

ÅRSSTÄMMA HANDLING nr 7
2018-03-09

Framställande av lekmanarevisorernas granskningsrapport





Förvaltnings AB GöteborgsLokaler

Granskning av verksamhetsåret 2017

Lekmannarevisorerna har avslutat granskningen av bolaget avseende verksamhetsåret 2017.

Våra iakttagelser och bedömningar framgår av *granskningsredogörelsen* som bifogas.

Vårt uttalande till årsstämman lämnas i en granskningsrapport. Granskningsrapporten skickas till bolaget *efter det* att styrelsen beslutat att fastställa årsredovisningen. Uttalandet i granskningsrapporten grundar sig på granskningsredogörelsen.

Vi vill betona vikten av att styrelsen vidtar lämpliga åtgärder med anledning av de rekommendationer som lämnas och vi vill därför ha ett yttrande från styrelsen. Av yttrandet ska framgå vilka åtgärder som bolaget har gjort eller planerar att göra med anledning av rekommendationerna. Yttrandet ska skickas till stadsrevisionen@stadsrevisionen.goteborg.se senast den 21 juni 2018.

Göteborg den 22 januari 2018

Tove Adlerberth
lekmannarevisor utsedd av
kommunfullmäktige

Ann-Britt Svensson
lekmannarevisor utsedd av
kommunfullmäktige



Förvaltnings AB GöteborgsLokaler

– granskning av verksamhetsåret 2017



Januari 2018

Förvaltnings AB GöteborgsLokaler. Granskning av verksamhetsåret 2017
Diarienummer: 0165/17

Lekmannarevisorer: Tove Adlerberth och Ann-Britt Svensson
Yrkesrevisor: Magnus Gréen

www.goteborg.se/stadsrevisionen

Foton: Lo Birgersson, Klas Eriksson och Carina Gran

Innehållsförteckning

Sammanfattning	4
Granskning av verksamheten	5
Grundläggande granskning	5
Granskning av systematiskt brandskyddsarbete	6
Granskning av informationssäkerhetsarbetet i Göteborgs Stad	13
Uppföljning av kameraövervakning	15
Lekmannarevisorernas uppdrag och rapportering	17
Språkbruk och revisionstermer	18

Sammanfattning

Styrelse och verkställande direktör ansvarar för att bolagets verksamhet bedrivs i enlighet med lagar och föreskrifter, bolagsordning samt ägardirektiv.

Lekmannarevisorernas uppdrag är att granska om bolagets verksamhet sköts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt samt om bolagets interna kontroll är tillräcklig.

Årets granskning av bolaget omfattar:

- grundläggande granskning
- systematiskt brandskyddsarbete
- informationssäkerhetsarbetet i Göteborgs Stad
- uppföljning av föregående års rekommendationer.

Granskningen visar att delar av bolagets verksamhet har brister som behöver åtgärdas. Därför lämnar vi följande rekommendationer:

Tabell: Sammanställning av rekommendationer

Område	Rekommendation
Systematiskt brandskyddsarbete	Lekmannarevisorerna rekommenderar verkställande direktören att utveckla och bedriva ett systematiskt brandskyddsarbete i enlighet med Göteborgs Stads säkerhetspolicy och riktlinje för systematiskt brandskyddsarbete (SBA)
Informationssäkerhetsarbetet i Göteborgs Stad	Lekmannarevisorerna rekommenderar styrelsen att säkerställa följsamhet mot gällande regelverk för informationssäkerhet. Lekmannarevisorerna rekommenderar styrelsen att stärka sin styrning och uppföljning av informationssäkerheten.

I övrigt bedömer vi att bolaget har skött verksamheten på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt samt att den interna kontrollen har varit tillräcklig.

Granskning av verksamheten

Styrelse och verkställande direktör ansvarar för att bolagets verksamhet bedrivs i enlighet med lagar och föreskrifter, bolagsordning samt ägardirektiv.

Lekmannarevisorernas uppdrag är att granska om bolagets verksamhet sköts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt samt om bolagets interna kontroll är tillräcklig.

Granskningen av verksamheten omfattar en grundläggande del, som är en översiktlig granskning av bolagets ledning och styrning samt interna kontroll samt uppföljning av tidigare års granskning.¹

Grundläggande granskning

Den grundläggande granskningen syftar till att översiktligt bedöma bolagets ledning och styrning samt interna kontroll. Det innebär att revisorerna löpande följer styrelsens protokoll och handlingar och informerar sig om verksamheten. Granskningen omfattar följande delar:

- följsamhet mot kommunfullmäktiges ägardirektiv
- följsamhet mot kommunfullmäktiges riktlinjer och direktiv för Göteborgs Stads bolag
- följsamhet mot kommunfullmäktiges budget
- följsamhet mot kommunfullmäktiges riktlinjer för styrning, uppföljning och kontroll
- följsamhet mot kommunfullmäktiges regler för ekonomisk planering, budget och uppföljning
- styrning och uppföljning av verksamhet och ekonomi
- beslutsunderlag
- hantering av särskilda uppdrag från kommunstyrelsen/kommunfullmäktige.

lakttagelser

Den grundläggande granskningen visar inte på några avvikelser.

¹ Se lekmannarevisorernas granskningsplan, april 2017

Bedömning

Lekmannarevisorernas översiktliga bedömning är att bolaget har en tillfredsställande ledning och styrning samt tillräcklig intern kontroll inom de områden som omfattats av den grundläggande granskningen.

Granskning av systematiskt brandskyddsarbete

Utgångspunkter i granskningen

Sedan år 2004 gäller lag (2003:778) om skydd mot olyckor. Den reglerar ansvarsskyldigheter och rättigheter för det breda begreppet skydd mot olyckor för den enskilde, för kommunen och för staten. Till denna lag har regeringen skrivit en förordning (2003:789) om skydd mot olyckor. Därutöver har Myndigheten för samhällsskydd och beredskap och Statens räddningsverk gett ut ett antal föreskrifter och allmänna råd.

För att uppfylla lagens krav har kommunfullmäktige beslutat att fastighetsägare och nyttjanderättshavare ska bedriva ett systematiskt brandskyddsarbete, förkortat SBA. Syftet med att systematiskt arbeta med brandskydd är att skapa en allmän medvetenhet hos anställda om de risker och de skyddsanordningar som finns. Det handlar också om att skapa förståelse för helheten kring SBA och hur det fungerar. Systematiskt brandskyddsarbete innebär att på ett strukturerat sätt planera, utbilda, öva, dokumentera, kontrollera, åtgärda och följa upp brandskyddsarbetet i organisationen. Utgångspunkten för säkerhetsarbetet i Göteborgs Stad är stadens säkerhetspolicy. Säkerhetspolicyn konkretiseras i en riktlinje för SBA. Denna riktlinje förtydligar, kompletterar och ställer i vissa avseenden högre krav än lagstiftningen inom området SBA.

Syftet med granskningen är att bedöma om bolaget bedriver ett systematiskt brandskyddsarbete i fastighetsägar- och förvaltarrollen.

Granskningen har genomförts som dokumentgranskning och intervjuer med medarbetare med delegerat ansvar för bolagets SBA. Granskningen omfattar brandskyddsarbete i fastighetsägarrollen och i förvaltarrollen. I denna granskning ingår inte SBA i de lokaler bolaget bedriver sin egen verksamhet i eller SBA i de kommersiella lokaler som bolaget ansvarar för hyresförvaltning av via avtal med bolagen inom Framtidenkoncernen.

Revisionskriterier som bedömningarna görs mot är hämtade från:

- Säkerhetspolicy för Göteborgs Stad
- Riktlinje för systematiskt brandskyddsarbete (SBA)
- Riktlinje för hantering av säkerhetsrisker
- Statens räddningsverks allmänna råd och kommentarer om systematiskt brandskyddsarbete (SRVFS 2004:3)

lakttagelser

Enligt riktlinjen ska alla de byggnader som staden äger, förvaltar eller bedriver verksamhet i ha ett dokumenterat SBA. Det ska finnas en överenskommelse som reglerar ansvaret mellan ägare/förvaltare och nyttjanderättshavare för samtliga byggnader som staden äger, förvaltar eller bedriver verksamhet i. Dessa aktörer ska ha en kontinuerlig samverkan kring brandskyddet.

Enligt brandskyddsplanen är bolagets verkställande direktör tillika brandskyddschef med ett organisatoriskt övergripande ansvar för SBA. Till sitt stöd har brandskyddschefen en brandskyddsorganisation med brandskyddscoordinator, brandskyddsansvariga (9 fastighetsförvaltare), brandskyddsombud (5 tekniska förvaltare) och övriga medarbetare. Till respektive roll har SBA-uppgifter (uppdrag) fördelats.

Brandskyddsarbetet som bolaget bedriver regleras i brandskyddsplan med tillhörande brandskyddsregler och utbildningsplan. Styrdokumentet finns publicerade i bolagets verksamhetshandbok. Enligt brandskyddsplan ska bolaget i varje egen fastighet och i varje förvaltningsuppdrag aktivt verka för ett tillräckligt förebyggande brandskydd. SBA-uppgifter som bolaget fördelar ansvaret för till hyresgäster² framgår av brandskyddsklausulen i lokalhyresavtalet. I samband med avtalstecknande mellan hyresvärd och hyresgäst överlämnas utöver avtal en skriftlig information till hyresgästen och i denna information ingår bland annat bolagets brandskyddsregler.

På övergripande nivå kan vi konstatera att bolaget har ett dokumenterat SBA (brandskyddsplan, brandskyddsregler och utbildningsplan) och i förvaltningsuppdrag finns överenskommelser som reglerar ansvar mellan såväl ägare och förvaltare (samarbetsavtal förvaltning) som mellan ägare och nyttjanderättshavare (brandskyddsklausul i lokalhyresavtal och brandskyddsregler) för samtliga byggnader bolaget äger och förvaltar.

Sammanfattningsvis visar granskningen ändå på följande avvikelser:

- Bolagets styrdokument för SBA möter inte på alla punkter eller fullt ut kraven i säkerhetspolicy för Göteborgs Stad och riktlinje för systematiskt brandskyddsarbete.

Bolagets styrdokument för SBA möter inte stadens krav på indelning av omfattningen av SBA per byggnad i grundläggande nivå, mellannivå och hög nivå. Bolagets riskbedömning svarar inte fullt ut mot riktlinjens krav på riskanalys. Styrelsen har inte

² I stadens riktlinje används nyttjanderättsinnehavare synonymt med hyresgäst.

definierat acceptabel säkerhetsnivå som brandskyddsarbetet kan följas upp mot.

- Personer med ett delegerat ansvar för SBA genomför inte fullt ut sina SBA-uppgifter enligt styrdokumentet.

Gäller specifikt brandskyddsdocumentation, uppdaterade ritningar och riskanalys/riskbedömning.

- Krav som riktlinje för systematiskt brandskyddsarbete ställer på verksamheter framgår inte specifikt av brandskyddsklausulen i lokalhyresavtalet.

Bolaget bör överväga att i brandskyddsklausulen av lokalhyresavtalet förtydliga att verksamheterna ska genomföra riskanalyser, egenkontroller och utrymningsövningar.

- Bolagets samarbetsavtal förvaltning med Göteborgs Stads Parkerings AB reglerar endast i allmänna ordalag att SBA ingår i förvaltningsuppdraget.

I samarbetsavtalet bör det förtydligas att SBA ingår i förvaltningsuppdraget.

- Anvisningen preciserar inte på ett tydligt sätt vilket övergripande ansvar för SBA som ligger i fastighetsägarrollen.

Bolaget bör i anvisningen förtydliga fastighetsägarens ansvar för kontinuerlig samverkan mellan fastighetsägare, förvaltare och nyttjanderättshavare. Bolaget bör överväga att ytterligare precisera vad inom SBA som ligger i fastighetsägarrollen.

En precisering av avvikelserna återges i kommande avsnitt mer i detalj.

Kategorisering av omfattningen av SBA i tre nivåer

Enligt riktlinjen för systematiskt brandskyddsarbete grundas SBA på helhetsbilden av byggnadens utformning, verksamheten, organisationen, brandtekniska installationer och riskbilden för respektive byggnad eller verksamhet. Alla verksamheter eller byggnader kräver därför inte lika omfattande SBA. I en verksamhet med få anställda i en mindre byggnad, utan särskilda krav på tekniska eller organisatoriska brandskyddsåtgärder, kan sannolikt information och kunskap enkelt förmedlas. Då kan den skriftliga dokumentationen begränsas i omfattning. Göteborgs Stad delar in omfattningen av SBA i tre nivåer: grundläggande nivå, mellannivå och hög nivå.

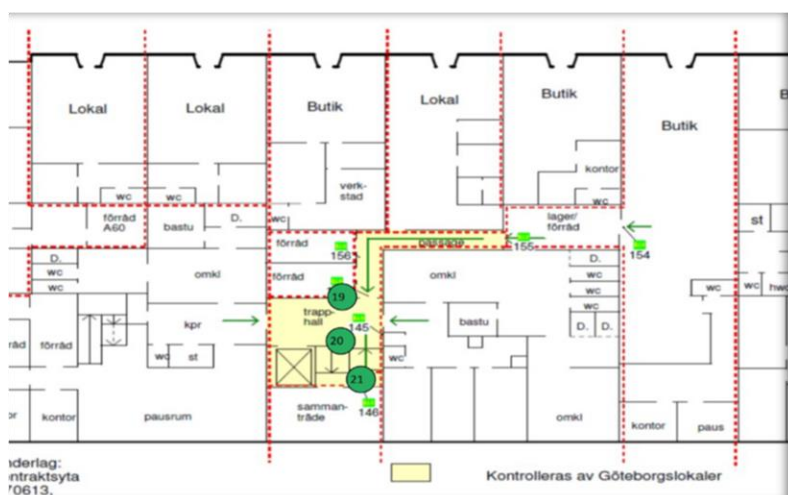
Bolaget har inte kunnat uppvisa en sammanställd indelning av omfattningen av SBA i grundläggande nivå, mellannivå och hög nivå. Intervjuer visar att omfattningen av SBA inte kategoriseras på det sättet.

Brandskyddsdocumentation och uppdaterade ritningar

Enligt riktlinjen ska varje byggnad med brandtekniska installationer beskrivas när det gäller installationernas utförande och funktion, hur dessa används vid brandtillbud samt hur de kontrolleras. Varje byggnad ska ha uppdaterade ritningar där brandcellsgränser och övrigt brandskydd är dokumenterade. En kort beskrivning av verksamheten ska också ingå. Dokumentationen ska vara tillräckligt omfattande för att säkerställa att skäligen brandskyddsåtgärder vidtas och hålls funktionsdugliga.

Av granskningen framkommer och i avstämningar bekräftas att det generellt sett finns byggnadsteknisk brandskyddsdocumentation med uppdaterade ritningar för byggnader vid de ombyggda torgen, exempelvis Bergsjön och Tuve Torg. Däremot saknas motsvarande dokumentation för byggnader vid de äldre torgen, såsom Kortedala.

Genom programmet för egenkontroller har det nyligen tagits fram uppdaterade ritningar för de lokaler bolaget ansvarar för och ska göra egenkontroller i (det vill säga de gulmarkerade gemensamma lokalerna i anslutning till nyttjanderättsinnehavarnas/hyresgästernas lokaler).



Som framgår av bilden omfattar de uppdaterade ritningarna i vissa fall även brandcellsgränser och brandskydd för nyttjanderättsinnehavarnas (hyresgästernas) lokaler. Däremot framgår av intervjuer att det saknas ritningar för minst två verksamhetslokaler.³

³ Det avser de lokaler som bolaget hyr ut till lokalförvaltningen och som lokalförvaltningen i sin tur hyr ut till äldreboendeverksamhet vid Länsmanstorget (Svartedalens äldreboende) och på Hundraårgatan i Kortedala (Sekel 182).

Risikanalyser, utrymningar och egenkontroll

Enligt riktlinjen ska verksamheten ha en dokumenterad riskanalys över verksamheten och i sin dokumentation beskriva: de risker som kan orsaka brand, de risker som uppstår vid en brand, vilka konsekvenser det medför för verksamheten och för varje identifierad risk, föreslå åtgärder för att minska sannolikhet och konsekvens. Enligt bolagets brandskyddsplan ska brandskyddsansvarig göra en riskbedömning för fastigheten. Enligt bolagets brandskyddsregler ska riskinventeringar genomföras.

Under intervjuer framkommer en uppfattning om att bolaget förhandlar bort brandskyddsarbetet till hyresgästen genom brandskyddsklausulen i lokalhyresavtalet. Av brandskyddsklausulen i lokalhyresavtalet framgår inte specifikt att verksamheten/hyresgästen ska göra riskanalyser enligt riktlinjen eller riskinventeringar enligt brandskyddsreglerna. Eftersom det inte följs upp vet bolaget inte om det görs riskanalyser enligt riktlinjen.

Bolaget kan inte uppvisa någon dokumentation på att det görs riskanalyser över de ytor som bolaget ansvarar för eller för fastigheten. Kraven på riskbedömningar för fastigheten i bolagets brandskyddsplan och krav på riskinventeringar i bolagets brandskyddsregler svarar inte heller fullt ut mot kraven på riskanalyser i fullmäktiges riktlinje för SBA.

Av intervjuer framgår att det är i verksamheterna som riskerna finns och därför menar de intervjuade att verksamheterna först behöver göra sina riskanalyser för att bolaget ska kunna bedöma riskerna för fastigheten.

Enligt riktlinjen ska det finnas en utrymningsorganisation som beskriver roller, genomförande och återsamlingsplats. Vidare ska utrymningsövningar genomföras kontinuerligt, i för verksamheten skälig omfattning, efter fastställd plan.

Riktlinjens krav på utrymningsorganisation, utrymningsplan och utrymningsövningar har inte förts över till hyresgästen genom brandskyddsklausulen i lokalhyresavtalet. Bolaget menar att det är hyresgästernas ansvar att öva utrymningar. Ändå har bolaget gjort insatser för att samordna utrymningsövningar i Hammarkullen. Eftersom det inte följs upp vet bolaget inte om verksamheterna övar utrymningar.

Verksamheterna ska göra egenkontroller. Egenkontrollerna ska dokumenteras och det ska framgå vad som kontrollerats, vad resultatet blev, när kontrollen genomfördes samt när åtgärd vidtagits.

Nyligen framtaget program för egenkontroller tillämpas på de lokaler som bolaget självt ansvarar för, det vill säga de gemensamma lokalerna i anslutning till nyttjanderättsinnehavarnas/hyresgästernas lokaler.

Bolaget har inte specificerat i brandskyddsklausulen att hyresgästen ansvarar för egenkontroller. Bolaget vet inte om verksamheterna gör

egenkontroller i sina lokaler, eftersom bolaget inte följer upp om verksamheterna genomför egenkontroller.

Utbildning i SBA

En utbildningsplan ska upprättas som innehåller vilken typ av utbildning som ges, när och hur ofta utbildningarna sker. Riktlinjen för hantering av säkerhetsrisker säger att grundutbildning SBA ska ges till alla medarbetare vartannat år, eller efter behov.

Granskningen visar inte på några avvikelser vad gäller utbildning i SBA.

Uppföljning av SBA

I säkerhetspolicyn beskrivs säkerhet som förmågan att upprätthålla en i förväg definierad risknivå. Bolagsledningen ska minst årligen följa upp att säkerhetsnivån är acceptabel med åiterrapportering till styrelsen.

Styrelsen har inte definierat en acceptabel risknivå som det systematiska brandskyddsarbetet kan följas upp mot. Enligt brandskyddsplan ska uppföljningen också omfatta utförda egenkontroller. Denna rapportering har ännu inte skett. Uppföljningen till styrelsen i säkerhetsrapporten kan därför utvecklas om den görs mot en i förväg definierad risknivå och bygger på rapportering från vad som framkommer i egenkontrollerna.

Specifikt för förvaltarrollen

Granskningen av systematiskt brandskyddsarbete har även genomförts hos systerbolaget Göteborgs Stads Parkerings AB. Några iakttagelser har relevans även för Förvaltnings AB GöteborgsLokaler.

Inför tecknandet av samarbetsavtal förvaltning år 2015 gick företrädare för bolaget och Parkeringsbolaget noggrant genom ritningarna och delade upp SBA-ansvaret för fastigheterna i tre separata delar:

- parkeringsanläggningen som parkeringsbolaget/fastighetsägaren ansvarar för
- trapphus och andra gemensamma lokaler som GöteborgsLokaler/förvaltaren ansvarar för
- butiks-, kontors- och andra verksamhetslokaler som hyresgästerna/nyttjanderättsinnehavarna ansvarar för.

Med denna ansvarsfördelning som grund upprättade bolaget sedan ett avtal daterat den 29 oktober 2015. Avtalet reglerar inte mer än i allmänna ordalag ("förvaltning, teknisk förvaltning och till förvaltning normalt hörande förvaltningsåtgärder") att brandskyddsarbete ingår i GöteborgsLokalers förvaltningsuppdrag. Intervjuer visar dock att båda parter är överens om att SBA ingår i förvaltningsuppdraget.

Parkeringsbolagets anvisning för SBA innehåller en lista med punkter som bolaget förväntar sig att GöteborgsLokaler ska utföra. Anvisningen

är inte kommunicerad och därför inte heller känd av GöteborgsLokaler. Eftersom samarbetsavtalet inte säger något specifikt om SBA följer GöteborgsLokaler sina egna styrdokument i detta förvaltningsuppdrag.

GöteborgsLokaler bedriver SBA i trapphus och gemensamma lokaler med utgångspunkt i sina egna brandskyddsregler. Parkeringsbolaget bedriver SBA i parkeringsanläggningen i enlighet med den egna anvisningen. Hyresgästerna ansvarar inom den hyrda lokalen för SBA enligt brandskyddsklausulen i lokalhyresavtalet. Helhetsbilden är att fastighetsägare, förvaltare och nyttjanderättshavare var och en bedriver sin del av brandskyddsarbetet i sin egen brandskyddsorganisation och efter sina egna regelverk.

Eftersom hyresförvaltningen ingår i avtalet är det GöteborgsLokalers utformning av brandskyddsklausulen i hyresavtalet som konkretiserar vilket ansvar hyresgästerna/nyttjanderättsinnehavarna har för SBA. Granskningen visar att stadens krav på verksamheterna: att genomföra riskanalyser, egenkontroller och utrymningsövningar, inte på ett tydligt sätt är reglerat i hyresavtalets brandskyddsklausul.

Specifikt för fastighetsägarrollen

Våra iakttagelser möter inte vad riktlinjen föreskriver i form av en kontinuerlig samverkan kring brandskyddet. Bolagets brandskyddsplan förtydligar att bolaget i vissa fall kan ta en aktiv roll för att initiera och samordna vissa delar av brandskyddet i en fastighet där det finns mer än en hyresgäst, men specificerar inte närmare vilket ansvar eller vilka uppgifter som ligger i denna roll. Vi menar att det i fastighetsägarrollen bör ligga att driva utvecklingen av en kontinuerlig samverkan mellan fastighetsägare, förvaltare och nyttjanderättshavare. Bolaget bör även överväga att ytterligare precisera fastighetsägarrollen så att bolaget kan ta ett övergripande ansvar för det systematiska brandskyddsarbetet.⁴

Övrig iakttagelse

Enligt riktlinjen ska det finnas rutiner som säkerställer att ritningar uppdateras och brandcellsgränser är intakta vid förändring i byggnadens konstruktion eller utformning.

För större lokalförändring kan intervjupersonerna redogöra för rutiner som säkerställer att brandcellsgränserna är intakta. Däremot kan de som

⁴ Stadens handbok för SBA utgår från att fastighetsägaren ska tillhandahålla brandskyddsdokumentation och uppdaterade ritningar för hela byggnaden. Statens räddningsverks allmänna råd menar att i de fall flera ägare eller nyttjare verkar inom en byggnad, till exempel i en butiksgalleria, bör en sammanställning finnas över de sammantagna riskerna och det övergripande brandskyddet.

arbetar som förvaltare inte redogöra för en rutin/kontroll som säkerställer att brandtätning sker vid enstaka kabeldragning genom brandcellsgräns.

Samlad bedömning

En samlad bedömning är att bolaget inte fullt ut bedriver ett systematiskt brandskyddsarbete varken i fastighetsägarrollen eller i förvaltarrollen.

Denna bedömning görs mot bakgrund av att bolagets brandskyddsarbete inte möter alla krav på SBA som ställs i säkerhetspolicy för Göteborgs Stad och riktlinje för systematiskt brandskyddsarbete (SBA).

Avvikelsena som sammanfattas på sidan 8 leder till att vi riktar följande rekommendation till bolaget:

Lekmannarevisorerna rekommenderar verkställande direktören att utveckla och bedriva ett systematiskt brandskyddsarbete i enlighet med stadens säkerhetspolicy för Göteborgs Stad och riktlinje för systematiskt brandskyddsarbete (SBA)

Granskning av informationssäkerhetsarbetet i Göteborgs Stad

Stadsrevisionens granskning av informationssäkerhetsarbete i Göteborgs Stad blev klar den 12 december 2017 och en revisionsrapport lämnades till styrelsen. Syftet med granskningen var att bedöma om styrelsen i Förvaltnings AB GöteborgsLokaler bedriver ett ändamålsenligt informationssäkerhetsarbete.

Förvaltnings AB GöteborgsLokaler var en av flera granskade nämnder och bolag.

lakttagelser

Nedan redovisas några av de brister som identifierades i granskningen. För vidare information hänvisar vi till rapporten *Granskning av informationssäkerhetsarbete i Göteborgs Stad*.

Följsamhet mot gällande regelverk för informationssäkerhet

Riktlinjen för informationssäkerhet anger att samtliga informationssystem ska finnas förtecknade. I förteckningen beskrivs ändamål samt ansvarsfördelning såsom informationsägare, systemägare etc. Granskningen visade att GöteborgsLokalers förteckning över informationssystem inte fullt ut innehåller de uppgifter som riktlinjen för informationssäkerhet föreskriver. Exempelvis saknas information om informationsägare.

Riktlinjen för informationssäkerhet anger att informationsklassning ska göras kontinuerligt av informationsägaren och att stadens modell ska användas. Riktlinjen gör dock ingen skillnad på om informationen

hanteras av ett lokalt verksamhetssystem eller ett kommungemensamt system. Verksamhetens ansvar för att informationen är rätt säkerhetsklassad följer av Policy och riktlinjer för användning av informationsteknik inom Göteborgs Stad. Granskningen visar att bolaget inte har klassat sin information i kommungemensamma system. Vidare visar granskningen att avseende verksamhetsspecifika system inom bolaget är det systemen som klassas snarare än själva informationen samt att klassningen inte sker kontinuerligt.

Riktlinjen för informationssäkerhet anger att det ska finnas en formellt beslutad driftsdokumentation. Granskningen visar att GöteborgsLokaler har driftsdokumentation för sitt verksamhetsspecifika system vi granskat men om driftsdokumentationen är formellt beslutad såsom riktlinjen anger har bolaget inte visat på.

Riktlinjen för informationssäkerhet anger att det ska finnas rutiner för incidenthantering vilket omfattar rapportering, loggning, åtgärdande, informationsspredning, eskalering, uppföljning och analys av incidenter. GöteborgsLokaler har dokumenterade rutiner för hantering av incidenter i det verksamhetsspecifika systemet. Det har i intervjuer uppgetts att rapportering av incidenter i det kommungemensamma systemet omfattas av dessa rutiner. Däremot saknar bolaget rutiner som omfattar övriga delar av incidenthanteringen för det kommungemensamma systemet, det vill säga loggning, åtgärdande, informationsspredning, eskalering, uppföljning och analys av incidenter.

Av riktlinjen för informationssäkerhet framgår att varje verksamhet ska besluta om den längsta tid som information kan vara otillgänglig eller system kan vara ur funktion innan verksamheten påverkas negativt. I intervju uppges Intraservice att det för de kommungemensamma systemen finns upprättade Service Level Agreements (SLA) som ska reglera den längsta tid som information kan vara otillgänglig eller system kan vara ur funktion. Vid granskningstillfället uppges i intervjuer att bolaget vid flera tillfällen efterfrågat SLA för de system de använder men inte fått del av dem. Enligt uppgift från bolaget pågår ett arbete med Intraservice avseende SLA.

Styrning och uppföljning av informationssäkerhetsarbetet

Enligt riktlinjen för informationssäkerhet ska informationsägare utses med ansvar för informationsklassning och informationens säkerhet. Granskningen visar att GöteborgsLokaler inte har utsett informationsägare för kommungemensamma system.

Krav på kunskaper i förhållande till arbetsuppgifter och kontinuerlig utbildning regleras i stadens säkerhetspolicy och riktlinje för informationssäkerhet. Granskning visar att GöteborgsLokaler har introduktion för nyanställda. Bolaget använder vid introduktionen en checklista men denna tar inte specifikt upp informationssäkerhet utan går igenom säkerhetsarbete, incidentsystem och personuppgiftslagen på en

övergripande nivå. Utöver introduktionen har bolaget deltagit Göteborgs Stads e-learning inom informationssäkerhet. Bolaget utbildar även systemägare (informationsägare) inom informationsklassning.

Det finns ett antal riktlinjer och regler inom staden som reglerar nämndernas och bolagens ansvar att säkerställa och regelbundet följa upp verksamhetens följsamhet mot bland annat regelverk och beslut. Granskningen visar att GöteborgsLokaler har systematiska och formaliserade kontroller av efterlevnaden avseende det verksamhetsspecifika system vi har granskat. De saknar dock motsvarande kontroller avseende det kommungemensamma system som vi har granskat.

Riktlinjen för informationssäkerhet anger att informationssäkerhetsnivån ska följas upp minst årligen i form av intern kontroll. Resultatet ska rapporteras till styrelsen. Granskningen visar att GöteborgsLokalers uppföljning och rapportering av informationssäkerhetsnivån bland annat sker inom ramen för det interna kontrollplanarbetet. Däremot kan vi efter granskning av den interna kontrollplanen konstatera att den bild som ges av informationssäkerhetsnivån inte är heltäckande. Bolaget uppger även att uppföljning sker genom säkerhetsrapport. Vår granskning av rapporten visar dock att informationssäkerhetsnivån inte följs upp specifikt.

Bedömning

Vår bedömning är att bolaget i huvudsak har god följsamhet mot gällande regelverk inom informationssäkerhetsområdet, men att det finns brister.

Lekmannarevisorerna rekommenderar styrelsen att säkerställa följsamhet mot gällande regelverk för informationssäkerhet.

Vi bedömer även att bolaget i huvudsak har god styrning och uppföljning av sitt informationssäkerhetsarbete, men att det finns brister.

Lekmannarevisorerna rekommenderar styrelsen att stärka sin styrning och uppföljning av informationssäkerheten.

Uppföljning av kameraövervakning

Lekmannarevisorerna granskade år 2016 bolagets kameraövervakning. Granskningen resulterade i att vi riktade följande rekommendation:

Lekmannarevisorerna rekommenderar styrelsen att se till att den verksamhetens kameraövervakning bedrivs på ett ändamålsenligt sätt

Vi har i år följt upp denna rekommendation genom att följa upp de nio avvikelser som låg till grund för rekommendationen.

lakttagelser

Sju av nio avvikelser har hanterats genom att bolaget har:

- flyttat ansvaret för all kameraövervakning från förvaltare till säkerhetschef
- stängt ner en anläggning för kameraövervakning
- klassat informationen som hanteras i kameraövervakning som känslig
- infört en behörighetskontroll för att få åtkomst till det inspelade materialet
- sett till att inloggning sker med smartkort, lösenord och under kameraövervakning
- regelbundet byte av lösenord till den it-utrustning och programvara som hanterar kameraövervakningen
- infört att säkerhetschef följer upp logglistor varje kvartal
- stärkt uppföljning av leverantörens säkerhetsarbete.

Kvarstående två avvikelser avser uppföljningen i säkerhetsrapporten. Dels möter uppföljningen inte lagstiftningens krav på att följa upp grad av intrång i den personliga integriteten på platser som kameraövervakas, dels har det inte gjorts uppföljning av om säkerhetsnivån vid hanteringen av det inspelade materialet var acceptabel. Bolaget har inte längre tillgång till bostadsbolagens enkätundersökningar om hyresgästernas upplevelse av trygghet och säkerhet. Detta eller ett liknande material skulle kunna användas för att analysera grad av intrång i den personliga integriteten. Uppföljning mot en i förväg definierad säkerhetsnivå gäller också uppföljningen av brandskyddsarbete och informationssäkerhet. På denna punkt har bolaget utlovat en förbättring i säkerhetsrapport 2017, som ska läggas fram för styrelsen i februari 2018.

Bedömning

Bedömningen är att bolaget är på god väg att ta hand om merparten av avvikelserna som låg till grund för rekommendationen. Med hänsyn till att bolaget inte förfogar över ett material för att följa upp intrånget i den personliga integriteten och är medveten om detta avsteg ser vi inget skäl till att låta denna avvikelse göra att vi håller kvar vid rekommendationen. Genom det planerade arbetet med att i säkerhetsrapport 2017 ta hand om kvarstående avvikelse bedömer vi rekommendationen omhändertagen.

Lekmannarevisorernas uppdrag och rapportering

Den kommunala revisionen är ett lokalt demokratiskt kontrollinstrument med uppdrag att granska den verksamhet som bedrivs i kommunen.

Lekmannarevisorer är förtroendevalda och utses av fullmäktige ur gruppen förtroendevalda revisorer (gruppen benämns som Stadsrevisionen). Lekmannarevisorerna har ett självständigt uppdrag att granska de bolag som helt eller delvis ägs av kommunen. I Göteborg utses i regel två lekmannarevisorer för varje bolag. Revisorerna är oberoende och granskar på fullmäktiges uppdrag och därigenom indirekt också för medborgarna.

Resultatet av lekmannarevisorernas granskning redovisas i granskningsrapport och granskningsredogörelse, en per bolag.

Revisorerna genomför också särskilda granskningar som i regel rör flera bolag och nämnder. Dessa redovisas i revisionsrapporter till fullmäktige löpande under året.

Revisorerna tar även varje år fram en årsredogörelse som sammanfattar all den granskning som gjorts i kommunen under det aktuella året.

Revisorernas rapporter hittar du på www.goteborg.se/stadsrevisionen.

Språkbruk och revisionstermer

När revisorerna har genomfört en granskning lämnar de ofta rekommendationer till de granskade nämnderna och bolagen. Ibland lämnar de även revisionskritik.

Rekommendationer lämnas då revisorerna ser brister i verksamheten. Rekommendationerna syftar till att utveckla och förbättra verksamheten.

Revisionskritik lämnas då revisorerna ser brister i verksamheten som är av mer allvarlig karaktär. Revisionskritik graderas genom begreppen erinran eller anmärkning. Anmärkning är allvarligast. När det gäller nämnderna kan en anmärkning lämnas med eller utan tillstyrkan om ansvarsfrihet.

Under kommande år följer revisorerna upp vilka åtgärder nämnden eller bolaget har gjort för att följa revisorernas rekommendationer.

Stadsrevisionen

Postadress: Box 2141, 403 13 Göteborg

Besöksadress: Stora Badhusgatan 6, Göteborg

Kontaktcenter: 031-365 00 00, kansli: 031-368 07 00

stadsrevisionen@stadsrevisionen.goteborg.se



**Göteborgs
Stad**