Göteborgs Stad

Åtgärder informationssäkerhet

Redogörelse för vidtagna åtgärder efter genomförd revision avseende verksamhetsåret 2024

2025-04-09

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2025-04-09	0.1	Upprättande av rapport	Stefhan Forsberg

Innehåll

1 Sammanfattning

Stadsrevisionen har genomfört en granskning av GSL, ett av de områden man valde att tita närmare på vid denna granskning var informationssäkerhet.

Vid revisionen framkom ett antal brister i efterlevnad av Stadens riktlinje för informationssäkerhet, rekommendationen som följde löd enligt följande:

”Bolaget rekommenderas att slutföra sitt arbete med att implementera fullmäktiges riktlinje för informationssäkerhet i sin verksamhet.”

Att implementera fullmäktiges riktlinje för informationssäkerhet är ett mycket omfattande arbete som spänner över flera år. Det handlar i grund och botten om att upprätta och införa ett systematiskt och riskbaserat arbete med informationssäkerhet eller som man också kallar det, ett ledningssystem för informationssäkerhet.

Det är viktigt att det finns en återkommande systematik i arbetet och att man arbetar prioriterat utifrån de risker som man identifierar. De åtgärder som införs ska vara verkningsfulla och leda till att förbättra GSL:s arbete med informationssäkerhet.

Med det sagt handlar det alltså inte bara om faktiska åtgärder som ska göras här och nu, det handlar lika mycket om att bygga säkerhetskultur och skapa en medvetenhet kring informations- och cybersäkerhet. Av den anledningen är detta ingen “Quick fix” utan det måste få ta tid.

Denna rapport kommer redogöra för de åtgärder som GSL har infört på kort och lång sikt för att omhänderta revisionspunkten.

2 Resultat

Redogörelse av GSL:s informationssäkerhetssamordnare

Området informationssäkerhet har vid både 2023 och 2024 års granskningar ej levt upp till kraven i Stadens riktlinje för informationssäkerhet.

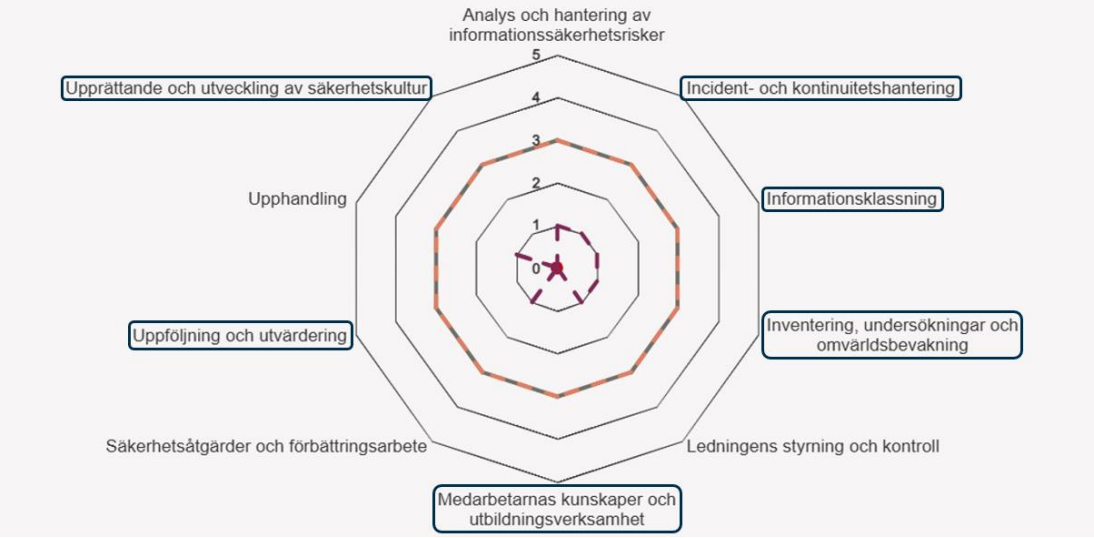
Inför verksamhetsåret 2025 har en rad åtgärder vidtagits och införts för att möta dessa brister och nå följsamhet mot Stadens riktlinje för informationssäkerhet. Dessa redogörs för i sin korthet här nedan:

- 2025-01-07 ny informationssäkerhetssamordnare tillika dataskyddskontakt påbörjar tjänst hos GSL, huvudfokus i uppdraget ligger på att nå följsamhet mot Stadens riktlinje för informationssäkerhet och arbeta med dataskydd (GDPR).

- 2025-02-19 Slutrapport som gör gällande huruvida GSL kommer omfattas av kraven i NIS 2 direktivet presenteras. Rapporten har presenterats för bolagsledningen och det finns en samförståelse kring resultatet. (Rapporten finns att ta del av i sin helhet på förfrågan).

- 2025-01-27 genomförs en GAP-analys/Nulägesanalys för att visualisera en tydlig bild av nuläge och önskat läge kopplat till Stadens riktlinje för informationssäkerhet samt NIS 2 direktivet och kommande cybersäkerhetslagstiftning.

  Analysen lyfter fram 6 områden som vi initialt behöver fokusera på och en ny mätning kommer genomföras Q2 2025. Nedan presenteras en översiktlig graf, och fokusområdena presenteras i löptext med genomförda åtgärder presenterade direkt efter respektive punkt.



2.1.1 Incident- och kontinuitetshantering

Utskick om incidentrapportering (2025-03-14)

Ny rutin för incidentrapportering kommuniceras ut till hela bolaget, denna nya rutin är beslutad av bolagsledningen och har justerats för att vara enklare för medarbetaren att tolka. Rutinen avser incidentrapportering både enligt GDPR och NIS 2 direktivet.

Översynen av kontinuitetshanteringen får avvakta till dess att informationsklassningen är genomförd. Emellertid har vissa väsentliga områden identifierats under tiden inventering och klassning har genomförts, något som eftersom tagits omhand av respektive chef i varierande omfattning.

2.1.2 Informationsklassning

Inventering och klassning har genomförts under hösten 2024 och våren 2025, vi har delat upp det i två olika steg, först har vi med hjälp av en konsult genomfört en inventering av informationsmängderna och därefter vid ett annat tillfälle har vi klassat informationen.

Klassningen är processbaserad och har genomförts i diskussionsgrupper med särskilt utvald personal från respektive verksamhetsområde. Det är Stadens fastställda klassificeringsstruktur som har använts och klassningstillfällena leds av en analysledare med kunskap om metodiken för hur klassning bör gå till.

Hela bolagets informationstillgångar bedöms 2025-04-09 vara färdigt inventerade. Klassning är pågående och presenteras enligt färdigställandegrad i procent per affärsområde.

Färdigställandegrad i procent

- Stadens Bud 100%
- Verksamhetsstöd 75%
- Finansiell Leasing 0%
- Operationell Leasing 0%
- Ledning 0%

Samtliga bolagets informationstillgångar beräknas vara färdigt klassade till 2025-06-30

2.1.3 Inventering, undersökningar och omvärldsbevakning

- Samtliga informationsmängder bedöms vara inventerade.

- En grundläggande inventering av informationssystem har genomförts men denna information är just nu under vidareutveckling, eventuellt konsulthjälp undersöks för att få stöd i att fastställa beroenden och samverkan mellan de olika systemen.

- Målet är att genomföra en omvärldsbevakning i strukturerad form årligen via analysmodellen PESTEL, denna analys ger en samlad bild över verksamhetens externa intressenter och förutsättningar som påverkar ledningssystemet för informationssäkerhet.

  PESTEL- modellen tar hänsyn till Politiska, Ekonomiska, Sociala, Teknologiska, Miljömässiga (E), Legala krav.

Löpande omvärldsbevakning inom området informationssäkerhet genomförs av i huvudsak säkerhetsavdelningen och utsedd information- och säkerhetssamordnare, nedan samanställning listar merparten av de etablerade kanalerna som används.

Forum

- Samarbetsforum SKR (Sveriges kommuner och regioner) Samarbetsrum - Logga in
- Kompetensforum hos ADDA (ett företag inom SKR) Kompetensforum
- Omvärldsbevakning säkerhet med SLK (ca 1 gång/mån).
- Samverkan med DSO Intraservice (Dataskyddsenheten)
- Nyhetsbrev/informationsträffar 2 gånger/år med dataskyddsfunktionen (SLK)
- MSB:s informationskanaler och konferenser MSB – Myndigheten för samhällsskydd och beredskap
- FRA FRA - FRA

Nätverk

- Samverkan med Intraservice i frågor rörande Informationssäkerhet, dataskydd IT och digitalisering.
- Dataskyddsgrupper, DSE hos Intraservice och DSF hos SLK (GDPR)
- Nätverk för IT- och kommunikation (2 gånger/år) internt GSL
- SLK:s nätverk för informationssäkerhet (2 träffar/år)

Övriga medier

- Göteborgs stads informationskanaler (i huvudsak Digitala navet) Informationssäkerhet
- CERT-SE (Computer Security Incident Response Team) CERT-SE - Sveriges nationella CSIRT
- NCSC Nationellt cybersäkerhetscenter
- Internetstiftelsen.se Internetstiftelsen

- Nyhetsbevakning

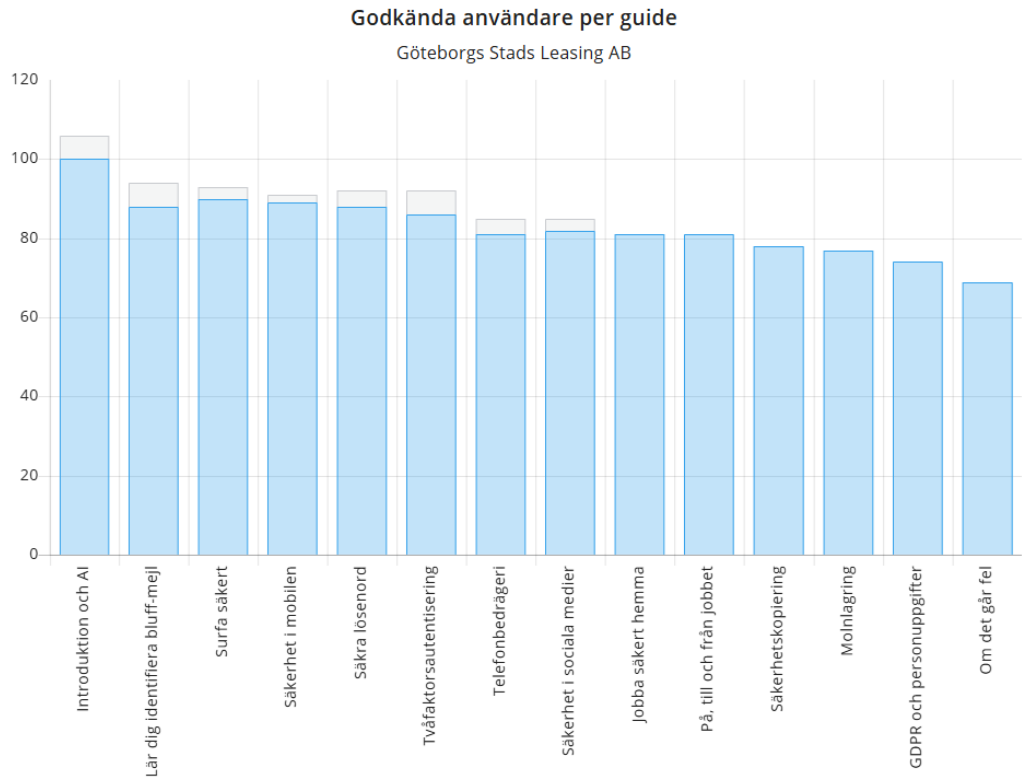
Lagbevakning

- Start | Sveriges riksdag
- lagen.nu
- Lagbevakning och lagefterlevnadskontroll, bl.a. Notisium: Logga in - Notisum

2.1.4 Medarbetarnas kunskaper och utbildningsverksamhet

En mätning av hur många som färdigställt utbildningen från Staden som heter Säkerhetsmedvetenhet och består av 14 små delutbildningar har genomförts och vid första mättillfället hade 60 personer slutfört samtliga avsnitt. Detta värde har till dagens datum (2025-04-09) höjts till 69 personer. Därmed tycks informationsinsatserna ha varit verkningsfulla. Denna punkt arbetar vi vidare med och målet är att samtliga medarbetare hos GSL ska genomgå utbildningen i sin helhet.

Resultat 2025-04-09



En annan utbildning som är obligatorisk vid nyanställning är utbildningen i dataskydd (GDPR) som erbjuds från staden genom Luvit och ska genomföras av samtliga medarbetare minst vid nyanställning. Utbildningen är ca 30 minuter lång och online.

Ytterligare krav för att höja medarbetarnas medvetenhet är att samtliga medarbetare ska känna till och veta vart man hittar våra regler för IT-användare Göteborgs Stads regel för IT-användare och E-post Microsoft Word - Göteborgs Stads regler för användande av epost 20181123.docx Chefer som arbetar åt verksamheten ska även ha kännedom om; Göteborgs Stads riktlinje för informationssäkerhet.

Därtill blir också arbetet med att klassa information och genomföra riskanalyser kanske de bästa utbildningstillfällena, dessa tillfällen används för att berätta mer om vad informationssäkerhet är och tillse att alla får en grundförståelse för området.

Informationssäkerhetssamordnaren har under våren deltagit i utbildningar hos Intraservice, utbildningarna avser både metodik kring klassning av information samt riskhantering enligt Intraservice modell.

2.1.5 Uppföljning och utvärdering

- Informationssäkerhet följs upp på möten med fastställda intervall med verksamhetschefen.
- Informationssäkerhet har fått eget utrymme på ledningens genomgång/utvecklingsmöten 2 gånger/år.
- Förnyad GAP-analys/nulägesanalys genomförs minst var 6 månad för att följa framdriften i arbetet med att införa ett systematiskt och riskbaserat arbete med informationssäkerhet.
- Uppföljning av informationssäkerhetsmål för 2025–2026.

Områden för mätning:

- Nivå hos Cybersäkerhetskollen från MSB

- Nivå på IT- säkkollen från MSB

- Uppföljning av delmål i dokumentet; Plan för informationssäkerhet.xlsx

- Uppföljning av identifierade informationssäkehetsrisker

2.1.6 Upprättande och utveckling av säkerhetskultur

- Kultur är ett område som är svårt att både förändra och mäta på ett bra sätt. Vid avsaknad av faktiska mätvärden att jämföra med kan man istället titta på vilka åtgärder som har genomförts för att bygga säkerhetskultur och göra ett antagande att det förhoppningsvis leder till ökad medvetenhet på arbetsplatsen.

En ytterligare indikator på att man faktiskt tycker det är viktigt med säkerhetsfrågor yttrar sig i hur många som tar sig tid i att prioritera och färdigställa utbildningen ”säkerhetsmedvetenhet” som vi också följer upp.

Informationssäkerhetssamordnaren brukar bli tillfrågad om stöd med riskanalyser, konsekvensbedömningar, upprättande av PUB-avtal med mera vid införande av nya system. Detta indikerar att det finns en medvetenhet kring informationssäkerhetsfrågorna. (Detta är också något som eventuellt skulle kunna generera framtida mätvärden/mål.)

Men det är svårt att säga om det är en följd av de åtgärder som genomförts eller om det beror på andra faktorer.

Några faktiska informationsinsatser som genomförts är följande:

- Information för bolagsledning (2025-03-06)
  Bolagsledningen informeras om kommande krav i NIS 2 direktivet samt det nya systemstödet för informationssäkerhet (ISDB). GSL är med i pilotfasen för införandet och har infört samtliga behandlingar i behandlingsregistret till ISDB. Importen var klar från GSL:s sida 2025-04-04

- Information på APT gällande NIS 2 direktivet.
  Kortfattad information på verksamhetsstöds APT i slutet av mars gällande NIS 2 direktivet och dess innebörd.

- Under v. 14–15 genomfördes informationsinsatser som knyter an till Internätstiftelsens kampanj ”TÄNK SÄKERT”. Under dessa veckor placerades informationsfolders ut i lunchrum och mötesrum samt att ett elektroniskt utskick gjordes som beskriver risker på internet och hur man kan testa om ens lösenord varit med i en lösenordsläcka.

3 Avslutande diskussion

Även om det kvarstår en hel del arbete för att kunna uppvisa en följsamhet mot Stadens riktlinje för informationssäkerhet är det min bedömning att vi har kommit en bra bit i vårt införande av ett systematiskt och riskbaserat arbete med informationssäkerhet. Det kanske mest krävande momentet med inventering och klassning ser ut att vara på plats under Q2 2025 och det är en viktig grund att ha på plats för fortsatt arbete på området.

Det nya NIS 2 direktivet som beräknas införas i Sverige genom Cybersäkerhetslagen lägger extra fokus på området informations- och cybersäkerhet. Men oberoende om kraven kommer från Stadens riktlinje för informationssäkerhet eller lagstiftning så är förfarandet detsamma.

Det handlar om att införa ett systematiskt och riskbaserat arbete med informationssäkerhet eller som man också kan kalla det, införa ett ledningssystem för informationssäkerhet. Detta är ett arbete som nu pågår med fullt fokus och resurser finns avsatta vilket skapar goda förutsättningar.

Stadens systemstöd ISDB kommer också vara en stor hjälp och effektivisera vårt arbete med informationssäkerhet och dataskydd.