Ledningens genomgång informationssäkerhet 2025

Sammanfattning

Ledningens genomgång innebär en genomlysning av befintligt ledningssystem för informationssäkerhet och förbättringsförslag med åtgärder. Bolagschef ska, enligt stadens tillämpningsanvisning för informationssäkerhet, minst årligen informera sig om bolagets informationssäkerhetsarbete. Det sker genom att bolagschef inhämtar rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren.

Bakgrund

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska 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 bolagschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. 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 2025[2] 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 bolagets verksamhetsuppdrag i budget och följa Riktlinje för informationssäkerhet i Stockholms stad.

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

---

[1] Stockholms stads kvalitetsprogram (start.stockholm)

[2] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet. I riktlinje för informationssäkerhet i Stockholms stad beslutad av kommunfullmäktige 2022-02-21, Dnr: 2021/866 står att ”Stadens inriktning är att informationssäkerhetsarbetet inom nämnder och styrelser ska utgå från den internationella standarden SS-ISO/IEC 27001/2. Informationssäkerhetsarbetet ska alltid utföras med hänsyn tagen till stadens övergripande mål samt till nämnders och styrelsers egna verksamhetsuppdrag.”

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. Tillämpningsanvisningen revideras årligen och fastställs av stadsdirektören. Tillämpningsanvisningen reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete.

SISAB har utarbetat en lokal tillämpningsanvisning LTA för informationssäkerhet som specificerar hur stadens övergripande ledningssystem och insatser appliceras inom SISAB. För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska SISAB 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.

Omvärldsbevakning- Förändringar i externa och interna frågor som är relevanta för ledningssystemet för informationssäkerhet

Krav på informationssäkerhet baseras dels på interna verksamhetskrav, dels på rättsliga och avtalsmässiga krav samt utifrån krav från intressenter. Informationssäkerhetsarbetet är därför inte isolerat, utan SISAB:s informationssäkerhet integreras i alla verksamhetsprocesser och samordnas med ledningsarbetet.

Vid internt utvecklingsarbete, särskilt vid framtagande av nya digitala tjänster, ska säkerställas att informationssäkerhets- och dataskyddsfrågorna alltid lyfts fram och ingår i arbetet.

Lagstiftning och avtalsmässiga krav

SISAB ser ständigt över de lagar och krav som är relevanta för verksamheten. Från och med 15 januari 2026 kommer nya cybersäkerhetslagen att gälla, lagen är den svenska implementationen av det så kallade NIS 2-direktivet som ämnar att stärka EU:s gemensamma cybersäkerhet. Den nya lagen innebär att offentliga verksamhetsutövare bland annat ska vidta åtgärder för att skydda sina nätverks- och informationssystem, och rapportera betydande incidenter. Det finns även krav på att ledningsgrupper ska delta i cybersäkerhetsutbildning.

Övrig påverkan

Av kommunfullmäktiges budget för 2026[3] tas det bland annat upp att staden ska ”utveckla och stärka arbetet med informationssäkerhet samt beakta risker och sårbarheter med generativ AI och syntetisk media”.

Risk och sårbarhetsanalys (RSA)

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. Under 2025 har arbetet gällande informationssäkerhet fokuserat på kontinuitetshantering. Ett arbete med framtagande av kontinuitetsplaner har genomförts under året. Kontinuerligt arbete med att fortsätta utveckla planerna och samordna med andra verksamhetsområden fortsätter under 2026. Under 2026 påbörjas en ny RSA-cykel, då en workshop planeras för en bredare involvering av medarbetare kopplat till RSA-arbetet.

Resultat av egen uppföljning (IKP)

Internkontrollen inom SISAB hanterar informationssäkerhet inom bedömningar kopplat till väsentlighet och riskanalys och kommer under 2026 särskilt kommentera det förebyggande arbetet kring processer gällande informationssäkerhet

Resultat från revisioner

Under år 2025 har inga rekommendationer från revisionen lämnats om informationssäkerhet.

Informationssäkerhetens prestanda

Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Lokala tillämpningsanvisningar avseende roller och ansvar, övergripande informationssäkerhet samt instruktioner för olika områden har tagits fram och revideras vid behov.

- Riktlinje för IT-användning
- Instruktion Informationssäkerhetsincident
- Instruktion distansarbete SISAB
- Instruktion för informationsklassning
- Instruktion för videomötestjänster.

De lokala tillämpningsanvisningarna kompletterar stadens centrala riktlinjer och tillämpningsanvisningar för informationssäkerhet och beskriver hur SISAB tillämpar de övergripande reglerna av informationssäkerhetsarbetet, roller och ansvar i den egna verksamheten.

Avvikelser och korrigerande åtgärder

Arbetet med att identifiera avvikelser och förstärka SISAB:s informationssäkerhet, både organisatoriskt och tekniskt fortgår. SISAB har under 2025 arbetat med att identifiera och förstärka de mest kritiska delarna av verksamheten. Detta arbete har framförallt

fokuserats på det tekniska nätverket (T-LAN) där flera insatser har gjorts för att förbättra cybersäkerheten i samarbete med leverantören. Det har bland annat:

- Genomförts penetrationstester på webapplikationer för att identifiera och åtgärda sårbarheter.
- Införts ett verktyg för förbättrad logginsamling och mönsteranalys för att kunna upptäcka intrång eller andra incidenter snabbare.
- Skett ett utbyte av gamla fysiska servrar.
- Införts ny programvara för mikrosegmentering, en uppdelning av nätverket i små delar för att begränsa spridningen av hot inom nätverket.

Utöver dessa tekniska åtgärder har det även införts en process för digital utveckling, revidering av instruktion för cybersäkerhet och även upprättats kontinuitetsplaner för verksamhetskritiska system.

Flera aktiviteter är planerade för 2026, däribland:

- vidare penetrationstester av servrar och webbapplikationer
- Återläsningstester av säkerhetskopior och testning av katastrofåterställningsplan
- Framtagning av fler träningsmoduler för att öka cybersäkerhetsmedvetandet
- Vidare utveckling av införd programvara och uppdatering till säkrare hårdvara

Incidentrapportering/statistik

Under perioden 3 november 2024 tom 3 november 2025 har 8 stycken informationssäkerhetsincidenter rapporterats i IA-systemet, en minskning jämfört med föregående år.

Av dessa 8 incidenter var endast en verksamhetspåverkande, detta var nätverksproblem i stadens nät, och en personuppgiftsrelaterad, SISAB-filmer med personuppgifter var uppladdade på Youtube. Resterande var rapporterade i informerande syfte så som borttabbade mobiler, kort och phishing-mail.

Resultat från övervakning och mätning

Informationssäkerhetssamordnare (ISAM) arbetar tillsammans med identifierade informationsägare med verktyg för efterlevnad som fungerar som hjälp för organisationen att stämma av organisationens efterlevnad av standarden SS/EN ISO 27001.

Identifiering av processer och oönskade händelser

Arbetet med klassning fortlöper och av bolagets ungefär 80 system och tjänster har 23 klassats och blir årligen omklassade. Fokus har legat på att klassa de mest kritiska systemen och tjänsterna, men klassningen är nu en del av alla upphandlingar för att försäkra att informationssäkerhetskraven är med i upphandlingskraven. Arkivfunktionen deltar för att försäkra att klassningarna förhåller sig till hanteringsanvisningarna.

Arbetet med att uppdatera bolagets register över behandling, registerförteckningen, fortlöper. Registerförteckningen ska vara processbaserad utifrån hanteringsanvisningarna.

Värdering och hantering av oönskade händelser

Många av verksamhetens informationstillgångar saknar informationsklassning. Dock har bolagets viktigaste system prioriterats och system, som enligt stadens nya tjänsteavtal ska flyttas, har klassats. Av de cirka 80 systemen är det ungefär hälften som är av sådan art att en klassning bör genomföras. Bedömningen är att säkerheten även i de oklassade systemen är fullt tillräcklig men med en klassning får vi dokumentation på att SISAB på ett strukturerat sätt har klassat informationen och kan matcha med rätt säkerhetsnivå. Arbetet fortsätter under 2026 med att informationssäkerhetsklassa tillgångarna enligt årshjulet[4].

Obligatoriska utbildningar inom Informationssäkerhet för medarbetare i staden

2025-11-05 21 hade 233 tillsvidareanställda genomfört den obligatoriska utbildningen i informationssäkerhet. 8 anställda har aldrig genomfört utbildningen och för 24 anställda har utbildningen utgått, vilket innebär att de har genomfört utbildningen men att det har gått mer än ett år sedan dess. För grundutbildningen i dataskydd är siffrorna likande med: 233 som gjort utbildningen, 17 där den utgått och 16 som aldrig gjort utbildningen. Information har gått ut till samtliga berörda chefer som har återkopplat om att de skall påminna sina medarbetare om att genomföra utbildningen.

Det är en klar förbättring mot föregående år då 139 medarbetare hade genomfört utbildningarna men det finns en utvecklingspotential så att det säkerställs en löpande en hög andel genomförda utbildningar.

För konsultkonton är siffrorna mycket sämre där endast 10 konsultkonton har genomfört respektive utbildning och 100 konsulter har aldrig genomfört utbildningen i informationssäkerhet och 95 har aldrig genomfört utbildningen i grundläggande dataskydd.

Här bör rutinen utvecklas för att säkerställa att konsulter med SISAB-dator genomför dessa utbildningar.

Årshjul

Anger informationssäkerhetssamordnarens årliga plan för informationssäkerhetsarbetet. Årshjulet utgår från stadens tillämpningsanvisningar för informationssäkerhet, SISAB:s informationssäkerhetsmål och övrigt som framkommer under verksamhetsåret inklusive dataskydd.

Regelbundna aktiviteter som genomförs årligen:

Några rekommendationer i DSO-årsrapport:

- Roll och ansvar för dataskydd i verksamhetsprocesserna, utifrån hanteringsanvisningarna, behöver sättas för att kunna systematiskt hantera t.ex. en begäran om tillgång till personuppgifter, ett registerutdrag.
- Arbetet med att uppdatera och förteckna personuppgiftsbehandlingar processbaserat i ett behandlingsregister behöver fortsätta under 2026 för att bland annat säkerställa laglig grund för hantering av personuppgifter.

[4] Lokala tillämpningsanvisningen Dnr SISAB 2025/42

- Fortsätta att ta fram styrdokument, strategier och uppdatera instruktioner såsom exempelvis angående de registrerades rättigheter, så som rätten till radering.
- Fortsätta att implementera tekniska och organisatoriska åtgärder i enligt med dataskyddspraxis, som exempelvis kryptering och pseudonymisering.
- Årlig översyn av integritetspolicy och instruktion/rutin för att säkerställa att integritetspolicyn internt- och externt tydligt informerar enligt gällande praxis.
- Införliva den nya mallen för konsekvensbedömning avseende dataskydd i verksamheten, likaså stadens mall för tredjelandsöverföringsbedömning.
- Utveckla rutinen för att säkerställa att konsulter med SISAB-dator genomför stadens utbildningar i dataskydd och informationssäkerhet

Planerade och genomförda aktiviteter samt planering inför kommande år

ISAM övriga händelsestyrda uppgifter:

- incidenthantering
- informationsklassningar
- följa upp anställningsförändringar - behörighetsrevision
- följa upp framtagna instruktioner
- kravhantering inför inköp/anskaffning system/tjänst och molntjänster
- remisshantering
- utbilda specifika målgrupper
- säkerställa systemlista med objektägare/processägare
- genomföra säkerhetsmånad i oktober

SISAB har arbete kvar avseende informationssäkerhetsklassificeringar samt även fortsatt utveckling av medarbetares kompetens där stadens obligatoriska utbildning är fortsatt prioriterat under 2026 och kommande år. En rutin för att säkerställa att konsulter med användarkonto hos SISAB genomför dataskydd- och informationssäkerhetsutbildningarna bör tas fram. Klassningsarbete och känslighet av information har tidigare i stor grad varit fokuserat på personuppgifter. Det kan dock förekomma känslig information i andra typer av data, till exempel ritningar. SISAB har i dagsläget inte till fullo sekretessklassat ritningar som innehåller känslig information om placering av skyddsvärda komponenter som brandlarm, inbrottslarm, servrar och nätverksutrustning. Ett arbeta att identifiera och sekretessklassa denna typ av ritningar behöver göras. Med hjälp av det systemstöd som finns i FasTwin bör detta prioriteras under 2026.

Under 2025 har stora framsteg gjorts med att tillsammans med driftleverantör förbättra den säkerheten på det tekniska nätverket, detta arbete bör fortsätta under 2026 för att säkerställa att säkerheten är tillräcklig enligt NIS2 och cybersäkerhetslagen. Vidare bör incidenthanteringen vidareutvecklas för att försäkra att verksamheten har kapaciteten att generera de incidentrapporter som krävs i tid.

Det krävs även ett arbete med att förbättra systemöversikten och försäkra att alla system är beskrivna och har systemägare och objektägare.

SISAB bör även utveckla styrningen kring generativ AI.

Informationssäkerhetsmål

Stadens tillämpningsanvisningar för informationssäkerhet består av övergripande mål. Målen har anpassats till SISAB:s lokala behov. Kortsiktiga informationssäkerhetsmål är mål som direkt eller indirekt uttrycker hur SISAB som organisation på cirka 1–2 år ska arbeta för att uppnå verksamhetens långsiktiga strategiska mål. De kortsiktiga målen är konkreta och har en tydlig koppling till de analyser som organisationen har gjort.

Effektmål anger vilken effekt SISAB eftersträvar på lång sikt genom organisationens informationssäkerhetsarbete. Målen handlar om hur SISAB ska stödja och förbättra organisationens informationssäkerhetsarbete. Resultatmål anger vilka resultat SISAB eftersträvar på lång sikt genom organisationens informationssäkerhetsarbete. Dessa mål handlar mer övergripande om hur SISAB som organisation långsiktigt ska arbeta med informationssäkerhet.

Kortsiktigt måste arbetet med att informationsklassa de system som ännu inte har klassats fortlöpa för att försäkra att känslig information har tillräckligt skydd. Arbetet med registerförteckningen bör även prioriteras. Målet är att den ska vara fullständigt ifylld och uppdaterad i enlighet med processerna i hanteringsanvisningen, och de system som är kopplade till processerna. All tredjelandsöverföring ska även vara dokumenterad i registerförteckningen.

Resultat från riskbedömning och status för riskbehandlingsplan

Riskbedömning är processen för att bestämma hur allvarlig en risk är. Allvarlighetsgraden bestäms utifrån en sammanvägning av både sannolikhet för risken och dess konsekvenser.

Handlingsplan är en ”att-göra-lista” som tar upp åtgärder som inte kan genomföras omedelbart.

SISAB:s riskbedömning genereras genom arbetet med informationsklassning. En handlingsplan erhålls efter klassningsarbetet. Handlingsplanen ligger till grund för riskanalysen där ställning skall tas över om standardåtgärderna är tillräckliga. Riskerna förs in i en åtgärdsplan (verktyg-utforma-åtgärdsplan).

Dataskyddsförordningen och Integritetsskyddsmyndigheten ställer upp kriterier för när en konsekvensbedömning avseende dataskydd ska genomföras, likaså vad som är dataskyddsrisker som har påverkan på individ.

Möjligheter till ständig förbättring 2025–2026

Under 2025 och 2026 föreslås följande prioriterade åtgärder som aktiviteter:

- att bolagets klassificeringstruktur och hanteringsanvisningar efterlevs processtyrt
- att informationssäkerhet följs upp vid leverantörsmöten
- att registerförteckningen fylls i fullständigt
- att en incidentrapporterings-procedur tar fram i enlighet med nya cybersäkerhetslagen
- att förbättra systemöversikten och förtydliga roller och ansvar

Planerade aktiviteter och prioriterat arbete under kommande perioder

SISAB behöver sammanfattningsvis:

1. Arbeta med att klassningars handlingsplaner fullföljs
2. Arbeta med att implementera de organisatoriska och tekniska åtgärder som krävs av nya Cybersäkerhetslagen
3. Tilldela informationsägare och systemägare för respektive system
4. Följa upp utbildningsinsatser för chefer och medarbetare och ta fram en rutin för att säkerställa att konsulter med användarkonto hos SISAB genomför utbildningarna
5. Kontinuitetsplanera för att motverka risker som är identifierade och prioriterade enligt RSA
6. Fastställa en AI-riktlinje för att motverka risker kopplat till generativ AI

Ebba Bock Agerman
VD

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Ebba Bock Agerman, VD	2025-11-27
Anders Lundbeck, Ekonomichef	2025-11-27