. Samtidigt beskriver intervjuade (bortsett från serviceförvaltningens verksamheter) en farhåga att de inte kommer att få det stöd som de har behov av i den fortsatta processen med åtgärder och för att upprätta uppdaterade kontinuitetsplaner. Detta mot bakgrund att det finns risk att tillgängliga resurser inte räcker till och det finns en uppfattning att de har behov av både kompetens och stöd i det operativa arbetet.

3.2.2 Risk för it-bortfall och tillhörande kontinuitetsplanering

Vi har tagit del av kommunens riskanalys och åtgärdsförslag för krisberedskap för perioden 2020–2023.[8] Underlaget innehåller bland annat information rörande kontinuitetsplaner. Det framgår att kommunens nämnder och bolag är ansvariga för att ta fram risk- och sårbarhetsanalyser samt att kontinuitetsplaner tas fram utifrån riskanalyserna. Kontinuitetsplaner ska tas fram både för förvaltningar och på kommunövergripande nivå.

I riskanalysen ingår bland annat ett scenario för cyberattack att använda som underlag i bedömningen, detta är framtaget av Länsstyrelsen.

I riskbedömningen ingår identifierade risker med koppling till it-avbrott:

- Störning eller avbrott av tele/IT, störningar i telefoni, IT, störningar i verksamhetssystem
- Cyberattack

[7] Beslutad av fullmäktige 2022-11-10 2022.
[8] Fastställd av kommunledningen 2019-09-18.

Av dokumentet framgår dock att scenariot endast bedömts på övergripande kommunnivå och intervjupersoner menar att det i den kommunövergripande risk- och sårbarhetsanalysen inte inkluderats. Det saknas enligt uppgift en övergripande kontinuitetsplanering.

De åtgärder som det bedömdes finnas behov av för att möta risker har enligt intervjuade i olika grad hanterats. Intervjuades uppfattning är dock att de åtgärder som genomförts främst har berört andra områden än it-avbrott och cyberattack. Exempel som lyfts är reservkraft och livsmedelsförsörjning.

3.2.2.1 Stickprov

Som del i metoden för granskningen har stickprov ingått. Stickproven var tänkta att genomföras genom en bedömning av ett antal inhämtade kontinuitetsplaner från respektive nämnd för att bedöma följande:

1. Har it-avbrott eller cyberattack inkluderats som händelse/scenario i nämndens risk- och sårbarhetsanalys?
2. Har it-avbrott eller cyberattack som händelse/scenario inkluderats i kontinuitetsplaneringen?
3. Innehåller kontinuitetsplanen i tillräcklig grad beskrivningar och en planering för hur verksamheten ska upprätthållas i händelse av it-avbrott eller cyberattack?
4. Har aktuella kontinuitetsplaner testats för att utvärdera om de skulle vara tillräckliga i händelse av it-avbrott eller om det finns behov av att utveckla och komplettera dessa?

Eftersom vissa underlag inom krisberedskapsarbetet är belagda med sekretess eller kan innehålla information som om den publiceras, skulle utgöra en sårbarhet för kommunen, så beskrivs inte kontinuitetsplaner eller motsvarande underlag på detaljnivå i rapporten.

Vi har tagit del av exempel på underlag som finns inom de olika verksamheter som ingår i granskningens avgränsning. Det är endast två av dessa dokument som har titeln kontinuitetsplan. Av kontinuitetsplanernas innehåll kan vi dock konstatera att det saknas planering över hur verksamheten kan upprätthållas eller vilka alternativa arbetssätt som ska träda in vid it-avbrott eller cyberattack.

I avsaknad av dokument som benämns kontinuitetsplan har vi i viss mån inkluderat en analys av andra inhämtade underlag för att bedöma om det finns likvärdig information för att bibehålla kontinuitet i samhällsviktiga verksamheter vid it-avbrott eller cyberattack.

De underlag som vi tagit del av i granskningen är bland annat risk- och sårbarhetsanalyser, åtgärdsplaner samt krisledningsplaner. Ett dokument som vi tagit del av är en Rutin för att säkerställa brukarens vård och stöd vid IT-avbrott som är upprättat inom vård- och omsorgsförvaltningen. Vi noterar att rutinen innehåller uppgifter som vid kortare avbrott skulle kunna utgöra ett tillräckligt underlag för att upprätthålla kontinuiteten. Rutinen tydliggör krav om att aktuell information och dokumentation om brukare finns tillgängligt i pappersakter, pärmar och liknande. Det finns därtill dokumenterade kontaktvägar till andra parter (interna och externa) som har

tillgång till viss information om brukare och patienter i händelse av att verksamheten inte har tillgång via egna system.

Övriga planer och underlag vi tagit del av saknar likvärdighet i utformning och omfattning vilket indikerar att det inte tidigare funnits en samordning och reglering över vad en kontinuitetsplan är och vad den behöver innehålla. Underlagen som vi tagit del av innehåller begränsad eller ingen information om hur verksamheterna ska upprätthållas i händelse av att tillgång till it, system och information.

Enligt uppgift från intervjuade har inga tester eller övningar genomförts av befintliga planer och rutiner utifrån händelsen it-avbrott. Det har dock på koncernledningsnivå genomförts en dialogövning avseende cyberattack och ytterligare övningar planeras att genomföras under hösten 2023.

Som komplement till de underlag vi tagit del av har muntliga beskrivningar gjorts för hur verksamheter har vissa rutiner och åtgärder på plats för att hantera it-bortfall för vissa aktiviteter. Exempelvis inom måltidsverksamheten finns rutiner för att skriva ut listor med information för beställning och planering för att kunna upprätthålla verksamheten under en acceptabel period. Inom försörjningsstöd finns alternativa sätt att göra utbetalningar eller för att säkerställa att individer kan få tillgång till medel utan att överföringar av utbetalningar kan göras.

Samtliga intervjuade beskriver dock att flertalet av de arbetssätt och rutiner som finns på plats endast skulle fungera under en begränsad tid och att ett längre it-bortfall skulle medföra allvarliga konsekvenser.

Det arbete som pågår i nuläget med uppdaterade risk- och sårbarhetsanalyser och tillhörande kontinuitetsplanering med stöd från beredskapssamordnare från kommunledningskontoret och serviceförvaltningen har gjort att flera verksamheter identifierat att tidigare åtgärder och kontinuitetsplaner (eller motsvarande underlag) inte varit tillräckligt utvecklade att utgå från i händelse av it-bortfall eller begränsad tillgång till system och information. De har även identifierat att det finns väsentliga beroenden mellan förvaltningarna, mellan förvaltningar och kommunala bolag samt till externa parter som inte i tillräcklig grad beaktats och inkluderats i tidigare bedömningar och åtgärder.

Intervjuade beskriver att beroendet av it, information och system samt tillhörande risker för it-avbrott och/eller cyberattack har fått ökat fokus i det arbete som genomförs i nuläget.

3.2.3 Bedömning

Vi bedömer att kommunstyrelsen i styrande dokument har tydliggjort kommunens process för risk- och sårbarhetsanalyser och tillhörande krav om kontinuitetsplanering för samhällsviktig verksamhet.

Emellertid har processen inte varit tillräckligt förankrad i kommunens verksamheter och vår bedömning är att nuvarande risk- och sårbarhetsanalyser (från 2019) inte i enlighet med styrningen har utgjort underlag för kontinuitetsplanering.

Våra stickprov visar att de underlag som är upprättade inte i tillräcklig grad beaktat hur verksamheter ska och kan upprätthållas i händelse av it-avbrott. Vår bedömning är att de planer som i nuläget finns inte är tillräckliga som planering för att säkerställa

verksamheternas kontinuitet vid it-avbrott utan alltför stor skadeverkan vilket är förenat med allvarliga risker.

Det pågår i nuläget ett aktivt arbete med att uppdatera risk- och sårbarhetsanalyser och att ta fram kontinuitetsplaner. Av de exempel vi tagit del av i stickprov kan vi konstatera att it-avbrott är inkluderat i processen som en väsentlig risk att hantera. Arbetet med kontinuitetsplaneringen är dock inte färdigställt vid tid för granskningen så att vi kan bedöma om dessa är tillräckliga.

Styrelse och nämnder har inte säkerställt att övningar genomförts för att testa den planering och de rutiner som finns framtagna för att säkerställa kontinuiteten i verksamheterna i händelse av it-avbrott.

3.3 Uppföljning av kontinuitetsplaneringen

Som vi beskrivit tidigare så uppfattas inte styrdokument tillräckligt förankrade så att aktiviteter, åtgärder och uppföljning genomförts i enlighet med de krav som ställs i styrdokument och underlag. Intervjupersoner menar att det även till viss del är en konsekvens av att resurser saknats både inom kommunledningskontorets säkerhetsfunktion och inom respektive förvaltning efter att säkerhetssamordnarna i förvaltningarna konsoliderats.

Av intervjuer framgår att uppföljning inte gjorts i tillräcklig utsträckning, exempelvis har inte någon uppföljning eller kontroll gjorts över att kontinuitetsplaner finns för samtliga samhällsviktiga verksamheter i enlighet med krav i styrande dokument. Enligt styrande dokument ska analyser tillsammans med identifierade åtgärder årligen följas upp och rapporteras till kommunstyrelsen. Av intervjuer framgår att detta inte har genomförts.

Vi noterar att uppföljningsformer beskrivs som en del i kommunens nya process för risk- och sårbarhetsanalys.

3.3.1 Bedömning

Vi bedömer att styrelser och nämnder inte har ett systematiskt arbetssätt genom internkontroll eller annan uppföljning att nödvändiga kontinuitetsplaner samt rutiner för att upprätthålla verksamhet finns och är aktuella. Detta då uppföljning inte har gjorts och granskningen visar att kontinuitetsplaner saknas till stor del.

Vi bedömer att både kommunstyrelsen och nämnderna har brustit i sitt ansvar då de inte säkerställt att tillräckliga kontinuitetsplaner finns för kommunens samhällsviktiga verksamheter i enlighet med krav i styrdokument och MSB:s föreskrifter. Detta riskerar att leda till att samhällsviktiga verksamheter inte kan upprätthållas i en godtagbar nivå i händelse av it-avbrott eller andra väsentliga händelser med påverkan på kontinuiteten.

Vi ser dock att den uppdaterade processen för risk- och sårbarhetsanalys är mer systematisk och inkluderar uppföljningsformer. Om den nya processen förankras i kommunens verksamheter finns det förutsättningar att uppföljningen av kontinuitetsplaneringen framgent kan stärkas.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning är att kommunstyrelsen och de nämnder som ingår i granskningen inte har tillsett en tillräckning styrning och uppföljning av kontinuitetsplaneringen. Vi ser därigenom en risk att de underlag som i nuläget finns tillgängliga inte skulle vara tillräckliga som planering i händelse av it-avbrott.

Ansvar och processen för risk- och sårbarhetsanalys inklusive kontinuitetsplanering är tydliggjord genom styrande dokument men de aktiviteter som det ställs krav om har inte genomförts. Det saknas därför i stora delar underlag i form av riskanalyser, åtgärder samt kontinuitetsplanering i händelse av it-avbrott.

Genom de stickprov av underlag som gjorts i granskningen konstaterar vi att verksamheternas kontinuitet vid it-avbrott inte beaktats i tillräcklig utsträckning vare sig i risk- och sårbarhetsanalyser eller i tillhörande kontinuitetsplanering. Vi bedömer att både kommunstyrelsen och nämnderna brustit i sitt ansvar då de inte har säkerställt att kontinuitetsplaner finns för kommunens samhällsviktiga verksamheter i enlighet med kommunens egna styrdokument och MSB:s föreskrifter. Vi bedömer att detta är förenat med risker, så som att samhällsviktiga verksamheter inte kan upprätthållas till en tillfredsställande nivå vid it-avbrott.

Vår granskning har samtidigt visat att kommunen i sitt pågående arbete med risk- och sårbarhetsanalys har gjort förstärkningar med stödresurser som bistår som processledare i verksamheternas arbete. I den tydliggjorda processen ingår att utifrån risk- och sårbarhetsanalyser fortsätta processen med en tillhörande kontinuitetsplanering. Förutsatt att den nya processen förankras i kommunens samtliga verksamheter och arbetet slutförs finns förutsättningar att kontinuitetsplaneringen kan stärkas.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen, i deras övergripande ansvar att:

- Tillse att styrande dokument med bäring på krisberedskapsarbetet är förankrade i kommunens verksamheter.
- Stärka uppföljning eller kontroll att de styrande dokumenten efterlevs avseende processen för risk- och sårbarhetsanalyser med tillhörande kontinuitetsplanering.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och nämnderna att:

- Tillse att det finns dokumenterade kontinuitetsplaner för samhällsviktig verksamhet och att dessa inkluderar planering vid it-avbrott.
- Säkerställ att övningar genomförs för att testa verksamheternas kontinuitetsplaner och rutiner.
- Stärka uppföljningen, antingen genom internkontroll eller annat systematiskt arbetssätt, för att säkerställa att kontinuitetsplaner finns framtagna för samtliga samhällsviktiga verksamheter.

Eskilstuna kommun
Granskning av kontinuitetsplanering avseende it-avbrott

2023-06-14

KPMG, dag som ovan

Jenny Thörn	William Andreasson	Mikael Lind
Verksamhetsrevisor	Verksamhetsrevisor	Certifierad kommunal revisor och kundansvarig

§ 159

KSKF/2023:308

Anmälan av kommunrevisionens granskning av kontinuitetsplanering avseende it-avbrott

Beslut

1. Kommunrevisionens granskning av kontinuitetsplanering avseende it-avbrott anmäls och nämndernas och bolagens svar ska redovisas till kommunfullmäktige.

Ärendebeskrivning

Kommunrevisionen har genomfört en granskning av kontinuitetsplanering avseende it-avbrott. Kommunstyrelsen, servicenämnden, socialnämnden, vård- och omsorgsnämnden, arbetsmarknads- och vuxenutbildningsnämnden och Eskilstuna Kommunföretag AB (Eskilstuna Kommunfastigheter AB och Eskilstuna Energi och Miljö AB) ska lämna svar på granskningen till kommunrevisionen.

———

Beslutet skickas till:
Kommunstyrelsen
Servicenämnden
Socialnämnden
Vård- och omsorgsnämnden
Arbetsmarknads- och vuxenutbildningsnämnden
Eskilstuna Kommunföretag AB