



Dokumentnamn: Försäkrings AB Göta Lejon rutin för utkontraktering av tjänster

Beslutad av:
VD

Gäller för:
Försäkrings AB Göta Lejon

Diarienummer:

**Datum och paragraf för
beslutet:**

[Text]

Dokumentsort:
Rutin

Giltighetstid:
Tills vidare

Senast reviderad:
2026-03-11

Dokumentansvarig:
Säkerhetschef

Bilagor:

Bilaga 1: Checklista

Bilaga 2: Definition av leverantörer av IKT-tjänster

Bilaga 3: Dokumentationsmall

Försäkrings AB Göta Lejon rutin för utkontraktering av tjänster

Enligt Göta Lejons strategi för säkerhet grundar sig på den befintliga riskstrategin inom bolagets riskhanteringssystem vilket är att öka sannolikheten för att bolaget ska uppnå de strategiska målen. Säkerhetsstrategin fastställer en strukturerad och långsiktig inriktning för hur organisationen ska skydda sina tillgångar, säkerställa verksamhetens kontinuitet och bygga en motståndskraftig säkerhetskultur. Effekter av oönskade och oväntade händelser ska minimeras. Säkerhetsstrategin utgör även bolagets IKT-strategi. Säkerhetsstrategin strategi gäller all verksamhet bolaget bedriver, oavsett om den utförs internt eller av extern part. Strategin ska alltid beaktas, oavsett om det gäller verksamhetsplanering, organisations- och verksamhetsutveckling, dagligt arbete eller system och tjänster.

Bolagets rutin för utkontraktering av tjänster tydliggör hur Göta Lejons strategi för IKT-tredjepartsrisk ska genomföras.

Rutinen har upprättats i enlighet med

- DORA Artikel 28-30
- RTS 2024/1773
- EBA riktlinjer för utkontraktering (EBA/GL/2019/02)
- Kommissionens delegerade förordning (EU) 2024/1774 (RTS om IKT-riskhanteringsverktyg, metoder och processer)

Syftet med denna rutin

Denna rutin utgör bolagets arbetsgång inför utkontraktering av tjänster.

Rutinen ska följas inför samtliga upphandlingar och inköp, inkl nytt införande eller byte av tjänst hos befintlig leverantör.

Vem omfattas av rutinen

Denna rutin gäller tills vidare för Försäkrings AB Göta Lejon.

Rutinen omfattar alla kontraktsförslag. Hela rutinen ska följas där en IKT-tredjepartsleverantör ska tillhandahålla en IKT-tjänst som stödjer någon del av verksamheten (avsett om funktionen bedöms som kritisk/viktig eller inte). Rutinen avbryts efter första steget om detta resulterar i att en IKT-tjänst inte kommer att tillhandahållas.

Koppling till andra styrande dokument

- Försäkrings AB Göta Lejons riktlinje för riskhantering och intern styrning och kontroll
- Försäkrings AB Göta Lejons riktlinje för säkerhet

Stödjande dokument

- Göta Lejons förteckning över bolagets leverantörer, tjänster och kritikalitetsbedömning

Rutin

Följande steg ska gås igenom inför utkontraktering av tjänster.

Steg 1. Behovsbeskrivning och första klassificering

Syfte: Att beskriva behov och göra en första bedömning om den planerade lösningen medför tillhandahållande av en IKT-tjänst av en tredjepartsleverantör.

Ansvarig funktion: Processägare och/eller avtalsansvarig ansvarar för att genomföra steget. Samverkan ska ske med IT-strateg.

Aktiviteter

- a) Beskriv behovet (syfte, process, berörda användare internt och externt, beroenden)
- b) Identifiera om lösningen innebär användning av extern IKT-tredjepartsleverantörer. Använd förteckning i Bilaga 2 som hjälp i denna bedömning
- c) Kontrollera mot befintliga interna lösningar – kan behovet lösas internt via befintliga tjänster?
- d) Gör en första bedömning om tjänsten kan komma att stödja en kritisk eller viktig funktion enligt Dora, dvs kan avbrott i tjänsten ha väsentlig påverkan på bolagets finansiella ställning, regelefterlevnad eller kontinuitet?
- e) Dokumentera om ärendet ska klassas som kritisk/viktig eller icke kritisk/viktig funktion

Om ovanstående behovsbeskrivning resulterar i att lösningen **inte** innebär användning av extern IKT-tredjepartsleverantör avslutas processen efter detta steg. Denna bedömning ska motiveras och dokumenteras (se nedan). Fortsatt arbete utförs i enlighet med process för inköp/upphandling. Om leverantören utgör utlagd verksamhet ska bolagets styrande dokument för uppdragsavtal och utlagd verksamhet följas.

Dokumentation

Kort beskrivning innehållande

- Beskrivning av behov och omfattning
- Beskrivning av föreslagen IKT-tjänst, alt varför tjänsten inte utgör IKT-tjänst
- Preliminär bedömning av kritisk/viktig eller icke kritisk/viktig funktion

Godkännande

Steget godkänns av IT-strateg, resultatet levereras till Riskansvarig.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 3 (definitioner), artikel 5 (styrning och organisation), artikel 6 och 8 (identifikation, klassificering och dokumentation av IKT-stödda funktioner och IKT-tillgångar)
- EBA riktlinjer för utkontraktering (EBA/GL/2019/02)

Steg 2 – Fortsatt bedömning av funktion och IKT-tjänst

Om den tjänst som ska utkontrakteras är en befintlig tjänst ska det avgöras om den tidigare genomförda bedömningen ska ändras eller kvarstå.

Syfte: Att avgöra om den berörda funktionen är kritisk eller viktig enligt Dora och därmed omfattas av skärpta krav.

Ansvarig funktion: Processägare. Samråd ska ske med riskansvarig och/eller avtalsansvarig, säkerhetschef, regelefterlevnad och IT-strateg.

Aktiviteter

- a) Kartlägg berörd process, ingående delprocesser och beroenden till andra system, leverantörer, informationsflöden.
- b) Gör en bedömning avseende kritisk/viktig funktion baserat på följande:
 - Påverkan på finansiell ställning vid avbrott eller fel
 - Risk för att avbrott eller fel medför att bolaget inte kan uppfylla tillstånds- eller regelkrav
 - Risk för att avbrott eller fel får betydande påverkan på bolagets kontinuitet i leverans mot kund
- c) Dokumentera motivering till klassificering av kritiskt/viktig funktion eller ej kritisk/viktig funktion
- d) Säkerställ att dokumentationen följer Göta Lejons förteckning över bolagets leverantörer, tjänster och kritikalitetsbedömning

Dokumentation

Protokoll över klassificering, inkl motivering och rekommendation till beslut.

Godkännande

Steget godkänns av Riskansvarig i samråd med IT-strateg och säkerhetschef.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 8:1, 8:5 (krav på identifikation, klassificering och dokumentation av funktioner, tillgångar och processer, inkl beroenden till IKT-tredjepartsleverantörer)
- Dora artikel 24:4a (krav på att bedöma om kontraktuellt arrangeman avser IKT-tjänster som stödjer kritisk eller viktig funktion innan avtal)
- Kommissionens delegerade förordning (EU) 2024/1774 (RTS om IKT-riskhanteringsverktyg, metoder och processer)

Steg 3 Samråd med regelefterlevnadsfunktion

Syfte: Att säkerställa att inga regelverk hindrar eller begränsar utkontrakteringen samt att identifiera eventuella krav som behöver beaktas inför upphandling och avtalsskrivning.

Ansvarig funktion: Bolagscontroller i samråd med regelefterlevnad.

Aktiviteter

- a) Identifiera vilken lagstiftning som tillämpas för den specifika funktionen som ska utkontrakteras (t ex Solvens II, FAL, GDPR)
- b) Kontrollera om funktionen omfattas av särskilda begränsningar för utkontraktering relaterat till Solvens II eller annat relevant regelverk
- c) Bedöm om det kan finnas hinder i att uppfylla tillsynsvillkor
- d) Bedöm om anmälan behöver göras till Finansinspektionen
- e) Dokumentera slutsatser och eventuella regulatoriska villkor såsom krav på avtalstexter, rapporteringsskyldigheter eller geografiska begränsningar

Dokumentation

Samråd med regelefterlevnadsfunktionen, som biläggs beslutsunderlaget.

Godkännande

Steget godkänns av Riskansvarig i samråd med IT-strateg och säkerhetschef.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 28:4b (krav att bedöma om tillsynsvillkor för utkontraktering är uppfyllda)
- Dora artikel 5 (ledningens ansvar att godkänna alla IKT-arrangemang)
- **RTS**

Kommenterad [PW1]: Ev ytterligare krav?

Steg 4 Riskanalys av den planerade IKT-utkontrakteringen (inkl koncentrationsrisk)

Syfte: Att identifiera och bedöma samtliga relevanta risker kopplade till det föreslagna kontraktuella arrangemanget, inkl IKT-risker, regelefterlevnadsrisker och IKT-koncentrationsrisk

Ansvarig funktion: Processägare och/eller avtalsansvarig i samarbete med säkerhetschef och IT-strateg. Om funktionen är en kritisk/viktig funktion ska även riskansvarig delta.

Aktiviteter

- a) Finns det genomförd informationsklassning som riskanalysen kan utgå från? Om inte genomför klassning enligt separat informationsklassning. Beakta särskilt om den planerade utkontrakteringen medför att nya, ännu ej klassade, informationsmängder kommer att produceras.
- b) Identifiera risker för konfidentialitet, riktighet och tillgänglighet enligt anvisning för riskhantering.
- c) Bedöm IKT-koncentrationsrisk avseende:
 - Kan det kommande avtalet medföra att Göta Lejon förlägger flera kritiska/viktiga tjänster hos samma leverantör?
 - Är leverantören svår att ersätta?
 - Finns långa underleverantörskedjor, särskilt i tredjeland?

Dokumentation

Riskanalys över utkontrakteringen.

Godkännande

Riskansvarig. Om utkontrakteringen avser kritisk/viktig funktion ska rapport presenteras för och godkännas av ledning.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 28:4c (identifiera och bedöma alla relevanta risker inklusive IKT-koncentrationsrisk)
- Dora artikel 29 (Preliminär bedömning av IKT-koncentrationsrisk, utbytbart och underleverantörskedjor)
- Dora artikel 8 (identifikation av IKT-tillgångar och beroenden)
- Kommissionens delegerade förordning (EU) 2024/1774 (RTS om IKT-riskhanteringsverktyg, metoder och processer)

Steg 5 Due diligence och lämplighetsbedömning av IKT-tredjepartsleverantör

Syfte: Att säkerställa att den kommande leverantören är lämplig, finansiellt stabil och uppfyller relevanta informationssäkerhets- och kontinuitetskrav innan avtal tecknas.

Ansvarig funktion: Säkerhetschef i samråd med inköpsansvarig, IT-strateg och riskansvarig

Aktiviteter

Om utkontrakteringen innebär köp på ramavtal ska nedanstående aktiviteter genomföras innan avrop görs. Om utkontrakteringen innebär en upphandling ingår nedanstående aktiviteter i arbetet med kravspecifikationen.

- a) Bedöm (vid avrop) eller kravställ leverantörens finansiella ställning och långsiktiga stabilitet.
- b) Bedöm (vid avrop) eller kravställ leverantörens status inom informations- och cybersäkerhet. Som underlag kan kravkatalog via KLASSA användas.
- c) Säkerställ att utfallet av kravställningen dokumenteras och bevaras. En samlad bedömning enligt accepterad /ej accepterad /accepterad med villkor ska finnas tillsammans med anbudsutvärdering

Dokumentation

Dokumenterad bedömning av kravställning. Detta kan vara en kravspecifikation ifylld av leverantören tillsammans med samlad bedömning enligt accepterad /ej accepterad /accepterad med villkor. Dokumentationen diarieförs tillsammans med avtalet.

Godkännande

IT-strateg godkänner säkerhetsdelen av upphandlingsunderlag. Säkerhetschef godkänner övergripande lämplighetsbedömning som del av beslutsunderlaget.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 28:4d (genomföra due diligence-granskning av potentiella tredjepartsleverantörer av IKT-tjänster)
- Dora artikel 28:5 (Endast ingå avtal med leverantörer som uppfyller lämpliga standarder för informationssäkerhet)
- EBA riktlinjer för utkontraktering (EBA/GL/2019/02)

Steg 6 Bedömning av intressekonflikter

Syfte: Att identifiera och hantera potentiella intressekonflikter relaterade till den föreslagna utkontrakteringen.

Ansvarig funktion: Bolagscontroller i samråd med regelförfarandefunktionen

Aktiviteter

- a) Identifiera potentiella intressekonflikter, t ex om leverantören har dubbla roller eller om tillhandahållandet av tjänsten kan skapa nya risker.
- b) Bedöm om intressekonflikterna kan hanteras genom avtal, styrning, organisatoriska åtgärder eller andra kontroller
- c) Dokumentera bedömningen, identifierade konflikter och föreslagna motåtgärder

Dokumentation

Bedömning av intressekonflikter, som bilaga till beslutsunderlag/dokumentation.

Godkännande

Bolagscontroller bekräftar att intressekonflikter är identifierade och hanterade på ett acceptabelt sätt.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 28:4e (krav att identifiera och bedöma intressekonflikter som utkontraktering kan orsaka)
- Dora artikel 28:5 (Endast ingå avtal med leverantörer som uppfyller lämpliga standarder för informationssäkerhet)
- EBA riktlinjer för utkontraktering (EBA/GL/2019/02)

Steg 7 Framtagning av avtalsutkast

Syfte: Att ta fram avtalsutkast som innehåller samtliga Dora-krav.

Ansvarig funktion: Processägare/avtalsansvarig, vid behov i samråd med riskansvarig och/eller IT-strateg

Aktiviteter

- a) Upprätta avtals- och SLA-förslag i enlighet med Göta Lejons avtalsmall för Dora-tillägg.

Dokumentation

Avtalsutkast, förslag till SLA samt eventuella ytterligare bilagor.

Godkännande

Avtalsutkast godkänns av Vd.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 30.

Steg 8 Strategi för utträde och kontinuitetsplanering

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

Syfte: Att säkerställa att Göta Lejon kan lämna avtalet utan oacceptabel störning och upprätta verksamhetens kontinuitet vid leverantörsproblem eller avslut.

Ansvarig funktion: Processägare/avtalsansvarig i samråd med riskansvarig och regelefterlevnad.

Aktiviteter

- a) Utforma utträdesstrategi för IKT-tjänster som stödjer kritiskt/viktiga funktioner
 - Undersök möjlighet till alternativa lösningar (intern lösning/annan leverantör)
 - Se över tidslinje och aktiviteter vid övergång
- b) Säkerställ att utträdesstrategin återspeglas i avtalsvillkoren
- c) Koppla utträdesstrategin till bolagets kontinuitetsarbete
- d) Dokumentera testplan för utträdesstrategin

Dokumentation

Skriftlig utträdesstrategi.

Godkännande

Godkänns av ledning.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 28:7-8 (krav på att kunna säga upp avtal samt ha dokumenterade exitstrategier).
- Dora artikel 11 (krav på kontinuitet)

Steg 9 Samlat beslutsunderlag och beslutsprocess

Syfte: Att säkerställa att bolagets ledning fattar beslut på ett korrekt, dokumenterat och spårbart underlag, i linje med Doras krav på styrning, ansvar och strategi för tredjepartsrisk.

Ansvarig funktion: Processägare/avtalsansvarig

Aktiviteter

- a) Sammanställ beslutsunderlag bestående av steg 1-8 ovan.
- b) Förbered beslutsmening utifrån alternativen Godkänn/Avslå/Godkänn med villkor.

Dokumentation

- Samlat beslutsunderlag.
- Protokoll från beslut.

Godkännande

All utkontraktering som omfattar IKT-tjänster beslutas av vd.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 5 (ledningens ansvar för IKT-risk)
- Dora artikel 6 (IKT-riskhanteringsram)
- Dora artikel 28:2 (Strategi för IKT-tredjepartsrisk)

Steg 10 Förberedelse av uppdatering av register över IKT-tredjepartsleverantörer

Uppdatering av register sker efter avtalstecknande. All information måste dock vara framtagen före beslut.

Syfte: Att säkerställa att all information som krävs enligt Dora för registret över IKT-tredjepartsleverantörer finns framme och är kvalitetssäkrad innan avtal tecknas, samt att all dokumentation är komplett för intern och extern granskning.

Ansvarig funktion: IT-strateg i samråd med Processägare/avtalsansvarig och bolagscontroller.

Aktiviteter

- a) Uppdatera register över leverantörer i enlighet med instruktion.

Dokumentation

Uppdaterat register över leverantörer.

Godkännande

IT-strateg godkänner register.

Referenser till Dora-artikel/teknisk standard

- Dora artikel 28:3, 9 (krav på register över kontraktmässiga arrangemang)

Bilaga 1 - Checklista

1. Är funktionen och IKT-tjänsten korrekt klassificerad och dokumenterad (steg 1-2)?
2. Är alla relevanta lagkrav och tillsynsvillkor identifierade (steg 3)?
3. Finns en dokumenterad riskanalys inkl koncentrationsrisk (steg 4)?
4. Är due diligence på leverantören komplett och dokumenterad (steg 5)?
5. Har intressekonflikter identifierats och hanterats (steg 6)?
6. Har rätt avtalsmall använts (steg 7)?
7. Om kritisk/viktig funktion – finns strategi för utträde (steg 8)?
8. Har ledning fått komplett beslutsunderlag och fattat beslut (steg 9)?
9. Är alla uppgifter klara för uppdatering av register över IKT-tredjepartsleverantörer (steg 10)?

Bilaga 2 - Definition av leverantörer av IKT-tjänster

Alla företag som tillhandahåller IKT-tjänster, inklusive:

- Molntjänstleverantörer: IaaS, PaaS, SaaS (AWS, Azure, Google Cloud, etc.)
- Hosting: Datacenter, colocation, managed hosting
- Säkerhet: Antivirus, brandvägg, SIEM, SOC
- Programvara som tjänst: Core banking, CRM, ERP, analys
- Nätverk: Uppkoppling, telekommunikation, CDN
- Betalningar: Processorer, acquirers, gateways
- Support och underhåll: IT-tjänster, applikationssupport
- Backup och DRP: Backup- och återställningslösningar