



Granskning av Göteborgs Stads Parkerings AB

– verksamhetsåret 2024

2025-01-31



Missiv till Göteborgs Stads Parkerings AB

Lekmannarevisorerna har avslutat granskningen av bolaget avseende verksamhetsår 2024.

Styrelse och verkställande direktör ansvarar för att verksamheten bedrivs enligt gällande bolagsordning, ägardirektiv och beslut samt de lagar och föreskrifter som gäller för verksamheten. Lekmannarevisorerna ansvarar för att granska verksamhet och intern kontroll samt pröva om verksamheten bedrivits enligt fullmäktiges uppdrag och mål samt de lagar och föreskrifter som gäller för verksamheten.

Granskning som har genomförts i bolaget under året presenteras i denna granskningsredogörelse. Av redogörelsen framgår de sakkunnigas iakttagelser och bedömningar.

Vi, lekmannarevisorer, hänvisar till de sakkunnigas redogörelse som grund för vårt uttalande till kommunfullmäktige. Vi ställer oss bakom de sakkunnigas bedömningar som framgår av denna redogörelse.

Vi bedömer sammantaget att bolagets verksamhet i huvudsak har skötts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt. Vi bedömer att bolagets interna kontroll i huvudsak har varit tillräcklig.

Följande rekommendation lämnas:

Bolaget rekommenderas att säkerställa följsamhet mot stadens riktlinje för informationssäkerhet.

Vi vill betona vikten av att styrelsen vidtar lämpliga åtgärder med anledning av den rekommendation som lämnas i granskningsredogörelsen.

Med anledning av rekommendationen vill vi också ha ett yttrande från styrelsen. Av yttrandet ska det framgå vilka åtgärder som styrelsen har gjort eller planerar att göra för att hantera rekommendationen.

Yttrandet ska skickas till stadsrevisionen@stadsrevisionen.goteborg.se senast den 19 juni 2025.

Göteborg den 31 januari 2025

Amandus Carlenfors
Lekmannarevisor

Erik Fristedt
Lekmannarevisor

Stadsrevisionens uppdrag

Stadsrevisionens uppdrag är att granska kommunens verksamhet. Granskningen sker på uppdrag av kommunfullmäktige som utser förtroendevalda revisorer som ansvarar för granskningen av nämnderna och kommunstyrelsen. Bland de förtroendevalda utser kommunfullmäktige även lekmannarevisorer. Lekmannarevisorerna ansvarar för granskningen av de bolag som kommunen äger.

De förtroendevalda revisorerna anlitar alltid sakkunniga biträden (yrkesrevisorer) som genomför granskningen. I granskningsredogörelserna presenterar yrkesrevisorerna den granskning de har gjort på bolagen. Granskningsredogörelserna ligger till grund för lekmannarevisorernas uttalande till kommunfullmäktige.

Viss granskning rapporteras till kommunfullmäktige löpande under året i särskilda revisionsrapporter. Du hittar alla stadsrevisionens redogörelser och rapporter på www.goteborg.se/stadsrevisionen, du kan också beställa dem från revisionskontoret, stadsrevisionen@stadsrevisionen.goteborg.se.

Diarienummer: SRV-2024-00074

Innehåll

1	Samlad bedömning.....	5
1.1	Rekommendation	5
2	Grundläggande granskning	5
2.1	Verksamhet	6
2.2	Ekonomi	6
2.3	Intern kontroll.....	6
2.4	Bedömning	7
3	Informationssäkerhet	7
3.1	Granskningsresultat.....	7
3.2	Bedömning	12
4	Uppföljning av tidigare granskning.....	13
4.1	Bolagets arbete med fastighetsunderhåll	13

1 Samlad bedömning

Varje år granskar lekmannarevisorerna bolagets verksamhet i den omfattning som följer av god revisionssed. Årets granskning består av

- grundläggande granskning
- informationssäkerhet
- uppföljning.

Revisionskontoret har faktaavstämt all granskning med bolaget.

Den samlade bedömningen, utifrån årets granskning av bolaget, är att verksamheten i huvudsak har bedrivits på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt. Vidare är bedömningen att bolagets interna kontroll i huvudsak har varit tillräcklig.

Genomförd granskning visar att det verksamhetsmässiga och ekonomiska resultatet är förenligt med ägardirektiv, kommunfullmäktiges mål och riktlinjer. Vi har inte noterat några väsentliga avvikelser i den grundläggande granskningen.

Granskningen av bolagets arbete med informationssäkerhet visar på förbättringsområden, men dessa är av mindre allvarlig karaktär och får därför inte genomslag på helhetsbedömningen.

Styrelsen har även agerat för att förbättra verksamheten utifrån tidigare års rekommendation om att upprätta långsiktiga underhållsplaner för bolagets fastigheter.

1.1 Rekommendation

Utifrån årets granskning lämnar vi följande rekommendation:

- Bolaget rekommenderas att säkerställa följsamhet mot stadens riktlinje för informationssäkerhet.

2 Grundläggande granskning

Den grundläggande granskningen syftar till att översiktligt bedöma bolagets ledning och styrning samt interna kontroll. Styrningen och kontrollen ska vara tillräcklig för att leva upp till mål, beslut och föreskrifter.

Den grundläggande granskningen består av tre övergripande revisionsfrågor:

- Har bolaget genomfört sitt uppdrag på ett ändamålsenligt sätt?
- Har bolaget en ändamålsenlig styrning, uppföljning och rapportering av sin ekonomi?
- Har bolaget sett till att den interna styrningen, uppföljningen och kontrollen är tillräcklig?

Granskningen är avvikelsebaserad och fokuserar i huvudsak på bolagets övergripande systematik, strukturer och arbetssätt.

2.1 Verksamhet

Bolaget ska genomföra sitt grunduppdrag enligt bolagsordning, ägardirektiv, gällande lag och författning samt enligt de mål och riktlinjer som fullmäktige har beslutat om. Fullmäktige har i budgeten fastställt övergripande mål som gäller för samtliga nämnder och bolag. Flera nämnder och bolag har även tilldelats specifika uppdrag som ska genomföras. Vi har översiktligt granskat hur bolaget har genomfört sitt grunduppdrag och arbetat med fullmäktiges mål och uppdrag. Vi har även granskat styrelsens protokoll och beslutsunderlag.

Granskningen visar att bolaget har planerat och genomfört grunduppdraget i enlighet med bolagsordningen och ägardirektivet. Vidare visar granskningen att bolaget i huvudsak har arbetat med de mål och uppdrag som fullmäktige har gett bolaget. Vi noterar dock att bolaget inte har beskrivit hur kommunfullmäktiges mål ska tas omhand i verksamhetsplanen för 2024. Bolaget har dock arbetat i stadens system för verksamhetsstyrning och där framgår det inom vilket målområde respektive mål ska tas omhand. Inför 2025 har styrelsen beslutat om en särskild genomförandeplan för kommunfullmäktiges mål. Denna innehåller beskrivningar om hur bolaget ska arbeta för att bidra till måluppfyllelse. Måluppfyllelsen och arbetet med fullmäktiges uppdrag har följts upp under året, i delårsrapporter och i årsrapporten.

Inga större avvikelser har noterats i styrelsens hantering vid beslutsfattande.

2.2 Ekonomi

Bolaget ska se till att verksamheten bedrivs inom de ekonomiska ramar som beslutats av styrelsen. Bolaget ska också se till att det finns en kontinuerlig ekonomisk uppföljning och rapportering. Vi har översiktligt granskat bolagets styrning av ekonomin samt dess ekonomiska uppföljning och rapportering.

Granskningen visar att bolaget har bedrivit verksamheten inom de ekonomiska ramarna för året. Granskningen visar vidare att bolaget har följt upp sin ekonomi kontinuerligt.

2.3 Intern kontroll

Bolaget ska se till att det finns ett systematiskt arbete med intern styrning och kontroll och riskhantering inom väsentliga områden. Bolaget ska även följa upp och utvärdera detta arbete. Vi har översiktligt granskat bolagets interna styrning, uppföljning och kontroll.

Granskningen visar att bolaget har upprättat en samlad riskbild och en internkontrollplan. Riskhantering har skett inom väsentliga områden. Granskningen visar även att den interna kontrollen har följts upp och att bolagets system för styrning, uppföljning och kontroll har utvärderats.

2.4 Bedömning

Revisionskontorets bedömning utifrån en översiktlig granskning är att bolaget i huvudsak har en tillfredsställande ledning och styrning samt tillräcklig intern kontroll inom de områden som vi har granskat.

3 Informationssäkerhet

Informationssäkerhet innebär att tillse att bolagets skyddsvärda informationstillgångar är tillgängliga, riktiga, konfidentiella och spårbara. Med informationstillgångar avses all information och informationshanterande resurser såsom manuella samt digitaliserade och it-baserade informationssystem. Bristande informationssäkerhet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas.

För att kunna säkerställa en tillräcklig nivå av informationssäkerhet är det av stor vikt att informationssäkerhetsarbetet är integrerat i bolagets övriga former för styrning. Samtliga anställda i en verksamhet har ett ansvar för att uppnå och behålla en god informationssäkerhet och det är viktigt att fördela och tydliggöra ansvar och roller i verksamheten. Det är också viktigt att utbilda anställda i förhållande till arbetsuppgifter och ansvar.

Syftet med granskningen är att bedöma om bolaget bedriver ett ändamålsenligt informationssäkerhetsarbete.

Revisionskriterier för granskningen har hämtats från Göteborgs Stads Säkerhetspolicy, Göteborgs Stads riktlinje för informationssäkerhet och Göteborgs Stads riktlinje för styrning, uppföljning och kontroll.

Granskningen har genomförts genom dokumentanalys och intervjuer.

3.1 Granskningsresultat

Göteborgs Stads metod för säker informationshantering bygger på ett antal steg där det första består av att klassificera information utifrån dess behov av skydd. Nästa steg är att genomföra en riskanalys och utifrån detta arbete ska organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder vidtas. Det är verksamhetens behov och informationens skyddsvärde som styr hur informationen ska skyddas.

3.1.1 Styrande dokument tydliggör hur bolaget ska arbeta

Bolaget har upprättat en anvisning för informationssäkerhet vilken syftar till att konkretisera stadens säkerhetspolicy samt riktlinje för informationssäkerhet. Därtill finns en anvisning för systemägarmodellen där roller och ansvar inom området tydliggörs. Bolaget har även upprättat följande rutiner:

- Rutin för informationssäkerhet
- Rutin tilldelning och kontroll av behörighet

- Rutin för it- eller säkerhetsincident
- Rutin för rapportering av personuppgiftsincident.

Genom dessa dokument finns en tydlighet kring hur bolaget ska arbeta med informationssäkerhetsfrågorna.

3.1.2 Arbete med att klassificera bolagets information pågår

Informationsklassificering möjliggör att information skyddas på ett adekvat sätt vilket höjer kvalitet och effektivitet genom att undvika att information får ett överskydd med höga kostnader som följd eller tvärtom att information inte får det skydd som den behöver. Styrelsen ansvarar för att bolagets information klassificeras utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet och att Göteborgs Stads klassificeringsmodell används.

Enligt bolagets rutiner för informationssäkerhet ska informationsklassning ske enligt Göteborgs Stads modell och det ska ske kontinuerligt. Bolaget har gjort en informationsklassificering i sin dokumenthanteringsplan. Den är dock inte fullständig och inte i linje med stadens nya modell för informationsklassificering.¹ Det pågår även ett arbete med att klassificera bolagets olika it-system. Vad gäller bolagets skyddsvärda information så har en särskild informationsklassificering skett av informationen i bolagets parkeringsapp. Denna behöver dock uppdateras då det var ett antal år sedan den genomfördes.

Enligt intervjuuppgift avvaktar bolaget ett stadengemensamt system och medtöd stöd innan klassificeringen av bolagets information färdigställs. Ambitionen är att arbetet ska vara klart under våren 2025.

3.1.3 Bolagets förteckning över informationstillgångar behöver kompletteras

Styrelsen ansvarar för att säkerställa att det finns en förteckning över verksamhetens informationstillgångar. Förteckningen ska innehålla sådan information som är nödvändig för återhämtning efter störning eller allvarlig incident. Förteckningen ska minst omfatta ändamål för behandling eller lagring av information, informationsägare, systemägare och tillgångens informationsklass utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.

Bolaget har förtecknat sina informationstillgångar genom systemägarmodellen och dokumenthanteringsplanen. Enligt intervjuuppgift så täcker dessa bolagets informationstillgångar på en övergripande nivå. Inom ramen för systemägarmodellen finns dock utrymme för att tydligare beskriva vilken information respektive system innehåller.

Bolagets förteckning omfattar ändamål för behandling eller lagring av information, informationsägare och systemägare. Som framgår i föregående stycke så kvarstår dock arbete med att klassificera bolagets informationstillgångar och

¹ Kommunfullmäktige beslutade den 25 maj 2023 om en ny modell för informationsklassificering. Den tidigare modellen byggde på tre konsekvensnivåer medan den nya består av fyra konsekvensnivåer.

tillgångens informationsklass framgår därför inte av förteckningen. Förteckningen innehåller heller inte sådan information som är nödvändig för återhämtning efter störning eller allvarlig incident.

3.1.4 Bolaget har genomfört riskanalyser

Det andra steget i arbetet med informationssäkerhet är att genomföra riskanalyser. Ett riskbaserat förhållningssätt i informationssäkerhetsarbetet innebär att varje verksamhet ska identifiera, bedöma och följa upp informationssäkerhetsrisker och utifrån detta vidta lämpliga säkerhetsåtgärder. Enligt stadens riktlinje för styrning, uppföljning och kontroll ska även bolagets riskhantering för olika riskområden sammanställas i en samlad riskbild för styrelsens verksamhetsområde.

Av bolagets rutin för informationssäkerhet framgår att det är nödvändigt att bolaget har en god kunskap om de hot, risker och sårbarheter som kan komma att påverka verksamheten och hur dessa ska förebyggas och hanteras. Denna kunskap får bolaget genom att arbeta systematiskt med risk- och sårbarhetsanalyser, omvärldsanalys och incidentanalys.

Bolaget har under 2023 genomfört en risk- och sårbarhetsanalys vilken bland annat omfattar informationssäkerhetsfrågor. Utifrån denna har även en handlingsplan med tillhörande åtgärder upprättats. Enligt intervjuuppgift så genomförs även riskanalyser inför införandet av nya it-system.

Vad gäller bolagets hantering av personuppgifter pågår flera konsekvensbedömningar enligt GDPR för de behandlingar som anses ha hög risk. Bland annat gällande betalning av parkering. I arbetet med detta ingår det också att göra riskanalyser.

Bolaget har inte lyft några informationssäkerhetsrisker i den samlade riskbilden till styrelsen.

3.1.5 Ansvar och roller har definierats

Enligt stadens riktlinje ska ansvaret för informationssäkerhet vara kopplat till ansvaret för övrig verksamhet. En viktig del i ansvarsfördelningen är att utse *informationsägare* och *systemägare* för den information som verksamheten hanterar. Informationsägaren är ansvarig för att klassificera och besluta om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav. Systemägaren har ett överordnat ansvar för administration, drift och säkerhet för ett system. Systemägaren ansvarar även för att systemet uppfyller lagkrav och de verksamhetskrav som fastställs av informationsägaren. Ett system kan innehålla information som tillhör flera informationsägare.

Av bolagets anvisning för informationssäkerhet framgår att ansvaret för informationssäkerheten är kopplat till ordinarie verksamhetsansvar. I bolagets rutiner för informationssäkerhet beskrivs bolagets organisation för informationssäkerhet och de olika rollerna såsom säkerhetsstrateg, informationssäkerhetsansvarig, informationsägare, systemägare, dataskyddsombud, dataskyddskontakt och

servicetekniker. Av bolagets anvisning för systemägarmodellen framgår vem på bolaget som är systemägare, systemförvaltare och informationsägare för respektive system.

Inom organisationen för informationssäkerhet ingår också att varje enskild medarbetare och uppdragstagare har ansvar för att uppnå och upprätthålla en god informationssäkerhet. Enligt intervjuuppgift genomförs utbildningar inom informationssäkerhetsområdet varje år och uppfattningen är att bolagets anställda är medvetna om sitt ansvar.

3.1.6 Tillgång till system- och driftdokumentation behöver säkerställas

Enligt stadens riktlinje ska det finnas system- och driftdokumentation för varje system. Styrelsen ansvarar för att säkerställa att det finns systemdokumentation som minst omfattar vilka olika komponenter systemen består av, en övergripande beskrivning av de olika delarnas uppgift och en dokumentation över de funktioner som är relevanta för informationssäkerheten. Det ska även framgå vem som är systemägare.

Vi har frågat bolaget om tillgången till system- och driftdokumentation för tre slumpmässigt utvalda system. Bolaget har uppgett att de har tillgång till system- och driftsdokumentation för dessa system. För två av systemen har bolaget dock uppgett att de har tillgång till system- och driftdokumentation via leverantörernas hemsida. När arbetet med informationsklassificering av bolagets it-system är klart kommer bolaget att säkerställa att systemdokumentation finns på plats för de högt klassificerade it-systemen.

3.1.7 Rutiner för behörigheter och åtkomst till information finns

Styrelsen ansvarar för att åtkomst och behörigheter lämnas restriktivt utifrån arbetsuppgift och organisatorisk tillhörighet. Enligt stadens riktlinje för informationssäkerhet ska behörigheter också följas upp vid behov, åtkomst till information ska bygga på användaridentiteter som kan spåras till fysisk person och autentisering och åtkomstkontroll till administratörs- och systemkonton ska ske med unika lösenord och baseras på flerkfaktorautentisering. Regelverk och rutin för registrering och avregistrering av behörigheter ska fastställas innan system tas i bruk.

Av bolagets rutiner för informationssäkerhet framgår att åtkomst till bolagets informationstillgångar ska ges restriktivt och styras utifrån medarbetarens uppgifter och dennes roll. Autentisering och åtkomstkontroll till it-baserade informationssystem ska baseras på minst lösenord och bygga på unika användaridentiteter som är personliga.

Bolaget har en dokumenterad rutin för tilldelning och kontroll av behörighet. Syftet med rutinen är att alla anställda ska ha tillgång till rätt information på rätt sätt för att kunna utföra sina arbetsuppgifter och vara medveten om sitt personliga ansvar. Av rutinen framgår ansvarsfördelningen inom bolaget, hur

beställning av behörigheter går till, kontroll av behörigheter och avslut av behörigheter. Enligt intervjuuppgift så är efterlevnaden av rutinen god. Vi har även ställt frågor om hur behörighetshanteringen för tre av bolagets system går till. Svaren indikerar att bolagets rutiner efterlevs.

3.1.8 Krav på informationssäkerhet ställs i avtal med leverantörer

Informationssäkerhet ska integreras i upphandling av system och kraven ska definieras utifrån informationsägarens informationsklassificering och riskbedömning. Förutom säkerhetskrav ska det också framgå i avtal med leverantörer hur ansvarsfördelningen ska se ut, hur informationen ska hanteras, återlämnas och hur den ska avvecklas.

Enligt bolagets rutiner för informationssäkerhet ska leverantörsavtal upprättas och dokumenteras. I dessa ska alla relevanta informationssäkerhetskrav ingå. För varje ny leverantör ska även en introduktion över informationssäkerhet ges.

Enligt intervjuuppgifter är det inte vanligt att bolaget inför nya egenuppladdade system utan det handlar framför allt om stadens system och i dessa fall finns krav på informationssäkerhet med.

Vi har ställt frågor om bolaget har ställt krav på informationssäkerhet samt upprättat personuppgiftsbiträdesavtal för tre slumpvis utvalda system. För ett av systemen har inga specifika krav på informationssäkerhet ställts. För två av systemen har krav på informationssäkerhet ställts i avtalen. För samtliga tre system har personuppgiftsbiträdesavtal upprättats.

3.1.9 Rutiner för hantering av incidenter finns

Styrelsen ansvarar för att säkerställa att inträffade incidenter hanteras och åtgärdas skyndsamt för att minimera skador i verksamheten. Informationssäkerhetsincidenter där anmälningsskyldighet finns enligt lag eller förordning ska anmälas till ansvarig myndighet.

Av bolagets rutiner för informationssäkerhet framgår hur informationssäkerhetsincidenter ska hanteras. Bolaget har även upprättat en särskild rutin för it- eller säkerhetsincident samt en särskild rutin för rapportering av personuppgiftsincident. Av dessa rutiner framgår hur inträffade incidenter ska hanteras och åtgärdas. Av rutinerna framgår även i vilka fall och till vilken myndighet en anmälan ska göras.

Enligt intervjuuppgift har bolaget haft relativt få incidenter de senaste åren och de incidenter som har skett har hanterats i enlighet med bolagets rutiner.

3.1.10 Kontinuitetsplan behöver upprättas

Styrelsen ansvarar för att säkerställa att det finns en åtgärdsplan, så kallad kontinuitetsplan, för att kritisk verksamhet fortsatt kan bedrivas på en acceptabel nivå vid en allvarlig störning eller avbrott.

Av bolagets rutiner för informationssäkerhet framgår att det ska finnas en dokumenterad och formellt beslutad kontinuitetsplan. Kontinuitetsplanen ska hållas aktuell och helt eller delvis testas årligen samt finnas tillgänglig för berörda i händelse av avbrott.

Bolaget har påbörjat ett arbete med att ta fram en kontinuitetsplan. Ambitionen är att den ska vara klar hösten 2025, det vill säga efter att arbetet med informationsklassificering är klart. Enligt intervjuuppgift har bolaget rutiner och beredskap för de mest kritiska systemen även om en formellt beslutad kontinuitetsplan inte finns på plats.

3.1.11 Uppföljning av bolagets arbete med informationssäkerhet sker

Styrelsen ska följa upp informationssäkerheten och vidta de åtgärder som krävs för att säkerställa att styrande dokument, lagar och andra regelverk inom informationssäkerhet efterlevs. Informationssäkerhet är också ett område som årligen ska följas upp i enlighet med *Göteborgs Stads säkerhetspolicy*. Bolagets ledning ska genom tydlig inriktning och fördelning av ansvar engagera sig i verksamhetens säkerhetsarbete och minst årligen följa upp att säkerhetsnivån är acceptabel, med återrapporering till styrelsen.

Enligt bolagets rutiner för informationssäkerhet ska uppföljning av informationssäkerhetsnivån i form av intern kontroll ske minst årligen och rapporteras till ledningen genom säkerhetsrapporten.

Bolagets arbete med informationssäkerhet återrapporeras årligen till styrelsen genom en särskild säkerhetsrapport. Säkerhetsrapporten för år 2023 beslutades av styrelsen den 8 februari 2024. Av rapporten framkommer bland annat att bolaget är certifierade enligt Payment Card Industry data security standard (PCI DSS). PCI DSS är en internationell informationssäkerhetsstandard som syftar till att skydda kortbetalningar och minska kortbedrägerier. Av rapporten framgår även att bolaget bedömer att informationssäkerhets- och dataskyddsnivån är tillräcklig.

3.2 Bedömning

Revisionskontorets bedömning är att bolaget delvis bedriver ett ändamålsenligt informationssäkerhetsarbete.

Granskningen visar att bolaget har styrande dokument som ger tydlighet kring hur bolaget ska arbeta med informationssäkerhet och ansvar och roller inom området har definierats. Arbetet följs även upp och återrapporeras årligen till bolagets styrelse.

Samtidigt visar granskningen att bolaget har en del arbete kvar att göra för att säkerställa följsamhet mot stadens riktlinje för informationssäkerhet. Bolaget behöver bland annat färdigställa det påbörjade arbetet med informationsklassificering samt ta fram och besluta om en kontinuitetsplan. När arbetet med informationsklassificering är klart bör bolaget även värdera om de

informationssäkerhetskrav som ställts i avtal med leverantörer är tillräckliga samt säkerställa att bolaget har tillgång till system- och driftdokumentation för väsentliga it-system.

Mot bakgrund av de iakttagelser som gjorts i granskningen lämnar vi följande rekommendation till bolaget:

Bolaget rekommenderas att säkerställa följsamhet mot stadens riktlinje för informationssäkerhet.

4 Uppföljning av tidigare granskning

I detta avsnitt redogör vi för uppföljningen av den rekommendation som har lämnats till bolaget tidigare år.

4.1 Bolagets arbete med fastighetsunderhåll

På uppdrag av lekmannarevisorerna granskade revisionskontoret 2021 bolagets arbete med fastighetsunderhåll. Granskningen resulterade i följande rekommendation till bolaget:

Bolaget rekommenderas att upprätta långsiktiga underhållsplaner för fastigheterna samt säkerställa att dessa upprätthålls.

Vi har följt upp denna rekommendation genom att granska styrelsens yttrande samt genom att ta del av hur bolaget arbetar med det nya fastighetssystemet. Uppföljningen visar att samtliga fastigheter som bolaget har underhållsansvar för har dokumenterats i systemet med hjälp av resultat från statusbesiktningar och dokumentation från tidigare underhållsåtgärder. Det nya fastighetssystemet stödjer även en långsiktig planeringshorisont.

4.1.1 Bedömning

Revisionskontoret bedömer att bolaget har omhändertagit rekommendationen.