Stockholmshem

Ledningens genomgång 2026
Informationssäkerhet

Innehåll

Om Ledningens genomgång

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

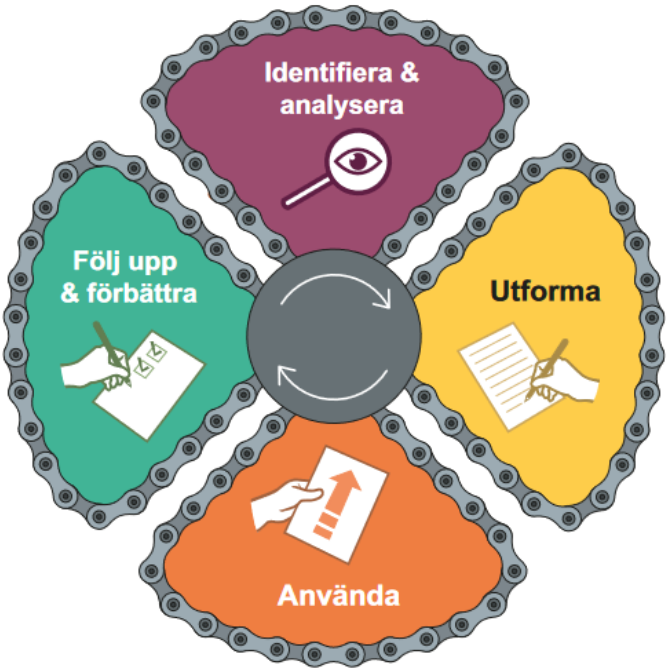
Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av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

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

Systematiskt informationssäkerhetsarbete

Precis som inom andra områden, till exempel ekonomi och kvalitetsstyrning, behöver arbetet med informationssäkerhet vara strukturerat och systematiskt för att bli effektivt. Den snabba utvecklingen inom informationshantering motiverar detta ytterligare, eftersom det ständigt kommer nya hot, nya tekniska möjligheter och förändrade lagkrav. Det räcker inte att införa ett antal säkerhetsåtgärder och sedan slå sig till ro, utan säkerhetsåtgärdernas effektivitet måste ses över regelbundet så att säkerheten över tid är anpassad till organisationens behov och förändringar i omvärlden.

MSB har tillsammans med experter tagit fram ett metodstöd för att bedriva ett systematiskt informationssäkerhetsarbete. Det baseras på standardserien ISO/IEC 27000, som är etablerad i Sverige och internationellt. För dig som chef finns också en översikt av stödet som ger en snabb överblick över de bärande beståndsdelarna i arbetet, som är samma för alla organisationer. Delarna är Identifiera och analysera, Utforma, Använda samt Följa upp och förbättra.


Identifiera &
analysera
Utforma
Använda
Följ upp
& förbättra

IT skyddsgrupp

- Informationssäkerhetssamordnare, ISAM
- IT-chef
- Säkerhetsstrateg
- Ordförande Dataskyddskommittén

Under 2025 har en ny ISAM utsetts på VD-stab och som övertagit ordförandeskapet för IT-skyddsgruppen. Möten har hållits regelbundet under året och har säkrat upp det systematiska arbetet. Även under 2026 kommer IT-skyddsgruppen hålla regelbundna möten för att upprätthålla informationssäkerheten enligt stadens LIS och Stockholmshems lokala anvisningar.
ISAM representerar Stockholmshem i de forum och samverkansgrupper som Stockholm stad anordnar inom informationssäkerhet, vilket säkerställer omvärldsbevakning, samordning och att nya krav och vägledningar hanteras strukturerat i organisationen.

Dataskyddskommitté

- Fredrik Beckman (IT) - Ordförande
- Informationssäkerhetssamordnare, ISAM
- Säkerhetsstrateg
- Joakim Cassepierre (HR)
- Niklas Dybeck (Ekonomi)
- Jessica Gjorshevski (B&T)
- Fatima Durrani (Förvaltningen)
- Patrik Gavander (VD-stab)
- Karin Thomasson (rådgivare Certezza)

Bolaget har under 2025 fortsatt med ett externt dataskyddsombud, Juristen Johan Åhs på Certezza, för att både höja och säkerställa kompetens, avlasta organisationen och minska risken för jäv i granskningen av dataskyddsarbetet. Uppdraget innebär att ombudet oberoende följer upp efterlevnaden av dataskyddsreglerna, ger råd till verksamheten och rapporterar till ledningen vid incident eller avvikelser.

Lösningen med externt dataskyddsombud planeras att kvarstå under hela 2026 och ses som en strategisk satsning för att höja bolagets kompetens och mognad inom dataskydd.

Ambitionen är att under perioden utvärdera alternativa långsiktiga lösningar (t.ex. intern funktion eller hybridlösning) och återkomma med förslag till ledningen.

Under året har kommittén genomgått en utbildning för att höja kunskapen kring dataskydd.

Dataskyddskommittén har träffats regelbundet under 2025 för att vara ett stöd till verksamheten i dataskyddsfrågor. En lärdom under gångna året är att det är svårt att säkerställa tillräckligt engagemang och kompetensförsörjning. Det innebär en risk för det systematiska dataskyddsarbetet försvagas och att efterlevnad av dataskyddsförordningen inte kan säkerställas på önskad nivå. På grund av detta kommer bolaget under 2026 genomföra förändringar i upplägget kring Dataskyddskommittén, mer information om detta kommer i dataskyddsombudets årsrapport.

Förkortningar

- ISAM = Informationssäkerhetssamordnare.
- DSO = Dataskyddsombud.
- LIS = Ledningssystem för informationssäkerhet. ISO 27000 Standar som ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet.
- RSA = Risk och sårbarhets Analys.
- VOR = Väsentlighets- och riskanalys.
- IKP = Internkontrollplan.
- KRT = konfidentialitet, riktighet och tillgänglighet (KLASSA)

Omvärldsbevakning

Hot, trender och omvärld

Under det gångna året har hotbilden inom informationssäkerhet fortsatt att förändras i snabb takt, både globalt och nationellt. Utvecklingen drivs av mer avancerade angreppsmetoder, ökad geopolitisk osäkerhet och ett skärpt regulatoriskt landskap. Nedan följer de viktigaste trenderna som påverkar organisationers riskläge och strategiska prioriteringar.

1. Ökade riktade attacker mot offentlig sektor och leverantörskedjor

Angrepp som utnyttjar sårbarheter hos tredjepartsleverantörer fortsätter att öka och blir allt mer sofistikerade. Flera incidenter under året, bland annat händelsen hos Miljödata, har

visat hur svagheter hos en extern part kan få breda och allvarliga konsekvenser för anslutna verksamheter. Angripare fokuserar ofta på tjänsteleverantörer som hanterar stora datamängder eller har åtkomst till flera kunder samtidigt. Detta understryker behovet av starkare kravställning, kontinuerlig uppföljning och en mer riskbaserad bedömning av leverantörsberoenden. Organisationer behöver i större utsträckning säkerställa att leverantörsskyddet är integrerat i hela livscykeln – från upphandling till löpande drift.

2. Fortsatt professionalisering av cyberkriminella aktörer

Ransomware-grupper utvecklas vidare och agerar i allt högre grad som organiserade brottsnätverk med tydlig arbetsfördelning och kommersiella incitament. Fokus ligger allt mer på datastöld och långsiktig utpressning snarare än enbart systemlåsning. Informationsläckage används för att öka pressen på drabbade organisationer, även om de vägrar att betala lösensumma. Angreppen riktas ofta mot IT-miljöer med bristande segmentering, låg loggningsnivå eller föråldrade system. Den ökade professionaliseringen innebär att även mindre organisationer riskerar att hamna i skottlinjen när angriparna automatiserar sina verktyg och metoder.

3. Ökad aktivitet kopplat till geopolitisk oro och digital suveränitet

Geopolitiska spänningar har lett till en ökning av statsstödda och politiskt motiverade cyberaktiviteter som syftar till att störa, påverka eller inhämta information. Sverige och övriga Norden är attraktiva mål för påverkanskampanjer, särskilt kopplat till samhällsviktig verksamhet och kritisk infrastruktur. Samtidigt ökar betydelsen av digital suveränitet**,** då allt fler verksamheter är beroende av globala molntjänster och leverantörer utanför EU:s jurisdiktion. Detta skapar nya risker kring kontroll över data, efterlevnad av internationell lagstiftning och potentiell exponering för utländska intressen. Organisationer behöver därför stärka sin förmåga att bedöma strategiska beroenden och säkerställa att kritisk information kan skyddas även vid förändrade geopolitiska förutsättningar.

4. Skärpta regulatoriska krav och nya styrmodeller

Regelverken kring informationssäkerhet och cybersäkerhet skärps successivt, med EU:s NIS2-direktiv som en central förändring för många verksamheter. Allt fler organisationer kommer att omfattas av krav på riskhantering, incidentrapportering och dokumenterad styrning av säkerhetsarbetet. Detta innebär att ledningen behöver ta ett tydligare ansvar för att säkerställa att strukturer, roller och processer är ändamålsenliga. Implementeringen av regulatoriska krav kräver ofta både organisatoriska och tekniska anpassningar. Det blir därför viktigare att arbeta proaktivt och att integrera efterlevnad i verksamhetens långsiktiga planering.

5. Framväxande teknologier och nya riskbilder

Den snabba utvecklingen inom AI, automatisering och avancerad dataanalys innebär både betydande möjligheter och risker. Angripare använder i ökad utsträckning AI för att automatisera intrång, förbättra phishingkampanjer och identifiera sårbarheter i stor skala. Samtidigt ger tekniken organisationer bättre möjligheter att upptäcka anomalier, stärka incidenthanteringen och effektivisera analyser. Den ökade tekniska komplexiteten bidrar dock till nya typer av risker, bland annat kring modellmanipulation, dataförgiftning och bristande transparens. Detta gör att behovet av tydliga etiska riktlinjer, teknisk kontroll och styrning ökar markant.

NIS2 och kommande cybersäkerhetslagen – Lägesbild för Stockholmshem

Under 2025 har vi följt branschens rekommendationer och löpande analyserat hur Stockholmshem påverkas av NIS2-direktivet och den nya svenska cybersäkerhetslagen som träder i kraft den 15 januari 2026. Arbetet har genomförts i nära dialog med våra syskonbolag för att säkerställa en gemensam tolkning och en samordnad förberedelse inom hela koncernen. Den samlade bedömningen är att Stockholmshem omfattas av regelverket mot bakgrund av att vår solcellsproduktion som matas ut på allmänna elnätet och därmed kan klassas som samhällsviktig funktion. Med största sannolikhet omfattas vi även av lagen mot bakgrund av att vi ses som laddningsoperatör, detta oaktat om vi har en leverantör som ombesörjer förvaltningen och driften av laddningspunkten.

Vad gäller vår solcellsproduktion har tillsynsmyndigheten MSB ställt frågan till EU-kommission om avsikten varit att samtliga juridiska personer som producerar el, per automatik ska omfattas av den kommande Cybersäkerhetslagen. Det får förstås att detta inte var Kommissionens avsikt och troligtvis kommer ett förtydligande i denna del men i dagsläget omfattas vi av lagen.

Det innebär att vi under 2026 behöver säkerställa att våra processer och arbetssätt uppfyller de krav som lagen sannolikt kommer att innebära. För verksamheter som omfattas krävs en anmälan till den myndighet regeringen utser, och denna ska göras i direkt anslutning till ikraftträdandet den 15 januari 2026. Det är dock först efter att tillsynsmyndigheterna (i vårt fall troligtvis MSB) har kommit med föreskrifter kommer det att klargöras vad som förväntas av oss.

NIS2 innebär krav på lämpliga och proportionella tekniska, organisatoriska och driftrelaterade åtgärder för att skydda verksamhetens nätverks- och informationssystem. Detta omfattar bland annat informationsklassning, risk- och konsekvensanalys, incidenthantering, samt stärkt styrning av leverantörsrisker. Många av dessa krav kan tillgodoses genom vårt fortsatta systematiska och riskbaserade informationssäkerhetsarbete, samt genom att följa stadens riktlinjer, tillämpningsanvisningar och etablerade processer såsom pm3.

Vad händer inom staden? – budget, inriktningar, lokala förändringar eller satsningar

Granskning av det systematiska informationssäkerhetsarbetet är från och med 2024 infört i VOR (Väsentlighets- och Riskanalysen i systemstödet Stratsys) och kommer att följas inom förfarandet av bolagets internkontroll.

Under 2025 har staden har fokus på att få fram rutiner för klassificering inom upphandlingsprocessen i syfte att stärka informationssäkerheten. ISAM har tagit del av andra verksamheters arbetssätt för att kommande år göra en satsning på Stockholmshems Inköpsenhet.

Staden har under året informerat om att förfarandet i utbildningsportalen kommer att ändras. Medarbetarna kommer inte längre få en automatisk årlig uppmaning om certifiering att gå utbildning i Dataskydd och informationssäkerhet, som är tvingande att årligen gå igenom. Stockholmshem kommer därför behöva sätta en rutin som säkerställer att medarbetarna går utbildningarna.

Staden har etablerat en CERT, stadens stöd vid it-säkerhetsincidenter och cybersäkerhet. Funktionen samarbetar med S:t Erik Kommunikation för att organisera arbetet och vi har redan märkt av nyttan.

Projektet att migrera lokala verksamhetssystem från GSIT-avtalet till det nya STA – Systemtjänsteavtalet har pågått under delar av 2025 och är nu färdigställt med restpunkten att IT-miljön behöver delas in i nya zoner, vilket sker genom Stadens projekt Långsikt.

Året som gått

- **Uppföljning**

Vad har verksamheten identifierat i RSA-arbetet

Behov av bättre säkerhetskopior som följer senaste ”best practice” med fokus på att skydda mot manipulation av redan tagna säkerhetskopior samt möjliggöra snabb återställning. Under året har bostadsbolagen gemensamt skickat in en skrivelse till SLK-IT kring behovet av s.k. Immutable Backups (backuper som har hög motståndskraft mot manipulation och det har nu införts som en standardtjänst för samtliga verksamheter inom Stockholm Stad.

Fortsatt behov av att härda och skydda våra IT-miljöer och informationstillgångar, vilket skett i stor omfattning under året tillsammans med externa experter.

Härdning av en IT-miljö (eng. hardening) innebär att man systematiskt minskar attackytan och stärker skyddet i servrar, klienter, nätverk, applikationer och molntjänster. Syftet är att ta bort onödiga funktioner, stänga säkerhetshål och göra miljön mer motståndskraftig mot intrång, sabotage och felkonfigurationer.

Resultatet från egen uppföljning (VoR och IKP)

Under 2025 har vi genomfört ett antal förbättringar inom ramen för VORen där det fanns två oönskade händelser för granskning;

- Brister i informationssäkerhet leder till att känslig information sprids
- En incident har inte rapporterats

Många åtgärder har skett under året, se nedan, för att generellt stärka informationssäkerheten. Avvikelse finns i att klassificeringen av systemen har släpat efter tidplanen och ska vara helt klart till 31 mars 2026. Under året har IT-skyddsgruppen arbetat för att följa årshjulet med de aktiviteter som ska genomföras. PEN-test har skett och åtgärder vidtagna.

För att minska risken för att inte incident rapporteras har informationen på Insidan förtydligats för att göra det enkelt för medarbetare att göra anmälan. Vi har också förtydligat skillnaden på en personuppgiftsincident och en IT-incident.

Resultatet från revisioner

Vi har svarat på inkomna revisionsförfrågningar och inte fått några anmärkningar eller åtgärdsförslag.

GDPR-årsrapport

En årsrapport tas fram av DSO, Johan Åhs, vilken föredras för styrelsen enligt arbetsordningen på ordinarie styrelsemöte i februari 2026.

Information om avvikelser (incidenter och andra händelser)

Under perioden har avvikelser identifierats inom bolagets och stadens gemensamma IT-miljöer. Samtliga händelser har hanterats enligt gällande processer och, där så varit relevant, rapporterats vidare till stadens centrala funktioner för incident- och riskhantering.

Arbetet har bland annat omfattat:

- **Identifierade säkerhetsbrister i stadens mobilplattform**, där utredning och åtgärdsarbete pågår i samverkan med stadens centrala IT-funktioner. Bolaget har vid behov gjort egna incidentanmälningar och säkerställt att risker hanteras i enlighet med styrande rutiner.

- **Stadens CERT** har kontaktat bostadsbolagen angående sårberhetskanning av externa servrar där med nedslag kring livscykelhantering. Stockholmshem tog ansvar för denna punkt och arbetade tillsammans med leverantören fram en lösning som samtliga systerbolag kunde använda.

- **Leverantör har av misstag, vid aktivering av AI,** på leverantörens egna testservrar fått spridning på e-postkonton. Hanterad av Bitr. DSO/Fredrik.

- **Felaktig behörighetshantering** vid införandet av ett nytt system ledde till att en entreprenör kunde komma åt och läsa en annan entreprenörs anbud. Händelsen är hanterad som en IT-incident och ett formellt klagomål har skickats till Leverantören av systemet för att få spårbarhet ifall det vid senare tillfälle behöver tas ytterligare juridiska åtgärder.

- Övriga aktiviteter

Utbildning / Awareness

Under 2025 har utbildningar fortsatt med s.k. Nanolearing inom området GDPR och dataskydd för Stockholmshems samtliga medarbetare.

Organisation GDPR / Dataskydd

Dataskyddskommittén har under 2025 arbetet i enlighet med de riktlinjer som ledningsgruppen antog 2025-02-24 ” Riktlinje för dataskyddsorganisationen vid Stockholmshem”. Kommittén har löpande under året arbetat med att digitalisera registerförteckningen från Excel till digitalform i verktyget DraftIT. Ett antal rutiner bla. ”Rutin för begäran om registerutdrag rättelse eller radering” och ” Rutin avseende skyddade personuppgifter för anställda” har kunnat fastställas.

Förvaltningsmodell PM3

Under 2025 har vi fortsatt att arbeta med etableringen av stadens förvaltningsmodell PM3 och har nu etablerat alla tio förvaltningsobjekten. Modellen har en viktig funktion framöver i att ansvarsfördelningen av it-tjänster tydliggörs så att klassificering sker inför, under och efter att nya tjänster implementeras. Alla berörda IT-tjänster ska vara klassificerade under Q1 2026.

Uppgraderingar och härdning av IT-miljön

Vi har under 2024 uppgraderat samtliga Windows 2012 till Windows 2022 samt samtliga SQL servrar till SQL server 2024 för att höja tillgänglighet och säkerhetsnivån. I detta har också systematiskt arbete med härdning av IT-miljön införts.

Säkrad Backuplösning

Under året har lösning implementerats för att säkra backuptagning för systemen Fast2, Flex samt Reskontran från stadens IT-miljö till vår egna IT-miljö för att ha denna identifierade kritiska data säkrad i flera IT-miljöer.

Framtagen Kamerarutin

Under året har en kamerarutin utvecklats för att tydliggöra rutiner och förhållningssätt kring

kamerabevakning inom våra förvaltningsområden. Rutinen är framtagen men ännu inte formellt beslutad av ledningsgruppen.

Hantering tjänstekort som identifikation

Under året har rutin tagits fram för hantering av tjänstekort som identifikation för att upprätthålla säkerhet och trygghet på våra kontor. På kontoret i Skärholmen har även krypteringsnivån på passagesystemet höjts till högsta tillgängliga (Mifare Desfire 3).

Rutin för Off-boarding

Under året har rutin tagits fram för att hantera off-boarding av medarbetare och konsulter vilket säkrar upp behörighetskontrollen så att vi inte har konton eller behörigheter kvar efter avslutad anställning eller uppdrag.

Upphandling med fokus på informationssäkerhet

Under året har Stockholmshem tagit del av Trafikkontorets fina arbete med informationssäkerhet vid upphandling. Arbetssättet kommer att inarbetas under 2026 för att stärka säkerhetsarbetet under kravställning, testning innan implementation samt uppföljning med leverantören.

Test av Phishing inom Stockholmshem

Under året har ett phishingtest genomförs genom att en kontrollerad, simulerad phishing-mejl skickas till alla medarbetare. Syftet var att kunna värdera mängden som öppnar mailet och klickar på länken eller lämnar ifrån sig uppgifter, vilket ger en bild av organisationens sårbarhet. Resultatet visade att behovet är stort att ha kontinuerlig utbildning för att höja säkerhetsmedvetenhet. Denna typ av aktivitet kommer vi fortsätta med under 2026.

Förbättringsaktiviteter för verksamheten under kommande 3-årsperiod

Det systematiska informationssäkerhetsarbetet innebär att vi löpande identifierar och hanterar risker, utbildar medarbetare, följer upp efterlevnad och förbättrar våra rutiner. Genom årshjulet i Stratsys följs aktiviteterna upp årligen inom ramen för ledningens genomgång. På så sätt säkerställer vi att vårt skydd av informationstillgångar är anpassat till nya hot, tekniska förändringar och gällande lagstiftning.

Löpande förbättringsaktiviteter under 2026, 2027 och 2028.

Förbättringsaktiviteter 2026

- Fortlöpande utbildning genomförs.
- Medverkan i stadens framtagande av underlag för upphandling av GSIT3.
- Genomför klassificeringar av befintliga IT-tjänster samt löpande av ny.
- PEN-tester i egen regi och i samarbete med våra systerbolag.
- Översyn av inköpsprocessen ur ett informationssäkerhets- samt dataskyddsperspektiv
- Anpassa systemmiljön mot Stadens Projekt Långsikt, nya zonmodellen

Förbättringsaktiviteter 2027

- Införandet av GSIT3 – Digital arbetsplats
- Fortsatta utbildningsinsatser.
- Fortsatt löpande översyn av befintliga klassificeringar.
- PEN-tester i egen regi och i samarbete med våra systerbolag.

Förbättringsaktiviteter 2028

- Fortsatt löpande översyn av befintliga klassificeringar.
- PEN-tester i egen regi och i samarbete med våra systerbolag.

Underskriftens äkthet valideras här: https://underskriftpas.stockholm.se/validera

Signerad av
Sofia Forsman

Signaturdatum
2025-12-03 13:15:47

Elektronisk underskrift

underskrift.stockholm.se

Signerad av
Åsa Wigfeldt

Signaturdatum
2025-12-03 14:55:21

Elektronisk underskrift

underskrift.stockholm.se