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

Granskning av kontinuitetshantering i händelse av it-avbrott

Rapport

Norrenergi AB

Solna stad

2025-12-11

Antal sidor 12

Innehållsförteckning

1	Sammanfattning	3
2	Bakgrund	5
3	Syfte, revisionsfrågor och avgränsning	6
3.1	<i>Avgränsning</i>	6
4	Revisionskriterier	6
5	Metod	7
6	Resultat av granskningen	8
6.1	<i>krav på arbetet med kontinuitetshantering</i>	8
6.1.1	Bedömning	9
6.2	<i>Arbetet med kontinuitetshantering</i>	9
6.2.1	Metod och genomförande av kontinuitetshantering	9
6.2.2	Åtgärder och reservrutiner	10
6.2.3	Bedömning	10
6.3	<i>Övning för att utvärdera kontinuitetsplaneringen</i>	11
6.3.1	Bedömning	11
6.4	<i>Uppföljning</i>	11
6.4.1	Bedömning	11
7	Samlad bedömning och rekommendationer	12

1 SAMMANFATTNING


Azets Revision & Rådgivning har av lekmannarevisorerna i Norrenergi AB fått i uppdrag att granska bolagets beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa som leder till it-avbrott. Uppdraget ingår i revisionsplanen för år 2025.

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

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

Bakgrunden till vår samlade bedömning är att granskningen visat att det saknas styrande dokument som reglerar krav på bolagets arbete med kontinuitetshandling. Det pågår ett arbete med att stärka bolagets informationssäkerhetsarbete vari kontinuitetsplanering är en del. Arbetet är dock i en uppstartsfas och dokumenterade kontinuitetsplaner saknas vid tid för granskningen. Inom bolaget har tekniska åtgärder vidtagits för ökad redundans och kontinuitet och det finns även ett stort antal instruktioner och rutiner i driftverksamheten för olika händelser. Vi bedömer dock att det finns risk för att dessa inte är tillräckligt välgrundade och aktuella. Detta mot bakgrund av avsaknad av strukturerad kontinuitetshandlingsprocess med analyser och bedömningar av konsekvenser och beroenden. Det har inte heller genomförts övningar för att utvärdera att nuvarande planer och rutiner är tillräckliga vid kriser eller händelser. Vi bedömer även att det saknas tillräckliga rutiner och systematik för uppföljning av arbetet och rapportering till styrelsen.

I det följande redovisas våra samlade bedömningar av respektive revisionsfråga.

<div style="display: flex; justify-content: space-between; padding: 5px;"> Nej Endast delvis I allt väsentligt Ja </div> 	
Revisionsfråga	Bedömning
Finns tydliggjorda krav avseende kontinuitetshandling och hur arbetet ska genomföras?	Nej
Finns dokumenterade kontinuitetsplaner eller motsvarande underlag som beskriver hantering om it-avbrott skulle inträffa?	Endast delvis
Har de samhällsviktiga verksamheterna analyserat sina kritiska beroenden till informationssystem och identifierat behov av åtgärder för att hantera it-avbrott?	Endast delvis
Har åtgärder vidtagits som stärkt förmågan att upprätthålla verksamheten på en tolererbar nivå i händelse av it-avbrott (exempelvis reservrutiner, analoga arbetssätt eller redundanta lösningar)?	Endast delvis

Har övningar genomförts för att utvärdera kontinuitetsplaner och tillhörande rutiner?	Nej
Finns en etablerad uppföljning och kontroll av arbetet med kontinuitetshantering?	Nej

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

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen att:

- Efterfråga tydliggörande i ägardirektiv om vilka krav och förväntningar som ägaren har på bolagets krisberedskapsarbete.
- Överväga att fatta beslut om följsamhet till Solna stads Handlingsplan för krisberedskap, så att arbetet inom koncernen utgår från gemensamma principer.
- Fastställa krav på bolagets krisberedskaps- och kontinuitetshanteringsarbete och genomföra arbetet för kritiska processer och leveranser.
- Tillse att identifierade kontinuitetsfrämjande åtgärder vidtas, alternativt kravställs hos externa leverantörer, i syfte att stärka motståndskraft och förmåga att fungera.
- Genomföra övning utifrån scenariot it-säkerhetshändelse/it-avbrott i syfte att utvärdera befintliga planer och rutiner.
- Etablera rutiner för uppföljning av krisberedskapsarbetet som säkerställer att styrelsen får den information som krävs för att ha insyn i bolagets krisberedskapsförmåga.

2 BAKGRUND

Azets Revision & Rådgivning har av lekmannarevisorerna i Norrenergi AB fått i uppdrag att granska bolagets beredskap och planering för att säkerställa kontinuitet i verksamheten om kritiska it-säkerhetshändelser skulle inträffa som leder till it-avbrott. Uppdraget ingår i revisionsplanen för år 2025.

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

Inom ramen för det kommunala åtagandet finns en rad samhällsviktiga funktioner, vilka om de inte fungerar kan leda till skada för såväl enskilda individer som samhället i stort. Dessa funktioner behöver fungera varje dag även om incidenter inträffar och det för verksamheten är ett så kallat onormalt läge.

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

Lag om motståndskraft hos kritiska verksamhetsutövare

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

Cybersäkerhetslagen

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

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

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

¹ Directive on the resilience of critical entities

² The Directive on Security of Network and Information Systems

3 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Granskningen har omfattat följande revisionsfrågor:

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

3.1 AVGRÄNSNING

Granskningen har avgränsats till att omfatta styrelsen för Norrenergi AB.

Granskningen har inte omfattat underlag eller information som är säkerhetsskyddsklassad.

4 REVISIONSKRITERIER

I granskningen har revisionskriterierna utgjorts av:

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

5 METOD

Granskningen har genomförts genom studium och analys av för granskningen relevanta styrande dokument. De dokument vi tagit del av är Solna stads Handlingsplan för krisberedskap 2024–2026, ägardirektiv samt dokumentet Säkerhetsmål – Ledningssystem för informationssäkerhet.

Intervjuer har genomförts med IT-chef samt säkerhetskonsult samt automationsingenjör med ansvar för OT-miljöer³.

Vidare ingick i granskningens metod att göra en aktgranskning i form av stickprovvis kontroll av dokumenterade kontinuitetsplaner. I dessa skulle en bedömning göras huruvida kritiska beroenden till informationssystem beaktats. Detta har inte kunnat genomföras då underlag saknats när vi efterfrågat dessa. Detta presenteras mer ingående under iakttagelse-avsnitten.

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



Samtliga intervjuade har getts möjlighet att sakgranska rapportens innehåll.

³ OT=Operational Technology. Processbaserad IT som nyttjas inom drift och anläggningar.

6 RESULTAT AV GRANSKNINGEN

6.1 KRAV PÅ ARBETET MED KONTINUITETSHANtering

Kommunfullmäktige i Solna stad har beslutat om Företagspolicy⁴. Policyn reglerar att kommunfullmäktige har det yttersta ägaransvaret för kommunens företag. Kommunens ledningsfunktion över företagen utgår från kommunfullmäktige antingen genom direkta direktiv eller genom delegerat förvaltningsuppdrag som kommunstyrelsen erhållit.

Vidare framgår målsättningen att verksamheten inom Solna stads totala organisation skall tillgodose intressen som gagnar organisationen i dess helhet. Alla former av suboptimeringar skall undvikas. Kommunstyrelsens uppdrag att samordna kommunens och företagens verksamhet ska respekteras.

Norrenergi AB ägs till 2/3 av Solna stad och 1/3 av Sundbybergs stad. I ägardirektiv för Norrenergi AB⁵ framgår att kommunfullmäktige i de båda kommunerna gemensamt utöver ägarrollen gentemot bolaget samt att kommunstyrelserna i de båda kommunerna gemensamt utöver tillsyn över bolaget. Det saknas reglering om krav på bolagets krisberedskapsarbete i ägardirektivet.

Kommunfullmäktige i Solna stad har beslutat om Handlingsplan för krisberedskapsarbetet 2024–2026⁶. Handlingsplanen syftar till att skapa en övergripande strategisk inriktning för stadens arbete med krisberedskap och civilt försvar. I handlingsplanen framgår att den omfattar alla nämnder, stiftelse- och bolagsstyrelser och ska användas som ett inriktande stöd för mer detaljerad och verksamhetspecifik planering. Handlingsplanen innehåller ett antal uppdrag för perioden 2024–2026 där genomföra kontinuitetsplanering är ett av dessa. Samtliga nämnder, stiftelser och bolag förväntas arbeta förebyggande med kontinuitetsplanering. Arbetet ska utgå från nämndens eller bolagets genomförda risk- och sårbarhetsanalys.

I Solna stads risk- och sårbarhetsanalys (publik version) ingår förteckning över de förvaltningar och bolag som har identifierats som samhällsviktig verksamhet. Norrenergis verksamhetsområden ingår inte i listan över kommunaltekniska funktioner som är identifierade som samhällsviktiga. Däremot så benämns verksamheten som ett kritiskt beroende för flertalet andra verksamheter som skulle få en stor påverkan om inte bolagets drift fungerar.

I intervjuer framkommer att Norrenergis styrelse inte fattat beslut om att handlingsplanen ska vara gällande för bolagets arbete. Vi har inte heller tagit del av några andra styrande dokument som beskriver krav på verksamheternas krisberedskaps- och kontinuitetshanteringsarbete.

Intervjuade beskriver att arbetet med kontinuitetshantering främst är en del av det arbete som initierats inom informationssäkerhet med målet att etablera ett ledningssystem för informationssäkerhet som motsvarar kraven för efterlevnad av NIS2-direktivet. Arbetet inleddes med en workshop med ledningen i maj 2024 där kravnivåer och mål fastställdes. En informationssäkerhetspolicy finns i utkastform men är inte beslutad av styrelsen. Bolaget har beslutat att genomföra sitt informationssäkerhetsarbete med grund i ett stödsystem där både

⁴ Beslutad 2004-03-29 § 20

⁵ Underlaget saknar uppgift om beslutsinstans och datering.

⁶ Beslutad 2023-12-18 KS/2023:262

kravnivåer och dokumentation sker. Vi har tagit del av dokumentation från systemet där målet som anges för arbetet är *”att ett långsiktigt arbetssätt etableras som stärker förmågan att hantera omvärldsförändringar och följa gällande lagstiftning”*. Detta ska uppnås genom ledningens inriktning och grundas i affärsdrivna prioriteringar, riskanalyser och kontinuitetsplanering.

I nuläget saknas dock dokumenterade riktlinjer för hur arbetet ska genomföras.

6.1.1 Bedömning

Vår bedömning är att det inte finns tydliggjorda krav avseende kontinuitetshandling och hur arbetet ska genomföras.

Vi baserar vår bedömning på att bolagets styrelse inte beslutat om styrande dokument som reglerar bolagets arbete med krisberedskap eller kontinuitetshandling. Ledningen har beslutat om en inriktning för arbetet med informations säkerhet men dokumenterade riktlinjer och styrning saknas. Det saknas därtill beslut om planeringsförutsättningar och krav om motståndskraft och uthållighet för bolagets förmåga om en kritisk it.

Vi bedömer att det finns ett särskilt ansvar att bedöma behov och krav inom området mot bakgrund av att flertalet andra samhällsviktiga verksamheter inom koncernen skulle få en väsentlig påverkan om bolagets drift inte fungerar tillfredsställande.

6.2 ARBETET MED KONTINUITETSHANDLING

Arbetet med kontinuitetshandling i bolaget uppges av intervjuade vara i en uppstartsfas. Ambitionen är att arbetet ska ske på avdelningsnivå och vara mer strukturerat enligt en fastställd process. I nuläget genomförs arbetet med kontinuitetshandling för it-avbrott i två parallella processer. Dels som del i det ordinarie process- och driftsarbetet, dels i etableringen av det systematiska informationssäkerhetsarbetet.

Informationssäkerhetsarbetet genomförs främst av CISO (Chief Information Security Officer) och IT-chef medan arbetet i driftsorganisationen leds av respektive avdelningschef. Därtill finns en automationsingenjör som har ansvar för bolagets OT-miljö. Intervjuade lyfter behovet av att arbetet genomförs mer samordnat och enligt en tydligare struktur där riskbedömning och åtgärder drivs av avdelningarna och inte från ett it-perspektiv.

6.2.1 Metod och genomförande av kontinuitetshandling

Som beskrivits tidigare så genomför bolaget kontinuitetsplanering inom ramen för informationssäkerhetsarbetet. I det digitala systemet som utgör grund för arbetet har särskilda kontroller valts ut som mappas mot olika regelverk som bolaget har att efterleva, exempelvis NIS2-direktivet (tillämpas från 2026 i svensk lag genom Cybersäkerhetslagen).

Arbetet med kontinuitetshandling beskrivs vara i uppstartsfas. Arbetet har initierats mot bakgrund av de nya lagkraven och drivs som ett utvecklingsarbete riktat mot Cybersäkerhetslagen. Det framhålls i intervjuer att det finns mycket kompetens och kunskap samt god medvetenhet om säkerhetsfrågor och behov av redundans och kontinuitet. Arbetet

har dock inte gjorts enligt en fastställd struktur och process tidigare. Nu har det inom bolaget satts samman en grupp som gemensamt arbetar med förbättringar. Med nya krav har det blivit en större medvetenhet även i ledningsgrupp och styrelse att säkerhetsarbetet behöver prioriteras och att det även kan innebära behov av investeringar för att inte riskera sanktioner vid brister i arbetet.

Det finns en systemförteckning med ansvarig systemägare, riskanalyser och identifierade skyddsbehov vilket gett en god kännedom om vad som är mest kritiskt och skyddsvärt.

6.2.2 Åtgärder och reservrutiner

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

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

Det finns inom bolaget en krispärm som ska fungera som stöd vid olika kriser och händelser. I pärmen ingår instruktioner i händelse av störningar eller it-avbrott. Vi kan dock konstatera vid granskning av krispärmen att vissa underlag inte har uppdaterats på några år. Enligt uppgift finns utöver krispärmen ett mycket stort antal instruktioner, rutiner och checklistor i driftverksamheten. Dessa täcker alla tänkbara situationer och händelser där medarbetare behöver få stöd i alternativ hantering.

I övrigt så framhålls särskilt att kontinuitetsfrämjande åtgärder vidtagits rent tekniskt för att anläggningar, system och kommunikation ska fungera med redundanta lösningar. Det finns även serviceavtal och beredskapsavtal för processmiljöerna där externa leverantörer kopplas in för felavhjälpning och återställning.

6.2.3 Bedömning

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

Vår bedömning är att bolaget endast delvis har analyserat sina kritiska beroenden till informationssystem samt endast delvis identifierat och vidtagit åtgärder för att kunna hantera it-avbrott.

Vi bedömer att det finns dokumenterade underlag med rutiner och instruktioner för olika händelser men att dessa inte är ett resultat av genomförd process för kontinuitetshandling där analyser och bedömningar gjorts av exempelvis konsekvenser och beroenden och resurser. Vi bedömer att bolagets beredskapsarbete skulle stärkas av att genomföras utifrån en systematisk och sammanhållen process.

Vi bedömer att ett antal åtgärder vidtagits men kan samtidigt konstatera att dessa inte baserats på ovan nämnda analyser och bedömningar vilket därför kan leda till risk att åtgärder inte står i

relation till beroenden och resurser som krävs för att säkerställa bolagets kontinuitet vid exempelvis it-avbrott.

6.3 ÖVNING FÖR ATT UTVÄRDERA KONTINUITETSPLANERINGEN

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

Norrenergi har genomfört vissa övningar men inte med inriktning på it-säkerhetsincident eller it-avbrott. Det innebär i sin tur att rutiner och instruktioner inte har utvärderats. Intervjuade beskriver därtill att de ser behov av att genomföra utbildning i kontinuitetshandling för ökad förståelse inför genomförande av kontinuitetsplaneringen för kritiska system och processer.

6.3.1 Bedömning

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

Vi baserar vår bedömning dels på att kontinuitetsplaner saknas varpå övningar för att utvärdera dessa och tillhörande rutiner inte har genomförts, dels på att övningar utifrån scenariot för it-avbrott inte har genomförts.

6.4 UPPFÖLJNING

Det saknas reglering över hur bolagets arbete med kontinuitetshandling ska följas upp eller hur rapportering till styrelsen förväntas.

Vi har inte tagit del av någon dokumenterad uppföljning. Intervjuade bekräftar att det saknas en strukturerad uppföljning. Det har inte heller skett någon särskild rapportering till styrelsen avseende bolagets kontinuitetsförmåga.

6.4.1 Bedömning

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

Vi baserar vår bedömning på att det saknas en strukturerad uppföljning och det saknas rapportering till styrelsen om bolagets arbete med kontinuitetshandling. Då styrelsen är ytterst ansvariga bedömer vi att det är väsentligt att rutiner för uppföljning och rapportering etableras.

7 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

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

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

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen att:

- Efterfråga tydliggörande i ägardirektiv om vilka krav och förväntningar som ägaren har på bolagets krisberedskapsarbete.
- Överväga att fatta beslut om följsamhet till Solna stads Handlingsplan för krisberedskap, så att arbetet inom koncernen utgår från gemensamma principer.
- Fastställa krav på bolagets krisberedskaps- och kontinuitetshandlingsarbete och genomföra arbetet för kritiska processer och leveranser.
- Tillse att identifierade kontinuitetsfrämjande åtgärder vidtas, alternativt kravställs hos externa leverantörer, i syfte att stärka motståndskraft och förmåga att fungera.
- Genomföra övning utifrån scenariot it-säkerhetshändelse/it-avbrott i syfte att utvärdera befintliga planer och rutiner.
- Etablera rutiner för uppföljning av krisberedskapsarbetet som säkerställer att styrelsen får den information som krävs för att ha insyn i bolagets krisberedskapsförmåga.

Datum som ovan

Azets Revision & Rådgivning AB

Mikael Lind

Certifierad kommunal revisor

Jenny Thörn

Verksamhetsrevisor