

# Risikanalyt uppdragsavtal Aktuariefunktionen

Uppdragstagare:	Nordic Actuary
Internt/Externt uppdragsavtal:	Externt
Ny/förnyat uppdragsavtal:	Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

**JA. Kontrollfunktionen blir mer oberoende med extern utövare då bolaget har få anställda och inte kan sysselsätta en aktuarie.**

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?

**JA. Krav på riktlinjer för uppdragets utförande samt samarbete och uppföljning finns i avtalet. Beställansvarig med kontrollansvar finns utsedd.**

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

**JA**

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

**JA**

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signerar av VD.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga

kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Beställansvarig med erforderlig kompetens är utsedd samt godkänd av FI.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets katastrofplan hur detta hanteras vid bortfall av den som innehar funktionen. Bolaget själv har dock inte ngn personal som kan hantera rollen som sådan, utan om bolaget ska hantera funktionen internt krävs en rekrytering av aktuarie.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Det avser en konsulttjänst och årligen fastställer styrelsen hur bortfall av sådan hanteras (i BCP-planen) samt VD uppdaterar löpande kontaktuppgifter till möjlig annan konsult.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**

# Risikanalyt uppdragsavtal GSIT

Uppdragstagare:	TIETO
Internt/Externt uppdragsavtal:	Externt
Ny/förnyat uppdragsavtal:	Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

(Innefattar även EIOPA 20-002) Riktlinje 8

**JA. Bolaget är för litet för att kunna ha en egen IT-avdelning och bygga upp och drifta, utveckla och vidmakthålla egna system och ha redundant funktion. Kostnaden står inte i paritet till nyttan av detta och skulle innebära att kundernas premier blev oskäligt höga. Att upphandla ett system på koncernnivå som även används av andra ger stordriftsfördelar som kommer kunderna till godo i form av ökad säkerhet, mindre kostnader och en effektiv förvaltning.**

De risker som är specifika för ett försäkringssystem via uppdragstagare är att få erforderlig säkerhet för informationen avseende åtkomst (säkerhet, inloggning och möjlighet att utfå information), tillförlitlighet (information inte förvanskas), kontinuitet hos uppdragstagaren, möjlighet till överföring m.m.

Bolaget konstaterar att allt detta regleras i upphandlingen och krav på leverantör samt tjänst inom ramen för LOU. Vidare finns en mycket stor säkerhetsorganisation med såväl dagliga, veckovisa och månadsvis kontroller på olika nivåer.

Det kvarstår alltid en risk att något fallerar, men detta får sättas i paritet till att bolaget inte kan hantera IT effektivt i egen regi. Således får ett visst mått av risktagande balanseras mot uppfyllande av verksamhetens krav att ha ett fungerande IT-stöd som är kostnadseffektivt.

Bolagets verksamhetssystem Insman ligger dock utanför GSIT och verksamheten däri kan fortgå som vanligt.

Riskerna med att ha IT via uppdragsavtal är enligt bolagets sammantagna bedömning, med hänsyn till reglering i upphandling av krav på leverantör och tjänst, väl balanserade. Vad avser kontinuitet, avtalsreglering, m.m. framgår det enligt nedan.

Vidare kan ledning avseende risker hämtas från genomförd informationsklassning och konsekvensbedömning (GDPR).

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?

**JA. Krav på riktlinjer för uppdragets utförande samt samarbete och uppföljning finns i avtalet. Beställaransvarig med kontrollansvar finns utsedd. Organisation för daglig, veckovis och månatliga kontroller finns reglerad.**

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

**JA**

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

**JA**

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signeras av VD eller delegerad inom Stockholm stad vid upphandling.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Beställansvarig med erforderlig kompetens är utsedd.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets IT-Avbrottsplan. Vidare innehåller avtalet med leverantören regler för avveckling, Bilaga 15 till avtalet.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Avtalet med leverantören innehåller dock en säkerhets- och kontrollorganisation som gö regelbundna testerm.m.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal. Vidare finns säkerhetskrav på behörigheter m.m i avtalet.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**

# Risicanalys uppdragsavtal försäkringssystem Insman

Uppdragstagare:	Ifacts
Internt/Externt uppdragsavtal:	Externt
Ny/förnyat uppdragsavtal:	Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

(Innefattar även EIOPA 20-002) Riktlinje 8

**JA. Bolaget är för litet för att kunna ha en egen IT-avdelning och bygga upp och drifta, utveckla och vidmakthålla egna system och ha redundant funktion. Kostnaden står inte i paritet till nyttan av detta och skulle innebära att kundernas premier blev oskäligt höga. Att upphandla ett system som även används av andra ger stordriftsfördelar som kommer kunderna till godo i form av ökad säkerhet, mindre kostnader och en effektiv förvaltning.**

De risker som är specifika för ett försäkringssystem via uppdragstagare är att få erforderlig säkerhet för informationen avseende åtkomst (säkerhet, inloggning och möjlighet att utfå information), tillförlitlighet (information inte förvanskas), kontinuitet hos uppdragstagaren, möjlighet till överföring m.m.

Bolaget konstaterar att allt detta regleras i upphandlingen och krav på leverantör samt tjänst inom ramen för LOU.

Det kvarstår alltid en risk att något fallerar, men detta får sättas i paritet till att bolaget inte kan hantera IT effektivt i egen regi. Således får ett visst mått av risktagande balanseras mot uppfyllande av verksamhetens krav att ha ett fungerande IT-stöd som är kostnadseffektivt.

Den största risken vid bortfall av systemet (kontinuitet) är att rapportering till FI försvåras genom att underlag måste tas fram för hand. Skaderegleringen kan dock fortsätta genom de upphandlade skadekonsulterna enligt försäkringsbrev och tillämpliga villkor. Avtalet reglerar även säkerhet/backup samt deponering av källkod.

Riskerna med att ha ett försäkringssystem via uppdragsavtal är enligt bolagets sammantagna bedömning, med hänsyn till reglering i upphandling av krav på leverantör och tjänst, väl balanserade. Vad avser kontinuitet, avtalsreglering m.m. framgår det enligt nedan.

Vidare kan ledning avseende risker hämtas från genomförd informationsklassning och konsekvensbedömning (GDPR).



2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?

**JA. Krav på riktlinjer för uppdragets utförande samt samarbete och uppföljning finns i avtalet. Beställaransvarig med kontrollansvar finns utsedd.**

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

**JA**

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

**JA**

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signeras av VD.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Beställansvarig med erforderlig kompetens är utsedd.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets IT-Avbrottsplan. Vidare får nytt system upphandlas och under tiden får skadehantering och försäkringsfrågor hanteras manuellt. I avtalet regleras såväl säkerhet/backup som deponering av källkod.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Det avser en IT-tjänst och årligen fastställer styrelsen hur bortfall av sådan hanteras (i IT-avbrottsplanen). Test återläsning sker ibland.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal. Vidare finns säkerhetskrav på behörigheter m.m i avtalet.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**

# Risikanalys uppdragsavtal Internrevisionsfunktionen

Uppdragstagare: Grant Thornton

Internt/Externt uppdragsavtal: Externt

Ny/förnyat uppdragsavtal: Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

**JA. Kontrollfunktionen blir mer oberoende med extern utövare då bolaget har få anställda och inte kan sysselsätta en internrevisor.**

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?

**JA. Krav på riktlinjer för uppdragets utförande samt samarbete och uppföljning finns i avtalet. Beställansvarig med kontrollansvar finns utsedd.**

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

**JA**

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

**JA**

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signeras av VD.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga

kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Beställansvarig med erforderlig kompetens är utsedd samt godkänd av FI.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets katastrofplan hur detta hanteras vid bortfall av den som innehar funktionen. Bolaget själv har dock inte ngn personal som kan hantera rollen som sådan, utan om bolaget ska hantera funktionen internt krävs en rekrytering av internrevisor.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Det avser en konsulttjänst och årligen fastställer styrelsen hur bortfall av sådan hanteras (i BCP-planen) samt VD uppdaterar löpande kontaktuppgifter till möjlig annan konsult.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**

# Risikanalyt uppdraasavtal Regelefterlevnadsfunktionen

Uppdragstagare:	WSA
Internt/Externt uppdraasavtal:	Externt
Ny/förnyat uppdraasavtal:	Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

**JA. Kontrollfunktionen blir mer oberoende med extern utövare då bolaget har få anställda och inte kan sysselsätta en regelefterlevnadsansvarig.**

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?

**JA. Krav på riktlinjer för uppdraas utförande samt samarbete och uppföljning finns i avtalet. Beställansvarig med kontrollansvar finns utsedd.**

3. Är det säkert att den externa uppdraaset inte leder till en materiellt lägre kvalitet av företagens internkontroll eller FI:s möjlighet att övervaka företagens regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

**JA**

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdraas tagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraaset så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

**JA**

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signerar av VD.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga



kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Beställansvarig med erforderlig kompetens är utsedd samt godkänd av FI.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets katastrofplan hur detta hanteras vid bortfall av den som innehar funktionen. Bolaget själv har dock inte ngn personal som kan hantera rollen som sådan, utan om bolaget ska hantera funktionen internt krävs en rekrytering av riskhanteringsansvarig.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Det avser en konsulttjänst och årligen fastställer styrelsen hur bortfall av sådan hanteras (i BCP-planen) samt VD uppdaterar löpande kontaktuppgifter till möjlig annan konsult.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**

# **RIKTLINJER FÖR UPPDRAGSAVTAL I S:T ERIK FÖRSÄKRING AB**

*FASTSTÄLLD AV STYRELSEN 2021-05-21*

## **INNEHÅLLSFÖRTECKNING**

<b>1</b>	<b>ALLMÄNT .....</b>	<b>3</b>
<b>2</b>	<b>SYFTET MED RIKTLINJERNA.....</b>	<b>3</b>
<b>3</b>	<b>ANSVARSFÖRDELNING .....</b>	<b>3</b>
<b>4</b>	<b>KRITISKA ELLER VIKTIGA OPERATIVA FUNKTIONER OCH AKTIVITETER.....</b>	<b>4</b>
<b>5</b>	<b>RISKANALYS.....</b>	<b>5</b>
<b>6</b>	<b>VERKSAMHETER SOM IDAG BEDRIVS PÅ UPPDRAGSAVTAL.....</b>	<b>5</b>
<b>7</b>	<b>MINIMIKRAV SOM SKA VARA UPPFYLLDA FÖR ATT VERKSAMHET SKA FÅ BEDRIVAS AV EXTERN PART GENOM UPPDRAGSAVTAL .....</b>	<b>6</b>
<b>8</b>	<b>UPPDRAGSAVTALETS INNEHÅLL.....</b>	<b>7</b>
<b>9</b>	<b>UPPFÖLJNING .....</b>	<b>8</b>
<b>10</b>	<b>ANMÄLAN TILL FINANSINSPEKTIONEN .....</b>	<b>8</b>
<b>11</b>	<b>DOKUMENTATION.....</b>	<b>9</b>
	<b>BILAGA 1 – RISKANALYS OUTSOURCING, (EX).....</b>	<b>9</b>

## **1 Allmänt**

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler” och har fastställts av styrelsen för S:t Erik Försäkring AB.

Riktlinjerna är föremål för revidering och skall fastställas årligen av styrelsen.

## **2 Syftet med riktlinjerna**

Riktlinjerna har till syfte att reglera vilken typ av verksamhet i bolaget som får läggas ut på uppdragsavtal samt under vilka förutsättningar detta får ske.

Ett uppdragsavtal får inte avse operativ verksamhet eller funktioner som är av väsentlig betydelse, om det kan leda till att:

- kvaliteten i företagsstyrningssystemet försämras väsentligt,
- den operativa risken i företaget ökar väsentligt,
- Finansinspektionens möjlighet att utöva tillsyn försämras, eller,
- försäkringstagarnas möjlighet till tillfredsställelse och fortlöpande service inte kan upprätthållas.

## **3 Ansvarsfördelning**

Styrelsen ansvarar ytterst för den verksamhet som utförs på uppdragsavtal.

Styrelsen ska fastställa huruvida en funktion eller aktivitet är kritisk eller viktig för företagets verksamhet och godkänna att sådan verksamhet får utföras genom uppdragsavtal. Beslutet skall föregås av en riskanalys enligt kap 5.

För uppdragsavtal avseende molntjänster ska EIOPA:s Riktlinjer om uppdragsavtal med molntjänstleverantörer (EIOPA 20-002) riktlinje 1 och 2 beaktas.

VD ansvarar för:

- att bolaget utövar sitt beställaransvar genom att på bolaget utse en ansvarig för den utlagda verksamheten och att ansvarig har tillräckliga kunskaper för att kunna leda och kontrollera tjänstleverantören. Kraven på ansvarig person framgår av bolagets Riktlinjer för lämplighet av styrelse, ledning och nyckelfunktioner.
- att minimikraven för outsourcing i kap 7 är uppfyllda,
- att styrelsen tillställs en riskanalys inför beslut om outsourcing avseende kritiska eller viktiga funktioner,
- att avtal upprättas med extern part i enlighet med LOU (avtal mellan S:t Erik Försäkring och S:t Erik Livförsäkring upprättas av styrelsen i enlighet med gällande firmateckningsrätt)
- att uppföljning sker av den verksamhet som utförs på uppdragsavtal

- att de som utför verksamheten på uppdragsavtal får del av och följer de riktlinjer och policys som antagits av styrelsen
- att godkänna upphandlingsunderlaget och tillställa detta till styrelsen för godkännande avseende kritiska eller viktiga funktioner
- att årligen rapportera utfallet (kontraktsuppföljning) av outsourcad verksamhet till styrelsen.
- att Finansinspektionen informeras om planerad eller förändrad outsourcing och ansvarig person

Av VD delegerad ansvarig person för den outsourcade verksamheten skall, med hänsyn till verksamhetens art och omfattning, löpande, följa upp uppdragstagarens arbete och ska minst årligen genomföra en dokumenterad utvärdering av verksamheten och rapportera den till VD.

Riskhanteringsfunktionen ansvarar för att på verksamhetens begäran bistå verksamheten i riskanalys vid kritiska eller viktiga funktioner.

Regelefterlevnadsfunktionen ansvarar för att på verksamhetens begäran bistå verksamheten i bedömningen av om ett uppdragsavtal, avseende kritiska eller viktiga, funktioner följer gällande regelverk eller inte.

Informationssäkerhetssamordnaren ansvarar för att på verksamhetens begäran bistå verksamheten i bedömningen av om ett uppdragsavtal, särskilt avseende IT system eller molntjänster, följer regelverket för informationssäkerhet och de krav eller åtgärder som erfordras.

#### **4 Kritiska eller viktiga operativa funktioner och aktiviteter**

En funktion eller aktivitet anses vara kritisk eller viktig om den är nödvändig för att bolaget ska kunna tillhandahålla tjänster i bolagets kärnverksamhet åt försäkringstagarna.

Vid en bedömning av om en funktion är kritisk eller viktig kan ledning hämtas från EBA:s riktlinje GL/2019/02.

För uppdragsavtal avseende molntjänster bör ledning hämtas från EIOPAS Riktlinjer om uppdragsavtal med molnleverantör (EIOPA 20-002) riktlinje 7.

Styrelsen har identifierat följande funktioner och aktiviteter som kritiska:

- VD
- aktuariella tjänster,
- IT
- oberoende granskare

- regelefterlevnad
- skadereglering
- försäkringshantering
- riskhantering
- ekonomi

## 5 Riskanalys

Riskanalys skall genomföras av bolaget och, avseende kritiska eller viktiga funktioner, vara ett underlag för styrelsens beslut om outsourcing. Vid förnyad outsourcing ska ny riskanalys genomföras om riskerna har ändrats.

Riskanalysen ska innehålla en beskrivning av:

- funktionen eller aktiviteten som uppdragsavtalet avser,
- beställaransvarig och erforderlig kompetens,
- hur minimikraven nedan säkerställs
- beredskapsplan för att avsluta uppdragsavtalet (skrivs in i bolagets krisplan),
- risken att minimikraven inte uppnås

Riskanalys utförs i enlighet med bilaga 1. För uppdragsavtal avseende molntjänster av kritiskt eller viktig funktion ska även EIOPA 20-002 riktlinje 8 och 9 beaktas.

## 6 Verksamheter som idag bedrivs på uppdragsavtal

Verksamhet som idag bedrivs på uppdragsavtal är:

- aktuariella tjänster,
- IT
- 
- internrevision
- regelefterlevnadsfunktionen
- riskhanteringsfunktionen
- skadereglering
- ekonomi

## **7 Minimikrav som ska vara uppfyllda för att verksamhet ska få bedrivas av extern part genom uppdragsavtal**

För att en verksamhet ska få läggas ut på uppdragsavtal krävs det att:

- tillräcklig beställarkompetens finns inom bolaget för att kunna upphandla och kontrollera den utlagda verksamheten,
- leverantören är ”fit” genom att ha tillräcklig kompetens för att långsiktigt utföra uppdraget med god kvalitet och med väl fungerande internkontroll,
- leverantören är ”proper” genom att kraven på lämplighet i LOU uppfylls,
- bolaget kan styra, följa upp och revidera uppdraget i tillräcklig omfattning,
- det kan säkerställas att gällande sekretesskydd kan vidmakthållas och regler avseende personuppgifter kan följas,
- bolaget och leverantören upprättar och vidmakthåller en beredskapsplan för den aktuella verksamheten i syfte att om möjligt mildra effekterna av oförutsedda händelser, övergång av verksamheten till annan leverantör eller bolaget,
- Finansinspektionens möjlighet att bedriva tillsyn av den aktuella verksamheten vidmakthålls och att uppdragstagaren samarbetar med Finansinspektionen gällande de funktioner eller verksamhet som omfattas av uppdragsavtalet samt på begäran ger Finansinspektionen faktiskt tillträde till dess lokaler,
- bolaget fortsatt kan tillgodose samtliga sina skyldigheter mot sina intressenter inklusive Finansinspektionen och samtliga kunder,
- uppdragstagaren ger försäkringsföretaget, dess revisorer och Finansinspektionen tillgång till uppgifter som rör de funktioner eller verksamhet som omfattas av uppdragsavtalet
- frågor kring jäv och intressekonflikter identifieras och utreds,
- att reglerna om offentlig upphandling följs,
- att gällande rätt följs i övrigt,
- den utlagda verksamheten regleras i ett skriftligt avtal där parternas samtliga rättigheter och skyldigheter regleras,
- kvaliteten i bolagets försäkringsstyrningssystem inte försämras väsentligt,
- den operativa risken i bolaget inte ökar väsentligt,
- försäkringstagarnas möjlighet till tillfredsställande och fortlöpande service kan upprätthållas

- verksamhetens övriga riktlinjer kan följas, särskilt avseende informationssäkerhet och personuppgifter
- För molntjänster av ska även EIOPA 20-002 riktlinje 2,6, 12 och 15 beaktas.

## **8 Uppdragsavtalets innehåll**

I avtal med extern part skall nedanstående punkter regleras. För molntjänster ska även EIOAP 20-002 riktlinje 10-13 och 15 beaktas.

- krav på tjänsten/varan – omfattning
- krav på leverantörens kompetens, kvalité och internkontroll
- avtalsperiod
- kontaktperson hos leverantören som är ansvarig för uppdraget
- partsoberoende (intressekonflikter)- riktlinjer avseende jäv och intressekonflikter och hur dessa kontrolleras
- riktlinjer för styrning, uppföljning och revidering av uppdraget
- ersättning, mervärdesskatt, prisjustering, fakturering och betalningsvillkor
- skatter och avgifter
- underleverantörer
  - samma ansvar som leverantören
  - efter Beställarens godkännande/anmälan till Beställaren
- personal - kompetens, förändringar
- marknadsföring
- rättigheter till material
- rättsintrång
- fel
- försening och brister i tillgänglighet
- sekretess
- information mellan parterna (inkluderar även att bolaget ska kunna ta del av leverantörens resultat om det är väsentligt för bolaget att få uppgift om detta)
- ansvar mellan parterna



- försäkring
- säkerhet
- force majeure
- ändringar och tillägg
- överlåtelse av avtal, rättigheter och skyldigheter
- uppsägning
- tillämplig lag och tvisteföra
- leverantören ska följa bolagets riktlinjer och policys
- personuppgifter
- särskilda kontraktsvillkor, bl a. antidiskrimineringsklausul
- beredskapsplan för oförutsedda händelser och återgång av verksamheten
- leverantörens medverkan vid upphandling och återgång och behjälplighet med eventuell överföring av uppdraget och uppgifter till en ny leverantör
- möjlighet för Beställaren och Finansinspektionen att bedriva tillsyn av den outsourcade verksamheten (detta inkluderar också att Beställarens interna och externa revisorer får tillgång till uppgifter om den utlagda verksamheten)

## 9 Uppföljning

Uppföljning av uppdragsavtal sker riskbaserat utifrån bolagets Instruktion för kontraktsuppföljning.

För molntjänster ska även EIOPA 20-002 riktlinje 11 och 14 beaktas.

## 10 Anmälan till Finansinspektionen

VD eller delegerad ansvarar för att anmälan till Finansinspektionen sker av:

- Ansvarig för verksamheten/funktionen på företaget
- Verksamhet som avser operativ verksamhet eller funktioner av väsentlig betydelse ska anmälas in innan avtalet börjar gälla samt snarast vid förändringar av densamma.

Vid uppdragsavtal som avser väsentliga funktioner ska en ansvarig för funktionen på företaget utses av VD och anmälas till Finansinspektionen.

För molntjänster ska EIOPA 20-002 riktlinje 4 beaktas.

## **11 Dokumentation**

Upphandling och dokumentation sker i bolagets upphandlings/avtalssystem samt under G/2.4 i bolagets databas beroende på typ av avtal.

För molntjänster ska även dokumentation enligt EIOPA 20-002 riktlinje 5 beaktas i tillämpliga delar.

## **Bilaga 1 – Riskanalys outsourcing, (ex)**

Avtal:

#### Intern/extern outsourcing:

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?
2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?
3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?
4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?
5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?
6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?
7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?
8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?
9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?
10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?
11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?
12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?
13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?
14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?
16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?
17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?
18. Innehåller BCP-planen en krisplan som ska testas regelbundet?
19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?
20. Har företaget tillräckliga resurser för att utföra tjänsten ?

# Risakanalys uppdragsavtal Riskhanteringsfunktionen

Uppdragstagare:	FCG
Internt/Externt uppdragsavtal:	Externt
Ny/förnyat uppdragsavtal:	Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

**JA. Kontrollfunktionen blir mer oberoende med extern utövare då bolaget har få anställda och inte kan sysselsätta en riskansvarig tjänst.**

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?

**JA. Krav på riktlinjer för uppdragets utförande samt samarbete och uppföljning finns i avtalet. Beställansvarig med kontrollansvar finns utsedd.**

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

**JA**

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

**JA**

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signerar av VD.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga

kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Fn är det VD.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets katastrofplan hur detta hanteras vid bortfall av den som innehar funktionen. Bolaget själv har dock inte ngn personal som kan hantera rollen som sådan, utan om bolaget ska hantera funktionen internt krävs en rekrytering av riskhanteringsansvarig.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Det avser en konsulttjänst och årligen fastställer styrelsen hur bortfall av sådan hanteras (i BCP-planen) samt VD uppdaterar löpande kontaktuppgifter till möjlig annan konsult.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**

# Risikanalyt uppdragsavtal SIKT

Uppdragstagare:	TIETO
Internt/Externt uppdragsavtal:	Externt
Ny/förnyat uppdragsavtal:	Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

(Innefattar även EIOPA 20-002) Riktlinje 8

**JA. Bolaget är för litet för att kunna ha en egen IT-avdelning och bygga upp och drifta, utveckla och vidmakthålla egna system och ha redundant funktion. Kostnaden står inte i paritet till nyttan av detta och skulle innebära att kundernas premier blev oskäligt höga. Att upphandla ett system på koncernnivå som även används av andra ger stordriftsfördelar som kommer kunderna till godo i form av ökad säkerhet, mindre kostnader och en effektiv förvaltning.**

De risker som är specifika för ett försäkringssystem via uppdragstagare är att få erforderlig säkerhet för informationen avseende åtkomst (säkerhet, inloggning och möjlighet att utfå information), tillförlitlighet (information inte förvanskas), kontinuitet hos uppdragstagaren, möjlighet till överföring m.m.

Bolaget konstaterar att allt detta regleras i upphandlingen och krav på leverantör samt tjänst inom ramen för LOU. Vidare finns en mycket stor säkerhetsorganisation med såväl dagliga, veckovisa och månadsvis kontroller på olika nivåer.

Det kvarstår alltid en risk att något fallerar, men detta får sättas i paritet till att bolaget inte kan hantera IT effektivt i egen regi. Således får ett visst mått av risktagande balanseras mot uppfyllande av verksamhetens krav att ha ett fungerande IT-stöd som är kostnadseffektivt.

Bolagets verksamhetssystem Insman ligger dock utanför GSIT och verksamheten däri kan fortgå som vanligt.

Riskerna med att ha IT via uppdragsavtal är enligt bolagets sammantagna bedömning, med hänsyn till reglering i upphandling av krav på leverantör och tjänst, väl balanserade. Vad avser kontinuitet, avtalsreglering, m.m. framgår det enligt nedan.

Vidare kan ledning avseende risker hämtas från genomförd informationsklassning och konsekvensbedömning (GDPR).

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?



**JA. Krav på riktlinjer för uppdragets utförande samt samarbete och uppföljning finns i avtalet. Beställaransvarig med kontrollansvar finns utsedd. Organisation för daglig, veckovis och månatliga kontroller finns reglerad.**

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

**JA**

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

**JA**

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signeras av VD eller delegerad inom Stockholm stad vid upphandling.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Beställansvarig med erforderlig kompetens är utsedd.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets IT-Avbrottsplan. Vidare innehåller avtalet med leverantören regler för avveckling, Bilaga 15 till avtalet.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Avtalet med leverantören innehåller dock en säkerhets- och kontrollorganisation som gö regelbundna testerm.m.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal. Vidare finns säkerhetskrav på behörigheter m.m i avtalet.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**

# Risikanalyt uppdraagsavtal Skadereglering

Uppdragstagare:	Crawford
Internt/Externt uppdraagsavtal:	Externt
Ny/förnyat uppdraagsavtal:	Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

**JA. Med det mindre antal skador som bolaget har kan inte en egen skadeorganisation med tillräcklig kompetens och redundans byggas upp som är ekonomiskt försvarbart.**

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?

**JA. Krav på riktlinjer för uppdragets utförande samt samarbete och uppföljning finns i avtalet. Beställansvarig med kontrollansvar finns utsedd.**

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

JA

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

JA

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signeras av VD.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga

kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Fn är det VD.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets katastrofplan hur detta hanteras vid bortfall av den som innehar funktionen. Bolaget själv har dock inte ngn personal som kan hantera rollen som sådan, utan om bolaget ska hantera funktionen internt krävs rekrytering av ett antal skadereglerare, som dock inte kan sysselsättas.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Det avser en konsulttjänst och årligen fastställer styrelsen hur bortfall av sådan hanteras (i BCP-planen) samt VD uppdaterar löpande kontaktuppgifter till möjlig annan konsult.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**

# Risikanalyt uppdraagsavtal Skadereglering

Uppdragstagarare:	Sedgwick
Internt/Externt uppdraagsavtal:	Externt
Ny/förnyat uppdraagsavtal:	Förnyat (tidigare upphandling löpt ut)

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

**JA. Med det mindre antal skador som bolaget har kan inte en egen skadeorganisation med tillräcklig kompetens och redundans byggas upp som är ekonomiskt försvarbart.**

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagarare) utförs under övervakade och säkra omständigheter?

**JA. Krav på riktlinjer för uppdragets utförande samt samarbete och uppföljning finns i avtalet. Beställansvarig med kontrollansvar finns utsedd.**

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

**JA. Krav på samarbete och uppföljning finns i avtalet, likväl som krav på tillgänglighet för FI att granska leverantören.**

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

N/A

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagarare dokumenterade i ett skriftligt avtal?

JA

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

**JA. Krav på tillgänglighet, uppföljning ansvar vid fel m.m. finns reglerat i avtalet.**

7. Specificerar avtalet att om uppdraagsagararen skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

JA

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

**JA**

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

**JA. Enligt riktlinjerna beslutar styrelsen om vilken verksamhet (verksamhetskritisk) som får hanteras via uppdragsavtal. Avtalen upphandlas och signerar av VD.**

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

**JA. Avtalet innehåller krav på samarbete från leverantörens sida vid ny upphandling eller om bolaget själv bestämmer sig för att överta funktionen.**

11. Säkerhetställer SLA-villkoren att uppdragstagaren samarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

**JA**

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

**JA. Kravställt i upphandlingen och redovisat vid anbudsgivande.**

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviteter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

**JA**

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

**JA. I tillämpliga delar, ex tillgänglighet, uppföljning m.m.**

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

**JA. Avtalet innehåller reglering av vad som avses vara fel, avtalsbrott m.m. samt vilka åtgärder som då kan vidtas.**

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga



kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

**JA. Fn är det VD.**

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

**JA. Framgår av bolagets katastrofplan hur detta hanteras vid bortfall av den som innehar funktionen. Bolaget själv har dock inte ngn personal som kan hantera rollen som sådan, utan om bolaget ska hantera funktionen internt krävs rekrytering av ett antal skadereglerare, som dock inte kan sysselsättas.**

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

**Nej. Det avser en konsulttjänst och årligen fastställer styrelsen hur bortfall av sådan hanteras (i BCP-planen) samt VD uppdaterar löpande kontaktuppgifter till möjlig annan konsult.**

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

**JA. Sekretessklausul finns i avtalet, likaså reglering av personuppgiftsbehandling. Om sådan sker upprättas även personuppgiftsbiträdesavtal.**

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

**JA. Kravställs i upphandlingsunderlaget.**