Stockholms stad

Ledningens genomgång år 2026

Stockholms Stadshus AB

Beslutad 2024-01-09
Reviderad [2024-11-19 och 2026-01-08]

Ledningens genomgång

Dnr: SSAB 2025/228

Kontaktperson: Johan Gagner

1, Vad är Ledningens genomgång?

Ledningens genomgång är ett begrepp inom informationssäkerhet som syftar till att de som ansvarar för informationssäkerheten inom en organisation, minst årligen ska informera sig om hur arbetet går.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare och om informationsklassningar och registerförteckning är genomförda.

Denna rapportering ska ge information och underlag till förvaltningschef/bolagschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltnings- och bolagschefer ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.[1]

I Anvisningar för nämndernas arbete med verksamhetsplan 2024 samt i motsvarande Anvisningar budget/VP 2024 koncernen Stockholms Stadshus AB som tas fram till bolagen uppmanas samtliga nämnder och bolagsstyrelser ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet för de kommande tre åren. Denna ska biläggas verksamhetsplanen. Planeringen för de kommande tre åren ska utgå från nämndens/bolagets verksamhetsuppdrag i budget och följa Riktlinje för informationssäkerhet i Stockholms stad.

I anvisningarna för budget/VP 2026 finns ingen motsvarande uppmaning men ledningens genomgång ska fortsatt tas fram enligt Riktlinje för informationssäkerhet och Funktionen för stadsövergripande informationssäkerhet på stadsledningskontoret. Enligt styrelsens arbetsordning föreläggs denna för koncernstyrelsen årets första ordinarie sammanträde.

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet

Innehållsförteckning

Ledningssystem för informationssäkerhet, LIS

Stockholms stads arbete med informationssäkerhet utgår från en så kallad ISO standard, ISO 27001. Det är en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information från hot och risker. Standarden ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet, LIS, som skyddar informationstillgångarna och ger en IT-process som är lättare att hantera, mäta och förbättra.

Stockholms stads informationssäkerhetsarbete regleras i en tillämpningsanvisning som är en bilaga till stadens Kvalitetsprogram[2]. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Stockholms Stadshus ABs räkning har vice vd fastställt en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom bolaget.

Vad påverkar Stockholms Stadshus ABs informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Stockholms Stadshus AB ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering. Bolaget har ingen direkt operativ verksamhet gentemot t.ex. medborgare, kunder, hyresgäster men hanterar information vad gäller styrning, stöd och uppföljning av bolagen inom koncernen. Bolaget använder nästan enbart stadens centralt upphandlade verksamhetssystem.

Omvärldsbevakning

Budgetuppdrag

- Moderbolaget Stockholms Stadshus AB har som uppgift att bl.a. svara för övergripande utveckling, strategisk planering, löpande översyn och omprövning, utöva ekonomisk kontroll och uppföljning, samt att utveckla styrformer och samspelet

[2] Stockholms stads kvalitetsprogram (start.stockholm)

mellan ägare, koncernledning och dotterbolag. I detta arbete samverkar bolaget med bland annat stadsledningskontoret vad gäller anvisningar och strategiska frågor inom informationssäkerhet. Samarbetet bör utvecklas den kommande treårsperioden.

- I budget 2024 och 2025 hade samtliga förvaltningar och bolag i uppdrag att fortsätta öka beredskapsförmågan, exempelvis genom att analysera och hantera risker och sårbarheter samt genom krisledningsplanering, kontinuitetshantering, systematiskt informationssäkerhetsarbete, krigsorganisation samt årliga, obligatoriska krisledningsövningar. Detta uppdrag ligger kvar 2026.

- Moderbolaget ska delta i arbetet inom stadens sektorsorganisation för civil beredskap genom deltagande i de två sektorerna *energiförsörjning* och *finansiella tjänster* samt deltagande i deras motsvarande stadsövergripande beredskapsråd samt i styrgruppen för civil beredskap.

Övrigt

- NIS2-direktivet (Network and Information Systems Directive 2 - Cybersäkerhetslagen) Regeringen beslutade den 11 december 2025 om en ny cybersäkerhetslag och cybersäkerhetsförordning. Dessa träder i kraft den 15 januari 2026.

  NIS2 är en uppdatering av det tidigare NIS-direktivet. Stockholms Stadshus AB har inte omfattats av det tidigare NIS-direktivet men några bolag inom koncernen har gjort det.

  Syftet med NIS2 är att säkerställa en hög nivå av informationssäkerhet i hela EU genom att stärka skyddet av samhällsviktiga tjänster som en följd av den ökade digitaliseringen och hotbilden av cyberhot.

  Varje verksamhetsutövare ska avgöra om de omfattas av cybersäkerhetslagen och anmäla sig till Myndigheten för samhällsskydd och beredskap (MSB) när lagen träder i kraft. För stadens samtliga stadsdelsförvaltningar och fackförvaltningar är kommunstyrelsen verksamhetsutövare och staden omfattas av sektorn ”offentlig förvaltning”. Säkerhetsavdelningen ansvarar, på kommunstyrelsens uppdrag, för att genomföra anmälan. För

bolagen gäller däremot att respektive bolag i egenskap av verksamhetsutövare själv ska identifiera om verksamheten omfattas av cybersäkerhetslagen samt genomföra anmälan till tillsynsmyndigheten. För vissa bolag är det tydligt att de omfattas utifrån att de tidigare träffats av NIS eller att kärnverksamheten ingår i någon av sektorerna i NIS2. Utmaningar i tolkningen består bland annat i tolkning av sektorer som digital infrastruktur och elektricitet där t.ex. fiber och solceller finns i vissa fastighetsbolag. Stadshus ABs bedömning är att bolaget inte omfattas av NIS2, eftersom bolaget inte uppfyller något av verksamhetskriterierna.

- Centralt i staden pågår ett utvecklingsarbete med processen för leverantörsuppföljning av centrala avtal med fokus på informationssäkerhetsfrågorna.

- Staden centralt har under 2025 utvärderat stadens befintliga ledningssystem för informationssäkerhet (LIS). Utvärderingen visar att dagens LIS behöver förändras för att mer ändamålsenligt möta de nya säkerhetsbehoven. Bland annat behövs standardisering av basprocesser inom informationssäkerhet och dataskydd. Med basprocesser menas bland annat arbetet med registerförteckning, klassning, riskanalys och hygienfaktorer inom it-säkerhet. Även förbättrad incidenthantering är ett område som behöver utvecklas under 2026 enligt utvärderingen.

  Årsredovisningslagen har anpassats till nya EU-direktiv (CSRD) om hållbarhetsredovisning. De nya kraven är väsentligt mer långtgående och kommer kräva utökade resurser men också mer insamling och redovisning av jämförbar och transparent data/information från dotterbolagen till bolagskoncernens redovisning. Bolaget har valt att använda en ny modul i Stadens system för integrerad ledning och styrning – ILS. Informationssäkerhetsperspektivet har ingått vid utformningen av modulen.

- I slutet av 2023 antogs ett nytt gallringsbeslut av Stadsarkivet vad gäller personalhandlingar. Stockholms Stadshus ABs avsikt var att dessa skulle användas som grund för arbetet med att ta fram tilläggsavtal till extern löneadministratör vad gäller gallring och arkivering av personalhandlingar i enlighet med det föreläggande bolaget

fick vid den inspektion som gjordes av Stadsarkivet hösten 2022. Efter vidare utredning med hjälp av arkivkonsult på Stadsarkivet och avstämning med extern löneadministratör finns det dock begränsningar i att genomföra gallring i enlighet med beslutet. Utredningen har istället föreslagit att en särskild gallringsframställan för de bolag som gemensamt använder detta system tas fram och hemställas till Stadsarkivet 2025. Detta har inte slutförts under året, arbetet fortsätter 2026.

- Stadens centrala informationssäkerhetsfunktion har tidigare rekommenderat Stockholms Stadshus AB att ansluta sig till registerförteckningsverktyget Draftit Privacy Records. Efter resonemang med bolagets externa dataskyddsombud är bolagets bedömning att det finns många fördelar med att använda Draftit men att Stockholms Stadshus AB som relativt litet bolag med elva anställda i dagsläget uppfyller kraven med den registerförteckning som finns upprättad idag i Excel. Argumenten är att bolaget har en relativt liten verksamhet som inte motiverar ett systemstöd, det skulle vara resurskrävande att föra över informationen i ett nytt system och det skulle skapa sårbarheter att uppgifterna finns i ett externt system som endast en medarbetare har utbildning i och tillgång till. Det finns i dagsläget inget ägardirektiv om att systemet måste användas.

  Staden centralt konstaterar att det idag är upp till varje förvaltning och bolag att upphandla och förvalta valfritt systemstöd för registerförteckning. Det finns ingen central styrning eller förvaltning av exempelvis DraftIT som många verksamheter valt att använda. Detta är en dyr, resurskrävande och ineffektiv modell för staden som helhet. Det finns därför planer på att istället gå över till en standardiserad funktionalitet för registerförteckning. Bolaget följer och anpassar sig efter nya direktiv under 2026.

- Stadens centrala informationssäkerhetsfunktion har tidigare rekommenderat förvaltningar/bolag att ansluta sig till Klassa för systematisk informationsklassning av verksamhetens tillgångar. Bolaget använder nästan enbart stadens centralt upphandlade verksamhetssystem. Bolagets bedömning är att det finns många fördelar med att använda Klassa men att Stockholms Stadshus AB som relativt litet bolag med tio anställda och endast ett system som inte är centralt upphandlat uppfyller kraven på informationsklassning

genom att säkerställa att centrala systemägare gjort normerande informationssäkerhetsklassningar för de system bolaget nyttjar i enlighet med DSOs rekommendationer.

Argumenten är att bolaget har en relativt liten verksamhet som inte motiverar användandet av Klassa, det skulle vara resurskrävande att utbildas i och införa ett nytt system och det skulle skapa sårbarheter att endast en medarbetare har kunskap tillgång till systemet. Det finns i dagsläget inget ägardirektiv om att systemet måste användas.

Under 2025 har informationsklassning dock utförts baserat på Bolagets information i majoriteten av de nyttjade systemen. Värdena är generellt lägre än de av staden normerande klassningarna. Dessa klassningar lagras ej i systemet Klassa.

Risk och sårbarhetsanalys

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleds 2026. Bolaget följer stadens risk- och sårbarhetscykel och instruktioner.

I RSA 2024 gjordes bedömningen att bolaget saknar samhällsviktig verksamhet men har däremot prioriterad verksamhet vad gäller styrning och beslutsfattande för bolagskoncernen samt faktura- och lönehantering för bolaget. Analysen landade i ett antal åtgärdsförslag och kontinuitetshanteringsplaner att hantera bl.a. vad gäller bortfall av infrastruktur, antagonistiskt hot samt sociala risker. Dessa prövas på nytt i RSA 2026.

Utöver bolagets egen risk- och sårbarhetsarbete kommer arbete ske inom områden som behandlas i stadens sektorsorganisation där Stadshus AB deltar i två sektorer.

Bolaget har uppfattat att staden ser över hur styrdokument och RSA-metoden kan utvecklas för att anpassas till de krav som ställs i NIS2/Cybersäkerhetslagen/CER.

Väsentlighets- och riskanalys (VOR) och internkontrollplan (IKP)

Genom en tillräcklig intern kontroll skapas förutsättningar för att upptäcka och förebygga risker i verksamheten samt säkra tillgångar, förhindra förluster och oegentligheter. Under 2025 har arbetet med internkontroll utvecklats av stadsledningskontoret i samverkan med Stockholms Stadshus AB och nya tillämpningsanvisningar tagits fram för bolagen. Internkontrollplanen för 2026 är framtagen utifrån dessa tillämpningsanvisningar.

Bland de obligatoriska processerna som ska ingå i väsentlighets och- riskanalysen finns Systematiskt informationssäkerhetsarbete. Stockholms Stadshus AB har bedömt att riskerna inom detta område (*Fastställa krav genom informationsklassning, Fastställa lokal anvisning för informationssäkerhet, informationssäkerhet inom upphandlingsförfarande, lokal rutin för behörighetshantering, Registerförteckning över personuppgifter, rutin för incidenthantering*) har låga riskvärden och dessa tas inte med i internkontrollplanen för 2026. Det finns tillräckliga rutiner för årlig översyn av *behörighetshantering* och *registerförteckningen över bolagets personuppgiftsbehandlingar* varför dessa inte längre behöver finnas med i internkontrollplanen.

Risker som identifierats i GDPR-årsrapport

GDPR-årsrapport är ett medel för styrelsen att ta emot de råd och rekommendationer som dataskyddsombudet (DSO) är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

I GDPR-årsrapport 2024 konstaterar DSO att verksamhetens dataskyddsarbete håller en hög nivå och att majoriteten av förra tillsynsårets föreslagna åtgärder har åtgärdats på ett lämpligt sätt.

DSO har granskat de sex obligatoriska granskningsområdena samt ett antal områden utöver de obligatoriska. Inledningsvis konstaterar DSO att verksamheten i hög utsträckning uppfyller de krav som ställs enligt dataskyddsförordningen och enligt den aktuella rapporten. DSO återger nedan de områden där vissa brister ändå finns som kan och behöver åtgärdas:

- DSO rekommenderar att de anställda får information om vad en personuppgiftsbehandling är och hur de ska gå tillväga vid en ny eller förändrad personuppgiftsbehandling, för att säkerställa att registerförteckningen återspeglar bolagets aktuella behandlingar.
- DSO rekommenderar att bolaget slutför arbetet med att kontrollera att samtliga genomförda informationsklassningar är aktuella, relevanta och att bolaget vid behov reviderar klassningarna.

- DSO rekommenderar att bolaget gör en inventering av samtliga pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter för att säkerställa att alla nödvändiga bedömningar genomförs.
- DSO uppmuntrar verksamheten att färdigställa en rutin för personuppgiftsincidenthantering som är anpassad för verksamhetens arbetssätt och övriga behov.
- DSO rekommenderar att de anställda får tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och allmänna handlingar.
- DSO rekommenderar bolaget att ta fram riktlinjer för hur AI får användas i verksamheten, för att säkerställa att AI hanteras på ett sätt som är förenligt med dataskyddsförordningen.

I samband med verksamhetsberättelse och bokslut tar bolaget del av dataskyddsombudets årsrapport för 2025 och stor hänsyn tas till eventuella rekommendationer till personuppgiftsansvarig som lämnas i rapporten. Nästa GDPR-årsrapport tas upp på koncernstyrelsemötet 13 april 2026.

Förbättringar för verksamhetens LIS

Stockholms Stadshus ABs lokala anvisning för informationssäkerhet

Den 16 september 2025 fastställde vice vd bolagets reviderade version av Lokal anvisning för informationssäkerhet. Anvisningen är förmedlad till medarbetare, diarieförd och finns tillgänglig för alla medarbetare på bolagets gruppdisk.

Åtgärder 2025

Under året har bland annat nedan arbete utförts:

- Översyn av Lokal anvisning för informationssäkerhet.
- Reviderad version av hanteringsrutin för informationssäkerhetsincidenter framtagen enligt rekommendation från DSO
- Revidering av nyttjandet av incidentrapporteringssystemet IA på börjats

- Behörighetshanteringsrutin efterlevd och dokumenterad.
- Medarbetare har genomfört Stadens utbildningar i informationssäkerhet och dataskydd
- Bolaget använder främst centrala system, men har påbörjat informationsklassningar för informationsmängden ur bolagets synvinkel i enlighet med DSOs rekommendationer
- Bolagets Dataskyddsombud har hållit en utbildning i GDPR och hantering av personuppgifter för bolagets medarbetare
- Bolaget har bidragit i stadens centrala arbete kopplat till personuppgiftsincidenten med miljödata. Bolaget omfattades inte av incidenten
- Bolaget har sett över och förenklat hanteringsanvisningar för hantering av allmänna handlingar

Åtgärder 3-årsplan

Under 2026 ska Stockholms Stadshus AB prioritera att:

- säkerställa att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbetet
- säkerställa att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- Utföra informationsklassningar
- årlig översyn av Lokal anvisning för informationssäkerhet
- årlig översyn av lokal rutin för informationssäkerhetsincidenter inklusive personuppgiftsincidenter på bolaget
- följa och vid behov uppdatera avtalshanteringsrutin
- följa och vid behov uppdatera behörighetshanteringsrutin
- ta fram gallringsframställan till Stadsarkivet för hantering av personaluppgifter i lönesystem
- Se över och vid behov uppdatera bolagets hanteringsanvisningar för hantering av allmänna handlingar
- Inleda ny risk- och sårbarhetsanalys där informationssäkerhet ingår i analysen
- Följa stadens nya inriktning för standardisering av basprocesser inom informationssäkerhet och dataskydd

Under 2027 ska Stockholms Stadshus AB prioritera att:

- säkerställa att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbetet.

- se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- gå igenom och uppdatera registret över personuppgiftsbehandlingar
- årlig översyn av Lokal anvisning för informationssäkerhet
- årlig uppdatering av Lokal incidenthanteringsrutin
- årlig behörighetsrevision (identitet och åtkomst)
- följa den framtagna rutinen för regelbundna informationsklassningar
- ta fram plan/rutin för hantering av digitala personalhandlingar/digital personalakt
- ta fram kontinuitetsplaner/åtgärdsplaner inom prioriterade verksamhetsområden utifrån RSA-analysSe över arkivfrågan kopplat till införandet ILS-modulen för hållbarhetsredovisning (CSRD).

Under 2028 ska Stockholms Stadshus AB prioritera att:

- säkerställa att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- säkerställa att genomgång av registret över personuppgiftsbehandlingar utförs
- genomföra årlig översyn av Lokal anvisning för informationssäkerhet
- genomföra årlig behörighetsgenomgång
- genomföra uppföljningar av övrig rutindokumentation t ex avtalshanteringsrutin, incidenthanteringsrutin m.m. utförs.
- följa den framtagna rutinen för regelbundna informationsklassningar

Fastställd av vice vd 2026-01-08