Stockholms stad

Ledningens genomgång

2026

Utbildningsförvaltningen

Kontaktperson: Mårten Nilsson Nyberg

1. Sammanfattning

Ledningens genomgång är ett begrepp inom informationssäkerhetsområdet som innebär att de som ansvarar för informationssäkerheten inom en organisation minst årligen ska informera sig om hur arbetet går och hur det utvecklas.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschefen inhämta en rapport – en så kallad *Ledningens genomgång* – från informationssäkerhetssamordnaren (ISAM).

Syftet med rapporten är att ge utbildningsnämndens ledning underlag för att bedöma om förvaltningens arbete med informationssäkerhet och dataskydd är tillräckligt, effektivt och har önskad verkan. Genomgången utgör en del av stadens ledningssystem för informationssäkerhet (LIS) och ger även underlag till verksamhetsplanering och intern kontroll.

Under 2025 har arbetet fokuserat på att förstärka förvaltningens systematiska informationssäkerhetsarbete, framför allt inom:

- Informationsklassningsprocessen
- Förberedelser inför den nya cybersäkerhetslagen (som träder i kraft den 15 januari 2026)

Rapporten redovisar faktorer som påverkar arbetet, resultat från uppföljningar, identifierade risker, avvikelser, samt planerade och föreslagna förbättringar.

Särskilt prioriterade aktiviteter för 2026 är:

- Målgrupps och situationsanpassade utbildningar inom informationssäkerhet och dataskydd.
- Implementering av lokala rutiner, arbetssätt och anvisningar för exemeplvis informationsklassning, behörighetshantering samt incidenthantering.
- Framtagande av förvaltningsövergripande kontinuitetsplan.
- Framtagande av förvaltningsövergripande risk- och hotbildsanalys inom cybersäkerhet.

Utöver ovan listade aktiviteter bedöms förvaltningens arbete även präglas mycket av den kommande cybersäkerhetslagstiftningen.

Särskilt prioriterade aktiviteter relaterat till den kommande lagstiftningen är att:

- Genomföra en analys av omfattning (verksamheter, system, nätverk).
- Kartlägga gap mot lagens krav samt upprätta en handlingsplan för åtgärder.
- Genomföra särskild utbildning för chefer och ledning.
- Anpassa lokala rutiner för kontinuitet och incidentrapportering.
- Säkerställa leverantörsavtal och tredjepartsrisker.

Rapporten redovisar även olika faktorer som påverkar eller kan komma att påverka verksamhetens ledningssystem för informationssäkerhet (LIS) under året.

Innehållsförteckning

1.2 Vad är Ledningens genomgång

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 genom en riktlinje för informationssäkerhet och tillhörande tillämpningsanvisningar som är en bilaga till stadens Kvalitetsprogram. Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete.

För utbildningsnämndens räkning har utbildningsdirektören fastställt en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom nämnden.

1.3 Faktorer som påverkar verksamhetens LIS

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska utbildningsnämnden 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.

Det riskbaserade förhållningssättet har sin grund i både interna samt externa hot vilket innebär att nämnden bland annat behöver hålla sig ajour med vad som händer i vår omvärld – likväl som att hålla sig ajour med vad som händer internt inom staden.

1.3.1 Omvärldsbevakning – hot, trender och ny lagstiftning

1.3.1.1 NIS2-direktivet (cybersäkerhetslagstiftningen)

I slutet av 2022 beslutade EU om ett nytt direktiv som ska ersätta nuvarande NIS-direktivet. Det nya direktivet har fått namnet NIS2.

I Sverige kommer NIS2-direktivet att införas genom en ny lag, cybersäkerhetslagen, som väntas träda i kraft 15 januari 2026.

Lagen innebär krav på att samhällsviktiga verksamheter ska arbeta strukturerat med informations- och cybersäkerhet.

För utbildningsnämnden innebär detta bland annat:

- Krav på systematiskt och dokumenterat säkerhetsarbete.
- Krav på riskhantering, incidentrapportering och kontinuitetshantering.
- Ansvar för ledning och styrelse.
- Säkerhet i leveranskedjan.
- Krav på utbildning för ledning och personal.

1.3.1.2 Säkerhetspolitiska läget i Europa

Det säkerhetspolitiska läget i Europa fortsätter att påverka hotbilden mot svenska myndigheter och kommuner. Rysslands invasion av Ukraina och Sveriges inträde i NATO har medfört en ökad exponering för cyberangrepp, desinformation och påverkanskampanjer.

Detta ställer ökade krav på robusthet, informationsklassning, incidenthantering och kontinuitetshantering samt att nämnden har en väl etablerad omvärldsbevakning och håller sig ajour med de hot som direkt eller indirekt kan komma att påverka nämnden.

1.3.1.3 Cyberattacker mot kommuner och myndigheter

Under 2024–2025 har flera svenska kommuner och myndigheter drabbats av cyberincidenter som påverkat tillgång till system och information. Detta inkluderar inte minst den uppmärksammade incidenten som inträffade hos leverantören Miljödata – som utbildningsnämnden även indirekt drabbades av.

Rapporter från MSB visar att störningar i leveranskedjor och hos externa leverantörer står för en ökande andel av incidenterna.

1.3.1.4 Artificiell intelligens (AI)

Utvecklingen av artificiell intelligens (AI) går snabbt och det finns en stor efterfrågan på att använda ny teknik. Med det så finns det också stora risker med användandet av AI och det kommer fortsatt ställa höga krav på arbetet med informationssäkerhet och dataskydd.

1.3.1.5 Adekvansbeslut om tredjelandsöverföring

I juli 2023 fattade EU-kommissionen ett nytt adekvansbeslut om tredjelandsöverföring till USA.

EU-kommissionens beslut innebär att överföringar som sker till organisationer som omfattas av ”EU-US Data Privacy Framework” nu kan ske utan att lämpliga skyddsåtgärder, såsom standardavtalsklausuler, behöver vidtas enligt artikel 46 i dataskyddsförordningen. Beslutet har överklagats och rättsläget är därmed osäkert.

1.3.2 Vad händer inom staden – inriktningar, lokala förändringar eller satsningar

Stockholms stad har under 2025 fortsatt sitt arbete inom informationssäkerhet och dataskydd, bland annat genom:

- Informations- och utbildningsinsatser.
- Samordnande förberedelser inför kommande cybersäkerhetslagen.

15 januari 2026 väntas cybersäkerhetslagstiftningen träda i kraft vilket kommer att påverka nämndes arbete med informationssäkerhet. Detta beskrivs mer ingående i avsnitt 1.4.2.

1.3.3 Vad har verksamheten identifierat i RSA-arbetet

Under 2024 genomförde nämnden RSA, Risk- och sårbarhetsanalys, steg 1-4. Under steg 1-4 har nämnden identifierat risker kopplade till informationssäkerhet och under 2025 har nämnden påbörjat arbetet med steg 5-6.

Syftet med steg 5-6 är att utifrån de identifierade riskerna, inom de samhällsviktiga uppdragen, planera och påbörja genomförandet av förmågehöjande åtgärder. Arbetet med åtgärder är något som fortsatt kommer pågå under 2026.

Verksamheten har identifierat tre övergripande risker inom de samhällsviktiga verksamheterna ”Utbildning för barn och unga - Praktisk, teoretisk och anpassad undervisning” samt ”Tillsyn av barn till vårdnadshavare som arbetar med annan samhällsviktig verksamhet (anpassad grund-gymnasieskola, fritidsverksamhet, KTT-korttids, elevboende)”.

Riskerna är formulerade på följande sätt:

- Förvaltningen brister i att upprätthålla informationens konfidentialitet: Information som verksamheten ansvarar för inom ramen för uppdraget kommer obehöriga till del på grund av exempelvis ett dataintrång.
- Förvaltningen brister i att upprätthålla informationens riktighet: Information som verksamheten ansvarar för inom ramen för uppdraget förvanskas medvetet eller omedvetet och/eller är inte riktig i den meningen att den är tillförlitlig och korrekt
- Förvaltningen brister i att upprätthålla informationens tillgänglighet: Verksamheten har inte tillgång till information och/eller IKT-tjänster som krävs för att genomföra utbildning, när den behöver det. Exempelvis på grund av att system eller nätverksresurser blir otillgängliga genom att trafik med stora datamängder riktas mot organisationens it-tjänster eller att it-tjänsterna blir otillgängliga på grund av en ransomware-attack.

1.3.4 Resultatet från egen uppföljning (VoR och IKP)

I väsentlighet- och riskanalysen (VoR) för 2025 fanns nedanstående oönskade händelser inom området informationssäkerhet.

- Anställda, konsulter och leverantörer har åtkomst till information som de inte ska ha tillgång till.
- Anvisningen följs inte och ansvaret för informationssäkerhet är inte tydligt.

- Incidenter rapporteras inte samt att åtgärder från incidenthanteringen inte implementeras.
- Åtgärderna från informationsklassningar och tillhörande riskanalyser efterlevs inte.
- Informationssäkerhet inkluderas inte från start vid anskaffning eller utveckling av varor och tjänster.

I internkontrollplanen (IKP) för 2025 fanns en (1) kontroll med (Anställda, konsulter och leverantörer har åtkomst till information som de inte ska ha tillgång till) som rör informationssäkerhet.

Uppföljning av de oönskade händelserna som lyftes i väsentlighet- och riskanalysen samt internkontrollplanen för 2025 har följts upp genom stickprover och observationer under året.

I tabellen nedan följer den uppföljning och bedömning som gjorts för respektive oönskad händelse i VoR:en samt IKP:n.

ID	Oönskad händelse i VoR samt IKP	Uppföljning av oönskad händelse	ISAM:s förslag på åtgärd
1	**Anställda, konsulter och leverantörer har åtkomst till information som de inte ska ha tillgång till**	Genom observationer och stickprovskontroller har det konstaterats att det fortsatt bland annat inte är möjligt att begränsa behörigheter till användare på det sätt som framkommer av kraven från informationsklassningar. Stickprov har även visat på brister i uppföljning av behörigheter. I flera fall har det identifierats att användare har behörigheter de inte längre har behov av och därmed inte längre är berättigade till.	ISAM föreslår i samsyn med DSO:s rekommendation som lyfts i GDPR-årsrapport att den pågående förvaltningsövergripande rutin som tas fram implementeras i verksamheten för granskning av användares behörigheter. Om inte annat framkommer av kraven från klassningen bör respektive verksamhet, minst årligen, granska sina behörigheter. Chef över respektive verksamhet är ansvarig för att behörigheterna hålls uppdaterade och aktuella och att behörighetsstyrningen ligger i linje med kraven som framkommer av klassningen.
2	**Anvisningen följs inte och ansvaret för informationssäkerhet är inte tydligt**	Genom en översyn av det systematiska informationssäkerhetsarbetet har det identifierats att det fortsatt finns brister i efterlevnad av den lokala anvisningen för informationssäkerhet. Det innefattar framför allt det ansvar som åligger de roller som pekas ut i anvisningen.	ISAM föreslår att den lokala anvisningen ses över och uppdateras under 2026 i syfte att ytterligare tydliggöra roller och ansvar för informationssäkerhetsarbetet inom nämnden. Utöver detta föreslås fortsatt arbete med att implementera anvisningen på utbildningsnämnden.

3	**Incidenter rapporteras inte samt att åtgärder från incidenthanteringen inte implementeras**	Genom de under året inrapporterade incidenterna bedöms anvisningen för hantering av informationssäkerhetsincidenter inte följas i den utsträckning som förväntas. Detta beror dels på att incidenter inte anmäls i enlighet med anvisningen men framför allt bedöms verksamhetens egen hantering av informationssäkerhetsincidenter inte efterlevas i tillräckligt stor utsträckning av vad som bedöms krävas. ISAM har genom observationer identifierat att hanteringen av informationssäkerhetsincidenter, i många fall, fortsatt löper vid sidan av den incidentprocess som sedan tidigare finns upprättad för de pedagogiska verksamheterna. Detta innebär att hanteringen av informationssäkerhetsincidenter idag inte är tillräckligt integrerat i det dagliga arbetet.	ISAM föreslår att anvisningen för hantering av informationssäkerhetsincidenter ses över och uppdateras i samråd med stadsledningskontorets pågående arbete med att ta fram en stadsövergripande hantering av incidenter, inte minst med beaktande av den nya cybersäkerhetslagstiftningen. Utöver detta föreslås fortsatt arbete med att implementera anvisningen inom nämnden.

4	**Åtgärderna från informationsklassningar och tillhörande riskanalyser efterlevs inte**	Baserat på observationer och stickprov bedöms åtgärder från informationsklassningar fortsatt vara bristfällig. Det beror främst på att nämnden inte fullt ut arbetat i enlighet med stadens metodstöd för informationsklassning. Verksamhetens självvärdering av informationssäkerhetsarbetet har inte följts upp. Stadens metodstöd ger en bra grund för hur krav och åtgärder ska efterlevas och följas upp. Utöver ovan finnas fortsatt förbättringspotential i kravställning och uppföljning av säkerhetsåtgärder gentemot leverantörer.	ISAM föreslår att nämnden följer samtliga steg och delmoment i stadens metodstöd för informationsklassning med tillhörande lokala tillägg och justeringar som tagits fram under året. Kravställning gentemot leverantörer behöver fortsatt utvecklas och anpassas från fall till fall. Idag sker den absoluta merparten av kravställning genom att bilägga de standardiserade kraven som kommer ut från SKR:s KLASSA-verktyg. Dessa krav är i grunden endast en utgångspunkt och är dessutom teknikneutrala vilket innebär att de behöver anpassas till det objekt och/eller den leverantör som kravställningen riktas mot. Även uppföljning gentemot leverantör bedöms behöva göras i större utsträckning än vad som nu görs.
5	**Informationssäkerhet inkluderas inte från start vid anskaffning eller utveckling av varor och tjänster**	Genom observationer har det identifierats att informationssäkerhet fortsatt inte är tillräckligt inkluderat från start. Detta bedöms vara en stor risk för nämnden då det får till följdeffekt att informationssäkerheten, i ett för sent skede, hanteras inom upphandlingsprocessen samt i projekt. Detta resulterar i att det blir svårt att på ett tillfredsställande sätt uppfylla kraven på informationssäkerhet, både på systemteknisk nivå men även kopplat till de aktuella leverantörernas systematiska informationssäkerhetsarbete.	ISAM föreslår att nämnden följer samtliga steg och delmoment i stadens metodstöd för informationsklassning med tillhörande lokala tillägg och justeringar som tagits fram under året. ISAM rekommenderar även att en lokal rutin, som kompletterar stadens riktlinje för informationssäkerhet med tillhörande tillämpningsanvisningar, tas fram i syfte att tydliggöra och synliggöra vad som behöver omhändertas och beaktas vid upphandling, anskaffning och utveckling av varor och tjänster samt när insatser behöver göras i upphandlingsförfarande och projekt.

1.3.5 Resultatet från övrig uppföljning

Under året har även andra uppföljningar inom området gjorts som inte omfattas inom ramen för de risker som lyfts i VoR och IKP. Dessa redovisas under detta avsnitt.

E-utbildning inom informationssäkerhet och dataskydd
Resultatet av genomförandegrad för e-utbildningarna för informationssäkerhet och dataskydd bedöms som lågt (se sammanställning nedan) varpå mer riktade insatser inom utbildning rekommenderas under 2026. Detta beskrivs mer ingående under avsnitt 1.5.

- **Resultat för e-utbildning inom informationssäkerhet**
  Totalt antal: 17 722st
  Certifierade: 1 357st vilket motsvarar 7,66%
  Ej certifierade: 10 516st vilket motsvarar 59,34%
  Pågår: 1 485st vilket motsvarar 8,38%
  Utgått: 4 364st vilket motsvarar 24,62%

- **Resultat för e-utbildning inom dataskydd**
  Totalt antal: 17 722st
  Certifierade: 1 403st vilket motsvarar 7,92%
  Ej certifierade: 12 489st vilket motsvarar 70,47%
  Pågår: 1 036st vilket motsvarar 5,85%
  Utgått: 2 794st vilket motsvarar 15,77%

Statistiken är framtagen ur utbildningsplattformen och genomfördes 2025-11-05.

Informationsklassningar
Flera av nämndens system och tjänster saknar fortsatt uppdaterade informationsklassningar och de informationsklassningar som gjorts inkluderar inte alltid implementation av faktiska tekniska och organisatoriska åtgärder. Med detta i beaktande rekommenderas fortsatt implementationsarbete i metoden för informationsklassning inom Staden. Detta beskrivs mer ingående i avsnitt 1.5.

1.3.6 Resultatet från revisioner

Inga tredjeparts eller interna revisioner av nämndens arbete med informationssäkerhet har gjorts under året. Nämnden rekommenderas dock arbeta för att säkerställa ett systematiskt och riskbaserat informationssäkerhetsarbete i enlighet med stadens riktlinjer och kommande cybersäkerhetslagstiftningen.

1.3.7 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudet (DSO) lämnar årligen in en årsrapport (GDPR-årsrapport) till nämnden i samband med verksamhetsberättelsen.

DSO:n har till uppgift att övervaka verksamhetens dataskyddsregelefterlevnad samt att ge råd och rapportera direkt till högsta förvaltningsnivå. Årsrapporten följer upp nämndens efterlevnad inom dataskyddsområdet. Förutom krav som berör informationssäkerhet inkluderas en rapportering av nämndens efterlevnad av exempelvis registrerades rättigheter, konsekvensbedömningar och hantering av personuppgiftsincidenter.

Inom informationsområdet och utifrån de avvikelser som DSO identifierat gentemot dataskyddsförordningens krav, ger DSO följande rekommendationer:

För att säkerställa en strukturerad och långsiktig kompetensutveckling rekommenderas att en strategisk utbildningsplan tas fram. En sådan plan bör utgå från verksamhetens behov, gällande regelverk och identifierade riskområden. Dessa insatser bör syfta till att:

- säkerställa att medarbetare får relevant och aktuell kunskap inom exempelvis dataskydd, informationssäkerhet,
- möjliggöra uppföljning och utvärdering av genomförda utbildningsinsatser,
- skapa förutsättningar för kontinuitet och ansvarsfördelning i utbildningsarbetet.

Planen bör fastställas årligen och inkludera både obligatoriska och behovsstyrda utbildningar samt tydliggöra målgrupper, ansvariga funktioner och tidpunkter för genomförande.

Flera av nämndens system och tjänster saknar uppdaterade informationsklassningar och de informationsklassningar som gjort inkluderar inte alltid implementation av faktiska tekniska och organisatoriska åtgärder. Uppföljning av behörigheterna visar att det i flera fall finns användare med behörighet till personuppgifter som förmodligen inte har behov av det. Dataskyddsombudet rekommenderar därför att:

- Uppdatering sker av samtliga IT-systems informationsklassningsprotokoll, vilka också inkluderar en handlingsplan och riskanalys med säkerhetsåtgärder. Säkerhetsåtgärderna ska implementeras och följas upp.

- Förvaltningsövergripande rutin/process tas fram för granskning av användares behörigheter. Respektive verksamhet bör minst årligen granska sina behörigheter.

Utöver rekommendationerna ovan som berör informationssäkerhet har DSO granskat och gett rekommendationer inom andra områden som berör efterlevnaden av dataskyddslagstiftning. Dessa krav och rekommendationer tas inte upp särskilt i denna rapport. I förslagen till förbättringar, i avsnitt 1.5 nedan, tas dock hänsyn till DSO:s samtliga rekommendationer.

1.3.8 Information om avvikelser (incidenter och andra händelser)

Under året har 41 incidenter rapporterats in främst relaterade till obehörig åtkomst samt felaktig hantering av personuppgifter varav 4 anmälts vidare som anmälningspliktiga personuppgiftsincidenter till IMY. Det är sannolikt att ytterligare incidenter har inträffat utan att ha identifierats eller rapporterats vilket indikerar ett behov av att förstärka utbildningsinsatser och öka medvetenheten inom nämnden. En sådan förstärkning är avgörande för att säkerställa att incidenter upptäcks, rapporteras och hanteras i enlighet med gällande rätt. Det är även sannolikt att fler incidenter kommer rapporteras under resterande del av året varpå siffran högst troligt kommer öka ytterligare innan årets slut.

1.4 Förbättringar som föreslås för verksamheten

Nedan följer förslag på förbättringsaktiviteter för verksamheten under åren 2026, 2027 och 2028. Förbättringarna baseras på de risker och oönskade händelser som lyfts i verksamhetens väsentlighets- och riskanalys samt internkontrollplan för 2026.

De föreslagna aktiviteterna baseras även på de risker som aktualiserats inom området genom nämndens risk- och sårbarhetsarbete (RSA) men även genom de stickprov och observationer som gjorts under året och som beskrivs mer ingående i avsnitt 1.3.4.

Utöver detta föreslås även aktiviteterna med hänsyn till rekommendationer från GDPR-årsrapport som DSO ansåg vara prioriterade utifrån risker för enskildas fri- och rättigheter.

1.4.1 Aktiviteter som fortsatt pågår under 2025

Under detta avsnitt listas de aktiviteter som initierats och är pågående under arbetet av sammanställningen för denna rapport. Dessa aktiviteter kommer fortsatt pågå under resterande del av året 2025.

Verksamhetsplan för samordningsfunktionen för informationssäkerhet och dataskydd
Framtagande av verksamhetsplan 2026 för samordningsfunktionen för informationssäkerhet och dataskydd. Beslut om verksamhetsplanen förväntas tas i förvaltningsledningen innan 2025 års slut.

Lokal rutin för behörighetshantering
Framtagande av förvaltningsövergripande rutin för behörighetshantering.

Användarvillkor för nyttjande av digitala enheter
Framtagande av användarvillkor för nyttjande av digitala enheter på utbildningsförvaltningen.

Lokal rutin för hantering av misstanke om överträdelse eller brott
Framtagande av lokal rutin för hantering av misstanke om överträdelse eller brott relaterat till användarvillkor för nyttjande av digitala enheter på utbildningsförvaltningen.

1.4.2 Aktiviteter under år 2026

Under detta avsnitt listas de aktiviteter som ISAM rekommenderar prioriteras under året 2026. Aktiviteterna utgår främst utifrån parametrarna att framtagande, implementation samt uppföljning av informationssäkerhets- och dataskyddsarbetet.

ID	Rekommenderad aktivitet	Beskrivning av aktiviteten	Åtgärdsansvarig
1	**Översyn av lokal anvisning för informationssäkerhet**	Årlig översyn och vid behov uppdatering görs av den lokala anvisningen.	ISAM ansvarar för översyn och uppdatering. Implementeringsarbetet hanteras främst genom samordningsfunktionen för informationssäkerhet och dataskydd.
2	**Översyn av anvisning för hantering av informationssäkerhetsincidenter**	Årlig översyn och vid behov uppdatering görs av anvisningen för hantering av informationssäkerhetsincidenter.	ISAM ansvarar för att aktiviteten genomförs.
3	**Uppföljning av behörigheter**	ISAM föreslår i samsyn med DSO:s rekommendation som lyfts i GDPR-årsrapport att den pågående förvaltningsövergripande rutin som tas fram implementeras i verksamheten för granskning av användares behörigheter.	Om inte annat framkommer av kraven från klassningen bör respektive verksamhet, minst årligen, granska sina behörigheter. Chef över respektive verksamhet är ansvarig för att behörigheterna hålls uppdaterade och aktuella och att behörighetsstyrningen ligger i linje med kraven som framkommer av klassningen.
4	**Uppföljning av utbildningsinsatser**	Årlig översyn och uppföljning av genomförandegrad för de obligatoriska e-utbildningarna inom informationssäkerhet och dataskydd.	ISAM ansvarar för att aktiviteten genomförs och hanteras vidare i samordningsfunktionen för informationssäkerhet och dataskydd på förvaltningen.
5	**Målgrupps- och situationsanpassade utbildningar inom informationssäkerhet och dataskydd**	Behovet av att ta fram målgrupps- och situationsanpassade utbildningar inom informationssäkerhet och dataskydd har lyfts och identifierats under året varpå framtagande av sådana rekommenderas under 2026.	ISAM ansvarar för att aktiviteten genomförs och hanteras vidare i samordningsfunktionen för informationssäkerhet och dataskydd på förvaltningen.

6	**Verksamhetsplan för samordningsfunktionen för informationssäkerhet och dataskydd**	Framtagande av verksamhetsplan för samordningsfunktionen för informationssäkerhet och dataskydd föreslås tas fram under 2026 i syfte att tydliggöra ansvar och förväntningar för funktionen och dess medlemmar under 2027.	ISAM ansvarar för att aktiviteten genomförs och hanteras vidare i samordningsfunktionen för informationssäkerhet och dataskydd på förvaltningen.
7	**Översyn av informationssäkerhet vid anskaffning och utveckling**	En översyn av processer och rutiner för informationssäkerhet vid upphandling, anskaffning och utveckling av varor och tjänster föreslås göras under 2026 i syfte att verksamheten på ett tydligare sätt och i rätt tid får med informationssäkerhet på ett fullgott sätt.	ISAM ansvarar för att aktiviteten genomförs med stöd av informationssäkerhetshandläggare på förvaltningen.
8	**Särskild utbildning för chefer och ledning i enlighet med krav från cybersäkerhetslagstiftningen**	Utöver de obligatoriska e-utbildningarna inom informationssäkerhet och dataskydd föreslås det från och med 2026 en gång per år hållas en särskild obligatorisk utbildning för chefer och ledning som ett led av kraven på utbildning i den kommande cybersäkerhetslagstiftningen.	Ansvar för framtagande av utbildningen förväntas hamna hos Stadsledningskontoret.

9	**Inventering och klassificering**	Inventering och översyn av it-komponenter, informationsmängder samt tillhörande verksamhetsprocesser. Översyn och uppdatering av befintliga som nya klassningar i enlighet med processen för informationsklassning i staden, vilka också inkluderar en självvärdering och handlingsplan för verksamheten samt riskanalys med tillhörande säkerhetsåtgärder. Förvaltningen bör även fortsatt arbeta med att implementera metoden för informationsklassningsprocessen som under året 2025 kompletterats med lokala anpassningar till Stadens metodstöd. Särskilt fokus bör läggas på att inventera och klassificera kritiska verksamhetsprocesser med tillhörande informationsbärare (informationssystem) som ett led i kraven från cybersäkerhetslagstiftningen. Även krav på arkivering och gallring bör omfattas i arbetet med detta.	Inom objektförvaltningen ansvarar objektägare för att tillse att klassning och handlingsplan sker inom objektet. Objektledare följer upp att skyddsåtgärder och säkerhetskrav tas omhand och rapporterar till objektägare. Objektsspecialist är ansvarig för åtgärdande.

10	**Kontinuitetshantering och katastrofåterhämtning**	Framtagande av förvaltningsövergripande kontinuitetsplan för hantering av störning och/eller förlust av kritisk aktivitet eller resurs. Bedöms som särskilt prioriterat, bland annat utifrån kommande lagstiftning inom området. I detta föreslås det även tas fram en komplett lista över prioritetsordning för system och tjänster i syfte att kunna prioritera återställning vid katastrofåterhämtning (disaster recovery).	ISAM ansvarar för att aktiviteten initieras med stöd av informationssäkerhetshandläggare på förvaltningen. Berörda roller enligt den lokala anvisningen för informationssäkerhet ansvarar för genomförandet. Inom objektförvaltningen ansvarar objektägare för att tillse att kontinuitetshantering sker inom objektet. Objektledare följer upp att relevanta åtgärder tas omhand och rapporterar till objektägare. Objektsspecialist är ansvarig för åtgärdande.

Övriga aktiviteter som bör initieras alternativt fortlöpa under 2026

- Initiera arbete med framtagande av förvaltningsövergripande risk- och hotbildsanalys inom informationsssäkerhetsområdet. Observera att detta ej är att likställa med de risker som lyfts i risk- och sårbarhetsanalysen (RSA).
- Påbörja arbete med att se över befintliga rutiner för introduktion för nya medarbetare samt hantering av anställningsavslut i termer av informationssäkerhet och dataskydd.
- Fortsatt arbete med konsekvensbedömningar och mitigerande riskhantering.
- Fortsatt arbete med hantering av skyddade personuppgifter på förvaltningen och i verksamhetssystem.
- Översyn av personuppgiftsbiträdesavtal och förvaltningens registerförteckning avseende personuppgiftsbehandlingar.
- Översyn och vid behov uppdatering av rutiner och anvisningar gällande personuppgiftshantering på förvaltningen.

Särskilt om cybersäkerhetslagstiftningen
Utöver ovan listade aktiviteter bedöms förvaltningens arbete även präglas mycket av den kommande cybersäkerhetslagstiftningen.

ISAM bedömer att särskilt prioriterade aktiviteter relaterat till den kommande lagstiftningen är att:

- Genomföra en analys av omfattning (verksamheter, system, nätverk).
- Kartlägga gap mot lagens krav samt upprätta en handlingsplan för åtgärder.
- Genomföra särskild utbildning för chefer och ledning.
- Anpassa lokala rutiner för kontinuitet och incidentrapportering.
- Säkerställa leverantörsavtal och tredjepartsrisker.

ISAM ansvarar för att aktiviteterna initieras med stöd av informationssäkerhetshandläggare på förvaltningen samt samordningsfunktionen för informationssäkerhet och dataskydd.

Berörda roller enligt den lokala anvisningen för informationssäkerhet ansvarar för genomförandet.

Nämnden utgår i övrigt från att Stockholms stad på ett övergripande

plan kommer styra arbetet med efterlevnad av kraven som följer av Cybersäkerhetslagstiftningen.

Övriga prioriterade aktiviteter från GDPR-årsrapport

- Kartläggning av utbildningsinsatser.
- Säkerställa funktioner för och verkställande av arkivering och gallring i förvaltningens IT-system.
- Översyn av processen för registerutdrag och framtagande av informationstexter.

Övriga risker som bedömts som låga med tillhörande rekommenderade åtgärder i GDPR-årsrapport föreslår ISAM tillsammans med DSO hanteras under 2027.

ISAM ansvarar för att aktiviteterna initieras med stöd av DSO på förvaltningen.

Berörda roller enligt den lokala anvisningen för informationssäkerhet ansvarar för genomförandet.

1.4.3 Aktiviteter under år 2027 samt 2028

Under detta avsnitt listas de aktiviteter som ISAM rekommenderar prioriteras under åren 2027–2028. Aktiviteterna utgår främst utifrån parametrarna att framtagande, implementation samt uppföljning av informationssäkerhets- och dataskyddsarbetet.

ID	Oönskad händelse i VoR samt IKP	Uppföljning av oönskad händelse	ISAM:s förslag på åtgärd
1	**Översyn av lokal anvisning för informationssäkerhet**	Årlig översyn och vid behov uppdatering görs av den lokala anvisningen.	ISAM ansvarar för översyn och uppdatering. Implementeringsarbetet hanteras främst genom samordningsfunktionen för informationssäkerhet och dataskydd.
2	**Översyn av anvisning för hantering av informationssäkerhetsincidenter**	Årlig översyn och vid behov uppdatering görs av anvisningen för hantering av informationssäkerhetsincidenter.	ISAM ansvarar för att aktiviteten genomförs.
3	**Uppföljning av utbildningsinsatser**	Årlig översyn och uppföljning av genomförandegrad för de obligatoriska e-utbildningarna inom informationssäkerhet och dataskydd.	ISAM ansvarar för att aktiviteten genomförs och hanteras vidare i samordningsfunktionen för informationssäkerhet och dataskydd på förvaltningen.
4	**Målgrupps- och situationsanpassade utbildningar inom informationssäkerhet och dataskydd**	Behovet av att ta fram och anpassa målgrupps- och situationsanpassade utbildningar inom informationssäkerhet och dataskydd bedöms löpande som aktuellt.	ISAM ansvarar för att aktiviteten genomförs och hanteras vidare i samordningsfunktionen för informationssäkerhet och dataskydd på förvaltningen.
5	**Särskild utbildning för chefer och ledning i enlighet med krav från cybersäkerhetslagstiftningen**	Årlig översyn och uppföljning av genomförandegrad för särskild utbildning för chefer och ledning i enlighet med krav från cybersäkerhetslagstiftningen.	ISAM ansvarar för att aktiviteten genomförs och hanteras vidare i samordningsfunktionen för informationssäkerhet och dataskydd på förvaltningen.

6	**Inventering och klassificering**	Inventering och översyn av it-komponenter, informationsmängder samt tillhörande verksamhetsprocesser. Översyn och uppdatering av befintliga som nya klassningar i enlighet med processen för informationsklassning i staden, vilka också inkluderar en självvärdering och handlingsplan för verksamheten samt riskanalys med tillhörande säkerhetsåtgärder. Särskilt fokus bör läggas på att inventera och klassificera kritiska verksamhetsprocesser med tillhörande informationsbärare (informationssystem) som ett led i kraven från cybersäkerhetslagstiftningen. Även krav på arkivering och gallring bör omfattas i arbetet med detta.	Inom objektförvaltningen ansvarar objektägare för att tillse att klassning och handlingsplan sker inom objektet. Objektledare följer upp att skyddsåtgärder och säkerhetskrav tas omhand och rapporterar till objektägare. Objektsspecialist är ansvarig för åtgärdande.
7	**Kontinuitetshantering och katastrofåterhämtning**	Årlig översyn och vid behov uppdatering görs av förvaltningsövergripande kontinuitetsplan för hantering av störning och/eller förlust av kritisk aktivitet eller resurs.	ISAM ansvarar för att aktiviteten initieras med stöd av informationssäkerhetshandläggare på förvaltningen. Berörda roller enligt den lokala anvisningen för informationssäkerhet ansvarar för genomförandet.
8	**Verksamhetsplan för samordningsfunktionen för informationssäkerhet och dataskydd**	Framtagande av en årlig verksamhetsplanen för samordningsfunktionens för informationssäkerhet och dataskydd.	ISAM ansvarar för att aktiviteten genomförs och hanteras vidare i samordningsfunktionen för informationssäkerhet och dataskydd på förvaltningen.

1.5 Sammanfattande bedömning

Informationssäkerhetsarbetet inom utbildningsförvaltningen bedöms vara på rätt väg. Det finns dock fortsatt behov av ledningens aktiva stöd och tydlig styrning för att möta de ökade kraven inom informationssäkerhet och dataskydd.