

Status

**Återremiss – handlingsplan avseende
dataskyddsombudets årsrapport samt uppdrag att
etablera dataskyddsorganisation**

Intraservice

2024-04-24

Innehåll

- Bakgrund
- Mål och mätbara aktiviteter kopplade till informationssäkerhet
- Status 2024-04-24
- Sammanfattning

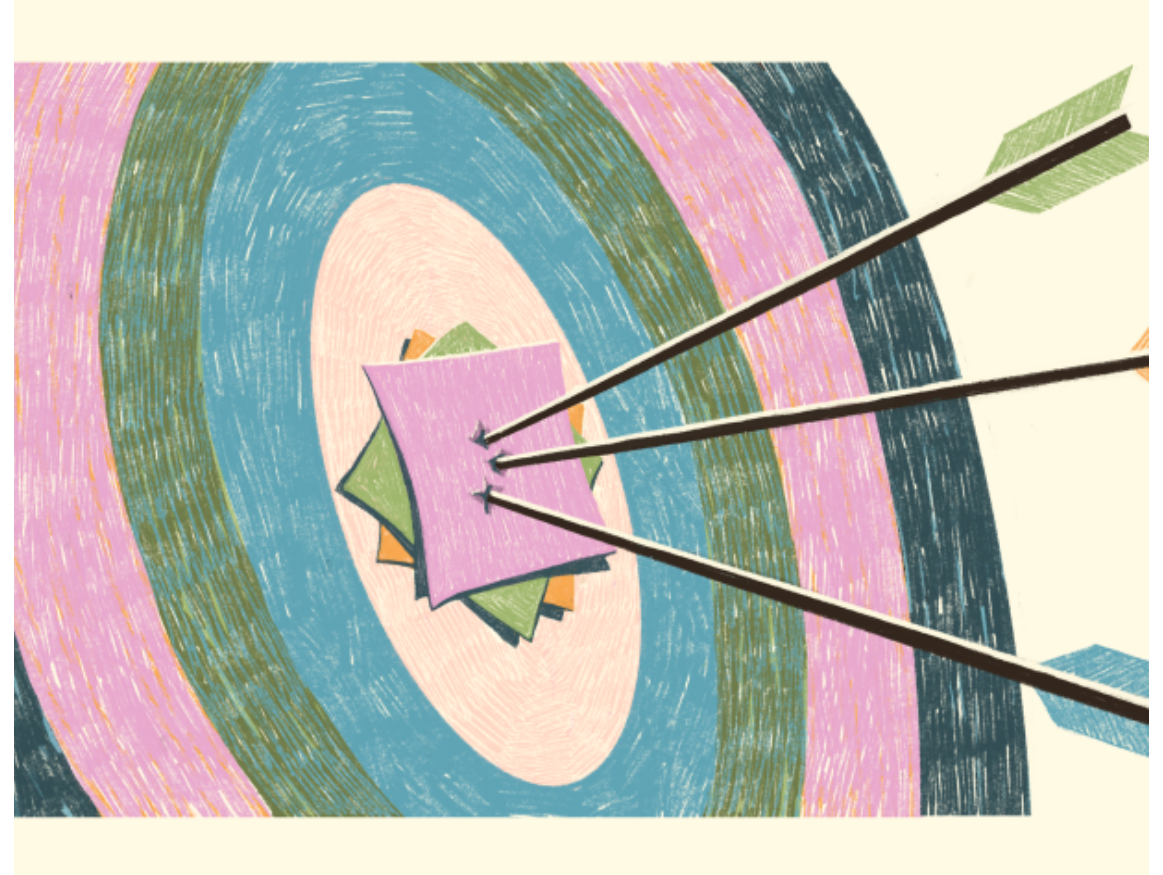
- Denna presentation presenterar status 2024-04-24 för projektet *Etablera systematiskt informationssäkerhetsarbete*
- Projekt har sin bakgrund i vad som tagits/tas upp i
 - 0120/22 Dataskyddsenhetens årsrapport 2022
 - 0351/22 Regionarkivets tillsynsrapport 2022
 - Intern utredning tillhörande informationssäkerhet
 - Intern utredning tillhörande arkivansvar och tekniskt arkivansvar
 - Göteborgs Stads styrande dokument
 - Information om kommande ändringar i Göteborgs Stads regel för IT-användare

Mål och mätbara aktiviteter kopplade till informationssäkerhet

(inkl. dataskydd, arkiv- och tekniskt arkivansvar)

Mål och mätbara aktiviteter kopplade till informationssäkerhet (inkl. dataskydd, arkiv- och tekniskt arkivansvar)

- **Mål**
 - Fastställande av
 - Organisation, roller samt vissa typer av ansvar och befogenheter
 - Delegation av vissa typer av befogenheter
 - Process och anvisning tillhörande
 - Informationsklassning
 - Riskhantering
- **Måldatum 2024-06-30**



Mål och mätbara aktiviteter kopplade till informationssäkerhet (inkl. dataskydd, arkiv- och tekniskt arkivansvar)

- **Mål**
 - Mätbara aktiviteter kopplade till projektets delprojekt kommer att presenteras i samband med nämndmöte juni 2024
 - Mätbara aktiviteter kommer då att presenteras tillhörande de delprojekt som är prioriterade
 - Måldatum kommer att sträcka sig över perioden juni – december 2024



Prioriterade delprojekt

Prioriterade delprojekt

- Ansvar Roller Mandat
- Informationsklassificeringsprocess
- Kontinuitetsplaner/Inventering av bastjänster
- Riskhanteringsprocess
- Systemstöd
- Detektering av tillgångar



Status 2024-04-24

Förslag till organisation

Informationsägare - Systemägare

Informationsägare

Intraservice nämnd

Text från Göteborgs Stads riktlinje för informationssäkerhet

”Ansvar och roller i informationssäkerhet I enlighet med vad som gäller för övrig verksamhet, är ansvaret för informationssäkerheten kopplat till ordinarie verksamhetsansvar. Det innebär att ansvarig nämnd/styrelse för en verksamhet också är ansvarig för att informationssäkerheten upprätthålls och efterföljs i denna verksamhet.

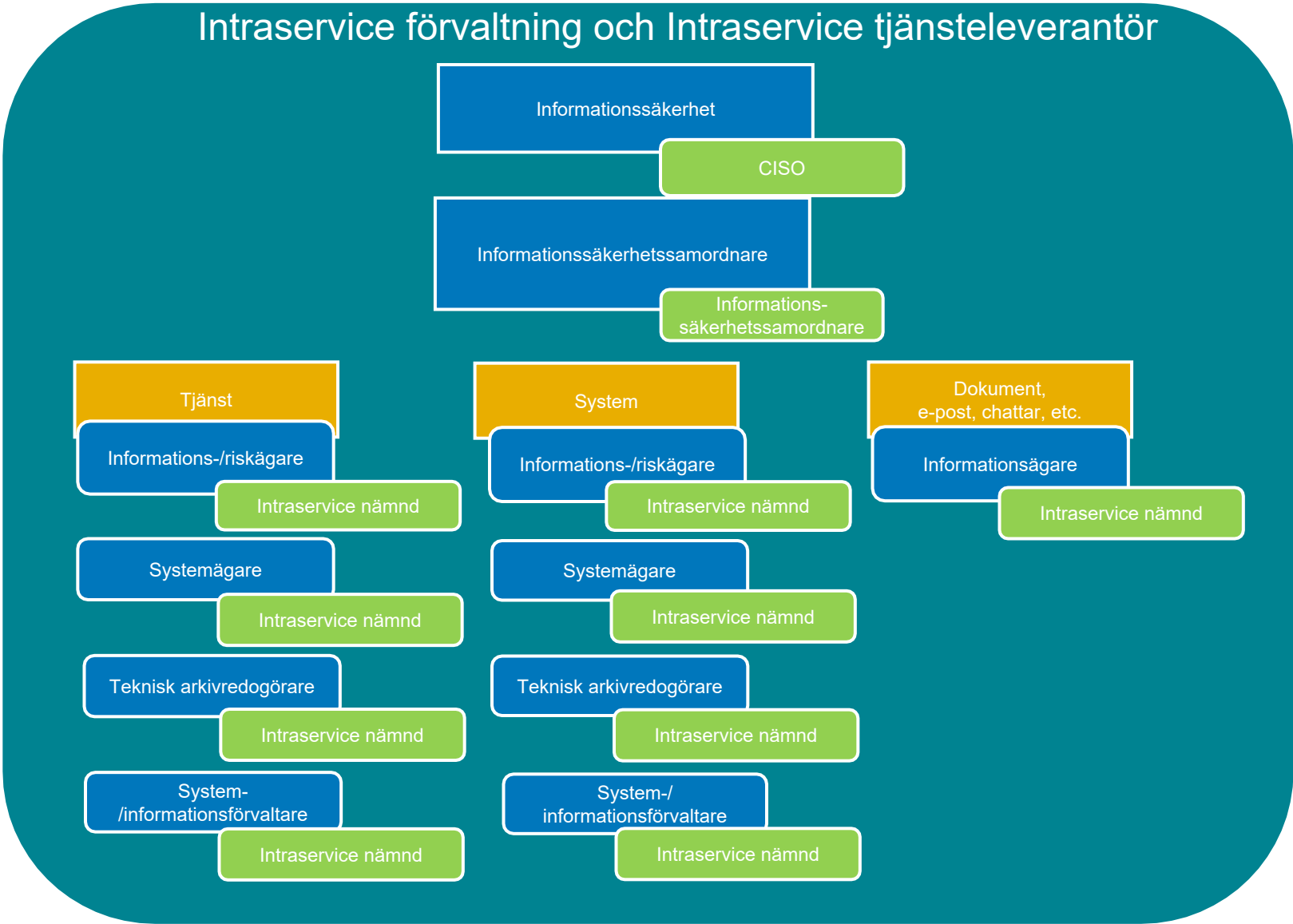
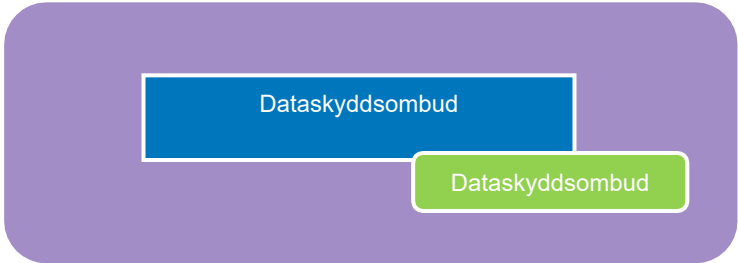
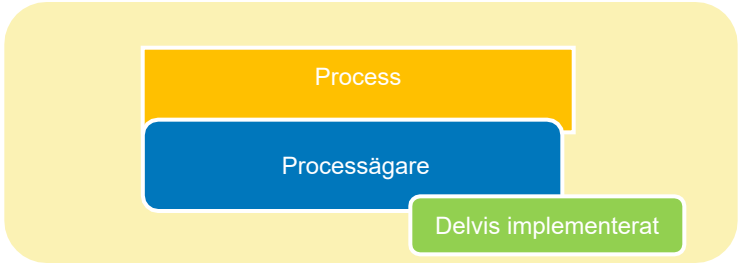
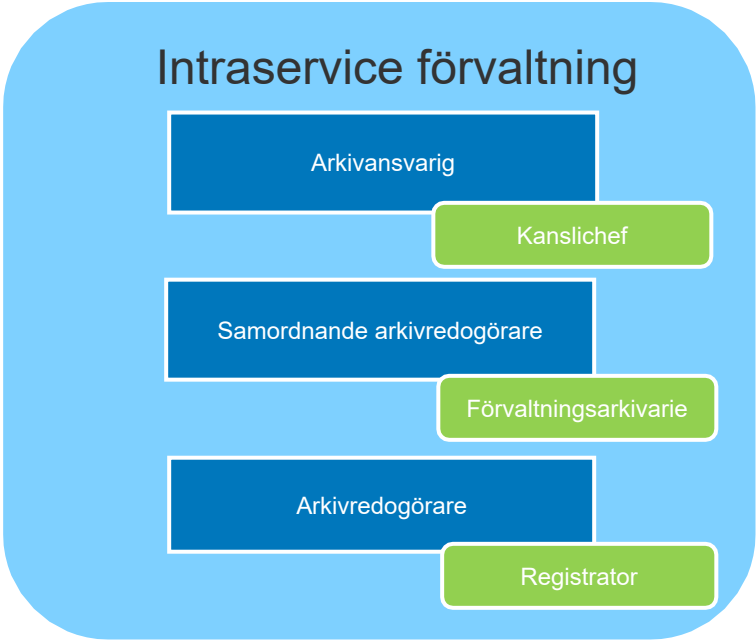
Informationsägare är den nämnd/styrelse som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten.

Informationssägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.

Systemägare är den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare.

Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.”

Organisation 2024-03-11



Organisation Förslag

Intraservice förvaltning

Arkivansvarig

Kanslichef

Samordnande arkivredogörare

Förvaltningsarkivarie

Arkivredogörare

Registrator

Process

Processägare

Verksamhetschef

Dataskyddsombud

Dataskyddsombud

Intraservice förvaltning och Intraservice tjänsteleverantör

Informationssäkerhet

CISO

Informationssäkerhetssamordnare
Teknisk arkivsamordnare

Informations-
säkerhetssamordnare

Tjänst

Informations-/riskägare

Verksamhetschef

Systemägare

Enhetschef

Teknisk arkivredogörare

Förvaltningsledare

System-
/informationsförvaltare

Medarbetare

System

Informations-/riskägare

Verksamhetschef

Systemägare

Enhetschef

Teknisk arkivredogörare

Förvaltningsledare

System-
/informationsförvaltare

Medarbetare

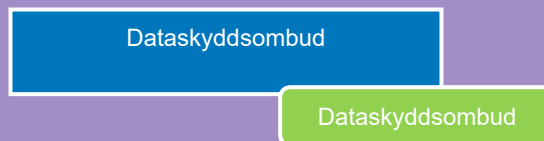
Dokument,
e-post, chattar, etc.

Informationsägare

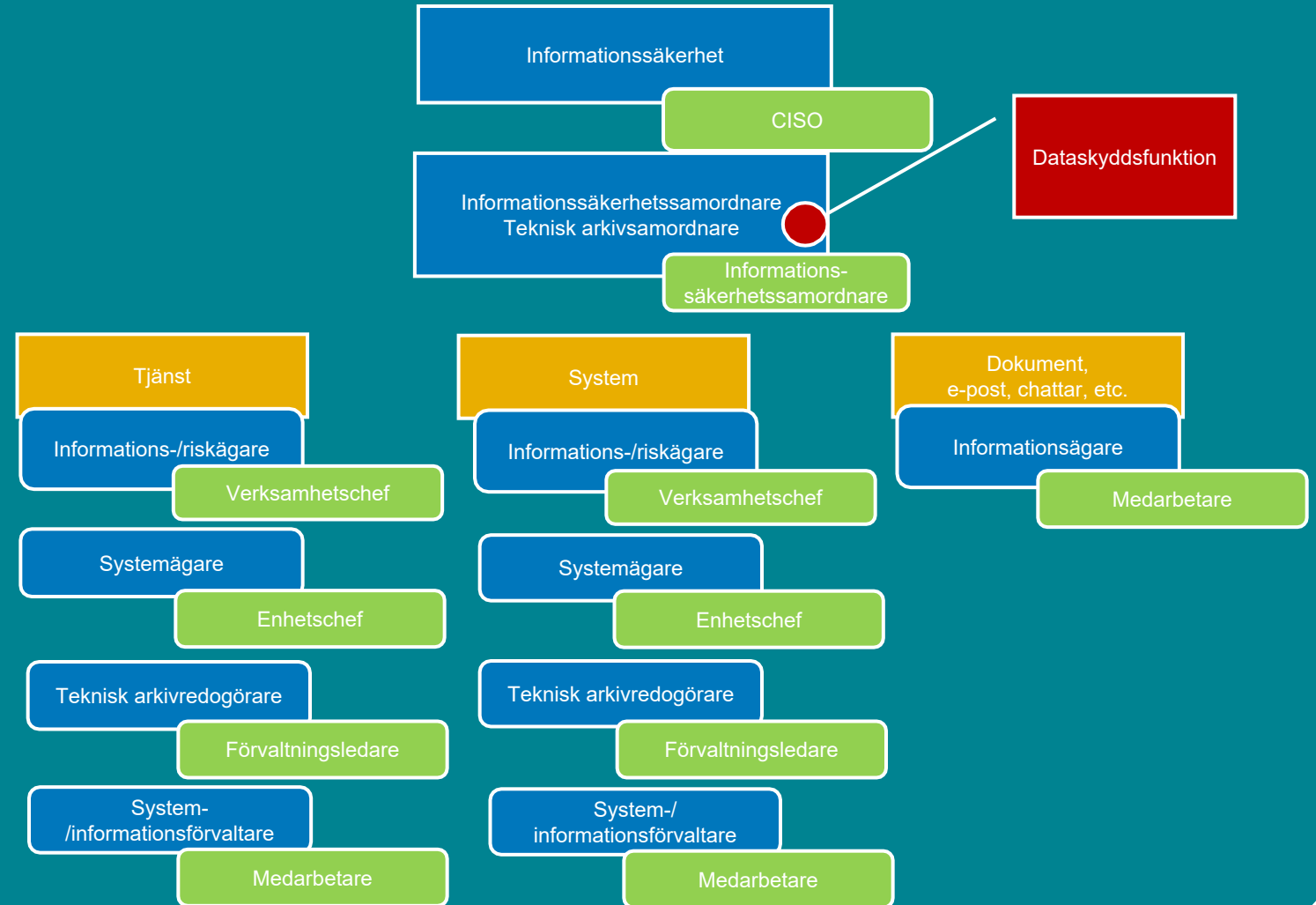
Medarbetare

Organisation Förslag

Intraservice förvaltning



Intraservice förvaltning och Intraservice tjänsteleverantör



Dataskyddsfunktion - Dataskyddskontakt

- Varje personuppgiftsansvarig organisation i Göteborg Stad ska ha minst en dataskyddskontakt.
- Förslag om etablering av en funktion med medarbetare som agerar som dataskyddskontakter. Funktionen bemannas av informationssäkerhetssamordnare.
- Dataskyddskontakt ska vara en kontaktperson till dataskyddsombudet och har som uppgift att kanalisera frågor från verksamheten till dataskyddsombudet.
- Dataskyddskontakten är den som kontaktar dataskyddsombud när deras roll bör/behöver involveras.
- Funktionen ska vara en central funktion som har en etablerad kommunikation (ex. kontinuerligt återkommande möten) med roller som operativt utför aktiviteter kopplade till dataskydd.
- Funktionen ska ge stöd och råd, och kontrollera efterlevnad.

Dataskyddsfunktion - Dataskydd



Dataskyddsförordningen
(GDPR)

- Dataskydd handlar om att skydda personuppgifter.
- Dataskydd är en del av vad som inkluderas i begreppet informationssäkerhet.
- Medarbetare inom Intraservice behöver agera utifrån vad Dataskyddsförordningen anger, men även utifrån den lagstiftning som i övrigt gäller för Intraservice som förvaltning och tjänsteleverantör (krav på leveransen).
- **Dataskyddsfunktionen ska medverka till att det blir lätt att göra rätt.**

Roller och ansvar

Vad innebär förändringen?

- Samtliga medarbetare påverkas
 - Alla roller får utökat och nya ansvar
- Befintliga processer behöver kompletteras
- Nya processer behöver skapas
- Befintliga styrande dokument behöver uppdateras
- Nya styrande dokument behöver tas fram
- Utbildningsmaterial behöver tas fram
- Samtliga medarbetare behöver utbildas



Säkerhet i flera lager

Säkerhet i flera lager



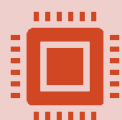
Göteborgs
Stad



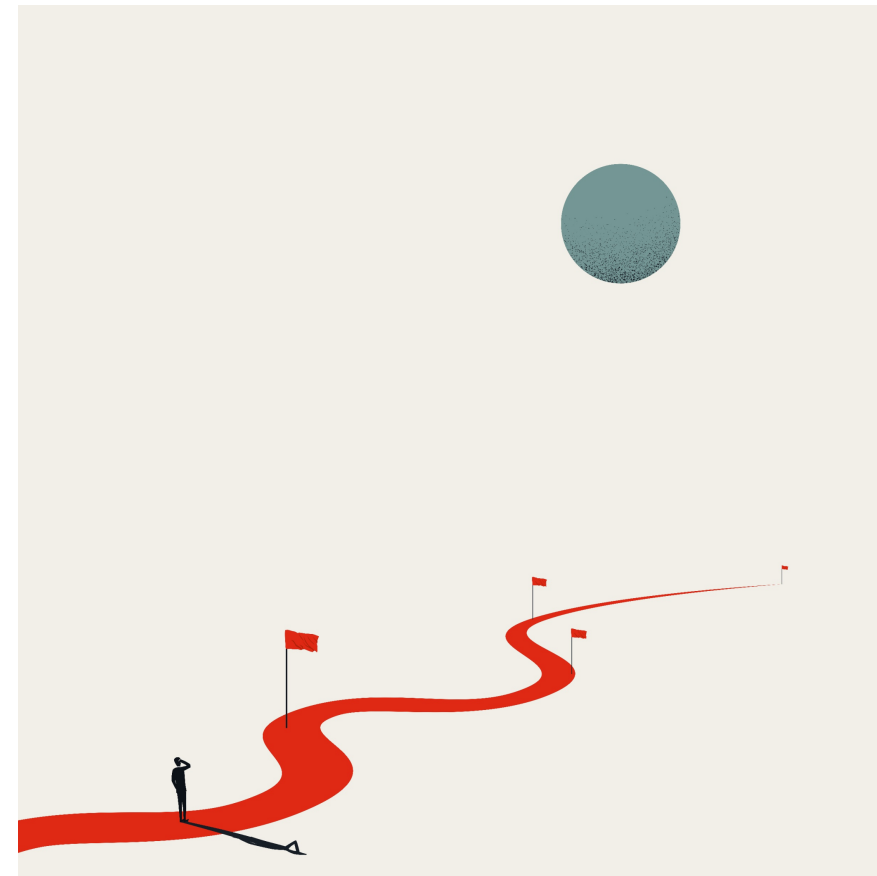
Behov finns av att implementera och verifiera säkerheten i Intraservice förvaltningsarbete och tjänsteleveranser i sin helhet



Det räcker inte att se till enskilda system eller funktioner



Säkerheten måste verifieras från det att exempelvis ett system med automatik fylls på med information till dess att tjänstens produkt används i det dagliga arbetet



Processer i flera lager – flera processägare – HR-processerna ett exempel

- Det finns idag processer som kan sägas vara "staden-övergripande", bland annat HR-processerna.
- HR-processerna kompletteras med det som benämns som arbetsformer.
- Ett exempel är arbetsformen för löneadministration och löneskuld.
- Denna arbetsform har ett beroende till process/er inom Intraservice tjänsteleverans/er.
- Exempelvis processen som bl.a. fyller Intraservice tjänst, *Stöd i arbete med löneadministration för förvaltningar och bolag*, med personuppgifter.
- De för Göteborgs Stad gemensamma processerna har processägare.
- Den process som bl.a. fyller tjänsten *Stöd i arbete med löneadministration för förvaltningar och bolag* med personuppgifter har en processägare som har sin hemvist inom Intraservice. Denne processägare är informationsägare för den information som processen skapar, nyttjar eller bearbetar. Som informationsägare är denne därtill riskägare.

Process där medarbetare ser resultatet

Korrekt lön

Process inom respektive förvaltning/bolag

Löneuppgifter

Kontroll av
löneuppgifter

Kontroll av
verkställd lön

Kontroll av
verkställd lön

Process inom tjänsten som utförs av Intraservices personal

Kontroll av
löneuppgifter

Rättelse av lön

Process inom tjänsten som utförs med automatik

Beräkning och
kontroll av
löneuppgifter

Verkställan av
löneunderlag

Process inom tjänsten som ger informationsbärare dess information

Organi-
sation

Person-
uppgifter

Avtal

Löneupp-
gifter

Fellista

Fellista

Grunderna inom informationssäkerhet

Grunderna inom informationssäkerhet

- Ett systematiskt informationssäkerhetsarbete börjar med att vi vet vilken information som ska skyddas - vi måste ha kunskap om
 - vilka informationsbärare som finns
 - vilken informationsklassning som gäller för processen som informationsbärare ingår i
 - vilka säkerhetskrav som gäller utifrån aktuell informationsklassning
 - vilka krav som finns för gallring och arkivering
 - vilka risker som kan identifieras och därutifrån
 - vilka säkerhetsåtgärder som finns och vilka säkerhetsåtgärder som behöver implementeras
- Därtill behövs processer och styrande dokument som stödjer arbetet med att kontinuerligt arbeta med förvaltningen av informationen

Informationsklassning

Informationsklassning initieras av *informationsägare*.

Informationsklassning ska utföras i samband med:

- Förändrad användning av information i en process eller förändringar av en process. Även förändringar i lagar, styrande dokument eller avtal som har påverkan på information i en process motiverar förnyad informationsklassning.
- Införskaffning av ny informationsbärare i form av exempelvis nytt system/ny applikation, övergång till molndrift eller annan form av utkontraktering. Informationsklassningen bör i dessa fall vara ett förberedande arbete inför ett upphandlingsprojekt eller liknande.
- Förändring av tjänst eller IT-lösning som påverkar informationsmängderna i en process.
- Periodicitet. Om informationsklassning inte har genomförts av någon annan anledning inom en period av fyra år ska en förnyad informationsklassning genomföras.

Riskhantering

Riskhantering

Förutom vad som tas upp i [Anvisning för styrning, uppföljning och kontroll \(goteborg.se\)](https://www.goteborg.se/Anvisning_för_styrning_oppfolljning_och_kontroll) ska riskhantering ske i samband med arbete kopplat till:

- Ärendehantering; Incident, problem, change, request
- Projekt och uppdrag
 - Exempelvis nyutveckling, inköp, etc.
- Förändringar av verksamhet, tjänsteleveranser eller annat som inte hanteras via ärendehantering, projekt eller uppdrag
- Årlig riskanalys av tjänst, tjänsteerbjudande och dess beståndsdelar
- Notera att bevarandeplan ska uppdateras utifrån genomförd riskanalys

Olika typer av risker

- Strategiska risker
- Finansiella risker
- Risker kopplade till efterlevnad av lagar/regelverk/styrande dokument
- Operativa risker

Olika roller hanterar olika typer av risker

Olika roller hanterar olika risknivåer (hög, medel, låg)

Befogenhet att hantera vissa risker styrs av verksamhetsansvaret

- Ex.:
 - Verksamhetschef för område A har befogenhet att hantera risker för område A, men saknar befogenhet att hantera risker för område B – D.
 - Avdelningschef för verksamhetsområdena A – D har befogenhet att hantera risker för område A - D.
 - Avdelningschef för verksamhetsområdena E – H har befogenhet att hantera risker för område E – H, men saknar befogenhet att hantera risker för område A – D.

Sammanfattning

Sammanfattning

Förvaltningen återkommer i juni 2024 med

1. Statusuppdatering projekt Etablera systematiskt informationsarbete
2. Ärenden kopplade till informationssäkerhet (inkl. dataskydd, arkiv- och tekniskt arkivansvar) rörande
 - Fastställande av
 - Organisation, roller samt vissa typer av ansvar och befogenheter
 - Delegation av vissa typer av befogenheter
 - Process och anvisning tillhörande
 - Informationsklassning
 - Riskhantering



Kontakt

Anna (Anna-Lena) Björk

Chief Information Security Officer (CISO)

Enhetschef Styrning och uppföljning av informationssäkerhet

GÖTEBORGS STAD Intraservice

Telefon: 031 367 00 00 | Mobil: 079 060 61 83

E-post: anna.bjork@intraservice.goteborg.se