Stockholms stad

Informationssäkerhet

Ledningens genomgång 2025

Stockholm Business Region

Beslutad: 2024-04-22
Reviderad: 2025-09-01

Ledningens genomgång

Dnr: 2025/205

Kontaktperson: Emil Brynielsson, ISAM

1 Sammanfattning

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* uppmanas samtliga nämnder och bolagsstyrelser att ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet under de kommande tre åren. Denna ska biläggas verksamhetsplan. Planeringen för de kommande tre åren ska utgå från nämndens verksamhetsuppdrag i budget och följa *Riktlinje för informationssäkerhet* i Stockholms stad.

Alla nämnder och bolagsstyrelser ska prioritera att inventera och informationsklassa informationstillgångar som används i verksamheten alternativt se över och uppdatera genomförda informationsklassningar enligt tillämpningsanvisningarna till stadens riktlinje för informationssäkerhet.

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet

Innehållsförteckning

2 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 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 riktlinje för informationssäkerhet och tillhörande tillämpningsanvisning som är bilagor till stadens Kvalitetsprogram[2]. Tillämpningsanvisningen revideras årligen och fastställs av stadsdirektören.

Tillämpningsanvisningen reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete.

2.1 Vad påverkar SBR informationssäkerhetsarbete

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Stockholm Business Region 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.

2.1.1 Budget 2025

Utifrån budget finns medel för extern DSO respektive rådgivning knuten till bolaget. Internt har bolaget ISAM-rollen utpekad. Medel finns även avsatta för ISAMs hela uppdrag. SBR har i budget för 2025 avsatt 300 tsek för extern rådgivning och konsultation.

I *kommunstyrelsens-forslag-till-budget-2024.pdf* anges vidare att beredskapsförmågan ska fortsätta öka, exempelvis genom att analysera och hantera risker- och sårbarheter samt genom krisledningsplanering, kontinuitetshantering, systematiskt informationssäkerhetsarbete, krigsorganisation samt årliga, obligatoriska krisledningsövningar.

[2] Stockholms stads kvalitetsprogram (start.stockholm)

2.1.2 Risk och sårbarhetsanalys

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel.

Bolagets organisation avseende riskhantering är organiserad med centrala funktioner (riskhanteringsfunktion, regelefterlevnadsfunktion, internrevision och arkivarie) samt därutöver ISAM och DSO.

Vad avser RSA hanteras dessa risker av verksamheten i samarbete med bolagets ovan beskrivna riskhanteringsfunktion. Varje risk har en riskägare och åtgärdsplan (såvida inte risken accepteras). Riskhanteringsfunktionen rapporterar risknivåer, riskhantering med mera till styrelsen vid behov. Riskhanteringsfunktionens arbete bör kontrolleras av internrevisionen.

Dokumentering ska ske enligt stadens riskanalysverktyg för informationssäkerhet.

2.1.3 Resultatet från revision

Inom området informationssäkerhet kan följande noteras

- Årsrapport 2024 från stadsrevisionen[3]
    - Rekommendation att genomföra informationsklassning av samtliga mindre informationstillgångar har utförts.

2.1.4 DSO rekommendationer och arbete 2025

Registerförteckning:

- Utvärdera arbetet med hur registerförteckningen ska hållas uppdaterad avseende nya behandlingar och systemförändringar.
- Effektivisera och använd de tekniska möjligheterna i systemstödet för registerförteckningen.
- Ta fram checklista utifrån punkterna ovan.

Styrdokument

- Dataskyddsombudet fortsätter sitt rådgivande och stödjande arbete vid framtagande och uppdatering av styrdokument, strategier samt rutiner avseende dataskydd. Rutin för den registrerades rätt till tillgång till personuppgifter, s.k. registerutdrag är framtagen.

[3] Rapport från stadsrevisionen. Dnr: RVK 2025/16

Tekniska och organisatoriska åtgärder och personuppgiftsincidenter

- Fortsätt att säkerställa att tekniska och organisatoriska åtgärder implementeras i enligt med dataskyddspraxis.
- DSO ska stödja med att upprätta en instruktion avseende legal praxis att beakta vid informationsklassning under 2025.
- Utbilda verksamheten i och involvera ISAM och DSO vid personuppgiftsincidenter.

Konsekvensbedömning avseende dataskydd

- Implementera Integritetsskyddsmyndigheten metodstöd och mallar för konsekvensbedömning.
- Metodstödet rekommenderas att ingå i strategidokument för att operativt användas för att hantera och minimera integritetsrisker.

Registrerades rättigheter

- Fortsätt att ta fram instruktioner avseende de registrerades rättigheter.
- Översyn av integritetspolicy för att säkerställa att den är i överenstämmelse med gällande rättspraxis.

ISAM har utifrån DSO:s rekommendationer uppdaterat registerförteckningen utifrån systemförändringar och tagit fram personuppgiftsbiträdesavtal med användande av stadens avtalsmall. Vid användande av stadens avtalsmall, som kvalitetssäkras av juridiska avdelningen, synliggörs tredjelandsöverföring av leverantör och tredjelandsöverföringsbedömningar kan utföras. Tredjelandsöverföringsbedömningar, s.k. TIA har genomförts under 2025. Stadsledningskontorets vid var tid uppdaterade mall har använts.

Ett arbete har även utförts med att uppdatera Intranätet med mallar och metodstöd.

En del i skyddet för individens personliga integritet är att SBR ska ge DSO insyn och tillse att denne kan utföra sina lagstadgade uppgifter. Detta omhändertas mycket väl av SBR.

3 Utvecklingsområden för verksamhetens LIS

3.1 SBR:s lokala anvisning för informationssäkerhet

Den 27/10 2023 fastställde VD *Lokala anvisning för informationssäkerhet* (reviderad 2024-11-05). Anvisningen är presenterad för samtliga chefer och finns även tillgänglig för alla medarbetare på bolagets intranät.

Enligt anvisningen har SBR flera aktiviteter som drivs löpande under hela året och av flera olika roller. Ett årshjul har tagits fram för att säkra att aktiviteter blir klara.

I samband med verksamhetsberättelse och bokslut tar bolaget del av dataskyddsombudets årsrapport och hänsyn tas till rekommendationer till personuppgiftsansvarig som lämnas i rapporten.

3.2 Kompetenslyft ledningsgrupp

Ledningsgruppen har genomfört ”*Kompetenslyft för ledningsgrupper inom informationssäkerhet*” kompetenslyft kring Informationssäkerhet med hjälp av en extern konsult. Arbetet behöver fortsätta löpande samt att tilltänkt framtida stadsövergripande stöd finns tillgängligt ”*Kompetenslyft och e-utbildning till ledningsgrupp, chefer och medarbetare*” där sökt bas främst här är det repetitiva över hela året samt möjlighet att, med underlag, kunna jobba med sin grupp. Fler liknande uppslag lär bli aktuella när behov uppstår.

3.3 SBRs prioritering för 2025 är:

- Arbetet utgår från informationshanteringen i verksamhetens ordinarie processer.
- Säkerställa att informationssäkerhets- och dataskyddsfrågorna lyfts fram och ingår i det interna utvecklingsarbete som pågår inom verksamheten, särskilt för nya digitala tjänster och verktyg som erbjuds.
- Lyfta chefsansvaret och att enkelt beskriva vilka uppgifter som ingår i ansvaret för olika roller, utifrån tillämpningsanvisningar till stadens riktlinje för informationssäkerhet och hur det kan integreras i vardagen.
- Se över incidenthanteringsprocessen (informations/IT-säkerhet och dataskydd) för att säkerställa att den bidrar till snabb identifiering, bedömning, hantering och återställning.

Incidenthanteringsprocessen kan även i sig bidra till att incidenter förebyggs.

4 Åtgärder kommande 3 år

Bolaget ska löpande följa upp att den lokala anvisningen för informationssäkerhet följs, främst med fokus på att:

- chef årligen ser till att samtliga medarbetare och konsulter genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd. Chefen uppmanas genomföra utpekade chefsutbildningar på stadens Intranät, se LÄNK (Utbildningar inom informationssäkerhet).
- följa upp och utreder de incidenter som verksamheten dokumenterar och rapporterar i IA[4].
- bolaget har ett ständigt systematiskt återkommande inslag av informationssäkerhet, genom att chefer själva går/genomför stadens kommande mindre ”tema-utbildningar” samt marknadsföra dessa för sina anställda.
- Objektägare ska:
  - tillse att informationstillgångar är klassade.
  - tillse att handlingsplaner från klassning tas om hand.
  - använder bolagets stödjande funktioner och rutiner.

4.1 Under 2026 ska SBR:

- utföra årlig översyn av Lokal anvisning för informationssäkerhet.
- fortsätta att komplettera objektansvar med processansvaret, väga med kopplingen till registerförteckning som baseras på personuppgiftsbehandlingar ur ett processperspektiv.
- tydliggöra ansvarsroller där identifierat behov av informationsklassning ännu inte upplevts få en rimlig effekt exempelvis om en teknisk skyddsåtgärd inte blir implementerad.
- tydliggöra informationssäkerhet inklusive dataskydd i inköpsprocessen tidigaste steg.
- säkerställ att informationssäkerhets- och dataskyddsfrågorna lyfts fram och ingår i det interna utvecklingsarbete som pågår inom verksamheten, särskilt vid framtagandet av nya digitala tjänster.

[4] Det finns dokumenteringskrav i bl.a. dataskyddsförordningen.

- årlig behörighetsrevision (identitet och åtkomst) av samtliga informationstillgångar/objekt.
- säkerställa att SBR:s hanteringsanvisningar och registerförteckning hålls uppdaterade i samarbete med registrator.
- uppmana chefer och medarbetare att gå stadens utbildningar.
- genomföra samt vid behov uppdatera årshjulet för informationssäkerhet.
- årlig översyn och vid behov revidering av Ledningens genomgång.

4.2 Under 2027 ska SBR:

- årlig översyn av Lokal anvisning för informationssäkerhet.
- etablera en rutin för regelbundna informationsklassningar.
- övergång till att informationsklassa informationen i processerna i objekten.
- årlig behörighetsrevision (identitet och åtkomst).
- följa den framtagna rutinen för regelbundna informationsklassningar.
- årlig översyn och vid behov revidering av Ledningens genomgång.

4.3 Under 2028 ska SBR

- årlig översyn av Lokal anvisning för informationssäkerhet.
- etablera en rutin för regelbundna informationsklassningar.
- utvärdera täckningen av att endast informationsklassa processer.
- årlig översyn av Lokal anvisning för informationssäkerhet.
- årlig behörighetsrevision (identitet och åtkomst)
- följa den framtagna rutinen för regelbundna informationsklassningar.
- granska hur väl lokal rutin för regelbundna informationsklassningar följs.
- öva utifrån kontinuitetsplaner.
- årlig översyn och vid behov revidering av Ledningens genomgång.