Stockholms stad

Ledningens genomgång 2025

Hässelby-Vällingby stadsdelsförvaltning

Sammanfattning

Rapporteringen Ledningens genomgång ska ge information och underlag till förvaltningschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltningschef ska säkerställa att aktiviteter som rör informationssäkerhet och dataskydd tas upp i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.

Rapporten går igenom analys av nuläget och kommer med rekommendationer för det fortsatta arbetet vad gäller informationssäkerhet. Rapporten går även igenom årets informationssäkerhetsincidenter samt gör en analys utifrån ISO 27001 för att kunna visa hur förvaltningens arbete med informationssäkerhet fortgår.

2025 har varit ett intensivt år utifrån informationssäkerhetsperspektivet. Förvaltningen har gått i väntans tider gällande NIS2, fått nya regler gällande kameraövervakning och sett informationssäkerhet ta plats i kommande budget. Under året har förvaltningen haft flera informationssäkerhetsincidenter men det som förvaltningen kommer minnas mest är Miljödata som fick stor påverkan bland annat för att anställda med skyddade personuppgifter fick dessa röjda.

Under året har arbetssätt och metoder för att underlätta och kvalitetssäkra betet tagit form och förankrats. ISAM och förvaltningschef har löpande avstämningar, trillingens samarbete har konkretiserats och blivit etablerat som ett arbetssätt som fler förvaltningar önskar följa efter.

Arbetet med att informationssäkerhetsklassa förvaltningens gedigna ”backlog” av oklassade digitala objekt har fått stå tillbaka till stor del för nya objekt som verksamheterna sett behov av att införa. Förvaltningen ser ett ökat incitament från verksamheterna att vara nyfikna på och vilka använda nya digitala verktyg i sitt arbete.

När nu 2025 närmar sig sitt slut så blir det mycket tydligt att digitaliseringen och informationssäkerheten är i otakt. Digitaliseringen skjuter iväg med en starkt uppåtgående kurva medan informationssäkerhetsarbetet inte klarar av att hålla jämna steg.

Men glädjande är att Cybersäkerhetslagen med (NIS2) med största sannolikhet börjar gälla i januari 2026, vilken kommer hjälpa till att ge fokus på informationssäkerheten och tydliggöra att det inte längre bara är en digitaliseringsfråga.

Louise Högberg
Informatiossäkerhetssamordnare (ISAM)
Hässelby-Vällingby stadsdelsförvaltning

Hässelby-Vällingby stadsdelsförvaltning
Stabsenheten

Hässelby torg 20-22, 3 tr
Box 3424
165 55 Hässelby
Telefon 08-50804501
louise.hogberg@stockholm.se
start.stockholm

Innehåll

Sammanfattning **1**

1. Systematiskt informationssäkerhetsarbete **3**

1.1 Vad är Ledningens genomgång 3

1.2 Ledningssystem för informationssäkerhet 3

2. Omvärldsbevakning – hot, trender och ny lagstiftning **4**

2.1 Cybersäkerhetslagen med NIS2-direktivet 4

2.1.1 Påverkan på Hässelby-Vällingby sdf *4*

2.2 AI-förordningen 5

2.2.1 Påverkan på Hässelby-Vällingby sdf *5*

2.3 Nya regler för kameraövervakning 5

2.3.1 Påverkan på Hässelby-Vällingby sdf *5*

3 Vad händer inom staden – budget, inriktningar, lokala förändringar och satsningar **6**

3.1 Centrala styrning 6

3.1.1 Påverkan på Hässelby-Vällingby sdf *6*

3.2 Lokal mognadsmätning 7

4 Uppföljning av informations-säkerhetsarbetet i Hässelby-Vällingby sdf **7**

4.1 Uppföljning av mål i verksamhetsplanen 2025 7

Förväntat resultat: *7*

4.1.1 Väsentlighets- och riskanalys samt Internkontrollplan *8*

4.2 Uppföljning av dataskyddsombudets årsrapport 2024 11

4.3 Information om avvikelser och incidenter 14

5 Förslag till förbättringar och aktiviteter **15**

5.1 Förbättringsaktiviteter 2026 15

5.1.1 Övergripande *15*

5.1.2 Kompetenshöjande insatser informationssäkerhet *15*

5.1.3 Uppdatering av styrdokumentation *15*

5.1.4 Informationklassning och konsekvensbedömning *16*

5.1.5 Pm3-specifikt *16*

5.2 Förbättringsaktiviteter 2027 16

5.2.1 Pm3-specifikt *16*

5.3 Förbättringsaktiviteter 2028 17

6 Förkortningar och begrepp **17**

1. Systematiskt informationssäkerhetsarbete

Ledningens genomgång är en del i ett systematiskt informationssäkerhetsarbete. Ledningen ska hålla sig informerad om informationssäkerheten i sin verksamhet. Stadsdelsnämnden är informations- och personuppgiftsansvarig medan förvaltningsdirektören är operativt ansvarig och ska se till att resurser finns, samt att medarbetare har den utbildning och information som krävs.

Övergripande informationssäkerhetsansvarig finns på stadsledningskontoret. Lokalt i nämnden finns en informatiossäkerhetssamordnare (ISAM). Informationssäkerhetens ansvar ska följa linjeorganisationens. Nämnden arbetar utifrån stadens riktlinjer och tillämpningsanvisningar och ska anta den lokala anvisningen.

1.1 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 inhämta en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, utbildning av medarbetare samt om informationsklassningar och registerförteckning är genomförda.

I denna genomgång presenteras status på olika aktiviteter och krav. Under sista delen presenteras förslag till förbättringsaktiviteter.

1.2 Ledningssystem för informationssäkerhet

Ledningssystem för informationssäkerhet (LIS) är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter vilket består av Stockholms stads övergripande tillämpningsanvisningar för informationssäkerhet samt de rutiner, guider och anvisningar som finns antagna.

Beslut om ledningssystem för Hässelby-Vällingby stadsdelsförvaltnings informationssäkerhet har tagits genom de lokala tillämpningsanvisningarna fastställda av direktör 2023-03-24. I den beskrivs förvaltningsspecifik organisation, årshjul och rutiner för verksamheten som rör informationssäkerhet. Den lokala tillämpningsanvisningen ha nu några år på nacken och håller på att revideras.

2. Omvärldsbevakning – hot, trender och ny lagstiftning

2.1 Cybersäkerhetslagen med NIS2-direktivet

Under 2025 har förvaltningen sett hur cyberattacker i olika former blir allt vanligare inom kommunal verksamhet. Förvaltningen behöver därför fortsätta värdera vår information och göra säkerhetsåtgärder för att skydda den.

NIS2 är ett EU-direktiv, vilket innebär att direktivet ska implementeras i nationell lag innan det börjar gälla. I Sverige implementeras direktivet i Cybersäkerhetslagen (CSL), vilken, med största sannolikhet, kommer att börja gälla den 15 januari 2026. Jämfört med det nu gällande NIS-direktivet skärps kraven för att säkra samhällsviktiga funktioner.

De grundläggande kraven är:

- Arbeta systematiskt och riskbaserat
- Identifiera och hantera risker
- Upprätta interna regler och arbetssätt
- Säkerställa kompetens och utbildning
- Vidta proportionella säkerhetsåtgärder

Cyberhetslagen pekar ut ledningens ansvar. Ledningen ska godkänna säkerhetsåtgärder samt övervaka genomförandet av dessa. Ledningen hålls även mer tydligt ansvariga för brister. Vidare är ledningen skyldig att genomgå utbildning. Ledningen bör även erbjuda regelbunden utbildning till övriga medarbetare.

Med Cyberhetslagen kommer det bli tydligare vad förvaltningen som myndighet ska göra och att kontroller och sanktionsavgifter kommer öka om vi inte klarar av att leva upp till lagstiftningen.

2.1.1 Påverkan på Hässelby-Vällingby stadsdelsförvaltning

Stadens centrala funktion (på SLK) för informationssäkerhet har fått resursförstärkning och funktionen har flyttats från Avdelningen för it och digitalisering till Säkerhetsavdelningen. Vilket sänder signaler att informationssäkerhet går från att vara en del i digitalisering till att vara en del i säkerhetsarbete. Framöver kommer förvaltningen se detta genom att exempelvis informationssäkerhet blir en allt viktigare del i verksamheternas kontinuitetsplaner. Förvaltningen ser fram emot att den centrala funktionen nu är bättre rustad för att ge stöd i kommande arbete och att samarbetet lokalt och centralt kan utökas.

Förändrade riktlinjer från staden gällande informationssäkerhet kommer innebära ett fortsatt ökat tryck på arbetet lokalt. Det kommer innebära att förvaltningen behöver lägga mer resurser för att svara upp mot lagkrav, stadens riktlinjer samt omhänderta fler och mer komplexa incidenter vid exempelvis cyberattacker. Chefer behöver ta ett större ansvar för att medarbetare tar del av utbildningar och information om vad som åligger varje medarbetare.

2.2 AI-förordningen

AI-förordningen trädde i kraft i augusti 2024. Ett av förordningens syften är att reglera och definiera vad man får och inte får göra med AI-hjälpmedel.

För all AI-behandling krävs fortfarande konsekvensbedömning utifrån dataskyddsförordningen och informationsklassning av användandet. Detta för att kontrollera att användningen följer lagstiftningen och rätt skyddsåtgärder är vidtagna.

Användandet av AI ökar i samhället och tjänster som bygger på AI blir allt fler. Användandet av AI inom kommunal verksamhet är fortfarande relativt begränsat. Men i och med att allt fler använder AI privat ökar kunskapen och nyfikenheten om hur AI kan användas även i tjänsteutövning.

2.2.1 Påverkan på Hässelby-Vällingby stadsdelsförvaltning

Allt fler tjänster och produkter får AI inbyggt från start och förvaltningen som användare förstår inte alltid att AI arbetar i bakgrunden. I rollen som ISAM är det ett konstant arbete med att bevaka om och hur dessa tjänster finns med vid t ex uppgraderingar av tjänster. Här är Zoom ett tydligt exempel, där AI-funktioner har funnit med vid uppgraderingar utan att dessa har informationssäkerhetsklassats innan driftsättning.

Förvaltningen ska uppmuntra och stödja verksamheterna i att använda AI på ett klokt och korrekt sätt. Medarbetare i förvaltningen kommer ofta till IT-strateg och ISAM och vill använda AI i tjänsten. Ibland rör det sig om tjänster som förvaltningen redan vet är osäkra till exempel på grund av tredjelandöverföringar. Förvaltningen försöker då hitta andra tjänster som kan motsvara verksamhetens behov.

2.3 Nya regler för kameraövervakning

Från den 1 april 2025 gäller nya regler för kamerabevakning. I och med de nya reglerna behöver inte längre ansökan om tillstånd för kamerabevakning göras hos IMY. Dock ska en intresseavvägning mellan bevakningsintresset och den enskildes intresse av att inte bli bevakad göras. Intresseavvägningen ska dokumenteras och den som bevakar ska även ha en förteckning med vissa uppgifter om den kamerabevakning som bedrivs eller som har upphört de senaste fem åren.

2.3.1 Påverkan på Hässelby-Vällingby sdf

I budgeten för 2026 uppmuntras stadens verksamheter till att använda möjligheten för kameraövervakning för att öka tryggheten för våra invånare. Viktigt är att förvaltningen görarbetet med både intresseavvägning och informationssäkerhetsarbetet samt dokumenterar detta. IMY är tillsynsmyndighet för kamerabevakning och precis som med alla andra nya digitala objekt måste förvaltningen göra ett informationssäkerhetsarbete innan kamerabevakning, på varje enskild plats, sätts upp och aktiveras.

3 Vad händer inom staden – budget, inriktningar, lokala förändringar och satsningar

3.1 Centrala styrning

I budgeten för 2026 ser förvaltningen att informationssäkerheten har fått tagit mer plats och att mer resurser avsatts. Det är glädjande att stadens centrala styrning tydligt pekar på att informationssäkerhet är en allt viktigare område och behöver få mer plats.

Under 2025 har staden blivit bättre på att genomföra normerande klassningar. Det finns mer systematik och metod. Socialförvaltningens arbetssätt att dela upp förvaltningarna i tre kluster (där trillingen är ett) och att respektive kluster får utse deltagare, har blivit ett allt mer tongivande arbetssätt. Glädjande är att det delvis är trillingens sätt att samarbeta som legat till grund för detta arbetssätt.

Förvaltningen fortsätter ha utmaningar där de från centralt håll inte har kunskap om att normerande klassningar inte behöver göras varken innan upphandling eller driftsättning. Här är det viktigt att förvaltningens avdelningschefer och andra nyckelpersoner vidarebefordrar information om nya objekt eller utveckling av befintliga objekt till förvaltningens ISAM. Att få fram kvalitativa normerande klassningar sparar tid när det kommer till det lokala arbetet.

3.1.1 Påverkan på Hässelby-Vällingby stadsdelsförvaltning

Förvaltningen behöver fortsätta ställa höga krav på informationssäkerheten inför och vid upphandlingar. Med den nya cybersäkerhetslagen kommer det även ställas krav på leverantörsuppföljning, något som åläggs den som köper tjänster och system.

Förvaltningen har även utmaningar lokalt med digitala objekt som driftsätts utan att det inte finns PUB-avtal eller att informationklassning är gjord. Det blir då svårt att i efterhand kravställa leverantörens skyldigheter när det kommer till hantering av exempelvis personuppgifter och att ta fram relevanta loggar vid incidenter. Även här har förvaltningens avdelningschefer en viktig roll att säkerställa att detta arbete görs korrekt.

I 2024 års rapport skrev ISAM att det behövs fler som arbetar med och har kompetens inom informationssäkerhet. Under hösten har förvaltningens stabsenhet börjat titta på en ny organisation där fokus är digitalisering och att informationssäkerheten är en del i detta. Det är ett arbetssätt som behöver dokumenteras och tydliggöras för medarbetar som arbetar med digitalisering och informationssäkerhet och för chefer och medarbetare. Det ska vara tydligt och enkelt för dem att veta var de ska vända sig när verksamheterna har behov som kräver ny eller utvecklad digitalisering.

3.2 Lokal mognadsmätning

Förvaltningens stabsenhet har genomfört en mognadsmätning av sitt informationssäkerhetsarbete utifrån MSB:s mall. Resultatet visar att arbetet har kommit långt, särskilt inom områdena kompetens och informationklassning, där man närmar sig de högsta mognadsnivåerna.

Arbetet präglas av tydliga rutiner och ett medvetet arbetssätt, men det finns fortfarande personberoenden och behov av ökad systematik, särskilt inom riskhantering, incidenthantering och uppföljning. Ledningen och nyckelpersoner behöver höja sin kompetens och förståelse för att informationssäkerhetsarbetet främst bör vara proaktiva insatser.

För att nå en önskad högre nivå inom mognadsanalysens samtliga områden krävs fortsatta kompetenshöjande insatser, förbättrad uppföljning och att chefer och verksamheter tar ett större eget ansvar för informationssäkerhetsarbetet. Sammantaget visar mätningen att förvaltningen tar informationssäkerhet på stort allvar och har goda förutsättningar att nå ännu högre mognad framöver. ISAM har för avsikt att göra denna mognadsanalys årligen för att kunna följa upp utvecklingen.

4 Uppföljning av informations-säkerhetsarbetet i Hässelby-Vällingby stadsdelsförvaltning

4.1 Uppföljning av mål i verksamhetsplanen 2025

Informationssäkerhet tas upp i verksamhetsplanen (VP) under nämndmål 3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden. Här följer en redogörelse för förväntade resultat för 2025 och status för dessa.

Förväntat resultat:

- **Alla verksamheter har uppdaterade kontinuitetsplaner som även inkluderar informationssäkerhet.**

  Status: Informationssäkerhet ingår som en del i dessa planer, vilket betyder att man inte bara tittar på hur man skyddar informationen i vanliga fall, utan också hur man säkerställer att informationen är tillgänglig och skyddad även under kris eller avbrott. Det kan till exempel innebära att man har säkerhetskopieringar och rutiner.

  Avdelningen för äldre, socialpsykologi och funktionshinder är i mål med detta arbete. Delar av avdelningen (främst myndighetsutövning) kommer troligen vara i mål innan årsskiftet.

- **Kunskapen om informationssäkerhet, dataskydd och objektsförvaltning i organisationen ökar.**

  Status: ISAM och DSO har genomfört utbildningar under året i form av riktade utbildningar till olika enheter och funktioner. Medarbetare har genomfört stadens e-utbildningar. ISAM och Pm3-ansvarig har i samband med informationsklassningsarbete ökat kompetensen hos objektspecialister, objektägare och objektledare.

- **Verksamhetssystem som omfattas av NIS har informationsklassats på lokal nivå.**

  Status: Följande objekt har informationsklassats under året: Pascal, Procedo och Life Care SP (rutinarbetet pågår och sedan ska förvaltningsplan skrivas). Följande objekt har inte klassats lokalt då central objektsförvaltning av olika orsaker inte har genomfört normerade klassning: E-hälsa (APO ex), VODOK, NPÖ, Para Inn och Para Sol. För det nya objektet DEBI pågår under november och december normerande klassningsarbete.

4.1.1 Väsentlighets- och riskanalys samt Internkontrollplan

Här följer en redogörelse för VoR och IKP för 2025 samt status och åtgärd:

Arbetssätt: Behörighetshantering

Oönskad händelse: Behörigheter avslutas inte i tid.

Sannolikt och allvarlig konsekvens; riskvärde 16 (till IKP).

- Åtgärd VoR: Objektspecialist med stöd av informatiossäkerhetssamordnare informerar och påminner chefer vid brister.
- Åtgärd VoR: Systematiskt följa upp behörighetshantering.

Status och åtgärder: Enligt nuvarande ledningsstruktur för objekt i förvaltning, rapporterar Objektspecialist i första hand direkt till Objektsledare/Objektsägare. Endast i ytterlighetsfall kontaktas ISAM för stöd med specifika frågor.

Förslag till åtgärd är att den årliga objektsuppföljningen i objektets förvaltningsplan, kompletteras med att också omfatta en kontroll av befintliga behörigheter till objektet.

Kontroller genom stickprov enligt förvaltningsplan var en åtgärd för 2025. Uppföljning hargenomförts på objektsnivå, d v s att kontrollerade objektet i förvaltning utifrån Pm3, har en i rutin dokumenterad behörighetshantering.

Oönskad händelse: Information hanteras på fel sätt.

Mindre sannolikt och kännbar konsekvens; riskvärde 6 (endast VoR).

Status och åtgärder: Fortsatt arbete med att påminna och stötta i rapportering i IA för att kunna jobba mer preventivt med att information inte hanteras korrekt. Kompetenshöjning hos medarbetare om vad som är ”rätt” sätt. Under hösten har ett nytt utbildningsmaterial tagits fram som fokuserar till stor del på att skapa en kultur där man som medarbetare ska våga fråga, göra fel och lära av misstag. Viktigt att nå ut till målgrupper som inte alltid har åtkomst till egna datorer och därmed försvårar för dem att ta emot information.

Oönskad händelse: Medarbetare har åtkomst till obehörig information.

Sannolikt och allvarlig konsekvens; riskvärde 16 (till IKP).

- Åtgärd VoR: En systematik införs för att säkerställa att chef följer upp om medarbetare har rätt behörighet.

Status och åtgärder: Systematiken har under 2025 inte tagits fram eller införts så fortsatt åtgärd blir att få till detta under 2026.

Oönskad händelse: Resurs- och kompetensbrist medför risker inom informationssäkerhetsarbete och objektförvaltning.

Sannolikt och kännbar konsekvens; riskvärde 12 (till IKP).

- Åtgärd VoR: Inventera behov, prioritera och utbilda medarbetare och chefer.

Status och åtgärder: Under 2025 har det inte varit allmänna utbildningar för chefer och medarbetare. Detta då det under våren var fokus på annat efter omorganisationen och under hösten inte funnits tid för ISAM att hålla utbildningar.

Arbetssätt: Incidenthantering

Oönskad händelse: Personuppgiftsincidenter anmäls inte.

Mindre sannolikt och allvarlig konsekvens; riskvärde 8 (endast VoR).

Oönskad händelse: Risker och konsekvenser av incidenter kvarstår.

Sannolikhet möjlig och allvarlig konsekvens; riskvärde 12 (till IKP).

- Åtgärd VoR: Plan för när åtgärder ska vara genomförda och beslutad av förvaltningsledningen.
- Åtgärd VoR: Systematisk uppföljning att åtgärder är genomförda.

Status och åtgärder: ISAM följer upp incidenter och åtgärder övergripande. Under 2025 har det inte funnit tid/resurser för att göra detta systematiskt från ISAMs sida. Detta blir en åtgärd för 2026.

Oönskad händelse: Att verksamheten inte har möjlighet att tillsätta resurser för att genomföra arbetet.

Sannolikhet möjlig och kännbar konsekvens; riskvärde 9 (endast VoR).

- Åtgärd VoR: Information och utbildning till chefer på exempelvis chefsforum.

Status och åtgärder: Med anledning av omorganisationen under våren 2025 hade vi som jobbar med informationssäkerhet en oro för att verksamheterna inte skulle ha möjlighet att tillsätta de resurser som behövs för informationssäkerhetsarbete i respektive verksamhet. Svårt att säga om det saknats resurser men framför allt har det märkts att många nya medarbetare och chefer inte har fått den information/utbildning som behövs inom området. Viss information har getts till chefer genom chefsbrev och intranät. Ingen riktad utbildning har hållits för chefer, dock finns digitala utbildningar på utbildningsplattformen.

Arbetssätt: Informationssäkerhet inom upphandlingsförfarande

Oönskad händelse: Information sprids och lagras och hanteras på ett oönskat sätt.

Sannolikhet möjlig och allvarlig konsekvens; riskvärde 12 (till IKP).

- Åtgärd VoR: Delta vid direktupphandling och upphandling för att bevaka att informationssäkerheten säkerställs.

Oönskad händelse: Upphandling av digitala objekt sker utan att informationssäkerhetsklassning och risk- och konsekvensanalys görs.
Sannolikhet möjlig och allvarlig konsekvens; riskvärde 12 (till IKP).

- Åtgärd VoR: Information till chefer om att de ska kontakta informatiossäkerhetssamordnare tidigt i processen inför inköp/upphandling.

Status och åtgärder: Ett samarbete med förvaltningens upphandlare har gjort att ISAM får nu information om upphandlingar och inköp som kommer till upphandlaren. ISAM har under 2025 i några fall bjudits in att delta i möten med leverantörer innan upphandling/avrop genomförts.

När det gäller verksamheterna finns ett stort jobb kvar att göra gällande att de, innan upphandling och avrop görs, behöver kontakta ISAM för att få hjälp med att ta fram krav kopplade till informationssäkerhet som ska finnas med i upphandling. Vi ser också att man inför digitala objekt och lägger in produktionsdata i form av personuppgifter utan att relevanta avtal finns på plats.

Den revidering av delegationsbeslut för inköp av digitala stödsystem som flyttas från som lägst biträdande enhetschef, till avdelningschef har inte riktigt gett den effekt som vi hoppades på.

4.2 Uppföljning av dataskyddsombudets årsrapport 2024

Dataskyddsombudets granskning av dataskyddsarbetet för 2025 redovisas i dataskyddsombudets årsrapport för 2026 vilken tas upp i nämnden.

I ledningens genomgång rapporteras återkoppling på åtgärder som ISAM har varit ansvarig för eller varit delaktig i och på de områden där DSO har gett rekommendationer till åtgärder.

Registerförteckning

I rapporten för 2024 angav DSO att registerförteckningen (DraftIT) bedömdes vara fullständig. Personuppgiftsbehandlingar tillkommer och förändringar görs i verksamheten vilket gör att dataskyddshandläggarna med stöd av DSO och ISAM löpande fortsätter arbetet, som nu är av underhållande karaktär. Det finns ett antal registreringar som väntar på att bli godkända av DSO. Det har varit ett tekniskt problem i DraftIT samt ett antal felregistreringar som bidragit till detta. Det är ett relativt omfattande arbetet för DSO att rätta upp de felaktiga registreringarna. ISAM och DSO har därmed kommit överens om att detta arbetet gör när vi under våren byter till en ny version av DraftIT.

Styrdokument

DSO rapporterade om svårigheten att hitta information på intranätet rörande informationssäkerhet och dataskydd. ISAM stödjer denna åsikt och får ofta hjälpa medarbetare och chefer i att hitta relevant information på intranätet.

I den nya mall för lokala tillämpningsanvisningar som staden tagit fram centralt har dataskyddsperspektivet tagits bort. I den uppdaterade lokala tillämpningsanvisningen som ISAM i skrivande stund arbetar med kommer dataskyddet att finnas med enligt DSOs rekommendationer.

Förvaltningen har under 2024 tagit fram dokumentation och mallar löpande i samband med införandet av Pm3. Dessa var planerade att 2025 publiceras på intranätet. Publiceringen under 2025 har prioriterats ner till förmån för mer direktriktade informationsinsatser. För att kunna uppnå önskat mottagande och förståelse för materialet, sågs behov av en djupare förankring och förståelse för förvaltningsmodellen i organisationen innan materialet publiceras på bredd. Med nu genomfört arbete och tydliga indikationer på att en sådan förståelse har börjat få fäste i organisationen är en publicering att se som lämplig under 2026.

Konsekvensbedömningar

Rutiner för konsekvensbedömningar finns på plats men arbetet med att genomföra dessa är individberoende. Förvaltningen behöver fortsätta arbetet med att öka verksamheternas förståelse för syftet med konsekvensbedömningar, hur dessa ska göras samt resurssättning. Under hösten har några lokala klassningar gjorts där en konsekvensanalys

behövts göras och verksamheten har då fått uppgiften att själva göra delar av denna. Resultatet har varit mycket bra och återkopplingen har varit att det varit lite svårt men samtidigt nyttigt och ett bra lärande.

Personuppgiftsincidenter

Kunskap om hur man hanterar personuppgiftsincidenter är en ”färskvara” skriver DSO i sin rapport. ISAM har under året tagit de tillfällen som givits till att informera om incidentrapportering och varför förvaltningen ska rapportera incidenter. Det är viktigt att få till en kulturförflyttning där medarbetare förstår varför en anmälan ska göras och inte bara gör det för att ”man ska”. ISAM har stöttat vid behov när personuppgiftsincidenter inträffat både vad gäller anmälan men också åtgärder. ISAMs uppfattning är att verksamheten blivit mer benägen att ta kontakt, berätta vad som hänt och komma med förslag på åtgärder.

Risker inom dataskydd som DSO tagit upp i 2024 års rapport

Risk 1 Osäker e-posthantering med personuppgifter

Den centrala objektsförvaltningen för Säkra meddelanden har meddelat att de risker som tidigare gjort att förvaltningen avstått från att införa användandet av Säkra meddelanden är sänkta eller eliminerade. Detta har gjort att förvaltningschefen tagit beslutet att förvaltningen nu kan börja använda tjänsten för att skicka meddelanden innehållandes personuppgifter och annan känslig information. Under hösten har ett arbete påbörjats med att införa Säkra meddelanden. Det lokala informationssäkerhetsarbetet pågår och beräknas vara klart under november. Två enheter inom förvaltningen har erbjudit sig att vara piloter och piloterna planeras genomföras under december månad. Samtliga enheter som avser använda tjänsten Säkra meddelanden behöver färdigställa egna rutiner innan de använder tjänsten. Verksamheterna beräknas kunna börja använda tjänsten efter årsskiftet.

Risk 2 Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor

Vid förfrågan kan sällan förvaltningsplaner och systemdokumentationer tas fram av leverantörer eller stadens egna centrala och lokala objektsförvaltningar. ISAM och Pm3-ansvarig arbetar löpande med detta genom införandet av Pm3 och genom att försöka komma in tidigt i processen för systemupphandlingar.

Efter att digitala objekt informationssäkerhetsklassats med stöd av ISAM lämnar ISAM över till Pm3-ansvarig som stöttar lokal objektförvaltningen med att ta fram förvaltningsplaner och rutiner.

Där det inte finns centrala mallar att tillgå tas egna mallar fram för att underlätta arbetet för verksamheterna lokalt.

De lokala tillämpningsanvisningarna håller i skrivande stund på att uppdateras. I denna ska det framgå vilken roll som har ansvar för objektets olika dokumentationsdelar. Under 2026 blir det en aktivitet att fortsätta informera om och implementera detta ansvar i verksamheten.

Risk 3 Tredjelandsöverföringar

Allt fler leverantörer går över till att endast tillhandahålla molntjänster och det är inte helt ovanligt att dessa har kopplingar till amerikanska företag. Förvaltningen behöver ha en exit-plan för användandet av dessa leverantörer. Att ta fram en sådan plan var planerad till 2025 men har ej gjorts. Främst på grund av att förvaltningen inte har haft någon sådan leverantör och därmed har arbetet inte prioriterats. På grund av att ISAM under 2025 har fått förhålla sig till ett ökat tryck och intresse kring informationssäkerhetsfrågor samt fått hanterat ett flertal informationssäkerhetsincidenter har vissa delar i uppdraget fått prioriteras om.

Under 2026 hoppas ISAM få resursförstärkning så att arbetet med att ta fram Exit-plan samt rutin för att genomföra TIA (Transfer Impact Assessment) kan prioriteras och genomföras.

Risk 4 Skyddade personuppgifter inom förskolan

ISAM har deltagit tillsammans med DSO i normerande klassning av Infomentor och i detta arbetet framfört behovet av att säkerställa att skyddade personuppgifter hanteras rätt.

Risk 5 Central objektsförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (stadsdelsförvaltningens) objektförvaltning

När förvaltningen ska införa nya digitala tjänster lokalt upplevs en viss problematik som ibland kan kopplas till resursbrist hos den centrala objektsförvaltningen. ISAM har dock under året snarare upplevt att problematiken ligger i att den centrala objektsförvaltningen inte har tillräcklig kännedom om avtal, hur tjänsten ska avropas och om PUB-avtal ska skrivas lokalt eller inte.

Risk 6 Ny teknik, t ex behandlings av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation

Under året har ett AI-verktyg införts i förvaltningen där ISAM har varit delaktig i informationssäkerhetsarbetet. Både ISAM och IT-strateg får löpande frågor om att använda AI-tjänster. Ofta är dessa tjänster sådana som inte är säkra att använda av olika anledningar. Förvaltningen försöker då rekommendera alternativ och också informera om informationsklassningsarbetet som ska göras innan användande. Med den nya Zoom-tjänsten, Nordic for Zoom, är förhoppningen att staden centralt kan ta ett ansvar för normerande arbetet av tilläggstjänster. Dessa tilläggstjänster kommer till stor del kunna tillgodose behov och efterfrågan hos verksamheterna.

4.3 Information om avvikelser och incidenter

Under året, fram till 11 november har ca 60 avvikelser rörande informationssäkerhet rapporterats, varav 55 avvikelser i IA. Förra året rapporterades ca 90 avvikelser fram till december. 20 av årets avvikelser är inrapporterade som personuppgiftsincidenter, i jämförelse med 16 2024. Cirka hälften är i skrivande stund klarmarkerade i IA.

Status på informationssäkerhetsincidenter, inklusive personuppgiftsincidenter, i IA per den 12 november 2025:

- Rapporterad: 10 st
- Under registrering:16 st
- Under utredning: 3 st
- Under åtgärd: 2 st
- Klar: 22 st
- Förfallen: 2 st

Flera av incidenterna som ligger *Under registrering* är inrapporterade under årets första kvartal. ISAM ser ett behov av att förvaltningsledningen informerar chefer om att följa upp rapporterade avvikelser i IA. Utan uppföljning och åtgärder kan vi inte effektivt och systematiskt använda avvikelserapportering för att jobba preventivt med risker inom informationssäkerhetsområdet.

Precis som föregående år är den vanligaste avvikelsen som anmäls att handläggare lägger in fel uppgifter i fel ärende i sociala system. Den främsta orsaken till detta anges som stress och att man har flera klienters utredningar öppna i systemet samtidigt.

Arten av incidenter varierar men några exempel är:

- Felaktigt skickat personuppgifter till tredje part, exempelvis annan förvaltnings socialtjänst, domstol eller klient (socialtjänst).
- Uppgifter om annan klient hittas efter avslut av utredning i fysiskakt (aktexpeditionen).
- Uppgifter om annan klient hittas digitalakt (socialtjänst).
- Sekretesshandlingar hittas där de kan kommas åt av obehöriga, som exempel liggandes vid skrivare, i hög med tomma plastfickor/interpostkuvert.
- Personuppgifter som läckt ut vid cyberattack (Miljödata).
- Phishing och spam via e-post.
- Post (även rek) innehållandes känsliga personuppgifter ”tappas” bort i förvaltningshuset.
- Mail som skickas enligt ppdl-lista och listan läggs inte i fältet för hemlig kopia. Vilket innebär att kontaktuppgifter till t ex anhöriga sprids.

Tre incidenter har rapporterats till Integritetsskyddsmyndigheten, IMY fram till november.

Inga NIS-incidenter har rapporterats från förvaltningen till MSB. Då de incidenter som skett inte har nått den nivå som kräver anmälan till MSB.

5 Förslag till förbättringar och aktiviteter

Förslagen till förbättringar och aktiviteter avser perioden 2026–2028. Då ledningens genomgång sker årsvis som en del av det systematiska arbetet, kommer anpassningar och nya krav att hanteras och föreslås, detta som en naturlig del av arbetet kommande år.

5.1 Förbättringsaktiviteter 2026

5.1.1 Övergripande

- Etablera en process för digitalisering med roller och ansvar, där informationssäkerhet är en del samt göra denna känd i verksamheten (i samarbete med IT-strateg)
- Aktiviteter för att göra förvaltningen compliant med Cybersäkerhetslagen.
- Införa ny modul för DraftIT samt utbilda våra dataskyddshandläggare i denna (i samarbete med DSO)
- Fortsätta arbeta in informationssäkerhet i enheternas kontinuitetsplaner (i samarbete med säkerhetsstrateg).
- Se över den fysiska informationssäkerheten.
- Fortsätta samarbetet i trillingen genom regelbundna möten för ISAM samt även träffar för enhetschefer och avdelningschefer.
- Fortsatt införande av Säkra meddelanden.
- Påbörja införande av Säker digital kommunikation (SDK).

5.1.2 Kompetenshöjande insatser informationssäkerhet

- Hitta rutin för att chefer och medarbetare genomföra de digitala utbildningarna på utbildningsplattformen samt uppföljning av genomförda utbildningar.
- Övergripande utbildningar på områdena informationshantering och informationssäkerhet fortsätter att hållas löpande av ISAM/arkivarie.
- Verksamheterna fortsätts även erbjudas anpassade utbildningar inom informationssäkerhet.
- Riktade kompetenshöjande insatser för nyckelfunktioner som exempelvis it-funktion, informationsredogörare och dataskyddshandläggare.
- Nå målgrupper av anställda som idag inte riktigt nås som exempelvis timvikarier och anställda som saknar tillgång till egen dator.
- Riktade kompetenshöjande insatser för eventuella nya områden och ledningsfunktioner som kommer att beröras av cybersäkerhetslagen.
- Få med information för nyrekryterade som en del i det strukturerade informationssäkerhetsarbetet.

5.1.3 Uppdatering av styrdokumentation

- De lokala tillämpningsanvisningarna håller i skrivande stund på att uppdateras. I dessa ska det framgå vem som har ansvar för objektets olika dokumentationsdelar. Under 2026 blir det en aktivitet att fortsätta informera om och införa detta ansvar.

- Rutin för incidentrapportering och andra stödjande dokument för verksamheterna i förvaltningen behöver årligen ses över.
- Metod tas fram för att kunna göra regelbundna uppföljningar av både rapportering och åtgärder.
- Rutin för NIS-incidenter behöver uppdateras med anledning av cybersäkerhetslagen.
- Exit-plan med anledning av användandet av leverantörer som nyttjar tredjelandsöverföringar.

5.1.4 Informationklassning och konsekvensbedömning

- Fortsätta lokalt klassningsarbete för våra system som omfattas av NIS-direktivet (hälso- och sjukvård).
- Delta i stadens normerande klassningar (i samarbete med trillingen), bland annat ny modul för Infomentor, kommunikationstjänster, och GSIT 3.0.
- Lokala klassningar av nya objekt inför upphandling och driftsättning.
- Lokala klassningar av befintliga systemstöd på objektlista (back-log).

5.1.5 Pm3-specifikt

- Fortsatt utrullning av pm3 till prioriterade objekt enligt objektslista.
- Årlig klassning av de objekt som under 2025 gått in i förvaltning enligt Pm3.
- Utbildning och stöd till befintliga objektsorganisationer (främst objektsledare och objektsägare).
- Kompetenshöjande insatser till chefer och ledande/stödjande funktioner i Pm3, exempelvis digitala informationstillfällen och på chefsforum.

5.2 Förbättringsaktiviteter 2027

- Intern förankring av beslut och rekommendationer att säkerställa information i linjeorganisationen. Det finns idag olika kunskap hos chefer, både inom och mellan förvaltningsområden. Vanligaste förklaringen till att chefer inte har hört om det kan vara att de inte har förstått, men slutresultatet är ofta detsamma. Det är brister i rutiner och processer.

- Fortsatta utbildningsinsatser kopplat till cybersäkerhetslagen. Troligen kommer även behovet av uppdaterade rutiner och riktlinjer löpa på in i 2027.

- Påbörja införande av att organisera det strukturerade informationssäkerhetsarbetet att omfatta processer.

5.2.1 Pm3-specifikt

- Fortsatt objektsinventering och komplettering av objektslistan avseende nya och gamla systemstöd.
- Fortsatt utrullning av pm3 till prioriterade objekt enligt objektslista.
- Årlig uppföljning och klassning av de objekt som gått in i förvaltning.

- Utbildning och stöd till befintliga objektsorganisationer (främst objektsledare och objektsägare).
- Kompetenshöjande insatser till chefer och ledande/stödjande funktioner i Pm3, exempelvis utbildningstillfällen, digitala informationstillfällen och på chefsforum.
- Påbörja införandet av en samlad objekts-/samarbetsyta för dokumentation och löpande arbete för respektive objekt/objektsledning.
- Påbörja införandet av portföljstyrning kopplat till Pm3.
- Bevaka och upprätta samverkan med/mellan objektsledningar för centrala- till lokala objekt där dessa är aktiverade.

5.3 Förbättringsaktiviteter 2028

- Ta fram förslag på tydligare mandat och en budgetstyrning kopplad mot dataskydd. Medel bör reserveras utöver det som rör inköp och upphandling. Det arbete som måste läggas ner på kontroller och skapande av formalia, är i många fall en stor del av kostnaden i tid räknat vid införande av nya it-objekt.

- Införa motsvarande förvaltning utifrån Pm3 att också omfatta tydliga processer och verksamhetsfunktioner.

6 Förkortningar och begrepp

ISAM – Informationssäkerhetssamordnare

DSO – Dataskyddsombud

Trillingen-Samarbete mellan ISAM i stadsdelsförvaltningarna Bromma, Järva och Hässelby-Vällingby. Som även delar DSO.

NIS - Rective on security of network and information systems - the NIS Directive.

CSL-Cybersäkerhetslagen

VOR – Väsentlighets och riskanalys

RSA – Risk och sårbarhetsanalys

IKP – Internkontrollplan

SLK – Stadsledningskontoret

PM3 – styr- och samverkansmodell för underhåll och utveckling av it-stöd

IMY – Integritetsskyddsmyndigheten

MSB – Myndigheten för samhällsskydd och beredskap

Tredjelandsöverföringar – Kallas så om personuppgifter ska överföras till länder utanför EU/EES-området.

CER-direktivet- (Directive on the resilience of critical entities) ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet.

Förkortningar och begrepp