Handläggare
Anna-Lena Björk, CISO – Enhetschef IT-säkerhet
Telefon: 079 060 61 83
E-post: anna.bjork@intraservice.goteborg.se

Återrapportering av uppdrag - ta fram en handlingsplan med tidplan för att omhänderta brister utifrån Stadsrevisionens granskning av verksamhetsåret 2022 kopplat till informationssäkerhet

Sammanfattning

2023-06-01 startade projektet Etablera processer och arbetssätt tillhörande styrning och uppföljning av informationssäkerhet. Projektets mål är att omhänderta brister som redovisas i dataskyddsombuds årsrapport 2021 och 2022 och Stadsrevisionens rapport 2022.

Förvaltningen har tidigare presenterat en översiktlig handlingsplan, senast under augusti månad 2023 inför möte med nämnden för Intraservice.

Som ett resultat av det arbete som påbörjats inom förstudien finns 2023-10-31 en uppdaterad version av handlingsplan med tillhörande tidplan (se bilaga 1). Utifrån vad som framkommit hittills under förstudiearbetet beräknas projektet pågå fram till halvårsskiftet 2026. Handlingsplanen redovisar pågående och planerade åtgärder utifrån dataskyddsombuds årsrapport 2021 och 2022 och Stadsrevisionens rapport 2022.

Projektet har idag identifierat 26 antal arbetspaket och uppskattat tids- och resursåtgång för åtgärder inom de arbetspaket som startat och beräknas starta under 2023. Arbete med att ta fram och justera tids- och resursuppskattningar kommer att fortsätta under projektet livscykel. Utifrån vad som framkommit hittills under förstudiearbetet beräknas projektet pågå fram till halvårsskiftet 2026.

Rekommendationer i Stadsrevisionens rapport 2022

Nedan ges en redogörelse av de rekommendationer som är kopplade till informationssäkerhet samt beskrivning av vad som kommer att utföras inom ramen för aktuellt projekt (omfattning), statusuppdatering, samt tidsuppskattning.

Åtgärder för att säkerställa en tillräcklig beredskap för att förhindra ett driftstopp i händelse av en it-attack

Stadsrevisionen rekommenderar nämnden att vidta åtgärder för att säkerställa en tillräcklig beredskap för att ***förhindra*** *och* hantera **ett driftsstopp** *i händelse av en it-attack.*

Granskningens revisionskriterier är:
• kommunallagen (2017:725) 6 kap 6 §
• reglemente för nämnden för Intraservice
• Göteborgs Stads policy för digitalisering och it
• Göteborgs Stads säkerhetspolicy
• Göteborgs Stads riktlinje för styrning av kommungemensamma interna tjänster
• Göteborgs Stads generella regler för kommungemensamma interna tjänster
• Göteborgs Stads riktlinje för informationssäkerhet
• Göteborgs Stads riktlinje för hantering av säkerhetsrisker
• Göteborgs Stads riktlinje för styrning, uppföljning och kontroll.

Omfattning

En tydlig, förankrad och fastställd organisation kring informationssäkerhet (inkluderande dataskyddsorganisation) och arkiv tydliggör vilka arbetsuppgifter och vilket ansvar respektive tjänsteperson i organisationen har och underlättar för kunskaps- och informationsspridning. Arbetet behöver bedrivas på både strategisk, taktisk och operativ nivå i organisationen och omfattar nämnden för Intraservices roll som egen myndighet och leverantör av tjänster. Arbetet är förvaltningsövergripande och har beröringspunkter till områden som rör, informationssäkerhet (som inkluderar administrativ och teknisk säkerhet) och arkiv. Samtliga områden hänger ihop och blir sammantaget kravställare på de tjänster som levereras. Perspektiven ska genomsyra arbetet med både utveckling och förvaltning och ställer krav på förvaltningens förmåga att arbeta tillsammans och se de ingående områdena som delar i en helhet som både hänger ihop och behöver styras utifrån ett helhetsperspektiv.

Projektet kommer att ta fram förslag till en förvaltningsövergripande organisering som innebär justering av ansvar, roller och mandat (befogenhet) för att säkerställa en ändamålsenlig styrning, hantering och uppföljning av informationssäkerhetsarbetet vilket inkluderar arbetet med dataskydd och arkiv. Anvisningar, rutiner, instruktioner, samt processer och arbetssätt kommer hjälpa till med att beskriva arbetsuppgifter kopplade till informationssäkerhet/dataskydd och arkiv.

Målet är att dataskydd och arkiv blir en integrerad del i allt arbete tillhörande informationssäkerhet, och att informationssäkerhet blir en naturlig del i det dagliga arbetet för alla roller.

Projektet kommer därutöver att se över/ge förslag på justering av/ta fram processer och arbetssätt tillhörande styrning, hantering och uppföljning av informationssäkerhetsarbetet inom förvaltningen och organisationen som ansvarar för leverans av tjänster. Det gäller administrativa arbetsuppgifter och arbetsuppgifter tillhörande fysisk säkerhet och IT-säkerhet.

Inom detta deluppdrag kommer även anvisningar, rutiner och instruktioner kopplade till informationssäkerhet att tas fram med mål att medarbetare inom Intraservice enkelt och lätt ska få handledning i det dagliga arbetet. För respektive roll behöver det vara tydligt om det finns särskilda sätt som arbetet ska utföras på och i så fall hur.

För att säkerställa att Intraservice får en tillräcklig beredskap för att förhindra ett driftstopp i händelse av en it-attack kommer projektet att börja med processer och arbetssätt för nyutveckling av tjänst och inköp av nya system/applikationer. Därefter är det dags för processer och arbetssätt kopplade till förvaltning, utveckling och avveckling av tjänst respektive system/applikation.

Det behöver finnas en tydlighet i vad varje medarbetare behöver ha kunskap om och hantera under en tjänsts och/eller ett systems/en applikations livscykel, men det gäller också att se till att system/applikationer når upp till gällande säkerhetskrav under hela livscykeln.

I detta ingår att säkerställa att det i processer och arbetssätt finns moment för genomförande av exempelvis risk- och sårbarhetsanalyser, tröskelanalyser/konsekvensbedömningar, omvärldsbevakningar, tester i samband med produktionssättning, penetrationstester vid införande av nya system/applikationer, dokumentation av personuppgiftsbehandlingar och säkerhetsåtgärder i tjänstespecifikationer och funktionsbeskrivningar, framtagande och uppdatering av kontinuitets- och återställningsplaner, rapportering av störningar, etcetera.

Projektet kommer också se över/ge förslag på justering av/ta fram processer och arbetssätt som bidrar till att förhindra och upptäcka intrång, och andra typer av händelser, som skulle kunna orsaka ett driftsstopp eller informationsläckage. Exempel på vad som kommer att ses över är processer och arbetssätt för arbete inom Security Operation Center, incidenthantering, förändringshantering och nätverkstjänster.

Utöver de revisionskriterier som Stadsrevisionens rapport 2022 refererar till kommer projektet att analysera och ta fram förslag på förbättringar utifrån vilka förmågor Intraservice kan komma att behöva nå upp till med tanke på NIS2 och CER (*The Directive on security of network and information system – the NIS Directive respektive Critical Entities Resilience Directive*). NIS 2 och CER är två direktiv som ska tillämpas inom EU från och med 18 oktober 2024. Övergripande kan sägas att NIS2 fokuserar på säkerhet i nätverk och informationssystem och att CER riktar in sig på störningar eller avbrott som föranletts av exempelvis naturolyckor, terroristattacker, pandemier eller andra allvarliga händelser. I egenskap av leverantör av gemensamma tjänster och tjänster tillhörande digital infrastruktur till samhällsviktiga verksamheter inom Göteborgs Stad kan Intraservice komma att erhålla krav som är förenliga med vad som direktiven anger.

Under januari 2023 genomfördes penetrationstester kopplade till att identifiera Intraservice förmåga att förhindra driftstopp i händelse av en it-attack. Penetrationstesterna omfattade cirka 10 % av nätverkslösningar som ingår i digital infrastrukturs tjänsteutbud.

Inom ramen för projektet kommer förslag att ges om fortsatta penetrationstester i avsikt att genomlysa ytterligare delar av nätverkslösningarna som ingår i digital infrastrukturs tjänsteutbud. Processer och arbetssätt kommer även att ta upp behovet av penetrationstester i samband med nyutveckling, förändring och återkommande uppföljning.

Utöver tydlighet i roller, ansvar och mandat, processer och arbetssätt behöver förvaltningen återkommande säkerställa att medarbetare har rätt kompetens och är

behöriga för de arbetsuppgifter som ska utföras. Projektet kommer att se över/justera/ta fram riktlinjer och rutiner kopplade till detta.

Processer och arbetssätt relaterat till uppföljning av vad som tas upp i styrande dokument kommer också att ses över/justeras och tas fram av projektet.

Projektet kan komma att identifiera behov av investering av hårdvara, system/applikation eller annan typ av teknisk lösning och ge förslag därom, men projektet kommer inte att ansvara för aktiviteter tillhörande investering/inköp.

Status 2023-10-31
Handlingsplanen och tidplanen som presenterades i augusti 2023 har uppdaterats och aktiviteter inom flera arbetspaket är påbörjade.

Den totala tidsperioden för åtgärder som ska stärka förvaltningens beredskap att förhindra ett driftstopp beräknas till 2023-10-01 – 2026-06-30.

Arbete pågår med framtagande av en plan för när leveranser kommer ske. Denna plan kommer att visa på beroenden mellan projektets arbetspaket. Initialt kommer denna typ av plan inkludera information om leveranser från de arbetspaket och aktiviteter som har startdatum under 2023.

Tidsuppskattning
Cirka 40 000 timmar har hittills uppskattats för de aktiviteter som hör till att säkerställa att Intraservice som förvaltning och leverantör av gemensamma tjänster och tjänster tillhörande digital infrastruktur har en tillräcklig beredskap för att förhindra ett driftsstopp i händelse av en IT-attack. Hur många timmar som tillkommer är 2023-08-09 svårt att uppskatta. Exempel på aktiviteter som är svåra att tidsuppskatta i det skede som uppdraget befinner sig är aktiviteter för verifiering/test av Intraservices förmåga att förhindra ett driftstopp. Det inkluderar verifiering/test av teknisk utrustning, tekniska lösningar, processer och arbetssätt, rutinbeskrivningar, samt respektive tjänsts och systems funktion.

Åtgärder för att säkerställa en tillräcklig beredskap för att hantera ett driftstopp i händelse av en it-attack

Stadsrevisionen rekommenderar nämnden att vidta åtgärder för att säkerställa en tillräcklig beredskap för att förhindra och **hantera ett driftsstopp** *i händelse av en it-attack.*

Granskningens revisionskriterier är:
• kommunallagen (2017:725) 6 kap 6 §
• reglemente för nämnden för Intraservice
• Göteborgs Stads policy för digitalisering och it
• Göteborgs Stads säkerhetspolicy
• Göteborgs Stads riktlinje för styrning av kommungemensamma interna tjänster
• Göteborgs Stads generella regler för kommungemensamma interna tjänster
• Göteborgs Stads riktlinje för informationssäkerhet
• Göteborgs Stads riktlinje för hantering av säkerhetsrisker
• Göteborgs Stads riktlinje för styrning, uppföljning och kontroll.

Omfattning
Projektet kommer att se över/föreslå/införa justeringar av incidenthanteringsprocessen i avsikt förbättra Intraservices förmåga att hantera ett driftsstopp.

Projektet kommer också att se över/föreslå justering av/ta fram processer och arbetssätt tillhörande kontinuitetshantering för, och återställning av, gemensamma tjänster och tjänster tillhörande digital infrastruktur.

Projektet kommer att se till att det för varje tjänst finns en kontinuitets- och återställningsplan och att dessa är beslutade och verifierade, samt att det finns en ägare till dessa planer och att en förvaltningsorganisation är etablerad.

Arbetet med att ta fram återställningsplan för gemensamma tjänster och tjänster tillhörande digital infrastruktur påbörjades i april 2022. Vid översyn av då befintliga återställningsplaner upptäcktes att Intraservice saknar information om hur tjänster, och de system som tjänsterna bygger på ska kategoriseras och prioriteras. Det framkom också att Intraservice saknar information tillhörande kundägda system för vilka Intraservice hanterar serverdriften för.

Informationsinsamling tillhörande kundägda system för vilka Intraservice hanterar serverdriften för påbörjades i maj 2022. På grund av utmaningar med datakvalitet och långa svarstider pågick denna informationsinsamling fram till och med december 2022. Vid översyn av inkomna svar konstateras att det saknades ytterligare information. Kunder behöver inkomma till Intraservice med systemdokumentation där det framgår hur Intraservice ska hantera återställning.

Ett deluppdrag startade upp 2023-05-03 inom projektet Etablera processer och arbetssätt för styrning och uppföljning av informationssäkerhet. Deluppdraget ska ansvara för framtagandet av kontinuitetshanteringsplaner och återställningsplaner för gemensamma tjänster och tjänster tillhörande digital infrastruktur.

Identifierade åtgärder består av framtagande av förslag till processer och arbetssätt, framtagande av anvisningar, rutiner och instruktioner, anpassning och förslag till anpassning av tjänster, samt förslag till och fastställande av kategorisering av tjänster och dess system.

Med kategorisering av tjänster och dess system avses att kategorisera tjänst och dess system och verktyg som samhällsviktig, verksamhetskritisk eller övrigt.

Kategoriseringen av tjänst och dess system och verktyg utgör styrningen av vilken tjänst och vilka system och verktyg som ska återställas i vilken ordning och vilka beroenden som finns till andra tjänster och system.

Utöver de revisionskriterier som Stadsrevisionens rapport 2022 refererar till kommer projektet/detta deluppdrag att analysera och ta fram förslag på förbättringar utifrån vilka förmågor Intraservice kan komma att behöva nå upp till med tanke på NIS2 och CER (*The Directive on security of network and information system – the NIS Directive respektive Critical Entities Resilience Directive*). NIS 2 och CER är två direktiv som ska tillämpas inom EU från och med 18 oktober 2024. Övergripande kan sägas att NIS2 fokuserar på säkerhet i nätverk och informationssystem och att CER riktar in sig på störningar eller avbrott som föranletts av exempelvis naturolyckor, terroristattacker, pandemier eller andra allvarliga händelser. I egenskap av leverantör av gemensamma tjänster och tjänster tillhörande digital infrastruktur till samhällsviktiga verksamheter inom Göteborgs Stad kan Intraservice komma att erhålla krav som är förenliga med vad som direktiven anger.

Deluppdraget kan komma att identifiera behov av investering av hårdvara, system/applikation eller annan typ av teknisk lösning och ge förslag därom, men deluppdraget/projektet kommer inte att ansvara för aktiviteter tillhörande investering/inköp.

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Incident och Kontinuitet.

Status 2023-10-31
Åtgärder pågår och kommer enligt beräkning pågå fram till och med 2026-06-30.

Arbete pågår med framtagande av en plan för när leveranser kommer ske. Denna plan kommer att visa på beroenden mellan projektets arbetspaket. Initialt kommer denna typ av plan inkludera information om leveranser från de arbetspaket och aktiviteter som har startdatum under 2023.

Tidsuppskattning
Cirka 12 500 timmar har hittills uppskattats. Hur många timmar som tillkommer är 2023-08-09 svårt att uppskatta. Exempel på aktiviteter som är svåra att tidsuppskatta i det skede som uppdraget befinner sig är aktiviteter för verifiering/test av återställning av tjänster och system. Det inkluderar verifiering/test av teknisk utrustning, tekniska lösningar, processer och arbetssätt, rutinbeskrivningar, samt respektive tjänsts och systems funktion efter återställning.

I avtal/överenskommelser med kund ta med krav tillhörande informationssäkerhet

Stadsrevisionen rekommenderar nämnden att vidta åtgärder för att säkerställa att de säkerhetskrav som Intraservice bedömer som nödvändiga inryms i avtalen med de som nyttjar Intraservice servrar för egna applikationer eller system.

Omfattning
Projektet kommer att inom detta deluppdrag se över/ge förslag på justering av/ta fram processer och arbetssätt som hanterar avtal och andra överenskommelser med kund.

Det inkluderar bland annat kundöverenskommelser som har fokus på informationssäkerhet eller inkluderar områden som faller inom området informationssäkerhet, exempelvis biträdesavtal och överenskommelse om att kund ansvarar för säkerhetsuppdatering av sina egna system/applikationer.

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Kund.

Status 2023-10-31
Datum för start av arbete med denna kontrollpunkt är planerat till 2024-02-01.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Kund: 2024-02-01 – 2025-06-30.

Förslag till justering av styrande dokument beräknas vara slutfört i juni 2024.
Arbetet med att genomlysa och föreslå förbättringar i processer och arbetssätt beräknas vara slutfört i sin helhet i juni 2025.

Observera att tidsuppskattning ännu inte genomförts, vilket innebär att datum för när åtgärder beräknas vara slutförda kan komma att ändras.

Tidsuppskattning
Tidsuppskattning ej ännu genomförd.

Förvaltningens organisering av säkerhetsarbetet

Stadsrevisionen rekommenderar nämnden att vidta åtgärder så att förvaltningens organisering av säkerhetsarbetet understödjer informationsflödet inom förvaltningsorganisationen och mellan förvaltningsorganisationen och nämnden.

Omfattning
Såsom omnämns som en åtgärd kopplat till att säkerställa att Intraservice har beredskap att förhindra ett driftstopp i samband med en it-attack ska projektet inventera och föreslå justering av ansvar, roller och mandat för att säkerställa att styrning, hantering och uppföljning av informationssäkerhet sker utifrån gällande krav. Detta omfattar Intraservice som förvaltning och Intraservice som leverantör av gemensamma tjänster, tjänster tillhörande digital infrastruktur, och uppdrag. Det gäller ansvar, roller och mandat kopplade till arbete inom och utanför processer.

En tydlig, förankrad och fastställd organisation kring informationssäkerhet (inkluderande dataskyddsorganisation) och arkiv tydliggör vilka arbetsuppgifter och vilket ansvar respektive tjänsteperson i organisationen har och underlättar för kunskaps- och informationsspridning. Arbetet behöver bedrivas på både strategisk, taktisk och operativ nivå i organisationen och omfattar nämnden för Intraservices roll som egen myndighet och leverantör av tjänster. Arbetet är förvaltningsövergripande och har beröringspunkter till områden som rör, informationssäkerhet (som inkluderar administrativ och teknisk säkerhet) och arkiv. Samtliga områden hänger ihop och blir sammantaget kravställare på de tjänster som levereras. Perspektiven ska genomsyra arbetet med både utveckling och förvaltning och ställer krav på förvaltningens förmåga att arbeta tillsammans och se de ingående områdena som delar i en helhet som både hänger ihop och behöver styras utifrån ett helhetsperspektiv.

Projektet kommer att ta fram förslag till en förvaltningsövergripande organisering som innebär justering av ansvar, roller och mandat (befogenhet) för att säkerställa en ändamålsenlig styrning, hantering och uppföljning av informationssäkerhetsarbetet vilket inkluderar arbetet med dataskydd och arkiv. Anvisningar, rutiner och instruktioner, samt processer och arbetssätt kommer hjälpa till med att beskriva arbetsuppgifter kopplade till informationssäkerhet/dataskydd och arkiv.

Målet är att dataskydd och arkiv blir en integrerad del i allt arbete tillhörande informationssäkerhet, och att informationssäkerhet blir en naturlig del i det dagliga arbetet för alla roller.

För respektive roll behöver det vara tydligt om det finns särskilda sätt som arbetet ska utföras på och i så fall hur. Anvisningar, rutiner och instruktioner kommer hjälpa till med att beskriva arbetsuppgifter kopplade till informationssäkerhet. Det gäller administrativa arbetsuppgifter och arbetsuppgifter tillhörande fysisk säkerhet och IT-säkerhet.

Projektet kommer också att inom detta deluppdrag se över/ge förslag på justering av/ta fram ledningsprocesser, inkluderande förvaltningens genomgång med nämnden för Intraservice och förvaltningens genomgång med ledningsgruppen för Intraservice. Det ska identifieras och fastställas när och hur avrapportering ska ske med nämnd, förvaltningens ledningsgrupp och övriga relevanta funktioner inom Intraservice. Det gäller årlig uppföljning, under verksamhetsåret återkommande uppföljningar, avvikelserapportering, etcetera.

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket AnsvarRollerMandat och Ledningsprocess.

Status 2023-10-31
Åtgärder tillhörande huvudpaket AnsvarRollerMandat och Ledningsprocess är påbörjade och beräknas pågå fram till 2024-06-30 respektive 2025-12-31.

Arbete pågår med framtagande av en plan för när leveranser kommer ske. Denna plan kommer att visa på beroenden mellan projektets arbetspaket. Initialt kommer denna typ av plan inkludera information om leveranser från de arbetspaket och aktiviteter som har startdatum under 2023.

Arbetspaketen AnsvarRollerMandat och Ledningsprocess har beroenden till flertalet projektets arbetspaket.

Tidsuppskattning
Hittills har cirka 7 000 timmar uppskattats för åtgärder tillhörande de två huvudpaket som omnämns ovan. Hur många timmar som eventuellt tillkommer är 2023-10-31 svårt att uppskatta.

Skyndsamt åtgärda brister som lyfts av dataskyddsombud

Stadsrevisionen rekommenderar nämnden att se till att de brister som lyfts av dataskyddsombudet åtgärdas skyndsamt.

Omfattning
Projektet kommer att omhänderta de brister som lyfts av dataskyddsombud. I den handlingsplan som tagits fram av projektet finns åtgärder kopplade till samtliga kontrollpunkter och särskilda iakttagelser.

De åtgärder som behöver omhändertas av Intraservice utifrån de brister som lyfts av dataskyddsombud är också åtgärder utifrån de rekommendationer som Stadsrevisionen presenterat kring förbättringar kopplade till informationssäkerhet.

Dataskyddsombuds årsrapport 2022 är specifikt inriktad på brister kopplade till dataskydd.

Status 2023-10-31
Åtgärder tillhörande huvudpaket AnsvarRollerMandat och Ledningsprocess är påbörjade och beräknas pågå fram till 2024-06-30 respektive 2025-12-31.

Projektet kommer därefter starta upp med åtgärder som ingår i övriga huvudpaket.

Arbete pågår med framtagande av en plan för när leveranser kommer ske. Denna plan kommer att visa på beroenden mellan projektets arbetspaket. Initialt kommer denna typ av plan inkludera information om leveranser från de arbetspaket och aktiviteter som har startdatum under 2023.

Arbetspaketen AnsvarRollerMandat och Ledningsprocess har beroenden till flertalet projektets arbetspaket.

Den totala tidsperioden för åtgärder kopplade till Dataskyddsombuds årsrapport 2021 och 2022 sträcker från 2023-10-01 till 2026-06-30.

Tidsuppskattning

Hittills har cirka 30 000 timmar uppskattats kopplade till åtgärder som är gemensamma utifrån dataskyddsombuds årsrapport 2021 och 2022. Hur många timmar som tillkommer är 2023-10-31 svårt att uppskatta. Förvaltningen återkommer med uppdaterad handlings- och tidplan.

Avgränsningar

Tidigare angivna avgränsningar i form av att projektet endast tar fram kravspecifikation för systemstöd gäller inte längre.

Projektet tar över planerade förstudie tillhörande systemstöd. En förstudie som skulle ha genomförts av avdelningen för Gemensamma tjänster. Ekonomiska medel kommer att föras över till projektet från Gemensamma tjänster.

Risker tillhörande genomförandet av projektet

Projektet har genomfört riskanalys och bland annat identifierat risker utifrån den ekonomiska situationen som råder inför verksamhetsåren 2024 och 2025. Det är risker som kan komma att påverka projektets möjligheter att genomföra identifierade åtgärder kopplade till dataskyddsombuds rapport 2021 och 2022, och Stadsrevisionens rapport 2022.

Det kan röra sig om risk för att resurser i form av expertstöd (konsulter) inte finns att tillgå, eller att rekrytering av egen personal inte är möjlig, utifrån tillgång till ekonomiska medel.

Expertstöd i form av sex konsulter kommer att bemanna upp projektet från och med 2023-09-01. Behov finns av att rekrytera egen personal till både projektaktiviteter (konsultväxling) och kommande förvaltning av det som projektet ska producera i form av processer, arbetssätt och styrande dokument.

Det är av stor vikt att det som projektet producerar kan lämnas över för förvaltning och vidareutveckling. Om inte så sker, kommer Intraservice att åter igen stå inför det faktum att genomförda åtgärder inte får den effekt som var planerad. Projektet refererar till konsultinsatser och andra typer av utvecklingsinsatser som genomförts under några års tid. Ett arbete som genomförts, men som inte är slutfört eller som inte förvaltats eller vidareutvecklats och som nu är oanvändbart till stora delar.

I övrigt ses risker i att projektaktiviteterna är omfattande i både tidsåtgång och komplexitet, vilket påverkar Intraservice förmåga att leva upp till gällande krav (de granskningskriterier som ligger bakom Stadsrevisionens rapport 2022, dataskyddsombuds rapport 2022 samt nya styrande dokument, nya lagar och förordningar) och Intraservice förmåga att förhindra och hantera incidenter, nu och en tid framöver.

Framgångar

Det arbete som utförts sedan senaste återrapporteringen i augusti har gett tydligare bild över åtgärder, omfattning, tids- och resursåtgång. Handlingsplanen och tidsplanen har uppdaterats. Dialoger med resursägare är påbörjade. Prioritering av åtgärder i handlingsplanen genomförs utifrån 1) behov och 2) efterfrågan.

Arbetet tillhörande framtagande och implementation av anvisningar, rutiner, instruktioner samt systemstöd kommer att utföras i dialog med Stadsledningskontoret med mål att

förvaltningar och bolag inom Göteborgs stad ska erhålla gemensamma processer och arbetssätt (inkl. systemstöd) (detta gäller bland annat för arbete med informationsklassning, riskanalyser, konsekvensbedömningar, med mera). Ett sådant arbetssätt ses som kostnadseffektivt och kvalitetshöjande för alla parter.