Göteborgs Stad

Processbeskrivning

Utföra riskhantering för informationssäkerhet

2024-05-24

Innehåll

1 Inledning

1.1 Grundinformation

Säkerhet och lokaler	Informationssäkerhet	Riskhantering Informationssäkerhet
Anna-Lena Björk	–	Marcus Broman
Anna-Lena Björk	–	SS-ISO/IEC 27001:2022 SS-ISO/IEC 27005:2022

1.2 Syfte

Syftet med detta dokument är att beskriva processen för att utföra riskhantering för informationssäkerhet, vilken riktar sig till alla medarbetare inom Intraservice.

En systematisk riskhantering av informationssäkerhet bidrar till förbättringar som kan kopplas till säkerheten i de tjänster som Intraservice levererar till andra, Intraservice egen användning av dessa tjänster samt förvaltningens riskhantering för informationssäkerhet som inte är tjänster till andra.

Följande fördelar bidrar processen för riskhantering för informationssäkerhet till:

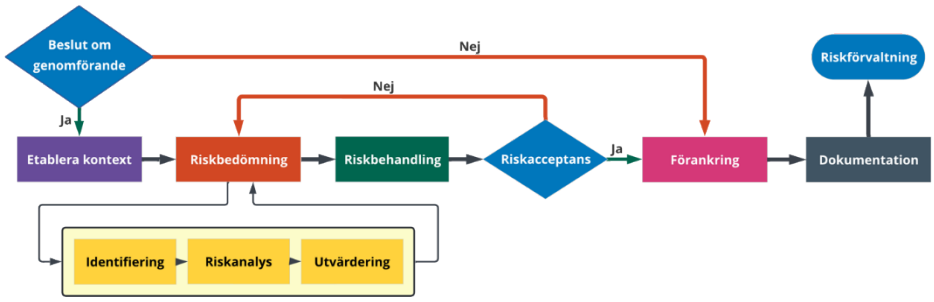
- Identifiering och utvärdering av risker, hot och sårbarheter i tjänsterna beskrivs tydligt för kunder, målgrupper och Intraservice medarbetare.
- Enhetlighet i bedömningar leder till att risker och konsekvenser i befintliga och framtida tjänster kommuniceras på ett standardiserat sätt.
- Förbättrad informationssäkerhet genom att risker och säkerhetsåtgärder i tjänster dokumenteras och upprätthålls på ett strukturerat och processorienterat sätt.
- Systematisk riskhantering förebygger och förbereder för kontinuitet och snabb återhämtning vid informationssäkerhetsincidenter.
- Transparens och ökad ansvarsskyldighet i hanteringen av informationssäkerhet ökar förtroendet hos både interna och externa intressenter.

1.2.1 Övergripande processöversikt – Utföra riskhantering för Informationssäkerhet

Processen för att utföra riskhanteringsarbetet för informationssäkerhet sker i flera nivåer. Fem processteg och två övergripande beslutspunkter bildar huvudmomenten på översta nivån. Processteget riskbedömning har dessutom tre underliggande delprocesser. Riskförvaltning är en egen process och beskrivs inte i detta dokument. Processtegen, med de underliggande stegen under riskbedömning, är:

1. Beslut om genomförande
2. Etablera kontext
3. Riskbedömning
    a. Riskidentifiering
    b. Riskanalys
    c. Riskutvärdering
4. Riskbehandling
5. Riskacceptans
6. Förankring
7. Dokumentation

Övergripande process för att utföra riskhantering för informationssäkerhet



Vart och ett dessa processteg innehåller underliggande delprocesser, vilka illustreras under avsnittet ***Error! Reference source not found.*** nedan.

1.2.2 Mål

Målet med processen Utföra riskhantering för informations¬säkerhet är att systematiskt identifiera och utvärdera hot och sårbarheter samt för att bedöma hur man kan implementera åtgärder för att minimera risker i verksamheter, tjänster, system och infrastruktur.

I det ingår att:

- Medarbetare ska kunna utföra riskhantering med ett stort mått av självständighet.
- Underlätta att kunna förstå, upptäcka, förebygga och mildra risker.
- Stödja välgrundade riskrelaterade beslut.
- Använda resurser effektivt och inte prioritera onödiga säkerhetsågärder.
- Förhindra katastrofer eller minska effeken av informationssäkerhetsincidenter.
- Stödet ska ge riskhanteringsarbetet en enhetlig hantering baserad på bästa praxis.
- Riskhantering ska fungera som en viktig del i utvecklingen för att införa nödvändiga säkerhetsåtgärder och upprätthålla informationssäkerheten.

1.3 Processberoenden

Följande processer har ett nära eller direkt beroende till processen Utföra riskhantering för informationssäkerhet. Följaktligen krävs ett nära samarbete mellan dessa processer.

Följande processer har ett nära eller direkt beroende till processen Utföra riskhantering för informationssäkerhet. Följaktligen krävs ett nära samarbete mellan dessa processer.

Process	Beroenden
Utveckla, förändra och införa tjänster	Utföra riskhantering för informationssäkerhet utgör en del av arbetet vid införande och större förändringar av tjänster.
Tillhandahålla interna verksamhetsspecifika system	Utföra riskhantering för informationssäkerhet utgör ett underlag av kravställningen vid tillhandahållande av myndighetsinterna system.
Uteckla och förvalta processer	Utföra riskhantering för informationssäkerhet bidrar med underlag för att informationssäkerheten omhändertas i Intraservices processer.
Genomföra informationsklassning	Informationsklassning bidrar med underlag till Utföra riskhantering för informationssäkerhet. Riskhantering kan även ske i informationsklassningsprocessen.
Intern efterlevnadskontroll	Efterlevnadskontroll sker årligen av säkerheten för tjänster, system och infrastruktur. Brister leder till behov av riskhantering för att säkerställa att åtgärder prioriteras ur informationssäkerhets-perspektiv.
Efterlevnadskontroll av leverantörer (Leverantörskontroll)	Riskhantering är ett underlag för att bedöma vilka leverantörer som ska kontrolleras. Leveratörskontroll är också ett underlag för att identifiera risker baserat på brister hos leverantörer.
Förvalta informationssäkerhetsrisker (under utveckling)	Förvalta informationssäkerhetsrisker är steget efter att utföra riskhantering. Riskförvalning är även input för återkommande priotering.

1.4 Roller och ansvar

Roll	Rollbeskrivning
Informationssäkerhetschef – CISO (Processägare)	Processägaren ansvarar för att en process är kundorienterad, ändamålsenlig och effektiv.
Processledare	Utses av processägaren för att löpande ansvara för utvecklingen av processen.
Informationsägare (chef)	Informationsägare ansvarar för att riskhantering genomförs samt för att utse analysledare.
Riskägare (chef)	Riskägaren tar emot resultatet och antingen accepterar risknivåer och åtgärdsplaner eller låter arbetet återgå för att hantera risker ytterligare. Riskägare kan vara samma som en informationsägare.
Analysledare (Riskmetodkunnig)	Ansvarar för genomförande av riskhantering och att riskhanteringen sker med stöd av processen. Analysledaren verkar som moderator vid eventuella riskworkshoppar och dokumenterar löpande riskbehandlingsplanen.
Deltagare (medarbetare)	Deltar i arbete och workshoppar eller blir intervjuade. Stödjer riskhanteringen med att riskbedöma och riskbehandla risker vid eventuella riskworkshoppar.

1.5 Relaterade dokument/informationskällor

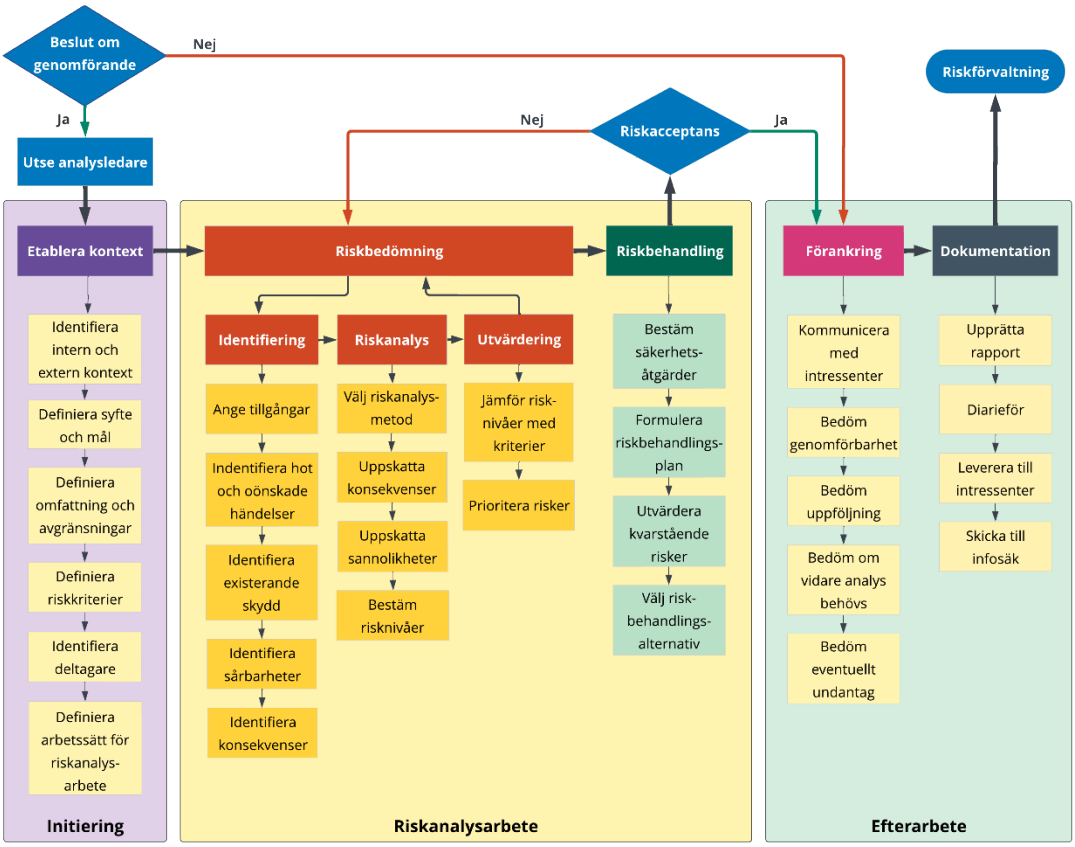
Exempel

Namn	Länk/Kontakta roll
Intraservice anvisning för riskbaserat informationssäkerhets-arbete	Intraservices informationssäkerhetschef (CISO)
Intraservices rutin för att utföra riskhantering	Intraservices informationssäkerhetschef (CISO)

1.6 Processkarta

Varje process utförs genom att en roll utför en aktivitet med hjälp av någon form av input som förädlas till ett förväntat resultat, en output. Illustrationen nedan visualiserar processens flöde för att Utföra riskhantering för informationssäkerhet. Inklusive roller, beslutspunkter (BP), processens input och output.

Intraservices process Utföra riskhantering för informationssäkerhet



1.7 Processkarta – detaljerad beskrivning

Tabellen nedan beskriver var och en av de ingående steg och komponeneter som processen Utföra riskhantering för informationssäkerhet består av. Inklusive roller, beslutspunkter (BP) och input respektive output.

N /BP	Utförare	Aktivitets-beskrivning	Input	Output
1	Informations-ägare	Behov av att utföra riskhantering.	Nytt utvecklingsprojekt, infomrationsklassning, säkerhetsdeklaration, riskuppföljning, efter-levnadskontroll eller spontant behov av riskhantering.	Konstaterat behov
BP	Informations-ägare	Beslutspunkt: Beslut om att genomföra riskhantering som åtföljs av en uppdragsbeskrivning	Nytt utvecklingsprojekt, infomrationsklassning, säkerhetsdeklaration, riskuppföljning eller ad hoc.	Om ja, uppdrags-beskrivning, gå till 3. Om nej, gå till 2.

2	Informationsägare	Dokumentera beslut.	Beslut om att inte påbörja riskhantering.	Gå till 29 och fortsätt därifrån för att fatta kompletterande beslut som behöver komplettera beslutet om att inte påbörja riskhantering.
3	Informations-ägare	Utse analysledare med riskmetodkunskap.	Lämplighetsbedömning.	Utsedd analysledare och ett uppstartmöte.
4	Informations-ägare	Öppna ärende i diariet.	Namnstandard från rutin.	Nytt ärende i diariet.
5	Analysledare	*Etablera kontext:* Identifiera intern och extern kontext.	Interna faktorer: intressenter, regelverk, informationsklassning, informationssystem, ekonomiska aspekter, tidsmässiga aspekter. Externa faktorer: Lagar, författningar, avtal, kravställnngar mot Intraservice, standarder, leverantörsfaktorer, omvärldshot och andra externa aspekter.	Definierad riskhanterings-kontext.
6	Analysledare	*Etablera kontext*: Definiera syfte och mål.	Uppdragsbeskrivning, Uppstartmöte.	Definierat syfte och mål med risk-hanteringen.
7	Analysledare	*Etablera kontext:* Definiera omfattning och avgränsningar	Uppdragsbeskrivning, Uppstartmöte.	Omfattning av aktuell riskhantering beskriven.
8	Analysledare	*Etablera kontext:* Definiera risk- och acceptenskriterier, såsom och den mängd av risk organisationen är villig att ta för att nå sina övergripande mål och tolerans för risker. (riskaptit)	Syfte och mål med riskhanteringen, Omfattningen av risk-hantering. Uppstartmöte.	Definierade kriterier för att utvärdera risker.
9	Analysledare	*Etablera kontext:* Identifiera deltagare som har teknisk, praktisk eller regulatorisk kunskap om riskområdet	Uppstartmöte. Medarbetare.	Lista på personer som deltar i riskhanteringen.
10	Analysledare	*Etablera kontext:* Definiera arbetssätt för riskanalysen. Metodval kan vara beroende på om en fullständig riskhantering behövs eller bara delar av processen. En hög risk eller dyr säkerhetsågärd kan	Syfte och mål med riskhanteringen, Omfattningen av risk-hantering. Definierad riskhanterings-kontext.	Val av risk-hanteringsmetod: Grundmetod eller förenklad metod, gå till 11 Utökad metod, gå till 12

		motivera en fördjupad analysmetod.		
11	Analysledare	Planera genomförande av riskbedömning. Skicka inbjudan till en eller flera riskworkshoppar.	Lista från punkt 9.	Mötesbokning.
12	Analysledare	Skicka begäran till enheten för informationssäkerhet för att fortsätta vidare med en utökad metod, som har liknande men andra steg för riskbedömning och behandling och under-liggande delprocesser. I övrigt är processen desamma.	Val av utökad metod.	Begäran om konsultation. Fortsatt riskanalysarbete sker enligt utökad metod fram till riskacceptans. Gå till 28.
13	Analysledare Deltagare	*Riskbedömning:* *Riskidentifiering:* Ange vilken eller vilka **informationstillgångar** som är inblandade eller hotade och behöver skyddas.	Informationsklassning. Brainstorming, omvärdsbevakning, identifiering genom föranalys, input från efterlevnadskontroll.	Beskrivna tillgångar på riskkort.
14	Analysledare Deltagare	*Riskbedömning:* *Riskidentifiering:* Identifiera potentiella **hot** mot informationstillgångar samt **oönskade händelser**.	Brainstorming, omvärdsbevakning, identifiering genom föranalys, input från efterlevnadskontroll.	Beskrivna hot och oönskade händelser på riskkort.
15	Analysledare Deltagare	*Riskbedömning:* *Riskidentifiering:* Identifiera **existerande skydd** för informations-tillgångar.	Beskrivna hot, oönskade händelser samt tillgångar. Brainstorming, identifiering genom föranalys, input från efterlevnadskontroll, input från tidigare riskhantering, Tjänstespecifikationer, funktionsbeskrivningar, annan dokumentation.	Beskrivna införda säkerhetsåtgärder på riskkort.
16	Analysledare Deltagare	*Riskbedömning:* *Riskidentifiering:* Identifiera **sårbarheter** (brister) som kan utnyttjas av hot mot informations-tillgångar.	Beskrivna hot, oönskade händelser, införda säkerhetsåtgärder samt tillgångar. Brainstorming, omvärdsbevakning, identifiering genom föranalys, input från efterlevnadskontroll.	Beskrivna sårbarheter på riskkort.
17	Analysledare Deltagare	*Riskbedömning:* *Riskidentifiering:* Identifiera **konsekvenser** av hot och sårbarheter (som leder till…). Ange även om konsekvenser avser konfidentialitet, riktighet och/eller tillgänglighet (K, R, T)	Beskrivna hot, oönskade händelser, tillgångar, sårbarheter samt införda säkerhetsåtgärder. Brainstorming, omvärdsbevakning, identifiering genom föranalys, input från efterlevnadskontroll.	Beskrivna konsekvenser samt om det avser K, R, T på riskkort.

18	Analysledare Deltagare	*Riskbedömning:* *Riskanalys:* Välj riskanalysmetod för att uppskatta risker manuellt eller med systemstöd. Välj mellan dold röstning och att genom diskussioner nå konsensus. (gäller grundmetod och förenklad metod.)	Valt arbetssätt för riskanalysarbete. Systemstöd (mentimeter eller annat stöd.) Riskkort. Förkunskaper om riskområdet.	Vald riskanalysmetod lämplig för ändamålet.
19	Analysledare Deltagare	*Riskbedömning:* *Riskanalys:* Uppskattning av hur allvarlig konsekvensen av den oönskade händelsen är. (gäller grundmetod och förenklad metod.)	Riskkort. Systemstöd (mentimeter eller annat stöd).	Bedömning av konsekvensen för varje identifierad risk.
20	Analysledare Deltagare	*Riskbedömning:* *Riskanalys:* Uppskattning av **sannolikheten** för en oönskad händelse. (gäller grundmetod och förenklad metod)	Riskkort. Systemstöd (mentimeter eller annat stöd) med dold röstning eller genom diskussioner för att nå konsensus.	Bedömning av sannolikhet varje identifierad risk.
21	Analysledare Deltagare	*Riskbedömning:* *Riskanalys:* **Bestäm risknivåer** som en kombination av den uppskattade sannolikheten och konsekvenserna för alla risker (riskscenarier). Risker kan plottas på en riskmatris. (Grundmetod och förenklad metod.)	Riskkort. Excelmall. Systemstöd (mentimeter eller annat stöd).	Lista eller riskmatris med risknivåer, som är en samman-vägning av analyserade riskers konsekvenser och sannolikheter.
22	Analysledare Deltagare	*Riskbedömning:* *Riskutvärdering:* **Jämför resultatet** av riskanalysen med de tidigare satta risk- och acceptanskriterierna.	Lista eller riskmatris med risknivåer. Definierade kriterier för att utvärdera risker. Excelmall. Systemstöd.	En lista med riskresultatet jämfört med riskkriterier.
23	Analysledare Deltagare	*Riskbedömning:* *Riskutvärdering:* **Prioritera risker** baserat på deras betydelse och nödvändighet av åtgärder.	En lista med riksresultatet jämfört med riskkriterier. Excelmall. Systemstöd.	En lista med riskresultatet sorterad i prioritetsordning av risknivåer.
24	Analysledare Deltagare	*Riskbehandling:* Välj **alternativ för riskbehandling** för varje risk: (a) reducera risk, (b) acceptera risk, (c) undvika risk eller (d) överföra risk.	En lista med riskresultatet sorterad i prioritetsordning av risknivåer. Excelmall. Systemstöd.	En lista med riskresultatet kompletterat med valda alternativ för riskbehandling.

25	Analysledare Deltagare	*Riskbehandling:* **Bestäm säkerhetsåtgärder** för risker genom att introducera, ta bort eller förändra säkerhetsåtgärder så att kvarstående risker kan revideras och bedömas som acceptabla.	Riskresultatet kompletterat med valda alternativ för riskbehandling. Excelmall. Systemstöd.	En lista med riskresultatet kompletterat med säkerhetsåtgärder som är effektiva (tekniska, organisatoriska, personrelaterade eller fysiska).
26	Analysledare Deltagare	*Riskbehandling:* **Formulera riskbehandlingsplan** med när åtgärd är tänkt att vara genomförd, resurser och ansvar för genomförande samt kvarstående risker. Riskbehandlingsplanen kan även omfatta en åtgärdslista där åtgärderna grupperas, vilket underlättar översikten vid implementering.	En lista med riskresultatet och säkerhetsåtgärder. Excelmall. Systemstöd.	*Riskbehandlingsplan:* Riskresultatet och säkerhetsåtgärder samt föreslagna resurser, ansvar och kvarstående risker. (Eventuellt även en åtgärdslista.)
27	Analysledare Deltagare	*Riskbehandling:* **Utvärdera kvarstående risker** genom att uppskatta sannolikhet och konsekvens för risker som återstår samt bestäm risknivån. (Grundmetod, ej förenklad.)	Riskbehandlingsplan. Excelmall. Systemstöd	Riskbehandlingsplan kompletterad med en uppskattning av sannolikhet, konsekvens och risknivå.
28	Analysledare Riskägare	*Riskacceptans:* Utvärdera om den kvarvarande risken är acceptabel baserat på riskacceptanskriterier.	Riskbehandlingsplan kompletterad med en uppskattning av sannolikhet, konsekvens och risknivå. Excelmall. Systemstöd.	Riskbehandlingsplan och annat underlag (eventuell presentation) som ger av samlad riskbild för riskägare.
BP	Riskägare	*Riskacceptans:* Dokumentera **beslut om att acceptera** nivåerna på kvarvarande risker som finns i riskbehandlings-planen. Alternativt återgår arbetet för att göra kompletterande bedömningar av risker och identifiera bättre åtgärder för att förbättra risksituationen.	Riskbehandlingsplan och annat underlag (eventuell presentation) som ger av samlad riskbild för riskägare.	Godkänd Riskbehandlingsplan, accepterade kvarvarande risker. Om Ja, gå till 29. Om Nej, gå tillbaka till *13 Riskbedömning* och upprepa de delar som behövs, specifikt från *22 Riskutvärdering* och framåt.

29	Riskägare (Analysledare)	*Förankring och granskning:* Kommunicera med intressenter för att inhämta intressenters uppfattningar av resultatet. Arbetet kan ske löpande, men behöver sammanfattas.	Risklista och riskbehadlingsplanen under sin utveckling genom processen.	Synpunkter och feedback på arbetet, om risker, orsaker, konsekvenser, sannolikheter och åtgärder.
30	Riskägare (Analysledare)	*Förankring och granskning:* **Bedöm genomförbarhet** av åtgärder som syftar till att reducera risker beroende på exempelvis kostnad, tidsåtgång, kompetens, komplexitet samt politisk viljeinriktning. Arbetet kan ske löpande, men behöver sammanfattas om det finns högt prioriterade åtgärder med låg genomförbarhet.	Risklista med prioriteringar och riskbehadlingsplan. Intressenters synpunkter och feedback på arbetet, om risker, orsaker, konsekvenser, sannolikheter och åtgärder.	Lista eller matris på bedöma åtgärders genomförbarhet.
32	Riskägare (Analysledare)	*Förankring och granskning:* **Bedöm om riskuppföljning behövs** för att verifiera att åtgärd går att genomföra eller har genomförts.	Lista eller matris för att bedöma åtgärders genomförbarhet.	Lista eller matris på bedömda åtgärders genomförbarhet med beskrivet underlag för om man bör följa upp riskanalysen.
BP	Riskägare	*Förankring och granskning:* Behövs riskuppföljning? Besluta om riskuppföljning och utse en eventeull utförare av riskuppföljningen.	Lista eller matris på bedömda åtgärders genomförbarhet med beskrivet underlag för hur man kan följa upp riskanalysen.	Om Nej, gå till 33. Om Ja, gå tillbaka till 22 samt utse en utförare.
33	Riskägare (Analysledare)	*Förankring och granskning:* **Bedöm om vidare analys behövs** för att utreda risker vidare. Detta kan innebära att använda en utökad metod för riskanalys. Alternativt återgår arbetet för att göra kompletterande bedömningar av risker och identifiera bättre åtgärder för att förbättra risksituationen.	Risklista och riskbehadlingsplan under sin utveckling genom processen. Intressenters synpunkter och feedback på arbetet: om risker, orsaker, konsekvenser, sannolikheter och åtgärder.	Underlag för bedömning om kvarvarande risker kan inte behandlas vidare med nuvarande metod. .

BP	Riskägare	*Förankring och granskning:* Behövs en vidare riskanalys? En hög risk eller dyr säkerhetsågärd kan motivera en fördjupad analysmetod.	Underlag för bedömning om kvarvarande risker kan inte behandlas vidare med nuvarande metod.	Om Nej, gå vidare till 34. Om Ja, välj utökad metod och skicka en begäran om konsultation till enheten för informationssäkerhet. Alternativt, gå tillbaka till *13 Riskbedömning* och upprepa de delar som behövs, specifikt från *22 Riskutvärdering* och framåt
34	Riskägare (Analysledare)	*Förankring och granskning:* **Bedöm eventuellt undantag** från styrdokument för Göteborgs Stad eller Intraservice.	Risklista och riskbehadlingsplan under sin utveckling genom processen. Intressenters synpunkter och feedback på arbetet. Dokumentation om risker, orsaker, konsekvenser, sannolikheter och åtgärder.	Underlag för bedömning om avvikelser sker genetomt styrdokument
BP	Riskägare	*Förankring och granskning:* Frångår riskacceptans styrande dokument?	Underlag för om bedömning av avvikelser sker gentemot styrdokument.	Om Nej, gå till 35. Om Ja, gå till Undantagsprocess.
35	Analysledare	*Dokumentation:* **Upprätta rapport** i wordformat och spara som PDF när rapporten är färdig. Ange åtgärder utan detaljer. Inkludera lista på risker i prioritetsordning. Dokumentation kan ske löpande genom processen, men behöver färdigställas.	Rapportmall i wordformat. Riskbehadlingsplan och annan dokumention (uppdragsbeskriving, kontext, underlag för riskacceptans mm).	Färdig riskrapport i word-format och i PDF-format.
BP	Riskägare	*Dokumentation:* **Diarieför**. Godkänn rapport och skicka rapport till diariet.	Färdig riskrapport i word-format och i PDF-format.	Färdig godkänd rapport i PDF-format diarieförd.

37	Riskägare	*Dokumentation* **Leverera till intressenter** och berörda, exempelvis kunder, närliggande tjänster eller verksamheter.	Färdig godkänd rapport i PDF-format diarieförd.	Skickade rapporter i PDF-format till olika intressenter (Exempel är processerna: Förändring, Incident, CAB, Inköp, Projekt, Säkerhets-deklaration och Efterlevnadskontroll.)
39	Riskägare	*Dokumentation:* Skicka till enheten för informationssäkerhet som sammanställer och aggregerar risker i ett riskregister genom processen riskförvaltning (under utveckling).	Färdig riskrapport i word-format och i PDF-format.	Skickade rapporter i word-format och i PDF-format till enheten för informationssäkerhet. Input till riskregister och processen riskförvaltning.

1.8 Mätning och uppföljning

Kategori	**Indikatorer**				**Typ**
Kritiska framgångsfaktorer (KFF) & Nyckeltal (KPI)	Mätetal/Metod	Normer	Intervall	Kvalitativ eller Kvantitativ	Värde, prestanda, kvalitet eller överensstämmelse.
KF #1 **Åtgärdsplaner i förvaltning baserade på genomgången riskhantering**					
KPI 1.1 Riskhantering gjord och dokumenterad minst en gång per enhet och år.	1.1.1 Riskhantering finns dokumenterad hos respektive enhet.	100% vs. 0%	Årligen	Kvantitativ	Värde
KF #2 Utvecklingsarbete föregås av genomgången riskhantering för att hantera info.säk.aspekter.					
KPI 2.1 Riskhantering gjord och dokumenterad för alla utvecklings-projekt.	2.1.1 Riskhantering finns dokumenterad hos respektive utvecklingsprojekt.	Ökande procent över tid.	Årligen	Kvalitativ	Värde