IKT-utkontraktering

Dokumentation inför beslut om avtalstecknande.

Organisation	Försäkrings AB Göta Lejon
Ärendenummer	
Leverantör (föreslagen)	
IKT-tjänst	
Avtalsansvarig	
Dokumentansvarig	
Version	1.0
Datum för upprättande	
Status	[ ] Utkast [ ] Under granskning [ ] Godkänd

Detta dokument är det samlade beslutsunderlaget och dokumentationspaketet för en enskild IKT-utkontraktering, i enlighet med DORA artiklarna 28–30 och tillhörande tekniska standarder. Fyll i varje avsnitt i tur och ordning och bifoga eventuella underlagsrapporter.

1. Steg 1. Behovsbeskrivning och första klassificering

Processägare / Avtalsansvarig i samverkan med IT-strateg

1.1. Beskrivning av behov

Beskriv varför denna IKT-tjänst behövs, vilka processer den stödjer, vilka användare som är berörda internt och externt och vilka beroenden som finns.

[Fritext]

1.2. Extern IKT-tredjepartsleverantör?

☐ Lösningen innebär användning av ny extern IKT-tredjepartsleverantör (inkl. moln, SaaS, PaaS, IaaS, drift, support)

☐ Tjänst finns via Intraservice men anses ej möta behov (motivera nedan)

☐ Behovet avser ny tjänst hos befintlig leverantör

Motivering varför intern lösning inte anses möta behov	

1.3. Preliminär bedömning om kritisk/viktig funktion enligt Dora

☐ Potentiellt – tjänsten kan stödja en kritisk eller viktig funktion

☐ Tjänsten bedöms ej stödja en kritisk eller viktig funktion - motivera nedan

Motivering ej kritisk/viktig funktion	

1.4. Godkännande – steg 1

Funktion	Namn	Datum
IT-strateg		

2. Steg 2 – Fortsatt bedömning av funktion och IKT-tjänst

Processägare i samverkan med riskansvarig och/eller avtalsansvarig, regelefterlevnad och IT-strateg.

2.1. Beskrivning av process och beroenden

Beskriv berörd process, delprocesser, system, leverantörer och informationsflöden.

[Fritext]

2.2. Bedömningskriterier kritisk/viktig funktion

☐Ja ☐Nej Materiell påverkan på finansiell ställning vid avbrott/fel

☐Ja ☐Nej Risk att bolaget inte kan uppfylla tillstånds- eller regelkrav

☐Ja ☐Nej Risk för betydande påverkan på tjänsters kontinuitet, kunder eller marknad

2.3. Klassificiering och motivering

☐ Klassificeras som: Kritisk eller viktig funktion

☐ Klassificeras som: Ej kritisk/viktig funktion

Motivering till klassificering	

2.4. Godkännande – steg 2

Funktion	Namn	Datum
Riskansvarig		

3. Steg 3 – Samråd med regelefterlevnadsfunktion

Bolagscontroller i samråd med regelefterlevnadsfunktion.

3.1. Tillämplig lagstiftning

☐ Solvens II

☐ FAL

☐ GDPR

☐ Annan (specificera nedan)

Specificera annan lagstiftning	

3.2. Begränsningar och tillstånd

☐ Tillsynsmyndighet (t.ex. FI) behöver informeras

☐ Förhandsgodkännande från tillsynsmyndighet krävs

☐ Inga regulatoriska hinder identifierade

Regulatoriska villkor och kommentarer	

3.3. Godkännande – steg 3

Funktion	Namn	Datum
Riskansvarig		

4. Steg 4 – Riskanalys

Processägare/avtalsansvarig samråd med säkerhetschef och IT-strateg.

4.1. Informationsklassning

☐ Informationsklassning genomförd och relevant

☐ Förnyad informationsklassning behöver genomföras

Referens till genomförd klassning	

4.2. Riskanalys

☐ Riskanalys genomförd och relevant

☐ Förnyad riskanalys behöver genomföras

Referens till genomförd riskanalys	

4.3. Bedömning av koncentrationsrisk

☐ Flera kritiska/viktiga tjänster förläggs hos samma leverantör

☐ Leverantören bedöms som svår att ersätta (”not easily substitutable”)

☐ Långa/komplexa underleverantörskedjor, särskilt i tredjeland

☐ Ingen väsentlig koncentrationsrisk identifierad

Sammanfattande bedömning av koncentrationsrisk samt ev åtgärder	

4.4. Godkännande – steg 4

Funktion	Namn	Datum
Riskansvarig		

5. Steg 5 – Due diligence och lämplighetsbedömning av leverantör

Aspekt	Kontroll	Motivering/referens till underlag
Finansiell stabilitet	[ ] Kreditrating eller annan extern bedömning kontrollerad	
Status informationssäkerhet och cybersäkerhet	[ ] Krav i KLASSA använd [ ] Annan kravställning (motivera)	

5.1. Samlad bedömning av due diligence

☐ Accepterad

☐ Accepterad med villkor (specificera nedan)

☐ Ej accepterad

Villkor/motivering	

5.2. Godkännande – steg 5

Funktion	Namn	Datum
IT-strateg		
Säkerhetschef		

6. Steg 6 – Bedömning av intressekonflikter

6.1. Identifierade intressekonflikter

☐ Leverantören har dubbla roller

☐ Oberoende mellan försvarslinjer kan ifrågasättas

☐ Tillhandahållandet av tjänsten kan skapa nya risker

☐ Annan intressekonflikt identifierad (specificera nedan)

☐ Ingen intressekonflikt identifierad

Annan intressekonflikt	

6.2. Motåtgärder och kontroller

Föreslagen kontroll och motåtgärd	

6.3. Godkännande – steg 6

Funktion	Namn	Datum
Bolagscontroller		

7. Steg 7 - Framtagning av avtalsutkast

7.1. Användning av mallar och checklistor

☐ Avtalsmall för Dora-tillägg har använts

7.2. Godkännande – steg 7

Avtalsutkast godkänns av vd.

Funktion	Namn	Datum
VD		

8. Steg 8 – Exitstrategi och kontinuitetsplanering

Detta steg omfattar endast leverantörsavtal som omfattar IKT-tjänster som stödjer kritiskt/viktiga funktioner.

8.1. Exitstrategi

Alternativa lösningar (intern lösning/annan leverantör)	
Tidslinje och aktiviteter vid övergång	
Hur exitstrategin återspeglas i avtalsvillkor	

8.2. Koppling till kontinuitetsarbete

BIA(RTO/RPO) är identifierat och återspeglas i kontinuitetsplan	
Testplan för utträde (när testas, omfattning, frekvens)	

8.3. Godkännande – steg 7

Funktion	Namn	Datum
Ledning		

9. Steg 9 – Samlat beslutsunderlag

9.1. Förteckning av ingående delar i beslutsunderlag

☐ Steg 1 – behovsbeskrivning och första klassificiering

☐ Steg 2 – fortsatt bedömning av funktion och IKT-tjänst

☐ Steg 3 – samråd med regelefterlevnadsfunktion

☐ Steg 4 - Riskanalys inkl koncentrationsrisk

☐ Steg 5 – Due diligence och lämplighetsbedömning

☐ Steg 6 – Bedömning av intressekonflikter

☐ Steg 7 – Avtalsutkast

☐ Steg 8 – Exitstrategi och kontinuitetsplanering (om kritisk/viktig funktion)

9.2. Rekommendation

☐ Godkänn

☐ Avslå

☐ Godkänna med villkor (lista villkor nedan)

Villkor för godkännande	

9.3. Beslutsform och protokoll

Beslutsform	
Datum för beslutsmöte	
Referens	

10. Steg 10 – Förberedelse av uppdatering av register över IKT-tredjepartsleverantörer

10.1. Genomgång av registeruppgifter

- ☐ Förteckning över nödvändiga registeruppgifter genomgången mellan IT-strateg, processägare/avtalsansvarig och bolagscontroller