FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Appendix G – Kontinuitetshantering för outsourcad verksamhet

Version 3.0
FSPOS AG KON, Fokusgrupp Kontinuitetshantering

Dokumenthistorik

Utgåva	Datum	Kommentar
1.0	2014-09-18	Första utgåva Appendix G – Kontinuitetshantering för outsourcad verksamhet publiceras i FSPOS Vägledning för kontinuitetshantering
2.0	2015-09-23	Utökad version av Appendix G – Kontinuitetshantering för outsourcad verksamhet
3.0	2017-01-24	Mindre justeringar av Appendix G – Kontinuitetshantering för outsourcad verksamhet

Sammanfattning

Under 2013 utvecklade FSPOS arbetsgrupp för Kontinuitetssäkring[1] en vägledning om kontinuitetshantering för aktörer i den finansiella sektorn. Vägledningen har sedan dess kompletterats i omgångar utifrån sektorns och de finansiella aktörernas behov. *FSPOS Vägledning för Kontinuitetshantering* inkluderar ett antal appendix, bland annat ett som beskriver hur en organisation kan arbeta med kontinuitetshantering i utlagda tjänster och processer (så kallad outsourcad verksamhet). Detta dokument består av innehållet i *Appendix G – Kontinuitetshantering för outsourcad verksamhet* samt ett självskattningsformulär gällande kontinuitetshantering för outsourcad verksamhet (avsnitt H.8. i *FSPOS Vägledning för Kontinuitetshantering*).

Kontinuitetshantering handlar om att säkerställa att en organisations kritiska verksamhet kan fungera på en tolerabel nivå, oavsett vilka störningar som inträffar. I flera fall omfattar den kritiska verksamheten även verksamhet som outsourcats till en leverantör. Beställaren, med ansvar för kontinuitetshanteringen av dess samlade verksamhet, måste därför samarbeta med sina leverantörer för att säkerställa kontinuitetshantering även för den outsourcade verksamheten.

Appendixet riktar sig till samtliga som är involverade i processen för kontinuitetshantering för outsourcad verksamhet och därmed till såväl verksamhetsansvariga, säkerhetsansvariga, kontinuitetsansvariga som beslutsfattare och ledningsfunktioner. Underlaget kan även användas för att skapa en ökad medvetenhet internt i den egna organisationen om kontinuitetshantering i samband med beslut om outsourcing av verksamhet.

Appendixet bygger på intervjuer med aktörer inom finansiell sektor och på internationella standarder. Dokumentet betraktar outsourcing utifrån ett livscykelperspektiv, där den outsourcade verksamheten bör följas från dess att beslut om outsourcing fattas till att avtalet avvecklas. Appendixet kompletteras även med en checklista som kan användas som operativt stöd i de olika livscykelfaserna.

[1] *FSPOS består av tre arbetsgrupper; AG Kontinuitetssäkring, AG Övning och AG Information.*

Innehållsförteckning

G.1. Kontinuitetshantering och outsourcing

Kontinuitetshantering handlar om att säkerställa att en organisations kritiska verksamhet kan fungera på en tolerabel nivå, oavsett vilka störningar som inträffar. I vissa fall är hela eller delar av den kritiska verksamheten utlagd till externa leverantörer (outsourcing). Organisationen ansvarar dock fortfarande för kontinuitet i verksamheten och måste därmed arbeta med kontinuitetshantering såväl för den interna som för den outsourcade verksamheten.

Outsourcinglösningar blir alltmer förekommande ur ett internationellt och sektorsövergripande perspektiv[2]. I Sverige finns ingen detaljerad reglering av outsourcad verksamhet för privata finansiella aktörer. Regleringen utgår istället ifrån en principnivå genom ett angivet ramverk i form av föreskrifter som fastställer ett antal skall-krav, medan det är upp till de enskilda aktörerna att på egen hand svara för *hur* kraven efterlevs. Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut[3] fastställer övergripande krav för utlagd verksamhet och ställer bland annat höga krav på den kompetens som ska finnas kvar inom organisationen. Ansvaret kan på så sätt aldrig flyttas ut från organisationen utan

Detta appendix har genomgående hämtat inspiration från internationella standarder[4], Solvens II[5], Basel[6] och Finansinspektionens föreskrifter FFFS 2014:1[7]. Appendixet fokuserar på outsourcing ur ett kontinuitetsperspektiv. På så sätt finns varken en ambition att ge en heltäckande bild av outsourcing som företeelse eller att beakta andra outsourcingaspekter vid sidan av kontinuitetshantering. Många av de resonemang som presenteras beskriver outsourcad IT-verksamhet till följd av att detta var ett vanlig förekommande exempel som nämndes under intervjuerna. Samma resonemang kan dock appliceras oavsett vilken verksamhet som en beställare väljer att outsourca, exempelvis verksamhet kopplad till personalhantering, lokaler etc.

Outsourcing ur ett livscykelperspektiv

Detta appendix betraktar outsourcing utifrån ett livscykelperspektiv. Inför outsourcing genomförs en analys kring om outsourcing är ett lämpligt alternativ för den utvalda verksamheten, vilka leverantörer som finns, fördelar och nackdelar med outsourcing etc. Analysen följs av ett beslut och därefter upprättas avtal med vald(a) leverantör(er).

---

[2] *Deloitte (2014). Deloitte's 2014 Global Outsourcing and Insourcing Survey – 2014 and beyond.*

[3] *Finansinspektionens författningssamling. Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS2014:1)*

[4] *Främst ISO/IEC 27036:2014 Information technology – Security techniques – Information security for supplier relationships*

[5] *Europaparlamentets och rådets direktiv 2009/138/EG. Om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II)*

[6] *Basel Committee on Banking Supervision (2005). Outsourcing in Financial Services*

[7] *Finansinspektionens författningssamling. Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS2014:1)*

Under avtalsperioden sker löpande uppföljning och samverkan och slutligen upphör avtalsperioden (antingen i förtid eller vid i förväg definierad tidpunkt) och verksamheten återtas eller läggs ut på nytt avtal. De fyra faserna illustreras i nedanstående figur.

Definition av outsourcingbegreppet

I Sverige används vanligen begreppet outsourcing som ett låneord för att beskriva det förhållande som uppstår när en organisation valt att lägga verksamhet (tjänster, processer, funktioner eller resurser) utanför den egna organisationen. Outsourcing brukar definieras som det förhållande där en organisation överlåter till en annan aktör att utföra en verksamhet som organisationen skulle kunna ha i egen regi. Outsourcing kan på så sätt vara mer eller mindre omfattande. Det kan handla om allt från utläggning av enstaka tjänster eller resurser till outsourcing av hela affärsprocesser eller driftsmiljöer.[8]

Den internationella standarden om informationssäkerhet vid leverantörsrelationer, ISO 27036[9], beskriver outsourcing som inköp av tjänster (med eller utan produkter) där leverantörens resurser används för att utföra delar av beställarens verksamhet. Såväl Basel som Solvens II och FFFS 2014:1 belyser att outsourcing handlar om utlagd verksamhet som i annat fall skulle utföras av den egna organisationen. Basel lyfter fram att det kan handla om verksamhet som beställaren skulle kunna utföra vid tidpunkten för outsourcingbeslutet såväl som på sikt. Basel betonar även att den outsourcade verksamheten ska bestå i löpande verksamhet och att den kan utföras av annan part inom den egna koncernen såväl som av en extern leverantör.[10] Solvens II (som använder sig av begreppet ”uppdragsavtal”) lyfter i sin tur fram att det kan handla om verksamhet som genomförs direkt av en leverantör eller genom underentreprenad.[11]

I denna vägledning används begreppet outsourcing fortsättningsvis för att beskriva utlagd verksamhet som beställaren skulle kunna bedriva internt. Den finansiella aktören som väljer att outsourca en del av sin verksamhet benämns fortsättningsvis ”beställare” och aktören som åtar sig att leverera efterfrågad verksamhet benämns fortsättningsvis ”leverantör”.

---

[8] *MSB (2013) – Vägledning – informationssäkerhet i upphandling*

[9] *Information technology – Security techniques – Information security for supplier relationships, ISO/IEC 27036*

[10] *Basel Committee on Banking Supervision (2005). Outsourcing in Financial Services*

[11] *Solvens II (artikel 13 punkt 28)*

Möjligheter och begränsningar med outsourcing

Precis som definitionen av outsourcing varierar mellan olika aktörer varierar också antalet outsourcinglösningar från single- och multisourcing till olika molnlösningar. Nyttan med outsourcing kan variera beroende på den lösning en beställare väljer för att såväl organisera som bedriva verksamheten i relation till leverantören. Det är därmed problematiskt att presentera konkreta möjligheter och begränsningar som gäller för samtliga outsourcinglösningar. Exempelvis kan en vald outsourcinglösning som möjliggör tillgång till expertkunskap och konkurrensfördelar samtidigt medföra reducerad kontroll eller andra kort- eller långsiktiga begränsningar. Nedan presenteras ett antal aspekter som ofta lyfts fram vid bedömning av möjligheter och begränsningar med outsourcing.

Ekonomiska aspekter

Ett vanligt argument för outsourcing är att det bedöms som mindre kostsamt att outsourca än att på egen hand utföra verksamheten. Huruvida så alltid är fallet kan dock diskuteras. Å ena sidan är investeringskostnaden för en intern konkurrenskraftig lösning i många fall högre än en outsourcinglösning då en leverantör kan nå stordriftsfördelar och därigenom minska kostnaderna. Vidare kan beställaren fokusera sina resurser på kärnverksamheten vilket kan leda till effektivitetsfördelar och ökat resultat. Slutligen kan en outsourcinglösning även t.ex. möjliggöra geografisk expansion vilken kan leda till ökade intäkter. Å andra sidan förutsätter en outsourcinglösning oftast att beställaren upprättar/behåller en intern organisation som innehar beställarkompetens avseende den outsourcade verksamheten, ansvarar för kontakt i det löpande arbetet och följer upp den outsourcade verksamheten. En sådan organisation kan, beroende på den outsourcade verksamhetens omfattning och komplexitet, vara kostsam och bidra till minskad lönsamhet. Denna kostnad underskattas ofta.

Kompetens hos leverantör och beställare

Tillgång till kompetens och expertis brukar nämnas som ett argument för outsourcing. Beställaren kan genom outsourcing få tillgång till kompetens, tekniska gränssnitt och lösningar som redan finns hos extern aktör, snarare än att behöva tillägna resurser till utveckling av detta internt. Exempelvis finns det internationella aktörer som specialiserat sig på olika delverksamheter där samarbete kan vara att föredra framför att utveckla kompetensen på egen hand. En nackdel kan å andra sidan vara att beställaren förlorar kompetens i samband med outsourcing av en process i och med att personal antingen förflyttas till leverantör eller slutar. Kompetensförlusten är i sig en utmaning för många beställare då kompetensen (som framförts ovan) behövs vid beställarorganisationen även om tjänsten som sådan outsourcats.

Det är lätt att undervärdera hur mycket tid och resurser som förutsätts finnas kvar inom den egna verksamheten även om en tjänst lagts ut till extern part. Detta gäller särskilt då outsourcing förflyttar verksamheten längre ifrån beställaren vilket i många fall minskar insynen i verksamheten och/eller ställer högre krav på uppföljning och kontroll.

Flexibilitet och innovation

Flexibilitet i kapacitetsutnyttjande kan underlättas i de fall en verksamhet outsourcats eftersom leverantörer ofta har möjlighet att skala upp/ner verksamheten. Detta kan vara betydligt svårare om verksamheten finns inom organisationen. Flexibilitet i verksamheten kan ge såväl operationella som ekonomiska fördelar. Samtidigt kan innovation och utveckling av verksamheten begränsas vid outsourcing eftersom leverantören troligtvis inte har samma känsla och ansvar för utvecklingsinsatser som om verksamheten bedrivits i beställarens egen regi. Outsourcing kan på så sätt möjligen influera innovationsförmågan om nödvändiga utvecklingsinsatser för ett mer säkert och effektivt system avstannar och endast de mest nödvändiga uppdateringarna genomförs.

Kontroll över outsourcad verksamhet

En av de största begränsningarna med en outsourcinglösning är att kontrollen över den outsourcade verksamheten starkt begränsas. Det kan exempelvis handla om minskad insikt i hur känslig information lagras, vilka redundanta lösningar som finns eller hur ofta reservlösningar testas. Det är också möjligt att leverantören i sin tur lägger ut delar av sin verksamhet till ytterligare leverantörer. Leverantörskedjorna kan på så sätt bli långa och komplexa och därmed svåra att ha kontroll över. Till viss del kan kontrollpunkter och begränsningar skrivas in i avtal, men en lika fullständig kontroll som om verksamheten drivs internt är mycket svår att uppnå.

Summering

Nedan listas en summering av de fördelar som en intern lösning respektive en outsourcinglösning kan innebära.

Intern lösning	Outsourcinglösning
• Bibehållen kompetens inom den egna organisationen • Ökad förmåga till kontroll • Ökad förmåga till styrning av verksamheten • Minskad risk för leverantörs-koncentrationer • Minskad risk för externa inlåsningseffekter	• Möjlighet till stordriftsfördelar • Möjlighet att tillgå expertkompetens • Ökad förmåga till flexibilitet • Möjlighet till ökad redundans genom ett större utbud av säkerhets- och kontinuitetslösningar • Ökad möjlighet till snabb utveckling av nya tjänster

G.2. Analys och beslut

Inför att en verksamhet ska outsourcas krävs en noggrann analys för att säkerställa att ett välgrundat beslut fattas. Bland annat bör en analys av vilken verksamhet som ska outsourcas genomföras, på vilket sätt outsourcingen ska ske och vilka risker för kontinuiteten i verksamheten som outsourcingen kan innebära. Detta gäller oavsett om det är befintlig eller ny, kompletterande, verksamhet som avses. Detta kapitel syftar till att ge stöd till analysen inför ett beslut om outsourcing.

Som ett ingångsvärde är det, ur ett kontinuitetsperspektiv, av vikt att personer från olika delar av verksamheten och med olika perspektiv deltar i analysen. Funktioner såsom systemägare, affärsägare, stödverksamheter, IT-drift/förvaltning, jurist, kontinuitetsansvarig, riskansvarig etc. bör bli involverade i beslutet om outsourcing. I hur stor utsträckning de olika funktionerna involveras varierar beroende på vilken tjänst som ska outsourcas och hur kritisk denna tjänst är. Viktigt är dock att alltid inkludera såväl strategisk, taktisk som operativ nivå i beslutet. Ur ett kontinuitetsperspektiv är det viktigt att alltid även inkludera en kontinuitetsansvarig i beslutet.

Val av verksamhet för outsourcing

Utgångspunkten bör vara att verksamheten som outsourcas ska kunna fortsätta levereras enligt kunders/medarbetares/andra intressenters krav, lika effektivt eller effektivare än om verksamheten behålls internt.

Särskilt noggranna analyser krävs om det är verksamhet som kan betraktas som kärnverksamhet som ska outsourcas. Det finns många aspekter att beakta om kärnverksamhet outsourcas till annan part, men ser man till lagstadgade krav finns ingen begränsning för vilken verksamhet som kan outsourcas.[12] Därmed är det möjligt att outsourca en så kallad kärnverksamhet så länge krav på verksamhetens funktion efterlevs. Samtidigt måste konstruktionen av affärsverksamheten givetvis vara begriplig för att tillståndet att bedriva verksamheten ska bestå.

Att göra en tydlig avgränsning för vad som är, eller bör utgöra, en beställares kärnverksamhet är dock inte alltid helt lätt. Särskilt i ett långsiktigt perspektiv då definitionen av beställarens kärnverksamhet kan förändras över tid, där det som idag inte är en kärnverksamhet mycket väl kan vara det om tio år eller tvärtom. Utvecklingen av mobila banktjänster utgör ett exempel; en verksamhet som möjligen initialt betraktades utgöra en stödtjänst för banker men som på förhållandevis kort tid växt till att bli en del av kärnverksamheten.

För finansiella aktörer begränsar reglerna[13] möjligheten att lägga över kritisk verksamhet till extern leverantör om:

- avtalet försämrar kvaliteten i företagsstyrningssystem,

[12] *Lag (2004:297) om bank- och finansieringsrörelse kap 6 och 7*
[13] *FFFS 2014:1, Solvens II*

- operativa risker ökar otillbörligt,
- tillsynsmyndigheternas möjlighet till kontroll begränsas eller,
- avtalet hindrar tillfredsställande service till beställarens kunder.

Därtill finns för försäkringsbolag en informationsskyldighet gentemot tillsynsmyndigheterna om en kritisk funktion eller verksamhet outsourcas samt en anmälningsplikt för finansiella aktörer om den outsourcade verksamheten genomgår väsentliga förändringar.[14] Detta, tillsammans med att förflyttning av delar av kärnverksamheten till extern aktör kan vara förenat med ett risktagande, tyder på att en beställare särskilt bör överväga om kritisk verksamhet bör flyttas över till en leverantör. Samtidigt kan det i vissa fall vara motiverat att göra just så, exempelvis för att nå viss expertkunskap.

Kontinuitetsanalys av den egna verksamheten

Kontinuitetsanalyser bör göras regelbundet i alla typer av organisationer, oavsett om verksamheten är föremål för outsourcing eller inte. Syftet är att förebygga och/eller minska konsekvenserna av störningar i verksamheten genom att ha kännedom om befintliga beroenden, hur störningar påverkar beställarens verksamhet i sin helhet samt vilka reservlösningar som finns eller bör implementeras. För verksamhet som outsourcas möjliggör dessutom en genomförd kontinuitetsanalys väl underbyggda och relevanta kravställningar på leverantörerna. I detta avsnitt beskrivs kortfattat hur en kontinuitetsanalys av verksamheten bör ske. För ett mer utförligt stöd i hur en kontinuitetsanalys bör genomföras, se *FSPOS Vägledning för kontinuitetshantering (2014).*

Kontinuitetsanalysen inleds med en kartläggning av verksamhetens kritiska processer, aktiviteter och resurser. I analysen kartläggs verksamhetens kritiska processer, en process åt gången. För processen dokumenteras kritiska aktiviteter och tillhörande resurser (både interna och externa). För aktiviteterna och resurserna anges tidsgränser för hur långa avbrott som kan tolereras för respektive aktivitet (maximal tolerabel avbrottsperiod), och vilka mål för återställningstider som därmed ställs på de stödjande resurserna. Tiderna sätts utifrån fastställda kriterier för när verksamheten drabbas av oacceptabla konsekvenser, exempelvis inom förtroende, ekonomi, servicenivå etc. I detta sammanhang är det viktigt att beställaren inte rakt av förutsätter att samma avbrottsperioder kan användas då verksamheten förflyttas till en leverantör. Istället bör beställaren noga analysera vilka effekter en eventuell outsourcinglösning får för angivna tider. Exempelvis kan outsourcing medföra längre ledtider och att den egna verksamheten behöver utökad tid efter att återställning hos en leverantör genomförts. Som beskrivet ovan är det viktigt att denna analys har genomförts innan beslut om outsourcing och att analysen ligger till grund för den senare kravställningen. Om kontinuitetsanalysen genomförs på en redan outsourcad verksamhet bör leverantören delta i analysen och ge ingångsvärden för de delar av verksamheten som ligger under dennes ansvar.

[14] *Solvens II (Artikel 49)*

Kontinuitetsanalysen leder fram till att en eller flera kontinuitetsplaner kan tas fram för verksamheten och dess kritiska resurser. Kontinuitetsplanerna ska beskriva alternativa lösningar för de fall de kritiska resurserna blir otillgängliga och på så sätt möjliggöra för verksamheten att fungera på en tolerabel nivå, oavsett vilka störningar som inträffar. Lösningarna beskrivs med fördel i konkreta termer exempelvis genom rutiner och checklistor. Planerna ska inkludera såväl intern som outsourcad verksamhet, även om de lösningar som beskrivs i planerna skiljer sig åt beroende på om verksamheten är intern eller outsourcad. Krav bör också ställas på leverantörerna att upprätta och underhålla egna kontinuitetsplaner för de processer/resurser de ansvarar för (se vidare avsnitt *4.2 Kravställning*).

TIPS FÖR GENOMFÖRANDE:

- Utgå alltid från den egna verksamhetens funktion vid överväganden om outsourcing.
- Avbrottsperioder som angetts för den egna verksamheten är inte nödvändigtvis desamma om en aktivitet eller process outsourcas till extern leverantör
- Säkerställ regelbundet uppdaterade kontinuitetsplaner för både intern och outsourcad verksamhet
- Använd FSPOS vägledning för kontinuitetshantering för stöd i analys av verksamheten

Riskanalys

Kontinuitetsanalysen bör kompletteras med en riskanalys där de risker som kan påverka kontinuiteten i verksamheten identifieras och vid behov åtgärdas. Ur ett bredare perspektiv bör riskanalysen täcka in alla typer av risker (strategiska, operativa, finansiella etc.), men inom ramen för detta appendix exemplifieras främst risker som bedöms kunna påverka kontinuiteten i en (outsourcad) verksamhet.

Riskanalysen och beställarens riskacceptans måste vara vägledande vid beslut om outsourcing. En riskanalys med kontinuitetsfokus leder till en djupare förståelse för de risker och hot som kan kopplas till verksamhetens kritiska resurser och avbrott i dessa. Exempelvis kan flytt av verksamheten till annat land – så kallad offshoring - vara att föredra för en typ av verksamhet medan samma lösning för en annan verksamhet kan vara mindre lyckad.

Att genomföra en riskanalys bör ses som en nödvändighet och kan ses utgöra en grund för uppföljning kring hur beställaren och leverantören hanterar riskerna i verksamheten, vilket även utgör ett krav från Finansinspektionen.[15] Verksamhetsansvariga för den verksamhet som övervägs outsourcas bör givetvis medverka för att se vilka effekter en

[15] *FFFS 2014:1 §10*

eventuell outsourcing skulle medföra. Det är även av vikt att i riskanalysen betrakta outsourcingen på kort såväl som lång sikt.

Riskanalysen kan genomföras enligt ett antal steg som anges i den internationella standarden för riskhantering[16]; etablera kontext (riskacceptans), identifiera risker, bedöma sannolikhet och konsekvens för respektive risk, utvärdera riskerna och ta fram åtgärdsplaner för de risker som inte kan accepteras.

Nedan presenteras ett antal risker som mer eller mindre bedöms kunna påverka kontinuiteten i verksamheten och som därmed bör inkluderas i riskanalysen. Kontinuitetsansvarig ansvarar inte för att identifiera samtliga risker utan behöver ingångsvärden från riskanalyser utförda av andra personer och enheter inom organisationen. Listan är på intet sätt uttömmande utan bör kompletteras utifrån den egna organisationen och den outsourcade verksamhetens förutsättningar.

Risktyp	Riskexempel
Strategisk risk	• Verksamhet kan vara oförenlig med beställarens strategiska målsättningar. • Otillräcklig kompetens eller underlåtenhet vid tillsyn av leverantören.
Risk – i relation till beställarens anseende	• Dålig service från leverantören. • Kundinteraktion överensstämmer inte med den standard som beställaren fastställt för dess egen verksamhet. • Leverantörens metoder är inte i linje med metoder som fastställts av beställaren.
Risk – i relation till regelefterlevnad	• Lagar (ex. sekretess eller tillsyn) uppfylls eller efterlevs inte tillräckligt. • Leverantören har otillräckliga system och kontroller för efterlevnad.
Operativa risker	• Tekniska problem. • Otillräcklig finansiell kapacitet för att uppfylla sina skyldigheter och/eller tillhandahålla lösningar. • Oegentligheter eller fel.
Avvecklingsrisk	• Ändamålsenliga avvecklingsstrategier finns inte. Detta kan uppstå utifrån en övertro på ett företag, förlust av relevant kompetens inom den egna organisationen för att ta tillbaka verksamheten i egen drift samt kontrakt som gör en snabb avveckling mycket kostsam. • Begränsad förmåga att ta tillbaka outsourcad verksamhet till annat land på grund av brist på personal eller komptensbortfall.
Geografiska risker	• Politiska, sociala och legala förutsättningar kan addera risk. • Kontinuitetsarbetet blir mer komplext.
Kontraktuella risker	• Förmåga att verkställa kontrakt. • Vid förlagd verksamhet i annat land (offshoring) är ”val av lag” viktigt.

[16] *Risk management - Principles and guidelines (ISO 31000:2009, IDT)*

Tillgänglighetsrisker	• Potentiell begränsning i förmåga att tillhandahålla information till den egna organisationen och till tillsynsmyndigheterna. • Svårigheter för tillsynsmyndigheterna att förstå verksamheten som outsourcats. (överblick, insyn).
Koncentrationsrisker	• Reducerad kontroll för beställaren. • Systematiska risker för den finansiella sektorn som helhet.

Mot bakgrund av genomförda kontinuitets- och riskanalyser kan ett medvetet och välgrundat beslut om outsourcing genomföras. Analysen av den aktuella verksamheten kan och bör ligga till grund för de kravställningar som görs vid den senare eventuella upphandlingen.

Val av leverantör

När en verksamhet outsourcas är det viktigt att ha en kännedom om leverantören, såväl i det inledande skedet som under löpande avtal. Valet av leverantör bör utgå ifrån en genomförd analys och utifrån ett förtroende för att leverantören förvaltar den aktuella tjänsten på ett förtjänstfullt sätt. Detta avsnitt beskriver områden som är värda att tänka på inför val av leverantör.

Företagsbesiktning

Att göra en företagsbesiktning, en så kallad due diligence, av den bäst lämpade leverantören kan ses som en förutsättning för att gå vidare i dialog om avtalsskrivning. En företagsbesiktning kan vara mer eller mindre omfattande beroende på den verksamhet som övervägs outsourcas, men innehåller vanligen delområdena finansiell, legal, skatte- och teknisk besiktning. Att granska en tilltänkt leverantör är viktigt för att kontrollera att leverantören kan tillhandahålla tjänsten över en längre tid. Företagsbesiktningar kan med fördel genomföras regelbundet även under löpande avtal. Detta då det inte är säkert att ägarförhållanden och dylikt är desamma under en längre tidsperiod. Vidare kan det vara framgångsrikt att efterfråga och utvärdera referenser från de aktuella leverantörerna.

Leverantörskedjor

Inför ingående av avtal med en leverantör bör beställaren även undersöka om underleverantörer kommer att användas för tillhandahållande av den aktuella verksamheten. Långa leverantörskedjor kan minska insyn och tillgänglighet i verksamheten ytterligare samt öppna upp för andra sårbarheter i tjänsten. I de fall där leverantörskedjor förekommer bör företagsbesiktning göras även av underleverantörerna och de bör också finnas med i analysen av den egna verksamheten (se avsnitt 3.2).

Kravställningar bör formuleras redan vid upphandlingen

Leveransmässiga villkor avseende kontinuitetshantering bör inte endast stipuleras vid ingående av avtal med en viss leverantör utan bör finnas med som skall-krav redan vid upphandlingen och fungera som urvalskriterier för vilka leverantörer som är lämpliga att sluta avtal med. Kraven bör utgå ifrån den tidigare analysen av verksamheten och de krav som ställs på den egna organisationen (se avsnitt 3.2).

Konkurrensutsättning och koncentrationsrisker

En beställare kan välja att outsourca en verksamhet till en enskild leverantör att förvalta (single-sourcing), eller att dela upp verksamheten i mindre delar och använda sig av flera leverantörer för olika delverksamheter (multi-sourcing). Båda lösningarna ställer krav på fungerande samverkan med leverantören/leverantörerna, medan den senare lösningen även förutsätter ett beställaransvar för koordinering mellan de externa leverantörerna.

För vissa typer av tjänster kan det vara en fördel att använda sig av flera leverantörer för samma tjänst, dels ur säkerhetssynpunkt då verksamhet kan växlas över och dels utifrån en ekonomisk aspekt där flera leverantörer medför ökad konkurrens och lägre pris. Även om en beställare väljer att använda sig av flera leverantörer finns risk att flera andra organisationer använder sig av samma leverantörer. Detta förhållande kan utifrån ett sektorsperspektiv sammanfattas med begreppet koncentrationsrisker. Ett exempel utgörs av att en beställare upphandlar en leverantör för IT-drift, en leverantör som även upphandlats för IT-drift av flera andra finansiella organisationer inom sektorn.

Från Finansinspektionen finns inga krav relaterade till koncentrationsrisker. Detta är dock något som aktörer själva bör överväga innan de väljer att lägga ut verksamhet till extern part då de fortsatt är ansvariga för verksamheten och möjligen inte vet exempelvis vilken prioritetsordning deras verksamhet har vid avbrott hos leverantören. För den finansiella sektorn är koncentrationsrisker högst relevanta att analysera och hantera ur ett kontinuitetsperspektiv.

TIPS FÖR GENOMFÖRANDE:

- Genomför företagsbesiktningar både vid ingående av avtal och regelbundet under gällande avtal
- Undersök, och vid behov begränsa, potentiella leverantörskedjor
- Ställ krav på alla delar av leverantörskedjan
- Fundera kring fördelar och nackdelar med single- respektive multi-sourcing
- Analysera och hantera eventuella koncentrationsrisker

G.3. Upprättande av avtal

Genom avtalsskrivningar som fastställer en tydlig ansvarsfördelning mellan beställaren och leverantören kan robustheten i den outsourcade verksamheten öka. Om rätt krav ställs och om beställaren har väl inarbetade rutiner för uppföljning och granskning kan outsourcing leda till bättre ”ordning och reda” och struktur på de utlagda tjänsterna än om de behållits internt. Samarbete och dialog med valda leverantörer vid såväl strategisk som operativ nivå är också centralt för att öka robustheten i den outsourcade verksamheten.

Detta kapitel syftar till att ge stöd vid upprättande (eller omförhandling) av avtal med outsourcingleverantörer.

Utgå från analys av verksamheten i kravställning

Finansinspektionens föreskrifter fastställer ett antal krav för outsourcingavtal gällande kritisk verksamhet, bland annat att beställaren säkerställer att regelverket följs och att leverantören har en strukturerad process för övervakning, men föreskrifterna ställer inte krav på hur kraven ska uppnås. På detta sätt gäller fortsatt principen om att de krav som ställs på bolagens egen verksamhet ska gälla även för outsourcad verksamhet. Hur detta genomförs är dock upp till de enskilda bolagen att svara för. Därmed blir beställarens kravställning vid avtalsskrivning viktig. Kravställningen bör utgå ifrån outsourcingens livscykel och bör därmed utgå från kontinuitets- och riskanalysen av den egna verksamheten. Kravställningar bör därtill vara tydligt preciserade i avtalet med leverantören, där tydlighet i begreppsdefinitioner vid avtalsskrivningen är centralt. Vid händelse av kris eller störningar är det av stor vikt att ha tydliga definitioner i avtalet av de åtgärder som ska vidtas och hur samverkan ska ske. Leverantörer har eventuellt ett incitament att definiera kris- och störningsbegreppen så brett som möjligt, medan en så tydlig definition som möjligt ligger i beställarens intresse.[17] Kraven bör inte enbart fokuseras till servicenivåer, utan bör exempelvis även inkludera hur dialog och kommunikation ska ske under löpande avtal samt hur och när avvecklingen av avtal kan ske.

Kravställning

I detta avsnitt ges exempel på kriterier som kan vara relevanta att inkludera i avtal med leverantörer. Viktigt att notera är att alla verksamheter och avtal är unika. Denna beskrivning är därför inte heltäckande utan beställaren måste säkerställa att samtliga relevanta kriterier är inkluderade i varje enskilt avtal.

Vid formulering av krav att inkludera i avtal är det viktigt att säkerställa att kraven i så stor utsträckning som möjligt är mätbara och med lämplig regelbundenhet är möjliga att följa upp.

---

[17] *www.outsourcing-center.com (Negotiating Effective Service Level Agreements)*

Fastställande av en tydlig ansvarsfördelning

Som tidigare nämnts ligger ansvaret för verksamheten kvar hos beställaren även om verksamheten outsourcats. En risk med att outsourca är att ansvarskänslan minskar. Det är därför viktigt att det finns en medvetenhet kring att ansvaret för de verksamheter som outsourcats förblir hos beställaren. I avtalen är det viktigt att utse enskilda personer som ansvarar för den outsourcade verksamheten.

För att leverantörerna ska kunna upprätthålla robusthet i sina tjänster och därmed kunna leverera det de åtagit sig att leverera förutsätts att både beställare och leverantör utser kontaktpersoner samt underhåller listor med kontaktuppgifter och delger dessa till varandra. Beroende på storlek och komplexitet på den outsourcade verksamheten bör ansvariga utses på strategisk, taktisk och operativ nivå. Exempel på ansvarsområden kan bestå i samverkan, teknik, ekonomisk uppföljning och granskning/revision. Det bör även tydligt framgå var den enes ansvar slutar och var den andres ansvar tar vid. Ansvarsfördelningen bör kunna styrkas med hänvisning till en formell arbetsbeskrivning där respektive funktions, tillika individs, ansvar finns noga beskrivet. Att säkerställa att en viss funktion har arbetstid och mandat att genomföra det ansvar som preciseras är också av vikt, inte minst då dessa uppgifter kan komma att efterfrågas av Finansinspektionen vid en granskning.

För förtydligande av roller och ansvar kan HUKI-modellen[18] användas. Modellen föreslår en ansvarsfördelning mellan beställare och leverantör utifrån de fyra ansvarsområdena: huvudansvariga, utförare, konsulterade och informerade, i förhållande till den outsourcade verksamheten.

TIPS FÖR GENOMFÖRANDE:

- Ansvaret för verksamheten och leverans till kund stannar alltid kvar hos beställaren
- Roller och ansvar bör specificeras i avtalet
- Utdelat ansvar bör kunna dokumenteras i en formell ansvarsbeskrivning

Ansvar för underleverantörer och leverantörskedjor

Det ligger i beställarens intresse att säkerställa att avtalet reglerar ansvaret gentemot eventuella underleverantörer. Detta är särskilt viktigt eftersom de regelefterlevnadskrav som ligger på beställaren fortsatt är gällande även om delar av verksamheten förflyttas till extern(a) part(er), vilket förutsätter en kontrollverksamhet från beställarens sida. Beställaren kan genom avtalet fastställa om underleverantörer kan användas för hela eller delar av den aktuella verksamheten.

[18] *Huvudansvarig, utförare, konsulterad, informerad. Kommer ifrån engelskans RACI (responsible, accountable, consulted, informed).*

Beställaren kan även fastställa att leverantören måste meddela beställaren om leverantören har för avsikt att använda sig av ytterligare underleverantörer för den outsourcade verksamheten under löpande avtal. Detta är av betydelse då en ökning av antalet leverantörer kan få omfattade konsekvenser för den egna kontrollverksamheten. Vid sidan av att beställaren ska vara informerad kan avtalet även redogöra för att beställaren måste konsulteras och lämna sitt medgivande innan underleverantörer används för den outsourcade verksamheten. Därmed ges möjlighet att genomföra t.ex. företagsbesiktningar och införa krav på kontinuitetshantering hos de aktuella underleverantörerna.

Leverantörskedjor är i många fall förekommande, vilket gör att kontrollen blir än svårare att behålla. Det krävs därför en avvägning av hur långt tillbaka i leverantörskedjan som beställaren bör ställa krav. Snarare än att ställa krav på leverantörernas underleverantörer regleras robusthet och redundans vanligen genom avtal med den egna leverantören, där påföljder för misslyckande att leverera utlovad tjänst beskrivs. Ett sätt att ställa krav på underleverantören är därmed att ställa krav på att leverantörerna ska ha höga krav på servicenivåer gentemot sina underleverantörer för att kunna garantera leverans i så stor utsträckning som möjligt.

Samverkan med leverantören

Vid fastställande av roller och ansvar bör även former för löpande dialog och kommunikation hanteras. Ett lämpligt sätt är att upprätta olika forum för samverkan med leverantören, exempelvis för kontinuitet, utbildning, säkerhetsfrågor, driftsfrågor etc. Beroende på den outsourcade verksamhetens omfattning och komplexitet kan dessa forum upprättas på olika nivåer. Hur forumen ska drivas och upprätthållas bör också anges i avtalen genom tydliga angivelser av ansvar, form och frekvens. Mer om hur dialogen och samarbetet med leverantören kan genomföras presenteras i kapitel 5.

Införlivande av regelförändringar

Beställaren bör säkerställa att leverantören kan uppvisa en strategi för hur den outsourcade verksamheten anpassas till eventuella regelförändringar. En nyckel i detta arbete är en samsyn mellan beställare och leverantör om hur regelförändringar ska tolkas. Då det i många fall kan finnas delade meningar om vad en regel innebär bör det tydligt anges i avtalen vem som har tolkningsföreträde.

Lagring av information och informationssäkerhet

Då informationsförluster inte är acceptabla är det en förutsättning att ställa krav på redundans när det gäller lagring av information så att informationen inte försvinner vid händelse av störningar eller avbrott i tjänsten. För att säkerställa redundans vid outsourcade IT-relaterade verksamheter kan exempelvis krav ställas på robust utrustning, skalskydd, speglad information, processer för releasehantering och geografiskt separata driftställen.

Avtalet bör även reglera hur leverantören hanterar känslig och konfidentiell information. Ett sätt att reglera detta är att säkerställa att det finns fastställda rutiner för hur leverantören hanterar känslig information samt att dess personal utbildas och övas regelbundet. Om beställaren outsourcar verksamhet som inkluderar lagring av personuppgifter, till exempel löneregister, måste personuppgiftslagen (PUL) tas i beaktande. Viktigt att notera är att det alltid är beställaren som är personuppgiftsansvarig. Datainspektionen är den myndighet som ansvarar för att behandlingen av personuppgifter sker på ett korrekt sätt. Datainspektionen kan ställa särskilda krav på bland annat autentisering och kryptering vid hantering av känsliga personuppgifter, brottsuppgifter och sekretesskyddade uppgifter.[19]

Vidare är det av vikt att redan vid upprättande av avtal tydliggöra vad som händer med den information som hanterats av en leverantör, då avtalet avbryts eller löper ut. Mer om informationshantering i samband med outsourcing ges i MSB-rapporten *Informationssäkerhet i upphandling*[20].

Fastställande av servicenivåer

Beställare bör ställa krav på sina leverantörer avseende tillgänglighet och service. Hur detta, rent tekniskt, uppnås lämnas ofta upp till leverantören att besluta. Kraven som ställs bör dels utgå från kontinuitetsanalysen och dels bero på ingångsvärden från leverantören för att säkerställa att kraven är möjliga att möta.

För att säkerställa tillgänglighet, service och kvalitet i den verksamhet som outsourcats anges vanligen servicenivåer i leverantörsavtal. Dessa anges i delavsnitt i det övergripande leverantörsavtalet och benämns *Service Level Agreement (SLA)*. Vid sidan av att anpassa den outsourcade verksamheten utifrån beställarens behov tydliggör SLA:er även vilka mål som leverantören har att förhålla sig till och kan på så sätt även användas inom kontrollverksamheten vid uppföljning av verksamheten.

Beroende på hur kritisk den verksamhet som outsourcats är kan servicenivåerna skilja sig åt och vara mer eller mindre specifika. För vissa verksamheter kan det vara rimligt att specificera servicenivåer kopplat till olika resurser, medan det för andra verksamheter räcker att specificera servicenivåer för den samlade outsourcade verksamheten. Ju högre servicenivåer som anges desto dyrare, därför kan en avvägning genom kostnadsnyttoanalys även vara att rekommendera. Nedan presenteras ett antal vanligt förekommande parametrar som är att överväga att inkludera i avtalet och som är kopplade till begreppen: tillgänglighet, maximalt antal fel, servicetid och åtgärdstid.

Tillgänglighet

Tillgängligheten för en outsourcad verksamhet eller tjänst beskrivs vanligen uttryckt i procent. Exempelvis innebär 90 % tillgänglighet att en verksamhet förväntas vara fri från

[19] *http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/*

[20] *MSB (2013). Vägledning: informationssäkerhet i upphandling – Informationssäkerhet i upphandling av system, outsourcing och molntjänster.*

avbrott 90 % av tiden. Ett annat sätt är att uttrycka tillgängligheten inverterat, det vill säga som otillgänglighet eller som avbrottstider, vilket bland annat görs i Kammarkollegiets ramavtal för varor och tjänster som upphandlas ofta[21]. Ett exempel på hur tillgänglighet och otillgänglighet kan uttryckas i avtal följer enligt nedan presenterad tabell.

Tillgänglighet	Otillgänglighet (per år)	Otillgänglighet (per månad)
90 %	876 timmar	73 timmar
99 %	87,6 timmar	7 timmar 18 minuter
99,9 %	8,76 timmar	43 minuter 48 sekunder
99,99 %	52 minuter 33 sekunder	4 minuter 22 sekunder
99,999 %	5 minuter 15 sekunder	26 sekunder

I vissa fall kan det vara lämpligt att ställa mer specifika krav gällande tillgänglighet, exempelvis kan krav ställas på högre tillgänglighet då verksamheten är särskilt känslig för avbrott. Detta kan vara under särskilda dagar i månaden, vissa dagar på året, eller under vissa tider på dygnet. Beställare bör som krav eller i dialog med leverantören tydliggöra hur tillgänglighetstiden räknas ut samt gärna även kräva att få se historiska siffror på tillgänglighet innan avtal skrivs på.

Maximalt antal avbrott

För vissa tjänster är det lämpligt att ställa krav på maximalt antal avbrott. Särskilt då frekvensen av avbrott är mer viktigt för verksamheten än hur långa avbrotten är. Beställare bör säkerställa att de tjänster som är särskilt känsliga för antalet avbrott garanteras en servicenivå med maximalt antal avbrott som kan accepteras. Maximalt antal avbrott bör precis som tillgänglighet även specificera vilken tidsperiod som gäller och leverantören bör även kunna uppvisa historiska siffror på antal avbrott hos den berörda tjänsten. Beroende på vilken verksamhet som outsourcats kan acceptansnivån för maximalt antal avbrott variera. Oavsett hur många avbrott som beställaren väljer att acceptera genom avtalet är det viktigt att säkerställa att beställare och leverantör har samma definition av begreppet ”avbrott”. Denna definition bör finnas med i avtalet, gärna med förtydligande exempel.

Servicetid och åtgärdstid

Krav bör även ställas på servicetid och åtgärdstid. Servicetid avser den tid som leverantören kan förväntas vara tillgänglig för att åtgärda eventuella avbrott. För mer kritiska tjänster, som har en högre servicenivå, är det vanligt och ofta lämpligt att ha servicetid dygnet runt alla dagar i veckan medan det för mindre kritiska tjänster är vanligt och ofta lämpligt att ha en mer begränsad servicetid. Servicetiden kan på så sätt variera från t.ex. ”*24/7 service*” till ”*service under kontorstid måndag till fredag 08.00-18.00*”, beroende på hur kritisk verksamheten anses vara.

[21] *Exempel på Kammarkollegiets ramavtal med olika leverantörer finns på www.avropa.se*

Åtgärdstid är i sin tur den tid som passerar från det tillfälle då avbrottet anmäls eller upptäcks av leverantören, till dess att det är åtgärdat och verksamheten är återställd till normalläge. Beställare bör se till att åtgärdstiden är tydliggjord i det avtal som upprättas och att åtgärdstiderna tillgodoser de krav som den egna verksamheten har, exempelvis genom *"Maximal åtgärdstid per avbrott under servicetid (timmar)"*. Kravställning på åtgärdstider gällande IT-system bör ta hänsyn till hur lång tid det tar från återstart av systemet till dess att alla eventuella följdverkningar har hanterats.

Larm och eskalering

Det är vanligt att servicenivåer som anges i avtal avser drift i normalläge. Men det är fördelaktigt att särskilda krav på servicenivå vid kriser och extraordinära händelser specificeras i avtalet. Därmed är det även viktigt att avtalet tydligt anger vad en extraordinär händelse eller krisläge innebär, samt huruvida det är leverantören, beställaren eller båda två som kan avgöra om en sådan händelse föreligger. Även force majeure bör definieras i avtalet och vilken/vilka av parterna som har möjlighet att besluta om denna typ av händelse föreligger.

TIPS FÖR GENOMFÖRANDE:

En klausul om force majeure kan formuleras enligt nedan*:

"Om någon av parternas skyldigheter förhindras på grund av krig, naturkatastrof, strejk, lockout, blockad eller annan liknande omständighet vilken part inte kunnat förutse eller påverka och där konsekvenserna inte kunnat undvikas, ska den part som inte har möjlighet att uppfylla sina skyldigheter vara befriad från dessa så länge hindret föreligger."

** Inspiration från Kammarkollegiets leveransavtal inom Företagshälsovård*

Exempel på andra krav som kan ställas är att leverantören har rutiner för larmning och eskalering till beställaren samt vilka kriterier som gäller för larmning. Leverantören bör också ha utsett ansvariga för kontakt med beställaren vid störningslägen. Detta är särskilt viktigt vid multi-sourcing, där det kan vara lämpligt att genomföra möten med alla berörda leverantörer.

Avtalet bör även tydligt definiera vid vilken grad av störning beställaren informeras, hur informationen förmedlas och till vem, samt vilken information som ska delges. Avtalet kan exempelvis stipulera att leverantören ska delge vilka tjänster som har drabbats eller vad prognosen för avhjälpning är. Ibland kan kravet på information definieras i termer av löpande statusrapporter och för mindre kritiska tjänster kan det till exempel räcka med en rapportering vid avbrott och en rapportering vid det slutgiltiga återställandet av tjänsten. Beställare bör även säkerställa att leverantören alltid har en kontaktperson som handlägger inkomna ärenden.

Som beställare är det viktigt att ha en dialog med leverantören om hur man som kund prioriteras i en krissituation samt vilka möjligheter det finns att påverka denna prioritering. Leverantörer har ofta en prioritetsordning bland sina kunder, denna är

dock sällan öppen och hur leverantören prioriterar framkommer först under, eller efter, en krissituation.

Viktigt är därmed att få leverantören att förstå vilken typ av verksamhet man driver och vilka konsekvenser ett avbrott i tjänsten får. Särskilt viktigt är detta om man driver samhällsviktig verksamhet, så att leverantören förstår omfattningen av de totala konsekvenser ett avbrott i verksamheten får.

Kontinuitetshantering och kontinuitetsplaner

Krav bör ställas på att leverantörer ska arbeta med kontinuitetshantering för kritiska verksamheter som outsourcats dit. Leverantörerna bör även ha säkerställt kontinuiteten för eventuella andra delar av dess verksamhet som vid avbrott kan påverka beställarens verksamhet.

Exempel på krav i relation till kontinuitetshantering kan vara att leverantörerna har genomfört processkartläggningar där kritiska delar av verksamheten identifierats, att maximalt tolerabla avbrottsperioder har identifierats och att kontinuitetsplaner för kritiska processer har tagits fram och regelbundet testas. Med fördel ställs även krav på att beställaren får ta del av kontinuitetsplanerna och testresultat, detta även hos leverantörens underleverantörer.

Övningar och tester

Beställaren bör ställa krav på att leverantörer regelbundet genomför strukturerade övningar och tester av sina system och rutiner. Dessutom bör det kravställas att resultaten inklusive eventuella åtgärdsplaner delges beställaren. Övningar och tester kan genomföras på flera olika nivåer, bland annat genom:

- Övning av personal för att säkerställa kompetens och öka erfarenheter.
- Skarpa tester för att testa leverantörens kritiska system, processer och beroenden och utröna hur länge leverantören kan klara sig utan dessa utan att det påverkar berörda aktörer i större omfattning. Detta kan göras till exempel genom test av alternativt driftställe samtidigt som ordinarie verksamhet fortgår på ordinarie plats eller genom test av reservkraft för att säkerställa att diesel räcker enligt utlovat.
- Genomgång av checklistor och rutiner.

Övningars och testers frekvens och omfattning bör också beskrivas i avtalet. De finansiella aktörerna kan därtill ställa krav på att gemensamma övningar ska genomföras, det vill säga övningar där både finansiella aktörer och leverantörer deltar. Detta för att testa bland annat samverkan, kommunikationsvägar och informationsdelning. Slutligen bör beställaren också kräva att leverantören bidrar med stöd/information till övningar och tester som utförs av beställaren själv, men som berör den outsourcade verksamheten.

Tillsyn och revision

Krav bör formuleras i avtalet om att beställaren får genomföra granskningar och revisioner av leverantörens system, processer, rutiner, eller leverantörens uppfyllnad av andra delar av avtalet. Granskningen av avtalet kan och bör ske i flera dimensioner, med fokus på exempelvis struktur, process och resultat. På strukturnivå granskas exempelvis de resurser som använts medan processnivån granskar hur dessa använts. Resultatnivån granskar avslutningsvis det resultat som uppnåtts.

Granskningar och revisioner kan antingen genomföras av beställaren själv eller av en tredje part som är betrodd av både leverantören och beställaren. En beställare kan med fördel avtala om att det är den egna organisationen som står för val av part för revision samt för egna platsbesök. Även när revision och annan granskning görs av extern part är det av vikt att inkludera dess regelbundenhet i avtalet. I tillägg ska det vara möjligt för Finansinspektionen att genomföra tillsyn av den verksamhet som läggs ut. I de fall där leverantörskedjor används bör revision även vara möjlig att genomföra hos underleverantörer. Därtill bör beställaren avtala om att ta del av resultat från de granskningar och revisioner som leverantören själv genomför.

Delgivning av analyser

Det får antas att samtliga leverantörer regelbundet följer upp och analyserar sitt övergripande kontinuitets-, risk- och säkerhetsarbete. Beställare bör begära att få ta del av de sammanställningar som berör den outsourcade verksamheten, exempelvis i form av resultat från riskanalyser eller revision av kontinuitetsarbetet. På så sätt kan beställaren aktivt påverka dess leverantörer inom områden där risk- eller kontinuitetsarbetet inte är tillräckligt. Beställaren bör därtill kravställa att leverantören skriftligt redogör för hur de uppfyller de krav som fastställts i avtalet och hur ofta denna rapportering ska ske.

Sanktioner och hävning av avtal

För att skydda beställaren och för att motivera leverantören att uppfylla överenskomna servicenivåer är det viktigt att avtalet även specificerar villkoren för händelser då leverantören misslyckas att uppfylla de avtalade kraven. Då åsidosättanden kan bero på flera orsaker är det viktigt att beställaren i dialog med leverantören tydligt klargör vad som innebär åsidosättande av avtal och det är även viktigt att avtalet tydliggör vilka fall som avser ”force majeure” och vilka som inte gör det. Vid större avvikelser eller avbrott kan det vara svårt att påvisa vilken skada som åsamkats, därför är det en god idé att på förhand definiera vilka sanktioner som bör gälla.

Sanktioner vid åsidosättande kan definieras på flera olika sätt, exempelvis genom en direkt finansiell sanktion eller genom krediter för framtida leveranser av den berörda tjänsten.[22] Vid sådana avsteg som leverantören kan åtgärda inom en rimlig tidsperiod är

[22] *www.iids.org (Managing Violations In Service Level Agreements)*

det naturligt att eftersträva en rättelse av avvikelserna i ett första steg. Vite kan i ett nästa steg användas som en påtryckning på leverantören i syfte att åstadkomma en rättelse. En hävning av ett avtal kan ses som en sista utväg vid grova och upprepade överträdelser.

TIPS FÖR GENOMFÖRANDE:

Ett bra verktyg som kan användas vid avtalsskrivning om olika sanktioner och dess eskalering är Kammarkollegiets vitesmodell.* Vitesmodellen ger beställaren styrmedel mot leverantören och utgår ifrån de servicenivåer som beställaren förväntar sig att leverantören ska svara mot. I modellen används en maximal procentsats för vite som varierar med ersättningens storlek. För en outsourcad verksamhet med två KPI:er och en maximal vitesprocentsats om 20%, skulle en beräkning av vite kunna se ut enligt följande:

Exempel – Vitesberäkning:	
KPI 1 - viktprocent	10 %
KPI 2 - viktprocent	10 %
Summa månatlig vitesprocentsats:	20 %
Fakturerat belopp:	200 000
Vitesbelopp:	40 000

**Bilaga Kammarkollegiets vitesmodell. IT Driftstjänster 2010.*

Ett annat verktyg som kan användas hävstång för att säkerställa att leverantören följer sina åtaganden kan vara att i avtalet definiera en möjlighet att gå över till en annan leverantör om avtalet inte följs. Avtalet kan exempelvis ge respektive part friheten att bryta avtalet då motparten ”grovt åsidosatt sina åtaganden”. Viktigt är då att avtalet även definierar vilka händelser som detta inkluderar.

Möjlighet till omförhandling och återtagning av verksamhet

Leverantörsavtal medför ofta långa bindningstider och/eller uppsägningstider. Sådana villkor gör det svårt att byta leverantör eller omförhandla befintliga avtal. Beställare bör därför säkerställa att avtalet inte utgör ett hinder för omförhandling eller byte av leverantör inom en rimlig tidsperiod, genom att noga utvärdera de villkor avseende bindningstider och uppsägningstider som erbjuds redan vid avtalsskrivningen.

Avtalet kan med fördel precisera regelbundna tidpunkter för omförhandling av avtal. Det ligger i såväl leverantörens som beställarens intresse att möjliggöra omförhandling av avtal då beställarens behov kan förändras över tid. En skrivelse i avtal kan exempelvis reglera att omförhandling av avtal görs en gång per år eller en gång vartannat år.

Möjligheten att ta tillbaka verksamhet om samarbetet fallerar bör inkluderas i avtalet. Exempelvis vid obestånd eller då det finns anledning att misstänka det. I de fall då avtalet hävs och den outsourcade verksamheten avvecklas eller återtas i egen regi bör

en plan för avveckling finnas. I Finansinspektionens föreskrifter preciseras att avvecklingsplaner ska finnas samtidigt som föreskrifterna inte omfattar instruktioner om hur planerna ska formuleras. I avtalet med leverantören gäller det därför att fastställa vilket ansvar som gäller då ett samarbete avslutas samt hur tjänsten ska återtas och inom vilket tidsperspektiv. Avtalet bör avspegla vad som förväntas av leverantören då outsourcingavtalet löper ut eller avslutas, exempelvis i form av vilken information som ska överlämnas eller vilka resurser och vilken kompetens som leverantören ska tillhandahålla under avvecklingsperioden. I avtalet kan även framgå att leverantören åtar sig att vara behjälplig vid förflyttning av tjänsten till annan part samt att inte blockera eller förhindra förflyttningen på något sätt. I vissa fall kan det även vara aktuellt att precisera vilka resurser som ska flyttas tillbaka. För IT-relaterade verksamheter kan det i detta sammanhang vara av vikt att definiera att resurser/tillgångar som utvecklats under tiden den outsourcade tjänsten löpt ska flyttas tillbaka i dess uppdaterade form.

För att säkerställa att den tid för avveckling som återges i avtalet är realistisk kan workshops anordnas med leverantören där avvecklingen diskuteras utifrån olika scenarier. Exempelvis kan det vid dialog med leverantören uppdagas att avvecklingen tar längre tid än vad som beskrivs i det ursprungliga avtalet. Mer om vad en beställare bör tänka på vid omförhandling och avveckling av outsourcad verksamhet presenteras i kapitel 6.

Flexibilitetsklausuler

Som påpekats tidigare förändras omvärlden, vilket kan kräva en regelbunden och eventuellt även en kontinuerlig anpassning av tjänster och härmed en flexibilitet hos leverantören som kan bli kostsam ur ett outsourcingperspektiv. Med bakgrund av detta kan så kallade flexibilitetsklausuler användas, vilka underlättar anpassningen till förändrade omständigheter. Dessa bör dock ur ett kontinuitetsperspektiv användas med viss försiktighet, där beställaren säkerställs tolkningsföreträde.

G.4. Uppföljning och samverkan

För att säkerställa att verksamheten ligger i linje med beställarens behov förutsätts en fungerande samverkan mellan leverantören och beställaren samt att den outsourcade verksamheten följs upp och utvärderas regelbundet.

Kapitlet beskriver områden som är viktiga att beakta under gällande avtal. Genom en fungerande samverkan och en regelbunden och tydlig uppföljning läggs även grunden för en god kontinuitetshantering i förhållande till den outsourcade verksamheten.

Löpande samverkan och uppföljning

Beroende på vilken verksamhet som outsourcats, exempelvis storlek och hur kritisk verksamheten är, samt hur många olika leverantörer som används kan olika leverantörsstrategier komma att bli aktuella.

Leverantörsrelationer kan vara ytliga såväl som djupa, där ytliga relationer inte behöver innehålla någon löpande samverkan eller dialog utan endast uppföljning på exempelvis årsbasis enligt kraven i avtalet. Djupa leverantörsrelationer kan inkludera löpande (t.o.m. daglig) samverkan i upprättade forum med utpekade ansvariga från både beställare och leverantör. En djup relation med leverantör är att föredra om det är en kritisk verksamhet som outsourcats. Om många leverantörer används blir denna typ av leverantörsstrategi dock kostsam. En avvägning bör därför göras mellan att ha många leverantörer för att sprida riskerna men samtidigt minska möjligheterna till täta leverantörssamarbeten, eller att ha få leverantörer där samverkan sker mer kontinuerligt och på olika nivåer. Att använda sig av få leverantörer och samtidigt ha ytliga relationer med dessa bör endast vara ett alternativ för outsourcing av tjänster som inte är av kritisk betydelse för beställaren eller dess intressenter.

Samverkansforum för löpande dialog och uppföljning

Eftersom de finansiella aktörerna i stor utsträckning utför samhällsviktig verksamhet bör djupa leverantörsrelationer med löpande dialog mellan beställare och leverantör oftast vara att föredra. Ett sätt att uppnå tätt samarbete med leverantören är att upprätta samverkansforum där de åtaganden som fastställts genom avtalet följs upp.

Samverkansforumen kan exempelvis bestå i regelbundna möten där olika problemställningar fångas upp. Forumen kan arrangeras på strategisk eller operativ nivå och kan även anordnas för enskilda sakfrågor som anses prioriterade för den outsourcade verksamheten, exempelvis kontinuitetsfrågor. Vid forumen bör de åtaganden som fastställts genom avtalet följas upp. Mötena bör formaliseras där respektive parts ansvar framgår tydligt. Som stöd vid uppföljning framtas med fördel olika checklistor.

Det är även viktigt att säkerställa att upprättade forum faktiskt fungerar. Ett stöd på vägen kan vara att utforma en samverkansmanual som instruerar i hur forumen ska hanteras. I manualen bör även kontaktuppgifter till parter inom den externa leverantören anges tydligt, samt vem inom den egna verksamheten som ansvarar för kontakten med leverantören i olika ärenden.

Uppföljningen som genomförs vid samverkansforumen bör grundas i en strategi för uppföljning som upprättas hos beställaren. Fokusområden för uppföljning kan med fördel skifta från år till år utifrån en långsiktig och gemensamt fastställd plan. Att, som tidigare påpekats, regelbundet ta del av resultat från leverantörens övningar och genomföra gemensamma övningar är också att föredra. Leverantören bör regelbundet avlämna analyser och rapporter till beställaren, i enlighet med vad som föreskrivits i avtalet. Analyserna och rapporterna bör bestå av skriftliga underlag då dokumentationen underlättar beställarens uppföljning. De skriftliga underlagen bör också kompletteras med muntliga redogörelser vid upprättade samverkansforum.

Checklistor och nyckeltal underlättar kontrollverksamheten

Det är viktigt att genomgående säkerställa att leverantören lever upp till de krav som preciserats i avtalet. Som beskrivet i avtalskapitlet är det därför av stor vikt att de krav som ställts i avtalet är möjliga att följa upp och mäta. För de aktörer som väljer att outsourca är det därmed viktigt att säkerställa att det finns tydliga interna rutiner och instruktioner på plats som möjliggör och underlättar uppföljning och kontroll. Detta är även ett krav från Finansinspektionens sida. Nyckeltal och KPI:er kan också användas inom kontrollverksamheten.

Från den beställande organisationen läggs resurser på att följa upp leverantörernas agerande. Det är därför av vikt att beställarorganisationen har en tydlig fördelning av ansvar för kravuppföljning inom den egna organisationen. Att outsourca en tjänst innebär att flera olika parter inom den egna organisationen är ansvariga för olika delområden, såväl för att upprätthålla relationen med leverantören som att kontrollera att avtalet efterlevs. Det kontraktuella ansvaret såväl som det driftsmässiga avtalet bör vara tydligt inom beställarens interna organisation och det bör finnas framtagna interna rutiner och stödmaterial, exempelvis checklistor. Checklistor kan utarbetas utifrån de krav som formulerats i avtalet, exempelvis för att säkerställa att leverantören har en kontinuitetsplan på plats. Dessa checklistor bör kontinuerligt följas upp och uppdateras. Det finns även en revisionsstandard (ISACA) som används av externa revisorer för att granska leverantörer; denna handlar både om hur de fysiska anläggningarna ser ut och hur leverantörens verksamhet som helhet sköts. Vid uppföljningen kan med fördel den företagsbesiktning som genomfördes innan avtal om outsourcing slöts ses över eftersom ägarförhållanden, samhällets förväntningar (t.ex. etiska regler) och dylikt kan förändras över tid.

Samverkan och uppföljning vid störningar och avbrott

Beställaren bör informeras i de fall där leverantören eskalerat till kris och bör även kontaktas för att lämna sitt samtycke innan återställning av verksamheten efter inträffad kris. Under ett avbrott bör beställaren även få kontinuerlig information kring händelseförloppet, påverkan på den outsourcade verksamheten och hur leverantören arbetar för att återupprätta verksamheten. Incidentanalyser, från inträffade störningar och avbrott, bör komplettera den regelbundna rapporteringen, där beställaren bör upprätta en rutin för att säkerställa att identifierade brister åtgärdats.

G.5. Utveckling och avveckling

I vissa fall kan det vara motiverat att bryta avtalet helt med leverantören. Avveckling av en tjänst bör dock noga vägas mot vad det innebär att byta leverantör eller att ta tillbaka de utlagda tjänsterna internt. Vid byte av leverantör behöver mycket arbete genomföras såsom ny behovsanalys och uppdatering av krav. Därtill måste revision av den tidigare dokumentationen för den outsourcade verksamheten göras igen.

Kapitlet beskriver två områden som är viktiga att beakta vid omförhandling av avtal eller vid avveckling av outsourcad verksamhet: utvärdering och erfarenhetsåterföring.

Utvärdering

Att tillvarata lärdomar från samarbetet med leverantören är av vikt oavsett om avtalet löpt ut och är föremål för omförhandling, eller om den outsourcade verksamheten ska avvecklas eller återtas. Genom att tillvarata erfarenheter från samverkan med leverantören kan framtida kravställningar anpassas så att de är realistiska och att de svarar mot beställarens verksamhetsbehov. Erfarenheter kan tillvaratas från genomförda samverkansforum såväl som från en självutvärdering kring hur verksamheten strukturerats, hur verksamheten utförts och vilket resultat som valt tillvägagångssätt medfört. Samtliga åtaganden som stipulerats i det tidigare avtalet bör även ses över och utvärderats, med uppgift att se om något åtagande bör utvecklas.

Vid tid för omförhandling eller byte av leverantör är det även av vikt att återgå till den interna analysen som gjordes innan beslut om outsourcing fattades. Där bör undersökas om någon/något av de förutsättningar och behov som lade grund för avtalsskrivningarna förändrats och om avtalsskrivningarna därmed bör utvecklas. Exempelvis kan behov av kontinuitet i tjänsten förändras om en resurs eller kompetenstillgång krävs under en specifik tid om dagen/månaden/året.

TIPS FÖR GENOMFÖRANDE:

Exempelfrågor som kan ställas vid utvärderingen:

- Vad fungerade bra?
- Vad fungerade sämre?
- Vilka var de initiala behoven och förutsättningarna?
- Har behoven och förutsättningarna förändrats?

Erfarenhetsåterföring

Det är viktigt att komma ihåg att det inte alltid är helt enkelt att återta eller flytta verksamhet som en gång outsourcats. Vid återtagning av verksamheten kan exempelvis nyrekryteringar och omfattande nyinvesteringar utgöra en förutsättning för att återtagandet av verksamheten ska kunna genomföras.

Vid avtalsskrivningen bör kravställningar för hur verksamheten återtas preciserats. När en beställare beslutat att återta outsourcad verksamhet bör beslutet kompletteras med en plan för erfarenhetsåterföring där beställaren redogör för hur organisationen ska ta tillvara på den kunskap som återförs från leverantören till beställarens egen verksamhet. Detsamma gäller om verksamheten flyttas till en annan leverantör, men då kan planen med fördel upprättas tillsammans med den nya leverantören.

Självskattningsformulär - Kontinuitetshantering för outsourcad verksamhet

Denna checklista är ett komplement till Appendix G i FSPOS vägledning för kontinuitetshantering. Checklistan kan användas för att underlätta arbetet med att säkerställa kontinuitetshantering i outsourcad verksamhet och ska ses som ett stöd vid analys, kravställning, uppföljning och utveckling/avveckling av outsourcing ur ett kontinuitetsperspektiv.

Nedan presenteras ett antal påståenden som är relevanta att beakta vid beslut om outsourcing, upprättande av avtal, uppföljning av gällande avtal samt vid eventuell avveckling av avtal. Tabellen beskriver även ansvarsområden för respektive påstående. Ansvarsområdena har fördelats utifrån HUKI-modellen och syftar till att visualisera ett förslag till ansvarsfördelning mellan beställare och leverantörer (se definitioner nedan). Då ansvar beror av vilken verksamhet som outsourcas och på vald outsourcinglösning ska de fördelningar av ansvar som anges nedan endast betraktas som förslag. Följaktligen behöver samtliga nedanstående ansvarsområden inte vara fastställda för en välfungerande kontinuitetshantering, utan det är upp till varje enskild organisation att besluta kring vilka ansvarsområden som är relevanta.

H – Huvudansvarig

U - Utförare

K – Konsulterad

I – Informerad

För varje påstående finns en hänvisning till relevant avsnitt i Appendix G för mer detaljerad information om påståendet.

Analys och beslut

Ansvar	Leverantör	Beställare	För stöd, se Appendix G	Kommentar
Beställaren har involverat funktioner från olika delar av verksamheten och med olika ansvarsområden i analysen. Ur ett kontinuitetsperspektiv är det viktigt att kontinuitetsansvarig och ansvarig för verksamheten som ska outsourcas har involverats. Utöver dessa kan exempelvis följande funktioner ha deltagit i analysen: - Jurister - Processansvariga - Systemägare - Riskfunktion - IT-drift/förvaltning		H	G.2.	
VAL AV VERKSAMHET FÖR OUTSOURCING				
Beställaren har genomfört en analys av den verksamhet som ska outsourcas. Analysen innehåller exempelvis: - Möjligheter och begränsningar med att outsourca den utvalda verksamheten - Bedömning om kraven på verksamhetens funktion kan efterlevas vid outsourcing - Bedömning av behov av rapportering/information till tillsynsmyndighet - Bedömning av om den tilltänkta verksamheten utgör kärnverksamhet eller ej		H	G.2.	
KONTINUITETSANALYS AV DEN EGNA VERKSAMHETEN				
Beställaren har inventerat tidigare kontinuitetshanteringsarbete utifrån den verksamhet som övervägs att outsourcas.		H	G.2.	
Beställaren har genomfört en kontinuitetsanalys av den aktuella verksamheten som ligger till grund för de kravställningar som stipuleras i avtalet med leverantören. I kontinuitetsanalysen ingår bland annat: - En processkartläggning där processens kritiska aktiviteter och resurser identifierats - Maximalt tolerabla avbrottsperioder (MTPD) för kritiska aktiviteter har definierats - Mål för återställningstider (RTO) för kritiska resurser har definierats - Mål för återställningspunkter (RPO) för kritiska resurser har definierats		H	G.2.	
Beställaren har vid behov reviderat och anpassat definierade avbrottstider för att vara tillämpbara och relevanta i en outsourcinglösning.	K	H	G.2.	
Beställaren har upprättat kontinuitetsplaner för verksamheten och dess kritiska resurser. Kontinuitetsplanerna innehåller reservlösningar för samtliga kritiska resurser, såväl interna som externa (outsourcade).	K	H	G.2.	

Om kontinuitetsanalysen genomförs på outsourcad verksamhet har leverantören involverats.	K	H	G.2.	
RISKANALYS				
Beställaren har genomfört en riskanalys utifrån identifierade riskområden, vilka bedöms kunna påverka kontinuiteten i outsourcad verksamhet på kort såväl som på lång sikt.	K	H	G.2.	
Beställaren har säkerställt att verksamhetsansvariga för den verksamheten som ska outsourcas har involverats i riskanalysen.		H	G.2.	
Riskanalysen genomförs enligt stegen i den internationella standarden för riskhantering; riskidentifiering, bedömning av sannolikhet och konsekvens, utvärdering av riskerna och framtagande av åtgärdsplaner.		H	G.2.	
Exempel på risker som beställaren bör inkluderas är bland andra: - Risker kopplade till kompetens (ex. förlust av kompetens och behov av kvarvarande kompetens inom organisationen) - Risker kopplade till ekonomi - Risker kopplade till tillsyn och granskning - Risker kopplade till förtroende - Risker kopplade till innovation och flexibilitet i den outsourcade tjänsten		H	G.2.	
VAL AV LEVERANTÖR				
Beställaren har genomfört en företagsbesiktning (due dilligence) av den bäst lämpade leverantören och referenser har efterfrågats. Exempel på kriterier att beakta i företagsbesiktningen är bland andra: - Finansiell styrka - Organisatorisk stabilitet - Referenser		H	G.2.	
Beställaren har genomfört regelbundna företagsbesiktningar efter det att en leverantör upphandlats.		H	G.2.	
Beställaren har begränsat antalet underleverantörer i avtalet och har genomfört företagsbesiktningar av dessa.		H	G.2.	
Beställaren har beaktat koncentrationsrisker.		H	G.2.	

Upprättande av avtal

Ansvar	Leverantör	Beställare	För stöd, se Appendix G	Kommentar
UTGÅ FRÅN ANALYS AV VERKSAMHETEN I KRAVSTÄLLNING				
Beställarens interna analys har legat till grund för de kravställningar som ställs i avtal med leverantör efter beslut om outsourcing.		H	G.3.	
Beställaren har fastställt tydliga begreppsdefinitioner i avtalet, där beställaren har tolkningsföreträde vid tvetydigheter.	I	H	G.3.	
KRAVSTÄLLNING				
Leverantören har utsett en ansvarig för dess kontinuitetshanteringsarbete kopplat till den outsourcade verksamheten och dokumenterat detta i en arbetsbeskrivning. Leverantören har informerat beställaren om vem som utsetts och delgett beställaren kontaktuppgifter. Den ansvarige har tränats och övats regelbundet (minst en gång per år).	H	I	G.3.	
Beställaren har utsett en ansvarig för dess kontinuitetshanteringsarbete kopplat till den outsourcade verksamheten och dokumenterat detta i en arbetsbeskrivning. Beställaren har informerat leverantören om vem som utsetts och delgett leverantören kontaktuppgifter. Den ansvarige har tränats och övats regelbundet (minst en gång per år).	I	H	G.3.	
Beställaren har genom avtalet säkerställt att leverantören konsulterar beställaren innan eventuella underleverantörer anlitas för tillhandahållande av den outsourcade tjänsten.	I	H	G.3.	
Beställaren har genom avtalet säkerställt att leverantören har höga krav på servicenivåer gentemot dess underleverantörer för tillhandahållande av den outsourcade tjänsten.	H	I	G.3.	
Beställaren har fastställt kriterier för löpande samverkan i avtalet. Exempelvis har former, frekvens och ansvar för samarbetsforum angivits.	K	H	G.3.	
Beställaren har genom avtalet säkerställt att leverantören tagit fram en strategi för hur den outsourcade verksamheten anpassas till eventuella regelförändringar.	H	K	G.3.	
Beställaren har genom avtalet säkerställt att leverantören en säker och separat förvaring av all dokumentation som kan härledas till den outsourcade tjänsten. Beställaren har genom avtalet säkerställt att leverantören har en fastställd rutin för hantering av konfidentiell och annan känslig information. Beställaren har genom avtalet säkerställt att leverantören löpande utbildar sin personal i informationssäkerhet i syfte att säkerställa att personalen förstår hur känsligt material ska hanteras och varför detta görs (minst en gång per år).	H	K	G.3.	
Beställaren har vid leverantören säkerställt: • Robust utrustning • Skalskydd	H	I	G.3.	

• Speglad information • Backuper för återställning av verksamheten • Geografiskt separata driftsställen I de fall där leverantören använder sig av alternativa datacenter har säkerställts att de alternativa datacentren inte är beroende av samma fysiska infrastruktur som den ordinarie platsen.				
Beställaren har genom avtalet säkerställt krav på tillgänglighet för tjänsten, där tillgänglighet fastställts i timmar och vid normalläge och vid kritiska tidpunkter.	K	H	G.3.	
Beställaren har genom avtalet fastställt krav på servicetid och åtgärdstid. • Maximal åtgärdstid per avbrott under servicetid (timmar) • Maximalt antal avbrott	I	H	G.3.	
Beställaren har genom avtalet fastställt en definition av force majeure samt vem som har tolkningsföreträde vid en sådan situation.	K	H	G.3.	
Beställaren har genom avtalet säkerställt att leverantören har definierat när en krissituation uppstår i relation till den outsourcade verksamheten. Beställaren har genom avtalet säkerställt att leverantören har fastställda rutiner för larm och eskalering samt en kontaktperson vid störningslägen. Kriterier för när larmning till beställaren ska ske anges i avtalet, exempelvis genom formuleringar såsom: • Rapport om genomförda/misstänkta intrång ska ske inom (X) antal timmar/dagar	H	I	G.3.	
Beställaren har avtalat om en prioritetsordning vid avbrott hos leverantören, i de fall det är möjligt.	K	H	G.3.	
Beställaren har säkerställt att leverantören har en strukturerad process för kontinuitetshantering, i vilken bland annat följande aktiviteter ingår: • Konsekvensanalys • Riskbedömning • Utveckling av kontinuitetsplaner • Tester, utbildningar och övningar • Löpande revidering och granskning	H	I	G.3.	
Beställaren har säkerställt att leverantören har fastställda kontinuitetsplaner för den outsourcade verksamheten. Dessa innefattar: • Reservrutiner (*Alternativa arbetssätt under pågående avbrott*) • Återställningsrutiner (*Hur återställningen av kritiska resurser sker efter ett avbrott*) • Återgångsrutiner (*Hur återgång till normalläge sker när den kritiska resursen är tillgänglig igen*)	H	I	G.3.	
Beställaren har säkerställt att kontinuitetsplanerna (som minimum) har inkluderat följande områden: • Organisation med kontaktinformation och tydligt angivna roller och ansvar (vid normalläge och vid kris) • Identifierade kritiska resurser och beroenden (ex. arbetsplatser, datacenter, system och lösningar, personal och expertis.) • En beskrivning av den övergripande IT-arkitekturen med detaljerade planer och processer för återställning av de individuella komponenterna inom olika IT-system	H		G.3.	

• Rutiner för intern och extern kommunikation • Historik över revidering av planer				
Beställaren har säkerställt att leverantören har granskat och uppdaterat kontinuitetsplanerna *minst* en gång per år. Granskningar av kontinuitetsplaner har därtill genomförts inom sex månader efter en signifikant organisatorisk- eller teknisk förändring samt efter en större incident.	H	I	G.3.	
Beställaren har säkerställt att leverantören har övat dess anställda i kontinuitetsplaner för den outsourcade verksamheten *minst en gång per år*. Genomförda övningar har dokumenteras och resultatet har rapporteras till beställaren.	H	I	G.3.	
Beställaren har säkerställt att leverantören årligen har testat kontinuitetsplanerna. Tester har också genomförts efter förändringar inom den outsourcade verksamheten. Processen för tester har inkluderat ett årligt testschema, förberedelser, dokumentation, rapport av testresultat samt implementation av åtgärdsplaner baserat på testresultaten.	H	I	G.3.	
Beställaren har genom avtalet säkerställt att leverantören genomför regelbundna övningar och tester av sina system och rutiner med kopplingar till den outsourcade verksamheten. Bland annat anges: • Typ av övningar • Frekvens • Målgrupp • Rapporteringskrav (exempelvis att åtgärdsplaner från övningar och tester ska delges beställaren)	H	I	G.3.	
Beställaren har genom avtalet säkerställt att gemensamma övningar kan genomföras vid behov och på initiativ av beställaren.	K	H	G.3.	
Beställaren har genom avtalet säkerställt att leverantören årsvis fastställt planer för övningar och test av den outsourcade verksamheten. För varje test har följande områden specificeras: • Beskrivning av de test som ska utförs • Frekvens av test (X ggr per år) • Uppskattad tid för planerat test	H	I	G.3.	
Beställaren har genom avtalet säkerställt möjligheten för tillsynsmyndigheter att genomföra tillsyn av den outsourcade verksamheten, enligt de skyldigheter som föreskrivs i: • Lag (2004:297) om bank- och finansieringsrörelse • Lag (2007:528) om värdepappersmarknaden Beställaren har genom avtalet därtill säkerställt möjligheten till egen- eller tredjeparts granskning och revision. Kraven specificerar exempelvis: • Att beställaren har full insyn i utlagd verksamhet för internkontroll • Frekvens för granskning och revision • Vem som har möjlighet att utföra granskning och revision (beställaren själv eller extern part) • Möjlighet till fysisk granskning av leverantörens lokaler • På vilka nivåer granskning och revision kan ske (exempelvis avseende struktur, process och levererat resultat)	K	H	G.3.	

Beställaren har genom avtalet säkerställt möjligheten att ta del av revisionsrapporter från granskningar och revisioner som leverantören själv genomför relaterat till den outsourcade verksamheten.	H	I	G.3.	
Beställaren har genom avtalet fastställt vilka sanktioner som vidtas vid avsteg från avtalet och vid vilka kriterier sanktionerna är möjliga att aktivera.	I	H	G.3.	
Villkor för när avtalet kan brytas har tydligt definierats. Definitionen inkluderar: • Vid (X) antal avbrott i den outsourcade verksamheten. • Då leverantören grovt åsidosatt dess åtagande. • Då leverantörens finansiella styrka att utföra verksamheten är ifrågasatt eller då större förändringar i processer/rutiner för den outsourcade verksamheten genomförts som påverkan kvaliteten i tjänsten.	I	H	G.3.	
Beställaren har genom avtalet säkerställt att omförhandling av avtal sker *minst* en gång vartannat år om inte annat avtalats.	K	H	G.3.	
Beställaren har utarbetat och fastställt en plan för hur den outsourcade verksamheten ska återtas efter avbrott. Beställaren genom avtalet även ställt krav på leverantören inför avveckling av den outsourcade verksamheten. Avvecklingsplanen och leverantörskraven bör exempelvis omfatta: • Vad som förväntas av leverantören vid avveckling av en outsourcad verksamhet, i form av informationsöverlämning, resursöverlämning, kompetensöverföring etc. • Leverantören tillhandahåller (X) personer med kompetensen (Y) som är behjälpliga vid flytt av verksamheten. • Leverantören åtar sig att på inget sätt blockera eller förhindra flytt av verksamhet. • Tidplan för återtagande av verksamhet uppgår till (X) månader. • Erfarenhetssammanställning och återkoppling.	I	H	G.3.	

Uppföljning och samverkan

Ansvar	Leverantör	Beställare	För stöd, se Appendix G	Kommentar
LÖPANDE SAMVERKAN OCH UPPFÖLJNING				
En strategi för leverantörsrelationer har tagits fram. Exempel på leverantörsstrategier kan vara exempelvis många leverantörer/ytliga relationer eller fåtal leverantörer/djupa relationer.		H	G.4.	
En samarbetsmanual har tagits fram för att reglera samverkan mellan beställaren och leverantören. Samarbetsmanualen har granskats och uppdaterats *minst* en gång per år eller då större förändringar i verksamheten genomförts.	K	H	G.4.	
Checklistor för uppföljning av kraven i avtalet mellan beställare och leverantör har tagits fram. Exempel på kriterier att inkludera i checklistorna är: - X antal möten har hållits på strategisk nivå - X antal möten har hållits på taktisk nivå - X antal möten har hållits på operativ nivå - Kontinuitetsplanerna har testats årligen - Beställaren har tagit del av X antal testprotokoll efter genomförda tester hos leverantören - X utbildningar för leverantörens personal har hållits - Resultat av löpande riskbedömning - Etc.	I	H	G.4.	
Checklistor har även utformats för leverantörens åtaganden. Exempelvis bör leverantören kvartalsvis avlämna rapporter på följande KPI:er: - Återställningstid (RTO) - Återhämtningspunkter (RPO) - Kontinuitetsplaner fastställda, granskade och uppdaterade (Ja/Nej) - Kontinuitetsplanerna är testade (Ja/nej) - Tester och övningar som genomförts (antal/år) - Genomförda övningar (Ja/Nej)	K	H	G.4.	
SAMVERKAN OCH UPPFÖLJNING VID STÖRNINGAR OCH AVBROTT				
Beställaren har genom avtalet säkerställt att leverantören har en lämplig organisation för återställning av den outsourcade verksamheten genom att säkerställa att leverantören har: • **(X)** personer behöriga fatta beslut om eskalering till kris och som kan fatta alla nödvändiga beslut i förhållande till en träffad incident. • Implementerade kontinuitetsplaner som går i linje med tillämpliga lagar. • Dokumenterade processer.	H	I	G.4.	

Beställaren bör säkerställa att leverantören har en strukturerad process för övervakning av den outsourcade verksamheten för att säkerställa tidig upptäckt av incidenter och störningar. Vid inträffade störningar och avbrott bör därtill säkerställas att rutiner finns för att: • Leverantören omedelbart informerar beställaren vid eskalering till kris. • Leverantören söker beställarens samtycke innan leverantören återställda tjänster efter en inträffad kris. • Leverantören informerar beställaren efter att verksamheten startas upp igen efter en inträffad kris. • Leverantören kontinuerligt avlämnar lägesrapporteringar till beställaren tills dess att den outsourcade verksamheten är fullt återställd. Efter inträffade störningar och avbrott bör beställaren säkerställa att: • Beställaren har informerats inom (x) min/timmar efter inträffade incidenter/genomförd återställning • Beställaren har delgivits åtgärdsplaner och/eller dokumenterade erfarenheter (x) dagar efter en inträffad händelse	H	I	G.4.	

Utveckling och avveckling

Ansvar	Leverantör	Beställare	För stöd, se Appendix G	Kommentar
Beställaren bör genomföra en utvärdering inom (x) dagar efter avveckling av en outsourcad verksamhet. Erfarenheter och lärdomar ifrån genomförd utvärdering bör användas vid kommande avtal.	K	H	G.5.	
Beställaren bör ta fram en plan för erfarenhetsåterföring som redogör för hur organisation ska ta tillvara på den kunskap som återförs från leverantören till beställarens egen verksamhet.		H	G.5.	