Göteborgs Stad

Samlad riskbild inkl. intern kontrollplan

Nämnden för Intraservice

Innehållsförteckning

1 Beskrivning av gemensamma begrepp

Riskområden

"Tillsammans med identifieringen av verksamhetens mål/uppdrag/skyldigheter utgör riskområdena ramen för riskhanteringen."

Hantera/Acceptera risk

Kontrollaktiviteter kan enbart skapas till identifierade risker med vald status: HANTERA.

Risker med vald status: ACCEPTERA kan även väljas Till Samlad riskbild

Till Samlad riskbild

"Det är varken lämpligt eller önskvärt att lyfta samtliga identifierade risker inom respektive riskområden till nämnd/bolagsstyrelse. En värdering och prioritering behöver göras och ställas samman till en samlad riskbild. Syftet med den samlade riskbilden är att ge en bild över verksamhetens mest väsentliga risker utifrån ett nämnd/bolagsstyrelseperspektiv.

Bedömningen av vad som är mest väsentligt måste alltid göras med utgångspunkt i uppdrag, skyldigheter och mål för verksamheten."

Intern kontrollplan

"Underlaget till den interna kontrollplanen bygger på den samlade riskbilden. Ett antal riskområden/processer (nämnd/styrelse väljer själv omfattning) som lyfts i den samlade riskbilden väljs ut för granskning/kontroll för att verifiera att redan införda åtgärder har fått avsedd effekt.

Syftet är att ta reda på om den interna kontrollen i verksamheten fungerar på ett tillfredsställande sätt men även att kunna ifrågasätta befintliga åtgärder och vid behov komma med förbättringsförslag (nya åtgärder)."

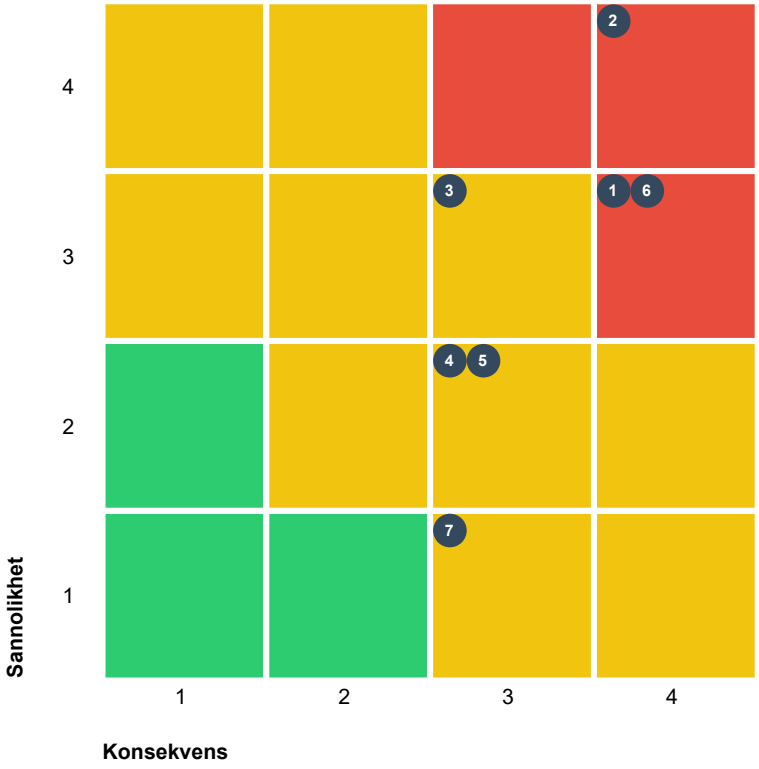
2 Inledning

Syftet med den samlade riskbilden är att ge en bild över verksamhetens mest väsentliga risker. Vad som är mest väsentligt är inte möjligt att på förhand definieras, men det kan vara risker som berör hela förvaltningen eller större delar av förvaltningen.

I den samlade riskbilden finns de risker som bedömts som väsentliga för Intraservice och som vi bedömt behöver åtgärdas för att begränsa riskerna.

Uppföljning av risker och internkontrollplanen kommer att ske i samband med den utökade uppföljningen, som görs i maj och november. Utöver detta följs även riskerna upp i samband med delårsrapport augusti och årsrapporten. Vid dessa tillfällen får även nämnden en återrapportering av uppföljningen av riskerna.

3 Sammanfattning av planen



3 Hög 4 Medium Totalt: 7

Hög	
Medium	
Låg	

	Sannolikhet	Konsekvens
4	Sannolik	Allvarlig
3	Möjlig	Kännbar
2	Mindre sannolik	Lindrig
1	Osannolik	Försumbar

Riskområde	Risk	Sannolikhet	Konsekvens	Riskvärde
Omvärld	1 **Säkerhetsläget**	3. Möjlig	4. Allvarlig	12. Hög
	2 **Cyberattacker**	4. Sannolik	4. Allvarlig	16. Hög
Strategiska	3 **Strategiska behov utifrån stadens utmaningar**	3. Möjlig	3. Kännbar	9. Mellan
	4 **Intäktsbortfall vid utträde av bastjänster och tilläggstjänster**	2. Mindre sannolik	3. Kännbar	6. Mellan
Operativa	5 **Bristande följsamhet till stadens riktlinje för inköp och upphandling samt till LoU**	2. Mindre sannolik	3. Kännbar	6. Mellan

Riskområde	Risk	Sannolikhet	Konsekvens	Riskvärde
Finansiella				
Regelefterlevnad och oegentligheter	6 **Informationssäkerhet**	3. Möjlig	4. Allvarlig	12. Hög
	7 **Oegentligheter**	1. Osannolik	3. Kännbar	3. Mellan
Stadenleveranser				

På förvaltningsnivå har förvaltningen bedömt att det är sju risker som behöver hanteras med åtgärder för att begränsa riskerna. Förvaltningens tre högsta risker är säkerhetsläget, cyberattacker samt informationssäkerhet. Detta ligger i linje med förvaltningens uppdrag som tjänsteleverantör.

Även om vi har bedömt sannolikheten att risken inom oegentligheter som låg så har vi bedömt att risken ändå ska ingå i förvaltningens samlade riskbild. Detta eftersom oegentligheter är ett område som vi hela tiden behöver informera om för att upprätthålla en god kultur.

4 Samlad riskbild med åtgärder

Riskens totala värde visas enligt följande risknivåer och färger:

4.1 Riskområde: Omvärld

4.1.1 Risk: Säkerhetsläget

Risknivå

12. Hög

Hantera

Riskbeskrivning
Den säkerhetspolitiska situationen har blivit sämre, men Försvarsmakten följer utvecklingen noga och bevakar Sveriges territorium och närliggande områden dygnet runt. Just nu ser Försvarsmakten inga oroande rörelser längs våra gränser, men ett väpnat angrepp mot Sverige kan inte uteslutas. Det kan heller inte uteslutas att militära maktmedel eller hot om sådana kan komma att användas mot Sverige.

Konsekvensbeskrivning
Förvaltningen informerar nämnden muntligt om konsekvenserna.

Existerande kontrollaktiviteter
Inpassering & behörighetskontroll (rondering), identitetskontroll vid rekrytering, lås & larm, efterlevnadskontroller på inpasseringskort (kontroll av att vi inte har kort utan behörig person), analys på ärenden i IA (skador hos personalen - bedöma om det är något som ökar och som kopplas till säkerheten), tvåpersonsattestering för utökad behröighet på inpasseringskort

Åtgärd - aktuell status	Beskrivning
Pågående **Ta fram övningsplan för områdena: incidenter, utrymning, kontinuitet, krisledning, beredskapsplan.**	
Pågående **Översyn av förvaltningens säkerhetsarbete för att optimera styrningen**	
Pågående **Implementera TIB-rollen i förvaltningen.**	

4.1.2 Risk: Cyberattacker

Risknivå

16. Hög

Hantera

Riskbeskrivning
Risk för cyberattacker

Konsekvensbeskrivning
Information kan bli tillgänglig för obehöriga personer och användas på felaktigt sätt. Bristande förtroende för Intraservice som leverantör. Förvaltningens tjänster ligger nere, vilket innebär att förvaltningens kunder inte kan utföra sitt uppdrag.

Existerande kontrollaktiviteter
Administrativa och tekniska säkerhetsåtgärder. Exempelvis åtkomstkontroll, kryptering, säkerhetskopiering, loggning, redundans av miljön, skydd mot skadlig kod, sårbarhetsscanning, utbildning av personal

Åtgärd - aktuell status	Beskrivning
Ej påbörjad **Översyn av incidentprocessen för att bedöma om de behöver kompletteras eller förändras.**	
Ej påbörjad **Säkerställa att cyberattacker är ett scenario i kontinuitetsplanerna.**	

4.2 Riskområde: Strategiska

4.2.1 Risk: Strategiska behov utifrån stadens utmaningar

Risknivå

9. Mellan

Hantera

Riskbeskrivning
Risk att vi inte kan möta kundernas strategiska behov utifrån stadens utmaningar

Konsekvensbeskrivning
Stadens övriga förvaltningar kan inte genomföra de förändringar som de behöver för att möta utmaningar i sin verksamhet. Detta kan innebära risk för lägre

måluppfyllelse av stadens övergripande mål. Det kan också innebära bristande förtroende för Intraservice.

Existerande kontrollaktiviteter
Regelbundna kundkontakter, omvärldsbevakning, uppdrag samordningsmodellen

Åtgärd - aktuell status	Beskrivning
Ej påbörjad **Strategisk dialog**	

4.2.2 Risk: Intäktsbortfall vid utträde av bastjänster och tilläggstjänster

Risknivå

6. Mellan

Hantera

Riskbeskrivning
Förvaltningens verksamhet är beroende av finansieringsmodellen där obligatoriska bastjänster och frivilliga tilläggstjänster finansieras av stadens förvaltningar och bolag. Risken uppstår om en eller flera förvaltningar/bolag väljer att träda ur antingen bastjänster eller tilläggstjänster.

Detta kan då leda till:

* Minskad intäkt som påverkar förvaltningens förmåga att täcka fasta kostnader, såsom personal och infrastruktur.
* Obalans i budgeten som kan resultera i ekonomiska underskott.

Konsekvensbeskrivning
För bastjänster:

Det finns en hypotetisk möjlighet med en utdragen process där kommunal förvaltning eller bolag kan lämna bastjänsten, om det skulle inträffa så riskeras underskott och neddragningar, vilket kan påverka kvaliteten och omfattningen av tjänster till övriga kunder.

För tilläggstjänster:

Tilläggstjänster har en snabbare utträdesprocess jämfört bastjänst, detta kan innebära att förvaltningen måste hantera plötsliga intäktsbortfall om en kund väljer att ej använda tilläggstjänsten.

Möjlighet att skala ner resurser snabbt kan vara begränsad, vilket leder till ökade fasta kostnader per kvarvarande kund vilket kan innebära att kunder väljer att lämna.

Existerande kontrollaktiviteter

Taktiskt möte - affärsberedning
Affärsråd

Åtgärd - aktuell status	Beskrivning
Ej påbörjad **Säkerställa att vi har avtal som minskar den ekonomiska risken**	Tilläggstjänster: avtal ska tecknas med kunder innan uppstart. Vid tecknande av avtal med kunder ska avtalen vara densamma eller ta hänsyn till avtal vi har med extern leverantör. Med nya riktlinjen blir inte tilläggstjänsterna lika valbara. Bastjänsterna: säkerställa att vi tecknar avtal där volymsändringar återspeglas i avtalen. Säkerställa om obligatoriska tjänster ska utträdas att det krävs det ett utträdesavtal.

4.3 Riskområde: Operativa

4.3.1 Risk: Bristande följsamhet till stadens riktlinje för inköp och upphandling samt till LoU

Risknivå

6. Mellan

Hantera

Riskbeskrivning
Risk att förvaltningen inte uppnår ej stadens syfte och mål med inköp och upphandling. Risk för att förvaltningen får revisionsanmärkningar.

Lagar och regler kring offentlig upphandling är strikta, och brott mot dessa kan få allvarliga ekonomiska och juridiska konsekvenser såsom:

Ogiltigförklarade avtal.
Skadeståndsanspråk från leverantörer.
Fördröjda projekt och ökade kostnader.

Konsekvensbeskrivning
Verksamheten följer inte stadens riktlinje för inköp och upphandling, ovetskap av att det finns en Intraservice anvisning för inköp och upphandling som följer stadens riktlinje. Ovetskap till fastställda Intraservice processer

Existerande kontrollaktiviteter
Kontroller sker mha KMD inköpsanalys / Internrevisionsplan

Därutöver bedriver upphandlare alla upphandlingar över 50.000kr, behöriga beställare bedriver direktköp upp till 10.000kr. Behöriga beställare ska göra inköp på upphandlade avtal.

Åtgärd - aktuell status	Beskrivning
Ej påbörjad **Säkerställa kunskap hos chefer, även de som varit här länge**	
Ej påbörjad **Utbilda i rutiner och processer**	

4.4 Riskområde: Regelefterlevnad och oegentligheter

4.4.1 Risk: Informationssäkerhet

Risknivå

12. Hög

Hantera

Riskbeskrivning
1. Risk för bristfällig hantering av informationstillgångar på grund av otydliga, ej uppdaterade eller avsaknad av, processer och arbetssätt, inklusive anvisningar, rutiner och instruktioner, samt avsaknad av eller otydliga ansvar och befogenheter.
Delvärdering Sannolikhet 3 och konsekvens 4

2. Risk för att obehöriga får tillgång till information utifrån otillräcklig administrativ respektive teknisk åtkomstkontroll.
Delvärdering Sannolikhet 3 och konsekvens 4

3, Risk för att information inte är korrekt, att informationen är manipulerad eller förstörd, utifrån otillräckliga administrativa respektive tekniska säkerhetsåtgärder.
Delvärdering Sannolikhet 3 och konsekvens 4

4. Risk för att informationen inte är tillgänglig när den behövs utifrån avsaknad av, bristfälliga eller ej uppdaterade, processer och arbetssätt, anvisningar, rutiner och instruktioner tillhörande kontinuitetshantering och återställning av tjänster.
Delvärdering Sannolikhet 3 och konsekvens 4

Konsekvensbeskrivning
Konsekvensen kan bli brister i robusthet i förvaltningens tjänsteleverans. Förtroendet för förvaltningen försämras. Konsekvens för stadens verksamhet att lagar och regelverk inte följs.

Inom ramen för begreppet informationssäkerhet inkluderas administrativa och tekniska säkerhetsåtgärder med mål att skydda information.
Det finns många risker inom detta område. Det går inte att skydda en verksamhet från alla risker. Det viktiga är att identifiera vilka konsekvenser olika risker får och

sätta in åtgärder för att minimera konsekvenserna.

Att ha väl etablerade processer och arbetssätt, tydliga anvisningar, rutiner och instruktioner är viktigt. Att genomföra informationsklassning, riskanalyser och konsekvensbedömningar, uppdateringar av mjuk- och hårdvara, endast tillåta godkänd utrustning, övervaka händelser i IT-miljön, upprätta olika nätverkssegment och skapa kontrollerade trafikflöden, gallra och arkivera, och tillse att rätt person får åtkomst till korrekt information när den behövs är några exempel på administrativa åtgärder som bidrar till att stärka skyddet av informationen. Det är också viktigt att administrativa regelverk hjälper till att bibehålla tjänsteleveransernas kontinuitet och att tjänster enkelt och effektivt kan återupptas i bruk efter en eventuell incident.

Förutom administrativa säkerhetsåtgärder är det av stor vikt att det finns tekniska skyddsåtgärder som hjälper till att förhindra att information hanteras på olämpligt sätt. Med tekniska säkerhetsåtgärder avses exempelvis teknisk åtkomstkontroll, filtreringsfunktioner som skyddar mot oönskad nätverkstrafik, kryptering, säkerhetskopiering, övervakning/loggning och virus/malwareskydd, men även säkerhetsåtgärder som är kopplade till fysisk säkerhet, exempelvis inpasseringssystem.

Regel- respektive lagöverträdelser, sanktionsavgifter, driftsstörningar och bristande tillit till Intraservice som förvaltning och leverantör är några exempel på tänkbara konsekvenser utifrån otillräckliga administrativa och tekniska säkerhetsåtgärder.

Existerande kontrollaktiviteter
Efterlevnadsrapport och åtgärdsplan gällande Informations- och dataskydd 2 ggr/år.

Åtgärd - aktuell status	Beskrivning
Pågående **Säkerställ process, ansvar och uppföljning av informationssäkerhetsanalys (projekt ESI)**	En rapport sammanställs två gånger om året efter intervjuer och kontroller av informationssäkerhet och dataskydd. Dessa förbättringsområden behöver åtgärdas och tilldelas en tydlig åtgärdsansvarig som återrapporterar förbättringar.

4.4.2 Risk: Oegentligheter

Risknivå

3. Mellan

Hantera

Riskbeskrivning
Risk för oegentligheter inom följande områden:
- Leverantörer,
- Rekrytering,
- Inhyrning av konsulter (vänskapskorruption - känner en konsult, mutor, jäv)

Konsekvensbeskrivning

Bristande förtroende för förvaltningen.

Existerande kontrollaktiviteter
Riktlinjer för portföljstyrning - jävsbedömning ingår inför uppstart av projekt. Konsultprövning. Rutiner för rekrytering finns, rekryteringsprocessen är dokumenterad och i den framgår det hur jäv ska hanteras i rekryteringsprocessen. Det framgår även hur utvärdering av kandidater ska göras.

Åtgärd - aktuell status	Beskrivning
Ej påbörjad **Informationsinsats till chefer**	Förvaltningen behöver löpande informera om gällande regler och rutiner för att upprätthålla en god kultur när det gäller oegentligheter. Informationen bör omfattas av flera områden. Information till chefer antingen på chefsforum, ALG eller annat forum. Informationen bör beröra flera områden, såsom HR, inköp och ekonomi. Informationen kan vara utformad i form av scenario som är aktuella för förvaltningen samt konsekvenser som kan uppstå

5 Samlad riskbild - Intern kontrollplan

Riskens totala värde visas enligt följande risknivåer och färger:

Enligt riktlinjen för styrning, uppföljning och kontroll ska en intern kontrollplan upprättas utifrån den samlade riskbilden. Den ska innehålla de områden som särskilt ska granskas för att verifiera att redan införda åtgärder har fått avsedd effekt.

Syftet med internkontrollplanen är att ta reda på om den interna kontrollen i verksamheten fungerar på att tillfredsställande sätt, men även att kunna ifrågasätta åtgärderna.

Förvaltningen har valt ut tre risker som ingår i internkontrollplanen. Två av förvaltningens högsta risker samt oegentligheter. Hur internkontrollerna genomförs i detalj kommer att tas fram tillsamman med ansvarig för respektive risk.

5.1 Riskområde: Omvärld

5.1.1 Risk: Cyberattacker

Risknivå

16. Hög

Riskbeskrivning
Risk för cyberattacker

Konsekvensbeskrivning
Information kan bli tillgänglig för obehöriga personer och användas på felaktigt sätt. Bristande förtroende för Intraservice som leverantör. Förvaltningens tjänster ligger nere, vilket innebär att förvaltningens kunder inte kan utföra sitt uppdrag.

Existerande kontrollaktiviteter
Administrativa och tekniska säkerhetsåtgärder. Exempelvis åtkomstkontroll, kryptering, säkerhetskopiering, loggning, redundans av miljön, skydd mot skadlig kod, sårbarhetsscanning, utbildning av personal

Kontrollaktivitet - aktuell status	Beskrivning
Ej påbörjad	Testa vårt skalskydd
Kontroll av den fysiska säkerheten	

5.2 Riskområde: Regelefterlevnad och oegentligheter

5.2.1 Risk: Informationssäkerhet

Risknivå

12. Hög

Riskbeskrivning
1. Risk för bristfällig hantering av informationstillgångar på grund av otydliga, ej uppdaterade eller avsaknad av, processer och arbetssätt, inklusive anvisningar, rutiner och instruktioner, samt avsaknad av eller otydliga ansvar och befogenheter.
Delvärdering Sannolikhet 3 och konsekvens 4

2. Risk för att obehöriga får tillgång till information utifrån otillräcklig administrativ respektive teknisk åtkomstkontroll.
Delvärdering Sannolikhet 3 och konsekvens 4

3, Risk för att information inte är korrekt, att informationen är manipulerad eller förstörd, utifrån otillräckliga administrativa respektive tekniska säkerhetsåtgärder.
Delvärdering Sannolikhet 3 och konsekvens 4

4. Risk för att informationen inte är tillgänglig när den behövs utifrån avsaknad av, bristfälliga eller ej uppdaterade, processer och arbetssätt, anvisningar, rutiner och instruktioner tillhörande kontinuitetshantering och återställning av tjänster.
Delvärdering Sannolikhet 3 och konsekvens 4

Konsekvensbeskrivning
Konsekvensen kan bli brister i robusthet i förvaltningens tjänsteleverans. Förtroendet för förvaltningen försämras. Konsekvens för stadens verksamhet att lagar och regelverk inte följs.

Inom ramen för begreppet informationssäkerhet inkluderas administrativa och tekniska säkerhetsåtgärder med mål att skydda information.
Det finns många risker inom detta område. Det går inte att skydda en verksamhet från alla risker. Det viktiga är att identifiera vilka konsekvenser olika risker får och sätta in åtgärder för att minimera konsekvenserna.

Att ha väl etablerade processer och arbetssätt, tydliga anvisningar, rutiner och instruktioner är viktigt. Att genomföra informationsklassning, riskanalyser och konsekvensbedömningar, uppdateringar av mjuk- och hårdvara, endast tillåta godkänd utrustning, övervaka händelser i IT-miljön, upprätta olika nätverkssegment och skapa kontrollerade trafikflöden, gallra och arkivera, och tillse att rätt person får åtkomst till korrekt information när den behövs är några exempel på administrativa åtgärder som bidrar till att stärka skyddet av informationen. Det är också viktigt att administrativa regelverk hjälper till att bibehålla tjänsteleveransernas kontinuitet och att tjänster enkelt och effektivt kan återupptas i bruk efter en eventuell incident.

Förutom administrativa säkerhetsåtgärder är det av stor vikt att det finns tekniska skyddsåtgärder som hjälper till att förhindra att information hanteras på olämpligt sätt. Med tekniska säkerhetsåtgärder avses exempelvis teknisk åtkomstkontroll,

filtreringsfunktioner som skyddar mot oönskad nätverkstrafik, kryptering, säkerhetskopiering, övervakning/loggning och virus/malwareskydd, men även säkerhetsåtgärder som är kopplade till fysisk säkerhet, exempelvis inpasseringssystem.

Regel- respektive lagöverträdelser, sanktionsavgifter, driftsstörningar och bristande tillit till Intraservice som förvaltning och leverantör är några exempel på tänkbara konsekvenser utifrån otillräckliga administrativa och tekniska säkerhetsåtgärder.

Existerande kontrollaktiviteter
Efterlevnadsrapport och åtgärdsplan gällande Informations- och dataskydd 2 ggr/år.

Kontrollaktivitet - aktuell status	Beskrivning
Ej påbörjad **Uppföljning av att projektet går enligt plan**	

5.2.2 Risk: Oegentligheter

Risknivå

3. Mellan

Riskbeskrivning
Risk för oegentligheter inom följande områden:
- Leverantörer,
- Rekrytering,
- Inhyrning av konsulter (vänskapskorruption - känner en konsult, mutor, jäv)

Konsekvensbeskrivning
Bristande förtroende för förvaltningen.

Existerande kontrollaktiviteter
Riktlinjer för portföljstyrning - jävsbedömning ingår inför uppstart av projekt. Konsultprövning. Rutiner för rekrytering finns, rekryteringsprocessen är dokumenterad och i den framgår det hur jäv ska hanteras i rekryteringsprocessen. Det framgår även hur utvärdering av kandidater ska göras.

Kontrollaktivitet - aktuell status	Beskrivning
Ej påbörjad **Kontroll av efterlevnaden av processerna när det gäller oegentligheter, jäv etc.**	