Granskningsrapport för 2023

Till årsstämman i Göteborgs Stadshus AB Org.nr: 556537–0888

Till kommunfullmäktige för kännedom

Vi, lekmannarevisorer i Göteborgs Stadshus AB, har granskat bolagets verksamhet under 2023. Granskningen har utförts av sakkunniga som biträder lekmannarevisorerna.

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.

Granskningen har utförts enligt aktiebolagslagen och kommunallagen, god revisionssed i kommunal verksamhet och kommunens revisionsreglemente samt utifrån bolagsordning och av årsstämman fastställda ägardirektiv.

En sammanfattning av granskningen har överlämnats till bolagets styrelse och verkställande direktör i en granskningsredogörelse.

Vi bedömer sammantaget att bolagets verksamhet har skötts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt.

Vi bedömer att bolagets interna kontroll har varit tillräcklig.

Göteborg den 19 februari 2024

Jonas Ransgård
Lekmannarevisor utsedd
av kommunfullmäktige

Torbjörn Rigemar
Lekmannarevisor utsedd
av kommunfullmäktige

Göteborgs Stad

Detta dokument är elektroniskt signerat.

Signed by: TORBJÖRN RIGEMAR
Date: 2024-02-19 15:32:37
BankID refno: e0a97bb9-494e-4b0a-bd54-0328b8c33e3b

Vice ordförande: Torbjörn Rigemar

Signed by: JONAS RANSGÅRD
Date: 2024-02-20 08:42:09
BankID refno: 2ca789d4-10aa-4a70-a351-e1d5287be910

Ordförande: Jonas Ransgård

Granskning av Göteborgs Stadshus AB

– verksamhetsåret 2023

2024-02-12

Missiv till Göteborgs Stadshus AB

Lekmannarevisorerna har avslutat granskningen av bolaget avseende verksamhetsåret 2023. All granskning som 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 och den rekommendation som framgår av denna redogörelse. Följande rekommendation lämnas:

Bolaget rekommenderas att stärka följsamheten mot fullmäktiges riktlinje för informationssäkerhet och fullmäktiges säkerhetspolicy.

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 den lämnade rekommendationen.

Yttrandet ska skickas till stadsrevisionen@stadsrevisionen.goteborg.se senast den 21 juni 2024.

Göteborg den 12 februari 2024

Jonas Ransgård
Lekmannarevisor

Torbjörn Rigemar
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: 0193/23

Innehåll

1 Samlad bedömning

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

- grundläggande granskning
- informationssäkerhet.

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.

Bedömningen grundar sig på iakttagelser i den grundläggande granskningen och i den fördjupade granskningen av informationssäkerhet.

I den grundläggande granskningen har det framkommit att bolaget gjort ett avsteg från fullmäktiges riktlinjer för ägarstyrning samt ägardirektivet avseende ett principiellt ärende. Vår bedömning är att hanteringen har varit felaktig då styrelsen inte beslutat om avsteget utan endast blivit informerade via vd-rapporteringen.

I granskningen av informationssäkerhet framkommer brister och avvikelser mot fullmäktiges säkerhetspolicy och riktlinje för informationssäkerhet. Samtidigt visar granskningen att det pågår ett utvecklingsarbete i samverkan med stadsledningskontoret. Bedömningen är att bolaget behöver se till att de iakttagelser som framkommer i granskningen omhändertas inom ramen för detta utvecklingsarbete.

1.1 Rekommendation

Utifrån årets granskning lämnar vi följande rekommendation till bolaget:

- Bolaget rekommenderas att stärka följsamheten mot fullmäktiges riktlinje för informationssäkerhet och fullmäktiges säkerhetspolicy.

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 genom budgeten gett stadens nämnder och bolag mål som de ska uppnå och uppdrag som de ska genomföra. Vi har översiktligt granskat hur bolaget har genomfört sitt grunduppdrag och arbetat med fullmäktiges mål och uppdrag, som berör bolaget. Vi har även granskat styrelsens protokoll och beslutsunderlag.

När det gäller de mål och uppdrag som fullmäktige gett bolaget visar granskningen att bolaget har arbetat med dessa i de delar bolaget bedömt möjligt. Måluppfyllelsen och arbetet med fullmäktiges uppdrag har följts upp under året, i delårsrapporter och i årsrapporten.

Granskningen visar att bolaget i allt väsentligt har planerat och genomfört grunduppdraget i enlighet med bolagsordningen och ägardirektivet. Revisionskontoret har gjort en iakttagelse avseende hanteringen av ett principiellt ärende.

2.1.1 Avsteg från fullmäktiges riktlinje för ägarstyrning

Ärenden av principiell beskaffenhet eller annars av större vikt ska i god tid lämnas till kommunfullmäktige för ställningstagande. Som koncernmoderbolag ska Stadshus yttra sig i dessa ärenden som kommer från de direktunderställda bolagen respektive dotterdotterbolagen.[1] Det är viktigt att ärenden hanteras i god tid så att varje nivå i processen ges möjlighet att bidra med sitt perspektiv, detta för att ägaren i sin tur ska kunna styra och påverka utvecklingen inom Göteborgs Stads bolag. För Stadshus del så ska bolaget ge ärendet en innehållsmässig förädling utifrån det egna uppdraget och relevant samt rimlig analys utifrån hela

[1] Göteborgs Stads riktlinjer för ägarstyrning och Göteborgs Stadshus AB ägardirektiv.

stadens perspektiv samt göra ett eget ställningstagande och yttra sig i frågan innan det överlämnas till nästa nivå.[2]

Under året har Stadshus hanterat flera ärenden av principiell beskaffenhet som kommit från bolagen inom koncernen. Styrelsen har tagit ställning till samtliga utom ett som rör en hemställan till fullmäktige från dotterbolaget Business Region Göteborg. Ärendet har istället hanterats genom att vice verkställande direktören vid två tillfällen lämnat information till styrelsen inom ramen för den månatliga vd-rapporten. Vid det första tillfället (februari) informeras styrelsen om att dotterbolaget inom kort avser att besluta om en hemställan till fullmäktige. Vid det andra tillfället (mars) framgår det av vd-rapporten att: ”Stadshus i samråd med stadsledningskontoret gjort bedömningen att ett undantag från ordinarie ärendeprocess är motiverat”. Vidare att ärendet ska beredas direkt av stadsledningskontoret med hänvisning till att det dels inte finns några särskilda aspekter på frågan ur ett Stadshuskoncernsperspektiv, dels att det finns ett behov av en kort handläggningstid.

2.2 Ekonomi

Bolaget ska se till att verksamheten bedrivs inom de ekonomiska ramarna 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 den interna kontrollen har följts upp och att bolaget har upprättat en samlad riskbild och en internkontrollplan. Riskhantering har i huvudsak skett inom väsentliga områden. I vår fördjupade granskning avseende informationssäkerhet redogörs för vissa iakttagelser kopplade till riskhantering (se avsnitt 3.1.4).

2.4 Bedömning

Utifrån en översiktlig granskning bedömer revisionskontoret att bolaget i huvudsak har en tillfredsställande ledning och styrning samt tillräcklig intern kontroll inom de områden som vi granskat.

[2] Göteborgs Stadshus AB:s anvisning för ärendeberedning inom koncernen.

Inom ramen för den fördjupade granskningen av informationssäkerhet är det vår bedömning att riskarbetet i vissa delar kan utvecklas (se avsnitt 3.2).

När det gäller beslutet att göra avsteg från den ordinarie ärendeberedningsprocessen är det vår bedömning att det även är ett avsteg från fullmäktiges riktlinjer för ägarstyrning och Stadshus ägardirektiv. Avsteg från fullmäktiges riktlinjer kan göras när det finns godtagbara skäl och ska alltid dokumenteras. Detta framgår av Göteborgs Stads riktlinjer för styrande dokument. Om den specifika riktlinjen anger vem som prövar avsteg ska prövningen göras i angivet organ, i andra fall bestämmer nämnd eller styrelse själv hur avsteget ska ske.[3] Stadens riktlinjer för ägarstyrning anger inte vem som ska pröva avsteg varför det är styrelsen som avgör hur avsteg ska göras. Revisionskontorets bedömning är därför att ärendet har hanterats felaktigt då styrelsen endast informerades om avsteget istället för att besluta om att så skulle ske.

3 Informationssäkerhet

Syftet med granskningen har varit att bedöma om Göteborgs Stadshus AB bedriver ett ändamålsenligt informationssäkerhetsarbete.

Metoden har utgjorts av intervjuer med företrädare för verksamheten och dokumentgranskning.

Iakttagelserna i granskningen bedöms mot följande revisionskriterier:

- Göteborgs Stads säkerhetspolicy
- Göteborgs Stads riktlinje för informationssäkerhet.

3.1 Granskningsresultat

Stadshus AB:s verkställande direktör är tillika stadsdirektör som leder stadsledningskontoret. Sedan årsskiftet 2022/23 delar Stadshus och stadsledningskontoret även lokaler. De båda verksamheterna är egna juridiska enheter men för att på olika sätt riskminimera och resurseffektivisera, i såväl det praktiska arbetet som i den förvaltningsinterna styrningen, finns en strävan att i möjligaste mån samverka i olika frågor. I samband med revideringen av fullmäktiges riktlinje för informationssäkerhet startades därför ett gemensamt utvecklingsarbete.[4] I detta ingår bland annat att identifiera vilka av stadsledningskontorets förvaltningsinterna styrande dokument som är möjliga att även omfatta Stadshus. Därutöver har en intern gemensam teamsyta skapats för att kunna planera gemensamma övningar och utbildningsinsatser samt dela information och länkar till samtliga medarbetare.

[3] Göteborgs Stads riktlinje för styrande dokument.
[4] Beslutades den 25 maj 2023.

3.1.1 Ansvarsfördelningen

Säkerhetspolicyn anger att varje förvaltnings/bolagschef ska utse en person med befogenhet att vara drivande och hålla ihop, initiera och genom stöd och uppföljning utveckla verksamhetens säkerhetsarbete.[5] Vid Stadshus har ansvaret för bolagets säkerhetsarbete fördelats till tre funktioner:

- administrativa koordinatorn fungerar som säkerhetschef/samordnare
- bolagsjuristen har dokumentansvar för säkerhetsskydd, krisledningsplan och beredskapsplan
- administrativa chefen utgör bolagets dataskyddskontakt.

3.1.2 Informationstillgångar

Styrelsen ansvarar för att säkerställa att det finns en förteckning över verksamhetens informationstillgångar. Med informationstillgångar avses verksamhetens information och de resurser som hanterar informationen. Det kan exempelvis vara dokument, lösenord, applikationer, tjänster, datorer, kompetens och rykte/image. Förteckningen ska innehålla information som är nödvändig för återhämtning efter en störning eller allvarlig incident. Den ska minst omfatta ändamålet med behandling eller lagring av information, informationsägare, systemägare och tillgångens informationsklass utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet. Styrelsen ska också säkerställa att det i förteckningen definieras och dokumenteras regler, lagar samt avtalsrättsliga åtaganden för respektive informationstillgång.

Enligt Stadshus nyttjar bolaget endast de kommungemensamma interna tjänsterna som levereras av Intraservice. Bolaget har ingen egenupprättad förteckning över sina informationstillgångar. Med syfte att säkerställa bolagets informationstillgångar har Stadshus begärt en sammanställning från Intraservice över vilka kommungemensamma tjänster som Intraservice levererar till bolaget. Under hösten har bolaget erhållit kundavtalet som upprättats mellan Intraservice och Stadshus avseende de kommungemensamma tjänsterna samt en Excel-fil innehållandes en specifikation för månadsfakturan för dessa tjänster.

Kundavtalet med Intraservice har upprättats den 15 juni 2023 och gäller från den 23 augusti 2023 och tills vidare. Avtalet reglerar parternas mellanhavanden med utgångspunkt i Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning. Avtalet reglerar följande tre huvudsakliga områden:

- Intraservice leveransåtagande
- kundens beställning, betalning och avtalade servicenivåer
- parternas samarbete.

Till avtalet finns flera bilagor bland annat en tjänsteförteckning över de tjänster som omfattas av avtalet samt kostnader för dessa. Revisionskontoret konstaterar

[5] Säkerhetspolicy för Göteborgs Stad (respektive verksamhet beslutar titel utifrån sin organisationsstruktur och tjänstenomenklatur).

att vare sig avtalet, bilagorna eller Excel-filen innehåller de krav som fullmäktige ställer i riktlinjen för informationssäkerhet.

3.1.3 Klassificering

Enligt riktlinjen för informationssäkerhet ansvarar styrelsen för att informationen klassificeras utifrån de ovan nämnda säkerhetsaspekterna och i enlighet med Göteborgs Stads klassificeringsmodell. Genom att klassa informationen utifrån vilket skyddsbehov den har skapas förutsättningar för att skydda informationen på lämpligt sätt. En korrekt klassning bidrar till att informationen vare sig får ett för högt skydd, vilket i sig kan medföra onödiga kostnader och en ineffektiv hantering, eller ett för lågt skydd. Stadshus saknar en aktuell klassificering av informationen som bolaget hanterar. Bolaget uppger att de tillsammans med stadsledningskontoret planerar att påbörja ett arbete med att klassificera informationstillgångarna.

3.1.4 Hantering av risker

Säkerhetspolicyn anger att säkerhetsarbetet ska bedrivas med utgångspunkt från kontinuerliga riskanalyser och med tyngdpunkt på förebyggande aktiviteter. Riktlinjen för informationssäkerhet anger att det ska finnas ett riskbaserat förhållningssätt. Det innebär att varje verksamhet ska identifiera, bedöma och följa upp informationssäkerhetsrisker. Stadshus riskhantering av informationssäkerhet ligger inom ramen för det ordinarie arbetet med intern styrning och kontroll. Utifrån en årlig riskanalys sammanställs väsentliga risker i bolagets samlade riskbild tillsammans med nödvändiga åtgärder. Som stöd i arbetet finns en anvisning för intern kontroll som omfattar sex riskområden varav it- och informationssäkerhetsrisker är ett. Styrelsens riskbild för 2023 innehåller två risker inom detta område:

- felaktiga behörigheter i system
- felaktig hantering av personuppgifter.

Utifrån identifierade risker ska styrelsen se till att lämpliga säkerhetsåtgärder vidtas, vilka dessa är ska framgå av riskbilden. Bolaget beskriver att risken för felaktiga behörigheter hanteras inom ramen för intraservice verksamhet genom en automatisk justering när en medarbetare slutar. Risken för felaktig hantering av personuppgifter beskrivs delvis hanteras genom dataskyddsombudets fördjupade kontroller. Revisionskontoret noterar att i den samlade riskbilden för 2024 saknas risker inom riskområde it- och informationssäkerhetsrisker. För 2024 har bolaget valt att, inom ramen för den interna kontrollplanen, särskilt kontrollera risken för felaktig hantering av personuppgifter. Skälen som anges är att två nya systemstöd har införts samt en stor andel personaltillsättningar under de senaste tre åren. Kontrollaktiviteterna ska ske dels genom utbildningsinsatser, dels genom stickprovskontroll av två slumpmässigt utvalda behandlingar som bolaget har angivit.

Stadens riktlinje omfattar alla informationstillgångar oavsett om de behandlas manuellt eller digitalt och oberoende av i vilken form eller miljö de

förekommer. Stadshus filial i Bryssel använder samma system som verksamheten i Göteborg därutöver även sociala medier. Detta för att effektivt kunna genomföra påverkan och omvärldsanalys bland annat genom att profilera Göteborg. Enligt uppgift deltar Brysselkontorets chef vid värderingen av identifierade risker i syfte att fånga specifika risker för denna verksamhet. Under 2023 har bolaget inte identifierat några informationssäkerhetsrisker för den verksamhet som bedrivs i Bryssel. Vi noterar att dataskyddsenheten lyfter risker med användandet av sociala medier i sina granskningar och att Stadshus har tagit ställning i frågan samt vidtagit vissa åtgärder. I dataskyddsenhetens årsrapport för 2022 sammanfattas identifierade risker i två rekommendationer för bolaget att prioritera under 2023. Den ena avser personuppgiftsregister och den andra it-system och digitala verktyg.

Av Stadshus tjänsteutlåtande till dataskyddsenhetens rapport framgår att lämnade rekommendationer kommer att beaktas i det pågående gemensamma arbetet med stadsledningskontoret.

När det gäller dataskyddsenhetens avrapportering av sina granskningar finns en strävan att i så stor utsträckning som möjligt föredra årsrapporterna muntligen för nämnder och styrelser. För 2022 bestämde dataskyddsenheten i samråd med Stadshus att det räckte med en skriftlig avrapportering till styrelsen.

3.1.5 Behörighetshantering

Riktlinjen för informationssäkerhet slår fast att det är styrelsen som ansvarar för att säkerställa att åtkomst och behörighet till information ges restriktivt utifrån arbetsuppgifter och organisatorisk tillhörighet samt att behörigheter följs upp vid behov. Vid byte eller förändring av tjänst ska behörigheter och åtkomst till information ses över, åtkomst till information ska bygga på personliga användaridentiteter och vara spårbar till en fysisk person. Styrelsen ska också säkerställa att regelverk och rutin för registrering och avregistrering av behörigheter fastställs innan system tas i bruk.

När det gäller behörighetshantering i systemen framkommer att det finns en otydlighet kring ansvaret. Stadshus uppger att i vissa fall hanteras behörigheter av bolaget och i andra fall av Intraservice. I samband med att Stadshus efterfrågade en förteckning över vilka tjänster som Intraservice tillhandahåller bolaget begärde bolaget även att Intraservice skulle beskriva hur behörighetshanteringen för respektive it-system såg ut. Vid tillfället för granskningen har bolaget inte erhållit någon sådan beskrivning från Intraservice.

3.1.6 Medarbetarnas skyldigheter

Styrelsen ansvarar för att säkerställa att medarbetare görs medvetna om sitt ansvar för informationssäkerhet och att de får den utbildning de behöver för att kunna utföra arbetsuppgifterna på ett säkert sätt. Utbildningen ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Inom ramen för det gemensamma arbete som pågår med stadsledningskontoret genomförs såväl informations- som utbildningsinsatser.

Styrelsen ansvarar även för att det görs kontroller innan en person anställs samt att anställda görs medvetna om sitt informationssäkerhetsansvar. Stadshus har en checklista för introduktion av nyanställda som även gäller när en medarbetare byter tjänst/roll inom bolaget samt praktikanter. Verkställande direktör är ansvarig för att introduktionen genomförs. En del i introduktionen avser genomgång av it-system, informationskällor och regelverk samt personuppgiftshantering.

Det är också styrelsens ansvar att se till att det finns en fastställd rutin för hantering av anställda och externa som avslutar sin anställning, uppdrag eller då avtal ändras. Rutinen ska bland annat säkerställa att informationstillgångar, utrustning och passerkort återlämnas. Stadshus har en checklista som ska användas när någon slutar eller tar längre tjänstledighet. Listan beskriver vice verkställande direktörens ansvar för att kontrollerna i checklistan genomförs. Bland annat återlämning av kontorsutrustning, behörighets-, samt informationshantering.

3.1.7 Incidenthantering

Styrelsen har ansvar för att inträffade incidenter hanteras och åtgärdas skyndsamt för att minimera skador i verksamheten och att informationssäkerhetsincidenter anmäls till ansvarig myndighet. Kraven kring incidenthantering förutsätter att det finns en kunskap i verksamheten både vad gäller att veta vad en incident är, och att ha en systematik för att fånga upp och hantera samt, vid behov, anmäla incidenter. Stadshus har upprättat en checklista vid incidentrapportering och en rapporteringsmall som nyligen uppdaterats utifrån en rekommendation från dataskyddsombudet. Bolaget har också tagit del av dataskyddsenhetens hjälpfrågor för riskbedömning vid personuppgiftsincident. Vi noterar att det uppges olika uppgifter i dokumenten avseende vart en anmälan om en incident ska skickas.

3.1.8 Uppföljning

Varje nämnd och styrelse ska följa upp informationssäkerheten och vidta de åtgärder som krävs för att säkerställa att styrande dokument, lagar och andra regelverk inom informationssäkerhet efterlevs inom den egna verksamheten.[6] Säkerhetspolicyn anger att säkerhet är en del av verksamhetens riskhantering och kan beskrivas som förmågan att upprätthålla en definierad risknivå. Bolagsledningen ska minst årligen följa upp att säkerhetsnivån är acceptabel med återrapportering till styrelsen. Åtgärdsområden som ska inkluderas i säkerhetsarbetet är personsäkerhet, fysisk säkerhet, informationssäkerhet och krisberedskap.[7]

Som tidigare nämnts ligger bolagets informationssäkerhetsarbete inom ramen för arbetet med intern styrning och kontroll med årlig rapportering till styrelsen. När det gäller säkerhetspolicyns krav om årlig uppföljning och rapportering till styrelsen om den acceptabla säkerhetsnivån uppger bolaget att ett arbete i samverkan med stadsledningskontoret är planerat. Anledningen till det planerade arbetet uppges vara en rekommendation som stadsrevisionen lämnade föregående

[6] Göteborgs Stads riktlinje för informationssäkerhet och Göteborgs Stads säkerhetspolicy.
[7] Göteborgs Stads säkerhetspolicy.

år till kommunstyrelsen kopplad till uppsiktsplikten över stadens samlade säkerhetsarbete. Bolaget uppger att det planerade arbetet ska säkerställa ett relevant och mer systematiskt arbetssätt. Stadshus genomför i dagsläget ingen särskild uppföljning, eller rapportering till styrelsen, av huruvida säkerhetsnivån är acceptabel för de åtgärdsområden som fullmäktige angett i säkerhetspolicyn.

3.2 Bedömning

Granskningen visar på brister och avvikelser mot fullmäktiges säkerhetspolicy och riktlinje för informationssäkerhet. Samtidigt visar granskningen att det pågår ett utvecklingsarbete i samverkan med stadsledningskontoret. Den sammanfattande bedömningen är att bolaget behöver se till att de iakttagelser som framkommer i granskningen omhändertas inom ramen för detta utvecklingsarbete i syfte att bedriva ett ändamålsenligt informationssäkerhetsarbete.

Revisionskontoret bedömer det som väsentligt att styrelsen säkerställer det egna informationsägarskapet och det ansvar som följer på det i förhållande till såväl Intraservice som till stadsledningskontoret. Vidare vad som är styrelsens ansvar oavsett vem som är systemägare eller var och vilka risker som identifierats samt vilka olika typer av dokument som ska finnas tillgängliga. När det gäller klassificeringen av informationstillgångarna är det styrelsens ansvar att se till att samtliga informationstillgångar som bolaget hanterar inom hela verksamheten ingår samt att verksamhetens behov och informationens skyddsvärde styr klassningen.

När det gäller bolagets riskhantering vill vi understryka vikten av att det är styrelsen som ansvarar för att åtgärder vidtas och att samtliga områden som fullmäktige definierat i säkerhetspolicyn omfattas av riskarbetet. En djupare riskanalys när det gäller Brysselkontorets verksamhet kan vara nödvändig för att säkerställa att väsentliga risker identifieras och alla informationstillgångar, inklusive de digitala, hanteras korrekt.

Avslutningsvis bedömer revisionskontoret att det är fullmäktiges intention att styrelsen ska ha information om olika säkerhetsaspekter även om det inte föreligger någon risk. Stadshus behöver därför se till att fullmäktiges krav om uppföljning så som det framställs i säkerhetspolicyn och riktlinjen för informationssäkerhet säkerställs.

Mot bakgrund av de iakttagelser som framkommit i granskningen lämnar revisionskontoret följande rekommendation till bolaget:

Bolaget rekommenderas att stärka följsamheten mot fullmäktiges riktlinje för informationssäkerhet och fullmäktiges säkerhetspolicy.