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

# Granskning av kontinuitetshantering i händelse av it-avbrott

**Rapport**

Bostadsstiftelsen Signalisten/Solnabostäder AB

Solna stad

2025-12-11

Antal sidor 12

## INNEHÅLLSFÖRTECKNING

---

<b>1</b>	<b>Sammanfattning</b>	<b>3</b>
<b>2</b>	<b>Bakgrund</b>	<b>5</b>
2.1	<i>Syfte, revisionsfrågor och avgränsning</i>	6
2.1.1	<i>Avgränsning</i>	6
2.2	<i>Revisionskriterier</i>	6
2.3	<i>Metod</i>	6
<b>3</b>	<b>Resultat av granskningen</b>	<b>8</b>
3.1	<i>KRAV PÅ ARBETET MED KONTINUITETSHANTERING</i>	8
3.1.1	<i>Bedömning</i>	8
3.2	<i>arbetet med kontinuitetshantering</i>	9
3.2.1	<i>Metod och genomförande av kontinuitetshantering</i>	9
3.2.2	<i>Åtgärder och reservrutiner</i>	9
3.2.3	<i>Bedömning</i>	10
3.3	<i>övning för att utvärdera kontinuitetsplaneringen</i>	10
3.3.1	<i>Bedömning</i>	10
3.4	<i>uppföljning</i>	10
3.4.1	<i>Bedömning</i>	11
<b>4</b>	<b>Samlad bedömning och rekommendationer</b>	<b>12</b>

# 1 SAMMANFATTNING

Azets Revision & Rådgivning har av lekmannarevisorerna i Bostadsstiftelsen Signalisten och Solnabostäder AB fått i uppdrag att granska stiftelsens och dotterbolagets 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 styrelserna har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.


**Vår samlade bedömning utifrån granskningens syfte är att stiftelsens och bolagets verksamhet inte är identifierade som samhällsviktiga och att det därför saknas formella krav om kontinuitetshandling. Vi bedömer dock att styrelserna, med den reservationen, 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 stiftelsens och bolagets arbete med krisberedskap och kontinuitetshandling. Arbetet bedrivs inom ramen för stiftelsens uppdrag där visst krisberedskapsarbete är genomfört, dock har inte scenariot it-avbrott varit en del av detta.

Arbetet med reservrutiner och åtgärder för att hantera it-avbrott har beaktats i andra analyser över stiftelsens mest kritiska system. För dessa har särskilda krav ställts hos driftsleverantören och det finns även vissa rutiner för manuella arbetsätt om ett it-avbrott skulle inträffa.

Då kritiska it-säkerhetshändelser och it-avbrott sannolikt skulle få en stor påverkan på stiftelsens uppgifter ser vi det som väsentligt att ytterligare analyser över kritiska informationsmängder eller processer bedöms som grund för kompletterande beredskapsplanering. Tillgängliga planer och rutiner behöver sedan utvärderas genom övning för att bedöma om dessa är tillräckliga för att verksamheterna ska fungera på en acceptabel nivå om en it-säkerhetshändelse eller it-avbrott skulle drabba stiftelsen.

I det följande redovisas våra samlade bedömningar av respektive revisionsfråga.

<div style="display: flex; justify-content: space-between; padding: 5px;"> <span>Nej</span> <span>Endast delvis</span> <span>I allt väsentligt</span> <span>Ja</span> </div> 	
Revisionsfråga	Bedömning
Finns tydliggjorda krav avseende kontinuitetshandling och hur arbetet ska genomföras?	Ja
Finns dokumenterade kontinuitetsplaner eller motsvarande underlag som beskriver hantering om it-avbrott skulle inträffa?	Endast delvis
Har de samhällsviktiga verksamheterna analyserat sina kritiska beroenden till informationssystem och identifierat behov av åtgärder för att hantera it-avbrott?	I allt väsentligt

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

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

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen i stiftelsen att:

- Efterfråga tydliggörande i stadgar om vilka krav och förväntningar som kommunen har på stiftelsens 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 krisberedskapsarbetet, exempelvis avseende planeringsförutsättningar om motståndskraft och förmåga för händelser och kriser.
- Utvärdera om det finns behov av beredskapsåtgärder specifikt kopplat till risken för it-säkerhetshändelser så att kritiska processer och tillgång till information kan säkerställas i händelse av avbrott.
- Genomföra övning 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.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen i dotterbolaget att:

- Genomföra en riskanalys för att bedöma om det finns faktorer att beakta i krisberedskapsarbetet och planeringen för att hantera it-säkerhetshändelser och avbrott som inte i nuläget inkluderats i stiftelsens risk- och sårbarhetsanalys och tillhörande åtgärder.

## 2 BAKGRUND

---

Azets Revision & Rådgivning har av lekmannarevisorerna i Signalisten fått i uppdrag att granska stiftelsens beredskap och planering för att säkerställa kontinuitet i verksamheten om kritiska it-säkerhetskäändelser 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 CER<sup>1</sup>-direktivet beslutat av EU. Direktivet ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet.

### **Cybersäkerhetslagen**

Med utgångspunkt från NIS<sup>2</sup>-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.

---

<sup>1</sup> Directive on the resilience of critical entities

<sup>2</sup> The Directive on Security of Network and Information Systems

## 2.1 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

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

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?

### 2.1.1 Avgränsning

Granskningen har avgränsats till att omfatta styrelsen för Signalisten och styrelsen för Solnabostäder AB.

Granskningen avser år 2025.

Granskningen har inte omfattat underlag eller information som är säkerhetsskyddsklassad.

## 2.2 REVISIONSKRITERIER

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen 6 kap § 6
- 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
- Bolagsordning
- Ägardirektiv
- Handlingsplan för krisberedskap 2024 - 2026

## 2.3 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, Stadgar för Bostadsstiftelsen Signalisten, Bolagsordning Solnabostäder, Affärsplan 2025, Krisplan, Internkontrollplan 2025, Styrelsens arbetsordning samt VD-instruktion.

Intervjuer har genomförts med VD och utvecklingschef.

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 kontinuitetsplaner ej varit tillgängliga och övriga underlag inte beskrivit rutiner för hantering vid it-avbrott. 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 RESULTAT AV GRANSKNINGEN

---

### 3.1 KRAV PÅ ARBETET MED KONTINUITETSHANDLING

Kommunfullmäktige har beslutat om Handlingsplan för krisberedskapsarbetet 2024–2026<sup>3</sup>. Handlingsplanen syftar till att skapa en övergripande strategisk inriktning för stadens arbete med krisberedskap och civilt försvar. Handlingsplanen omfattar alla nämnder, stiftelse- och bolagsstyrelser och ska användas som ett inriktande stöd för mer detaljerad och verksamhetsspecifik planering.

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, stiftelsens eller bolagets genomförda risk- och sårbarhetsanalys.

Vi har i granskningen fått uppgift om att stiftelsen och bolaget inte har fattat något beslut om att anta Handlingsplan för krisberedskap som styrning för arbetet. Vi har genom dokumentgranskning kunnat konstatera att det utöver handlingsplanen saknas reglering över arbetet med krisberedskap. Vi har inte i erhållna dokument som stadgar för stiftelsen, bolagsordning för Solnabostäder, arbetsordning för styrelsen, VD-instruktion eller Affärsplan noterat att krisberedskap eller ansvar inom området nämns.

I Solna stads Risk- och sårbarhetsanalys (RSA) ingår att definiera vilka av koncernens verksamheter som identifierats som samhällsviktiga. Tillhandahållande av bostäder och lokaler ingår dock inte i den förteckning som presenteras i stadens RSA vilket är i linje med Myndigheten för samhällsskydd och beredskaps förteckning över samhällsviktiga verksamheter. Intervjuade från stiftelsen bekräftar att även de gjort samma bedömning vilket innebär att stiftelsen inte har något formellt krav om kontinuitetshandling.

#### 3.1.1 Bedömning

---

Vår bedömning är att det finns tydliga krav på stiftelsens och bolagets arbete med kontinuitetshandling. Då verksamheterna inte är samhällsviktiga saknas formella krav om kontinuitetsplaner.

---

Vi baserar vår bedömning på att kravet om kontinuitetshandling riktas till verksamheter som är identifierade som samhällsviktiga vilket inte tillhandahållande av fastigheter eller lokaler bedöms som. Vi bedömer dock att det finns behov av att tydliggöra krav avseende stiftelsen och bolagets arbete med beredskap för it-avbrott då detta troligen riskerar att påverka verksamheterna i hög grad om en sådan händelse skulle inträffa.

---

<sup>3</sup> Beslutad 2023-12-18 KS/2023:262

## **3.2 ARBETET MED KONTINUITETSHANDLING**

Stiftelsen har genomfört arbete med krisberedskap, bland annat genom risk- och sårbarhetsanalys där stiftelsen använt samma metodik som staden. I arbetet hade de stöd från stadens säkerhetsskyddschef. Styrelsen har enligt intervjuade varit aktivt involverade i framtagandet av risk- och sårbarhetsanalysen, bland annat genom deltagande vid en strategidag samt en efterföljande värderingsövning. Inom ramen för RSA-arbetet har styrelsen identifierat risker och relevanta åtgärder. Genomförandet av åtgärder har sedan bedrivits i ledningsgruppen.

Stiftelsen har en dokumenterad krisplan i vilken det ingår vissa bedömningar som kan utgöra stöd vid störningar eller avbrott.

Inom stiftelsen ansvarar i nuläget utvecklingschef för arbetet med risk- och sårbarhetsanalys, krisorganisation och krisplan. Stiftelsen har sett behov av att ha en säkerhet- och beredskapssamordnare men har inte någon sådan funktion på plats i nuläget. Intervjuade framhåller it-samordnare och även arkivare, som har rollen dataskyddsbud, som väsentliga då det gäller informationshantering och systemsäkerhet.

### **3.2.1 Metod och genomförande av kontinuitetshandling**

Stiftelsen har en dokumenterad krisplan. Enligt underlaget syftar den till att ge en översiktlig struktur om en kris skulle inträffa och beskriva de resurser som kan behövas vid en kris. Planen ska kunna användas som stöd när en kris inträffar och inkluderar processen från när ett larm initieras till avslut och uppföljning av krissituationen.

### **3.2.2 Åtgärder och reservrutiner**

Stiftelsen framför i intervju att dokumentationen kring kontinuitetsplanering i dagsläget främst utgörs i den krisplan som finns. Bland annat ingår i den vissa kritiska beroenden som identifierats. Förutom det som ingår i krisplanen så beskriver intervjuade att det finns en god medvetenhet om behov av redundans och kontinuitet där reservrutiner finns upprättade. Som exempel finns som bilaga till planen checklistor för hantering av specifika händelser, exempelvis strömavbrott och bortfall av värmeförsörjning. Det saknas i nuläget checklista för it-störning eller avbrott.

Intervjuade uppger dock att stiftelsen flertalet gånger gjort bedömningar av vilka av deras system som är mest kritiska (dock inte inom ramen för krisplanen). Stiftelsen har därefter i avtal med extern driftsleverantör ställt ett antal krav inom bland annat tillgänglighet till verksamhetssystem. Det finns en tydlig kravbild för hur länge ett system får ligga nere samt backuprutiner, krav på incidenthantering, krav på driftssäkerhet osv.

Alternativa lösningar finns identifierade, exempelvis möjligheten att övergå till analogt arbete med papper och penna vid systembortfall, samt att vissa funktioner såsom vatten- och värmeförsörjning som är automatiserade kan övergå till manuell drift.

### 3.2.3 Bedömning

---

Vi bedömer att stiftelsen inte har något krav om dokumenterade kontinuitetsplaner. Vi bedömer att bolaget genom andra processer i allt väsentligt har analyserat kritiska beroenden till informationssystem samt vidtagit åtgärder som analyser visat behov av.

---

Då stiftelsen inte har något formellt krav om dokumenterade kontinuitetsplaner så saknas sådana i nuläget. Vi konstaterar att stiftelsen genom andra processer analyserat kritiska beroenden samt även hos externa leverantörer krävställt åtgärder i syfte att säkerställa tillgänglighet och återställning i händelse av störning eller avbrott. I enlighet med krav i styrande dokument, så har bolaget en Risk- och sårbarhetsanalys samt krisplan som beskriver vissa beroenden och åtgärder för att hantera kriser och störningar. Det finns även analyser och åtgärder i syfte att skydda information och system samt vid behov utföra arbetet med manuella arbetsätt och rutiner.

### 3.3 ÖVNING FÖR ATT UTVÄRDERA KONTINUITETSPLANERINGEN

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

Intervjuade beskriver att stiftelsen identifierat behovet av att genomföra en krisövning för att utvärdera tillgängliga planer och rutiner. En övning är planerad att genomföras under hösten 2025 för att identifiera konkreta förbättringsåtgärder.

#### 3.3.1 Bedömning

---

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

---

Stiftelsen har inte genomfört någon övning för att utvärdera krisplan och tillhörande rutiner. Övning är planerad vilket vi bedömer är en väsentlig del för att identifiera ytterligare behov av åtgärder samt planering vid kriser och händelser.

### 3.4 UPPFÖLJNING

Stiftelsens internkontrollplan för 2025 är baserad på risk- och sårbarhetsanalysen som genomfördes 2024<sup>4</sup>. Internkontrollplanen innehåller inte några kontrollområden inom krisberedskap eller kontinuitetshandling avseende it-säkerhetshändelser eller it-avbrott.

Någon annan uppföljning eller rapportering har inte genomförts enligt muntliga uppgifter i intervjuer.

---

<sup>4</sup> Internkontrollplan 2025 baserad på risk- och konsekvensanalys 2024

### 3.4.1 Bedömning

---

Vår bedömning är att stiftelsen inte har något krav om uppföljning och kontroll av arbetet med kontinuitetshantering.

---

Som nämnts i tidigare avsnitt så har inte stiftelsen något krav om kontinuitetshantering varpå vi gör bedömningen att de inte heller har krav om uppföljning och kontroll inom området. Vi bedömer dock att det är väsentligt att styrelserna erhåller information om förmåga att hantera kriser och händelser varpå en uppföljning och rapportering bör etableras i någon form.

## 4 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

---

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

**Vår samlade bedömning utifrån granskningens syfte är att stiftelsens och bolagets verksamhet inte är identifierade som samhällsviktiga och att det därför saknas formella krav om kontinuitetshandling. Vi bedömer att styrelsen för stiftelsen, där krisberedskapsarbetet genomförs, endast delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.**

Utifrån resultatet av vår granskning rekommenderar vi styrelsen att:

- Efterfråga tydliggörande i stadgar om vilka krav och förväntningar som kommunen har på stiftelsens 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 krisberedskapsarbetet, exempelvis avseende planeringsförutsättningar om motståndskraft och förmåga för händelser och kriser.
- Komplettera krisplanen med reservrutiner för it-avbrott samt utvärdera om det finns behov av beredskapsåtgärder specifikt kopplat till risken för it-säkerhetshändelser.
- Genomföra övning 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.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen i dotterbolaget att:

- Genomföra en riskanalys för att bedöma om det finns faktorer att beakta i krisberedskapsarbetet och planeringen för att hantera it-säkerhetshändelser och avbrott som inte i nuläget inkluderats i stiftelsens risk- och sårbarhetsanalys och tillhörande åtgärder.

Datum som ovan

Azets Revision & Rådgivning AB

Mikael Lind

*Certifierad kommunal revisor*

Jenny Thörn

*Verksamhetsrevisor*