FI-tillsyn

Styrning och kontroll av it-verksamheten i försäkringsföretag

Nr 8

15 november 2018

15 november 2018
Dnr 18-9203

INNEHÅLL

FI-tillsyn

Finansinspektionen publicerar återkommande tillsynsrapporter i en numrerad rapportserie. Tillsynsrapporterna är en del i FI:s kommunikation. Rapporterna behandlar genomförda temaundersökningar och annan tillsyn som FI utför. Genom rapporterna informerar vi om vilka iakttagelser som FI gjort och om sina förväntningar i olika frågor. Detta kan vara till stöd för företagen i deras verksamhet.

Sammanfattning

Digitaliseringen i den finansiella sektorn ökar. Försäkringsföretagen har överlag en god styrning och kontroll av sin it-verksamhet, visar denna rapport. Men FI har också hittat fall där försäkringsföretag har svårt att överblicka och hantera konsekvenserna av sina uppdragsavtal. En viktig orsak till detta är att utlagd it-verksamhet inte är lika transparent som när den drivs i egen regi.

Digitaliseringen i den finansiella sektorn ökar samtidigt som nya innovationer skapar produkter, affärsmodeller och samarbetsformer som ställer högre krav på riskhantering, styrning och kontroll av it-verksamheten än tidigare. Detta gäller särskilt styrning och kontroll av it-verksamhet som omfattas av uppdragsavtal eftersom utlagd verksamhet inte är lika transparent som när den drivs i egen regi.

Samtidigt kan utläggning av it-verksamheten leda till både kvalitetshöjningar och besparingar. Nya eller små aktörer inom försäkring kan med moderna och jämförelsevis billiga tjänster från professionella it-leverantörer konkurrera på marknader som de annars inte skulle haft tillgång till.

Omfattningen av uppdragsavtal kan i hög grad påverka ett försäkringsföretags förmåga att överblicka och hantera konsekvenserna av sina it-strategiska vägval. Givet den ökade digitaliseringen visar FI:s analys att det finns förbättringsområden som behöver särskilt fokus:

- Uppdaterade it-strategier.
- Komplett översikt över it-leverantörer, inklusive leverantörer som inte bidrar till leverans av it-funktioner av väsentlig betydelse.[1]
- Beskrivningen av konsekvenser av utlagd verksamhet.
- Styrdokument för uppdragsavtal.
- En klar uppfattning om hur ett uppdragsavtal ska avslutas.
- Regelbunden kontroll av den utlagda verksamheten för att avgöra om riskbedömningen som gjordes vid upphandlingstillfället fortfarande är aktuell.
- Regelbunden test av beredskapsplaner.
- Medvetenhet om operativa risker i styrprocesserna.
- Utbildning och systematisk bevakning av cyberrisker.

1 I kommissionens delegerade förordning (EU) 2015/35 av den 10 oktober 2014 om komplettering av Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkringsverksamhet (Solvens II), (EU-förordningen) och i Eiopas riktlinjer för företagsstyrningssystem, EIOPA-BoS-14/253 (Riktlinjerna) används begreppet ”kritiska eller viktiga operativa funktioner eller verksamheter”. I Försäkringsrörelselagen (2010:2043), (FRL), används begreppet ”operativ verksamhet eller funktioner av väsentlig betydelse”.

Bakgrund, syfte och genomförande

Digitaliseringen i den finansiella sektorn ökar samtidigt som nya innovationer skapar produkter, affärsmodeller och samarbetsformer som ställer högre krav på försäkringsföretagens riskhantering, styrning och kontroll av it-verksamheten.

Branschtäckande enkät 2016

År 2016 genomförde FI en enkätundersökning[2] som omfattade alla svenska försäkringsföretag. En av observationerna från enkäten var att 60 procent av alla it-relaterade incidenter rör intern eller extern infrastruktur. FI såg också att uppdragsavtal inom it-verksamheten var utbrett, att utnyttjande av så kallade molntjänster var växande och att vissa leverantörer skulle kunna utgöra en koncentrationsrisk.

Cyberrisker i fokus 2017

Under 2017 ökade antalet cyberattacker markant. I julbrevet till försäkringsföretagen i december 2017 underströk FI vikten av skyddsåtgärder och ändamålsenliga beredskapsplaner för att företagen skulle kunna förebygga och hantera cyberrisker. FI pekade också på behovet av en särskilt stark styrning och kontroll av uppdragsavtal inom it-verksamheten givet riskerna som identifierats under 2016 och 2017.

Fördjupade analyser 2018

För att följa upp insikterna från 2016 och 2017, och öka FI:s kunskap om försäkringsföretagens styrning och kontroll av it-verksamheten genomfördes fördjupade analyser i ett urval av försäkringsföretagen under februari–maj 2018. Försäkringsföretagen valdes i första hand baserat på vilken leveransmodell de valt för it-verksamheten, både vad gällde gruppinterna och externa it-leverantörer.

FI granskade först företagens it-strategier, styrdokument för uppdragsavtal och beredskapsplaner. Under april och maj genomfördes platsbesök där de sju utvalda försäkringsföretagen i detalj redogjorde för styrning och kontroll av it-verksamheten med särskilt fokus på uppdragsavtal.[3]

Insurtech 2019

Nya innovativa försäkringsprodukter och nya tekniska möjligheter är en av orsakerna till att FI under 2018 valde att analysera styrning och kontroll av it-verksamheten med särskilt fokus på utlagd verksamhet. Ny teknik, nya affärsmodeller och nya samarbetsformer ställer höga krav på operativ riskhantering, styrning och kontroll. FI vill därmed säkerställa att tolkning och tillämpning av det svenska regelverket vad gäller it-verksamheten i försäkringsföretag är relevant och rimlig i förhållande till förändringarna vi ser på försäkringsmarknaden. Under 2019 kommer detta arbetet att fortsätta, både i samarbete med Eiopa[4] och i form av en dialog med svenska Insurtech-företag.

2 Se https://www.fi.se/sv/publicerat/nyheter/2016/resultat-av-enkat-till-forsakringsforetag/

3 Se agenda, bilaga 1.

4 FI deltar i Eiopas Insurtech Task Force.

Strategi

Omfattningen av uppdragsavtal kan i stor grad påverka ett försäkringsföretags förmåga att överblicka och hantera konsekvenserna av sina it-strategiska vägval. De granskade it-strategierna var också i vissa fall föråldrade. Vissa försäkringsföretag saknar en översikt över leverantörer som inte bidrar till leverans av väsentliga[5] it-funktioner. Generellt är beskrivningen av konsekvenser av utlagd verksamhet bristfällig.

IT-STRATEGI

I ett försäkringsföretag ska det finnas en klart definierad riskhanteringsstrategi som överensstämmer med företagets övergripande affärsstrategi. Strategins mål och ledande principer, godkända risktoleransgränser och ansvarsfördelningen på företagets samtliga verksamhetsområden ska dokumenteras[6], och det är därför viktigt att it-verksamhetens mål och inriktning är relaterade till affärsstrategin.

Den dokumentation som försäkringsföretagen skickade till FI innan platsbesöken innehöll i huvudsak deras strategiska val och avvägningar för it-verksamheten i förhållande till försäkringsverksamheten, men innehållet var i vissa fall föråldrat.

Under de efterföljande platsbesöken kunde företagen redogöra för hur man arbetade med it-strategiska frågor i praktiken, särskilt i relation till sina viktigaste leverantörer. Hos vissa företag ser FI en tydlig koppling mellan styrdokument, processer och strategier, medan det i andra företag är svårare att bedöma hur de strategiska vägvalen tillämpas.

FI observerade fall där vissa strategier leder till praktiska problem med styrning och kontroll. De organisatoriska vägval man hade gjort var gynnsamma ur ett kostnadsperspektiv, men försämrade viktiga intressenters möjligheter att påverka it-verksamhetens prioriteringar. I vissa styrelser var beslutspunkter om it i praktiken informationspunkter.

Vad gäller de strategiska vägval ett försäkringsföretag gör för it-verksamheten lägger FI stor vikt vid följande frågeställningar:

- Hur avgör företaget att verksamhetens system, resurser och rutiner är lämpliga i förhållande till verksamhetens kontinuitetskrav?[7]
- Hur identifierar och värderar företaget risker i it-verksamheten i förhållande till andra strategiska risker som it-riskerna påverkar:[8]

5 I tillsynsrapporten används ”väsentlig” där det i vissa lagtexter står ”kritisk eller viktig”.

6 Artikel 259.1 a EU-förordningen.

7 10 kap. 3 § FRL.

8 10 kap. 6 § FRL.

  - i samband med förändringar av företagets affärsstrategi?[9]
  - i större projekt och investeringar?[10]
- Hur identifieras, bedöms och hanteras nya it-behov i förhållande till verksamhetens övergripande affärsmål?[11]

FI bedömer att försäkringsföretagen generellt kan redogöra för detta men att omfattningen av uppdragsavtal, både inom och utanför en koncern, i stor grad kan påverka ett företags förmåga att överblicka och hantera konsekvenserna av it-strategiska vägval. It-organisationens struktur och beslutsprocesser kan också ha en stor påverkan på hur väl man lyckas. Formella processer kan till exempel vara ineffektiva, inaktuella, gynna särskilda intressen eller helt enkelt inte tillämpas.

STRATEGISKA VAL FÖR IT-PRODUKTIONEN

Ett viktigt strategiskt vägval för ett försäkringsföretag är att fastställa hur it-verksamheten ska drivas och av vem. I den fördjupade analysen begärde FI att försäkringsföretagen skulle redogöra för hela it-verksamhetens leveransstruktur, det vill säga it-tjänster som

a) produceras inom företaget;

b) levereras av dotter-, syster- eller moderföretag;

c) levereras av externa parter via dotter-, syster- eller moderföretag;

d) levereras av externa parter direkt till företaget;

e) levereras av externa parters underleverantörer, eller där externa parters underleverantörer bidrar till leverans av en tjänst.

FI upptäckte brister i redogörelsen av tjänster där leverantörers underleverantörer på något sätt utför eller bidrar till en it-leverans. Bristerna kan i första hand härledas till att företagen drar en gräns för hur långt ut i leveranskedjan det är rimligt att utöva kontroll. Generellt drar försäkringsföretagen gränsen vid utlagd verksamhet som bedömts vara av väsentlig betydelse.

Utan en komplett översikt av it-produktionens arkitektur är det svårt för ett försäkringsföretag och dess beslutsfattare att ta ställning till hur olika typer av förändringar i verksamheten påverkar eller påverkas av förändringar i leverantörsstrukturen och it-arkitekturen. Utan en sådan översikt är det även svårt att bedöma om en del av arkitekturen blir mer eller mindre viktig eller mer eller mindre sårbar över tid. En komplett leverantörsöversikt innebär inte att man behöver tillämpa samma principer för riskhantering, styrning och kontroll för alla leverantörer.

9 Artikel 262.1 a i EU-förordningen.

10 Artikel 269.1 d i EU-förordningen.

11 Artikel 258.6 i EU-förordningen.

Styrning och kontroll

Försäkringsföretagen använder generellt beprövade och ändamålsenliga modeller för sin styrning och kontroll av it-verksamheten och samverkan med it-leverantörer. Omfattningen av styrdokument för uppdragsavtal skiljer sig mellan försäkringsföretagen. Styrdokumenten FI granskade var av varierande kvalitet och ofta kompletterade med andra dokument eller rutiner för att uppfylla lagkraven. Vissa försäkringsföretag saknar en klar uppfattning om hur ett uppdragsavtal ska avslutas.

STYRDOKUMENT FÖR UPPDRAGSAVTAL

Ett styrdokument för uppdragsavtal krävs enligt 10 kap. 2 § försäkringsrörelselagen[12]. Dokumentet ska fastställas årligen av styrelsen.

Omfattningen av styrdokument för uppdragsavtal skiljer sig åt mellan försäkringsföretagen som ingick i den fördjupade analysen. FI kunde inte i de granskade styrdokumenten otvetydigt konstatera att alla regelkrav[13] var uppfyllda, trots att det fanns referenser till kraven i dokumenten. I dialog med företagen framkom det däremot att det som saknas i styrdokumenten ofta fanns någon annanstans, fast mer eller mindre dokumenterat.

I den mån styrdokumentet kompletteras av andra instruktioner eller rutiner bör det finnas tydliga referenser till dessa så att även ovana medarbetare, vikarier eller nya resurser kan utföra uppgifterna utan brister eller fördröjning.

Det fanns inga genomgående svagheter som alla försäkringsföretagen hade gemensamt. Bristerna FI observerade skilde sig mellan företagen och vissa företag hade styrdokument med bara enstaka brister.

AVTALSUTFORMNING

I den fördjupade analysen begärde FI att försäkringsföretagen skulle redogöra för avtalens[14] utformning enligt ett urval av följande lagstadgade krav:

- Försäkringsföretagets och FI:s rätt till uppgifter som rör den verksamhet eller de funktioner som omfattas av uppdragsavtalet.[15]
- Försäkringsföretagets och FI:s rätt att genomföra inspektioner på plats i tjänsteleverantörens lokaler.[16]
- FI:s rätt att ställa frågor direkt till tjänsteleverantören.[17]

12 Försäkringsrörelselag (2010:2043), (FRL).

13 Artikel 274 i EU-förordningen och riktlinje 63 i Riktlinjerna.

14 Avtal avseende kritiska eller viktiga it-funktioner.

15 Artikel 274.4 h i EU-förordningen.

16 Artikel 274.4 h i EU-förordningen.

17 Artikel 274.4 i i EU-förordningen.

- Att tjänsteleverantörens skyldigheter och ansvarsområden inte ska påverkas av någon underentreprenad;[18]
- Försäkringsföretagets rätt att avsluta uppdragsavtalet utan att det inkräktar på kontinuitet och kvalitet av tjänster gentemot försäkringstagarna.[19]

Alla de granskade försäkringsföretagen kunde visa att avtalen som ingick i den fördjupade analysen innehöll avsnitt som täckte dessa rättigheter och skyldigheter. Försäkringsföretagen kunde också ge exempel på inspektioner på plats hos tjänsteleverantörer som utförts utan begränsningar.

Som framgår av promemoria som FI tidigare har publicerat i fråga om revisionsrätt och molntjänster[20] är frågan om revisionsrätt inte oproblematisk, särskilt vad gäller mindre försäkringsföretag och deras förhandlingsposition gentemot stora leverantörer. FI:s åsikt är att revisionsrätten inte är förhandlingsbar, men att tillämpningen av den måste avgöras av försäkringsföretaget från fall till fall.[21]

I EU-förordningens avsnitt om uppdragsavtal anges att tjänsteleverantören ska informera om alla händelser som kan inverka materiellt på dennes förmåga att effektivt utföra de funktioner och verksamheter som omfattas av uppdragsavtalet i enlighet med tillämpliga lagar och föreskrifter.[22]

FI:s tolkning är att detta inte bara gäller planerade händelser som till exempel uppgraderingar, byte av lokaler eller nya ägare, utan även operativa företeelser, incidenter och nästan-incidenter som händelsevis inte påverkade leveransen av it-tjänsten. Sådana händelser kan till exempel omfatta hög personalomsättning, brist på nyckelkompetenser, eller fysiska eller digitala intrång i produktionsmiljön som inte föranleder produktionsavvikelser.

SAMVERKAN MED LEVERANTÖRER

Ett uppdragsavtal inskränker inte ett försäkringsföretags ansvar[23] och kvaliteten i försäkringsföretagets företagsstyrningssystem får inte försämras väsentligt vid utlagd verksamhet.[24] Ett försäkringsföretag måste kunna visa att styrning och bevakning av it-verksamheten är ändamålsenlig[25] och hur verksamheten uppfyller kraven på riskhantering[26].

I praktiken innebär detta att samverkan med leverantörer inom it-verksamheten bland annat ska omfatta följande:

18 Artikel 274.4 k och l i EU-förordningen.

19 Artikel 274.4 e i EU-förordningen och Riktlinje 63 d i Riktlinjerna.

20 Se *Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer* som publicerats på fi.se.

21 Med ”inte förhandlingsbar” menas att ett uppdragsavtal inom it-verksamheten minst måste omfatta revisionsrätt enligt de lagkrav som finns.

22 Artikel 274.1 c i EU-förordningen.

23 10 kap. 19 § FRL.

24 10 kap. 20.1 § FRL.

25 Se särskilt artikel 258.1 b och j i EU-förordningen.

26 Artikel 259.1-3 och 260.1 f i EU-förordningen.

- Det ska finnas ett effektivt samarbete och en effektiv rapportering och förmedling av information på alla relevanta nivåer i samverkansmodellen.[27]
- Samverkansmodellen ska klart ange rapporteringsvägar och fördelning av funktioner och ansvarsområden.[28]
- Samverkansmodellen ska beakta art, omfattning och komplexitet hos de inneboende riskerna i företagets verksamhet.[29]
- Det ska finnas informationssystem som levererar fullständig, tillförlitlig, klar, konsekvent utformad och relevant information i rätt tid om verksamheten, de åtaganden som gjorts och de risker som företaget är exponerat för.[30]
- Styrdokumentet för hantering av operativ risk bör fastställa vilka riskerna är och hur de kan reduceras, definiera aktiviteter och processer för att hantera de operativa riskerna inklusive de it-system som stödjer dem, och ange risktoleransgränser för de viktigaste operativa riskerna som företaget kan exponeras för.[31]
- Kontroll- och rapporteringsorganen inom internkontrollsystemet bör ge företagets förvaltnings-, lednings- eller tillsynsorgan relevant information för beslutsprocesserna.[32]
- Framväxande risker på operativ, taktisk och strategisk nivå ska identifieras, bedömas, sammanställas och eskaleras inbegripet de it-system som berörs.[33]
- Risktoleransgränser för de områden som är viktigast när det gäller företagets exponering för operativ risk ska kunna fastställas.[34]

Alla försäkringsföretag som ingick i analysen hade samverkansmodeller som omfattade operativa, taktiska och strategiska möten och informationsutbyten. Försäkringsföretagens representation i de olika forumen var snarlika förutom på strategisk nivå där vissa försäkringsföretag valt att inte involvera sin verkställande direktör medan andra sett det som en självklarhet att göra det.

FI observerade också att hur samverkansmodellerna utformas till viss del är beroende av försäkringsföretagets förhandlingsposition. Vissa stora it-leverantörer anpassar sina samverkansmodeller efter försäkringsföretagets önskemål medan andra är mindre flexibla. Vissa leverantörer godtar försäkringsföretagets standardavtal som bas för

27 Artikel 258.1 a i EU-förordningen.

28 Artikel 258.1 b i EU-förordningen.

29 Artikel 258.1 b i EU-förordningen.

30 Artikel 258.1 h i EU förordningen. Kravet gäller oberoende av om en funktion eller aktivitet utförs i försäkringsföretaget eller hos en leverantör, ref. 10 kap. 19 § FRL.

31 Riktlinje 21 i Riktlinjerna.

32 Riktlinje 39 i Riktlinjerna.

33 Artikel 260.1 f och 269.1 e i EU-förordningen, och riktlinje 21 i Riktlinjerna.

34 Riktlinje 21 c i Riktlinjerna.

leveransen, medan andra bara levererar tjänster utifrån sina egna avtalsmallar.

FI vill understryka att det ställs höga krav på transparens från leverantörerna för att ett försäkringsföretag ska kunna uppfylla regelkraven, oberoende av vilka mallar som ligger till grund för uppdragsavtalen.[35]

FI kan konstatera att försäkringsföretagen generellt har god översikt över sina it-leverantörer, men att jämförbara försäkringsföretag som köper samma it-tjänst från samma leverantör gjorde olika bedömningar om it-leverantörernas och deras underleverantörers relevans vad gäller styrning och kontroll.

Skillnaderna i bedömningarna beror framförallt på olika åsikter om hur rimligt det är att kontrollera perifera underleverantörer, och svårigheter med att skapa tydliga gränsdragningar för hur olika typer av tjänster ska kategoriseras[36]. Men skillnaderna beror också på erfarenheter försäkringsföretagen har gjort när beredskapsplanerna har testats. Det visar i sin tur vikten av att regelbundet testa beredskapsplanerna för att uppnå ändamålsenlig samverkan, styrning och kontroll av uppdragsavtal inom it-verksamheten.

SÄRSKILDA OBSERVATIONER OM MOLNTJÄNSTER

Uppdragsavtal får inte avse operativ verksamhet eller funktioner som är av väsentlig betydelse om det kan leda till att den operativa risken i företaget ökar väsentligt. Försäkringsföretag måste därför kunna redogöra för bland annat informationssäkerhet och fysisk säkerhet i infrastrukturen, oberoende av var informationen lagras eller bearbetas.

Försäkringsföretagen måste själva ta ställning till om riskhantering, styrning och kontroll av varje del av it-verksamheten är ändamålsenlig, givet de olika tjänsternas betydelse för försäkringsverksamheten och i ljuset av kraven på riskhantering, konsumentskydd, integritet och kontinuitet.[37]

I de fall FI diskuterade molntjänster med försäkringsföretagen i den fördjupade analysen lades mycket kraft på att förstå företagens geopolitiska omvärldsbevakning och hur den påverkar försäkringsföretagens beslut och bevakning av molntjänsterna.

FI bedömer att försäkringsföretagens styrning och kontroll generellt är ändamålsenlig i förhållande till molntjänsternas utformning, men att försäkringsföretagen bör ha en tydlig uppfattning om politiska system och praxis i länderna där data lagras eller bearbetas.

AVVECKLING AV UPPDRAGSAVTAL

Försäkringsföretagen i analysen kunde visa att man säkerställt rätten att avsluta ett avtal utan att det inkräktar på kontinuitet och kvalitet av tjänster gentemot försäkringstagarna. På frågan om dokumentation av företagets tillvägagångssätt för att avsluta uppdragsavtal som omfattar

35 Se även avsnittet om molntjänster.

36 Till exempel ”vad är en molntjänst”, ”vad är ett system”, ”vad är en funktion”.

37 Se också *Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer*, publicerad på FI:s webbplats.

kritiska eller viktiga funktioner[38] visade det sig dock att vissa av de presenterade tillvägagångssätten endast bestod av rudimentära planer, i nivå med en projektmall. I praktiken var alltså tillvägagångssättet att etablera ett tillvägagångssätt när det behövdes.

Förklaringen som gavs till detta var att omvärlden och förutsättningar förändras i så snabb takt att avvecklingsplanerna ständigt skulle behöva uppdateras. För att undvika risken att ha en inaktuell plan när den väl behövs valde man i stället att bara ha en mall.

Även om det finns en viss rimlighet i detta resonemang anser FI att en rudimentär projektmall för att avveckla ett uppdragsavtal inte är tillfredsställande. Avvecklings- och återtagsplaner bör innehålla konkreta aktiviteter som försäkringsföretaget avser att genomföra, och aktiviteterna som beskrivs bör vara så detaljerade att det går att ta ställning till om och hur och med vilka förutsättningar de låter sig genomföras. Flertalet försäkringsföretag lyckades tydligt förklara detta för FI.

Observera att vid upphandling av viktiga it-tjänster brukar det ingå att köparen tar ställning till vilken strategi för avslutande (exitstrategi) som ska tillämpas om och när avtalet sägs upp. Exitstrategins omfattning ingår således i beslutsunderlaget när företaget väljer leverantör i syfte att skapa medvetenhet och förebygga inlåsningseffekter.

38 Riktlinje 63 d om styrdokument för uppdragsavtal i Riktlinjerna.

Riskhantering

I vissa försäkringsföretag saknas regelbunden kontroll av den utlagda verksamheten för att man ska kunna avgöra om riskbedömningen som gjordes vid upphandlingstillfället fortfarande är aktuell. Att regelbundet testa sin beredskapsplan är lika viktigt som att ha en sådan. I vissa försäkringsföretag underskattas också operativa risker i de övergripande styrprocesserna. Alla försäkringsföretagen i analysen arbetar dock systematiskt med att bevaka cyberrisker. De använder också utbildning och informationsspridning som en viktig del av skyddsåtgärderna.

IT-VERKSAMHET AV VÄSENTLIG BETYDELSE

Ett försäkringsföretag ska kunna redogöra för hur det identifierar, sammanställer, eskalerar och bedömer framväxande risker på operativ, taktisk och strategisk nivå i verksamheten, inbegripet de it-system som berörs.[39] Försäkringsföretaget ska också kunna redogöra för vilka effekter ett uppdragsavtal har på företagets verksamhet.[40]

Försäkringsföretag som ingått eller överväger att ingå ett uppdragsavtal bör i styrdokumentet för uppdragsavtal ange vilken process som de ska följa, hur urvalet ska gå till och hur avtalet ska följas upp.[41] Här ingår särskilt en beskrivning av processen för att bestämma om en funktion eller aktivitet är kritisk eller viktig, det vill säga av väsentlig betydelse.

FI kom fram till att processen för att fastställa om en utlagd funktion är av väsentlig betydelse typiskt sett var knuten till inköpsprocessen och varje enskilt upphandlingstillfälle. De flesta av försäkringsföretagen som analyserades har processer för att i någon form bevaka om bedömningen ska ändras. Men FI observerade också fall där en sådan uppföljning saknas eller processerna brister.

FI anser att ett försäkringsföretag regelbundet bör utvärdera om utlagda tjänster har ändrat karaktär, det vill säga om tjänsterna över tid har blivit mer eller mindre kritiska för verksamheten respektive mer eller mindre sårbara än vid upphandlingstillfället.[42] Även i andra regelbundna process- och rutinbedömningar bör hänsyn tas till framväxande risker på operativ, taktisk och strategisk nivå.

KONTINUITET I VERKSAMHETEN

Ett försäkringsföretag ska ha en beredskapsplan[43] och riskhanteringssystemet ska innefatta strategier för att identifiera, värdera, övervaka, hantera och rapportera risker som de är eller kan bli exponerade för samt deras inbördes beroende[44]. Ett försäkringsföretag måste således inte bara ha kontroll över riskbild,

39 Artikel 269.1 e i EU-förordningen och Riktlinje 21 i Riktlinjerna.

40 10 kap. 19 § FRL och artikel 260.1 f och 274 i EU-förordningen.

41 Riktlinje 63 i Riktlinjerna.

42 Artikel 274.5 i EU-förordningen och riktlinje 63 i Riktlinjerna.

43 FRL 10 kap. 3 §.

44 FRL 10 kap. 6 §.

beredskap och skyddsåtgärder hos sig och sina leverantörer utan även hos leverantörernas underleverantörer.

Försäkringsföretagen i den fördjupade analysen hade valt olika sätt att utforma sina beredskapsplaner. Vissa företag höll beredskapsplanen på en övergripande nivå och kompletterade planen med checklistor och rutinbeskrivningar i andra dokument och verktyg. I andra företag var den dokumenterade beredskapsplanen det verktyg de avser att använda i en krissituation.

Inom ramen för den fördjupade analysen ville FI säkerställa att beredskapsplanerna uppfyllde fyra viktiga kriterier[45]:

- Beskrivning av verksamheten och vilka scenarier planen avser att förebygga och hantera.
- Handlingsalternativ för de olika scenarierna.
- Införande i verksamheten, det vill säga hur man praktiskt ska gå tillväga vid olika händelser.
- Ständig förbättring, det vill säga att regelbundet testa och uppdatera planen så att den till varje tid är aktuell och relevant.

Genomgående för alla granskade beredskapsplaner var att det krävdes ytterligare förklaringar vid platsbesöken för att FI skulle kunna bilda sig en uppfattning om planerna var ändamålsenligt utformade och uppfyllde sina syften.

Granskningen visade också att realistiska tester av beredskapsplanen i normalfallet inte leder till slutsatsen att allt går som planerat utan att man alltid stöter på överraskningar, upptäcker svagheter och får viktiga nya insikter.

Alla försäkringsföretagen i den fördjupade analysen kunde redogöra för leverantörernas beredskapsplaner och deras status.[46] FI bedömer att företagen överlag har ändamålsenliga beredskapsplaner, men att alla har förbättringspotential i någon del av planernas livscykel. Att företagen regelbundet testar planerna är avgörande för att de ska kunna identifiera var förbättringsbehovet finns.

ÖVERVAKNING AV OPERATIVA RISKER

Ett uppdragsavtal inskränker inte ett försäkringsföretags ansvar[47] och ett försäkringsföretag måste kunna visa hur kraven på riskhantering uppfylls i verksamheten[48].

Verksamhetens riskhanteringssystem ska omfatta att identifiera, värdera, övervaka, hantera och rapportera risker samt deras inbördes beroende och systemet ska vara integrerat i företagets organisations- och beslutsstruktur.[49]

Operativa risker innefattar alla typer av it-risker och kravet om att noggrant och korrekt registrera uppgifter om företagets verksamhet

45 Detta kallas ofta kontinuitetsarbetets livscykel.

46 Artikel 274.5 d i EU-förordningen.

47 10 kap. 19 § FRL.

48 Artikel 259 och 260.1 f i EU-förordningen.

49 10 kap. 6 § FRL.

och interna organisation omfattar även företagets it-verksamhet och dess organisation.[50] Vid uppdragsavtal har försäkringsföretaget det fullständiga ansvaret för att den utlagda verksamheten utförs enligt gällande lagar och andra regler. Företaget måste därför kunna redogöra för alla delar av it-verksamheten, oberoende av var och av vem den utförs.[51]

Vad gäller rapporterings- och övervakningsrutiner[52] tillämpar alla försäkringsföretagen i den fördjupade analysen någon form av regelbunden statusrapportering i förhållande till den avtalade leveransen. Vissa företag använder styrkort med nyckeltal och indikatorer som återanvänds i taktiska och strategiska fora.

Hur företagen ska utforma kontrollmiljön och hur de ska tillämpa olika typer av kontroller gentemot leverantörer finns generellt beskrivet i styrdokument eller handböcker. I styrdokument för uppdragsavtal saknas dock ofta referenser till stödjande dokument respektive var det finns beskrivning av vilka effekter uppdragsavtalen har för försäkringsföretagets verksamhet.[53]

I försäkringsföretag som ingår i en försäkringsgrupp (eller motsvarande) är det stora skillnader på vilket inflytande vissa av företagen har när syster- eller moderföretag levererar en it-tjänst som antingen produceras centralt eller levereras av en extern leverantör till hela gruppen.[54] I försäkringsgrupper där det enskilda försäkringsföretagets inflytande är starkt deltar företaget i gruppgemensamma beslutsfora där ansvar, mandat och handlingsfrihet är tydliga och väl förankrade.

I försäkringsgrupper där det enskilda försäkringsföretagets inflytande är svagt fattas beslut centralt utan att företaget involverats i nämnvärd omfattning. Styrdokument (och även beslutsdokument) kan ange att processen ska vara annorlunda, men i praktiken kan inte försäkringsföretaget som får tjänsten levererad via ett annat företag i gruppen påverka tjänsten eller beslutet. Beslutspunkten på styrelsens agenda är i realiteten en informationspunkt.

Sammanfattningsvis är övervakningen av operativa risker i försäkringsföretag i stor grad fokuserad på mätetal och processer som avser själva it-produktionen. I vissa försäkringsföretag kan FI konstatera att man underskattar övervakning och hantering av svagheter som kan uppstå i nyckelprocesserna som ska leda till att it-verksamheten producerar ändamålsenliga tjänster.

50 Artikel 258.1 i i EU-förordningen

51 Artikel 258.1 b i EU-förordningen

52 Artikel 274.1 i EU-förordningen.

53 Artikel 274.1 i EU-förordningen.

54 Artikel 274.2 i EU-förordningen.

CYBER- OCH INFORMATIONSSÄKERHET

Vid försäkringsföretagens redogörelse av cyberrisker var FI:s huvudsakliga intresse att förstå hur företagen arbetar med bevakning av cyberrisker generellt och hur de identifierar cyberrisker som är särskilt relevanta för deras verksamhet.[55]

Inga av företagen tog självmant upp frågan om i vilken grad risker förknippade med politiska system och praxis i tredje land utgjorde ett hot mot deras it-verksamhet. FI anser att det är viktigt att utvärdera och bevaka det geopolitiska läget i samband med utläggning av it-verksamhet utanför EU, och att även granska it-leverantörernas ägar- och koncernkonstellationer.

I tillägg till informationssäkerhet och fysiska skyddsåtgärder[56] arbetar försäkringsföretagen i analysen med utbildning och informationsspridning för att höja riskmedvetandet hos sina medarbetare. Höga chefsbefattningar från försäkringsverksamheten ingår ofta i arbetsgrupper som fokuserar på cyberrisker.

FI kan konstatera att alla försäkringsföretag som ingick i den fördjupade analysen arbetar systematiskt med cyberrisker och kan redogöra för vilket hot olika typer av risker utgör och vilka konsekvenser de får om de inträffar. Många av företagen understryker vikten av lokal kunskap i tillägg till de risker som är kända globalt.

Det framgår dock av redogörelserna att både risker och konsekvenser ofta är svåra att bedöma och att kunskapen som krävs kring dessa frågor blir alltmer specialiserad.

55 Artikel 260.1 f i EU-förordningen.

56 Se eget avsnitt.

Bilaga 1

INFORMATION FI BEGÄRDE INFÖR PLATSBESÖK

- Styrdokumentet för verksamhet som omfattas av uppdragsavtal;[57]
- Beredskapsplan, inklusive utfallet av senaste test av planen;[58]
- En lista över leverantörer av it-tjänster och vilka tjänster de levererar;[59]
- It-strategi eller motsvarande som visar hur it-verksamheten är organiserad och hur it-verksamheten är avsedd att främja företagets strategiska mål;[60]
- Internrevisionsfunktionens bedömning av företagets företagsstyrningssystem avseende it-verksamheten och uppdragsavtalen de senaste två åren, under förutsättning att funktionen har granskat dessa delar under nämnd tidsperiod.[61]

MÖTESAGENDA[62]

1. Redogör för it-verksamhetens leveransstruktur[63], dvs. vilka tjänster som
    a. produceras inom företaget;
    b. levereras av dotter-, syster- eller moderföretag;
    c. levereras av externa parter via dotter-, syster- eller moderföretag;
    d. levereras av externa parter direkt till företaget;
    e. levereras av externa parters underleverantörer (eller där externa parters underleverantörer bidrar till leverans av en tjänst).
2. Redogör för företagets process för att fastställa och dokumentera om en funktion eller aktivitet som omfattas av ett uppdragsavtal är en kritisk eller viktig funktion eller aktivitet.[64]

57 10 kap. 2 § första stycket punkt 4 FRL.

58 10 kap. 3 § FRL.

59 17 kap. 5 § FRL.

60 Artikel 258.1 b i EU-förordningen.

61 10 kap. 17 § FRL.

62 Agendan skiljde sig något mellan försäkringsföretagen beroende på koncernstruktur.

63 Artikel 258.1 b i EU-förordningen.

64 Riktlinje 63 a i Riktlinjerna.

3. Redogör för
    a. vilka av tjänsterna i punkterna 1.a–1.e ovan som bedömts vara kritiska eller viktiga;[65]
    b. hur samverkan med leverantörerna av dessa tjänster ser ut, (t ex. uppföljning och framåtblickande planering).

I agendapunkterna 4–7 nedan önskar FI att företagets redogörelser fokuserar på ett urval av tjänsterna. Vilka tjänster och leverantörer det rör skickas från FI till företaget ungefär en vecka innan mötet.

4. Redogör för hur företaget övervakar de operativa riskerna förknippade med punkterna 1.a–1.e ovan.[66] I denna punkt önskar FI att företaget även redovisar
    a. vilka rapporterings- och övervakningsrutiner som tillämpas *per leverantör*[67];
    b. status och omfattning av leverantörernas beredskapsplaner,[68] (med status menas när planen senast uppdaterades och testades);
    c. vilken kontroll och inflytande företaget har vad gäller leveranser från dotter-, syster- eller moderföretag;[69]
    d. vilken kontroll och inflytande företaget har vad gäller leveranser från externa aktörer som sker via dotter,- syster- eller moderföretag.[70]
5. Redogör för hur den fysiska och digitala säkerheten ser ut där information bearbetas och lagras
    a. i företaget;[70]
    b. i dotter-, syster- eller moderföretag;[71]
    c. hos externa parter;[71]
    d. hos externa parters underleverantörer.[71 och 72]
6. Redogör för *varje avtals utformning* vad gäller
    a. företagets och FI:s rätt till uppgifter som rör den verksamhet eller de funktioner som omfattas av uppdragsavtalet;[73]

65 Riktlinje 60 i Riktlinjerna.

66 Artikel 260.1 f i EU-förordningen.

67 Artikel 274.1 i EU-förordningen.

68 Artikel 274.5 d i EU-förordningen.

69 Artikel 274.2 i EU-förordningen.

70 Artikel 258.1 j i EU-förordningen.

71 10 kap. 20 § punkt 2 FRL och artikel 274.3 a, e och f i EU-förordningen.

72 10 kap. 20 § punkt 3 FRL.

73 10 kap. 22 § punkt 2 FRL och artikel 274.4 h i EU-förordningen.

b. företagets och FI:s rätt att genomföra inspektioner på plats i tjänsteleverantörens lokaler;[74]

c. FI:s rätt att ställa frågor direkt till tjänsteleverantören, som ska besvara frågorna;[75]

d. att tjänsteleverantörens skyldigheter och ansvarsområden inte ska påverkas av någon underentreprenad.[76]

e. rätt att avsluta avtalet utan att det inkräktar på kontinuitet och kvalitet av tjänster gentemot försäkringstagarna.[77]

7. Redogör för var och en av tillvägagångssätten som planerats för att avsluta uppdragsavtalen i punkt 6 ovan.[78]

8. Redogör för de cyberrisker företaget identifierat som relevanta för verksamheten och vilka skyddsåtgärder företaget tillämpar.[79]

   Med cyberrisker menar Finansinspektionen risker som uppkommer vid användning av elektroniska data och dess överföring över exempelvis internet och telekommunikationsnätverk.

74 10 kap. 22 § punkt 3 FRL och artikel 274.4 h i EU-förordningen.

75 Artikel 274.4 i i EU-förordningen.

76 Artikel 274.4 k och l i EU-förordningen.

77 Artikel 274.4 e i EU-förordningen.

78 Artikel 274.4 e i EU-förordningen och riktlinje 63 d i Eiopas riktlinjer.

79 Artikel 260.1 f i EU-förordningen.

Bilaga 2

BEGREPP OCH DEFINITIONER

Cyberrisker: Risker som uppkommer vid användning av elektroniska data och dess överföring över exempelvis internet och telekommunikationsnätverk.

Informationssäkerhet: Skydd av konfidentialitet, riktighet och tillgänglighet hos information.

Insurtech: Ny teknik och innovativa lösningar som gör det möjligt att skapa nya, bättre eller billigare försäkringsprodukter.

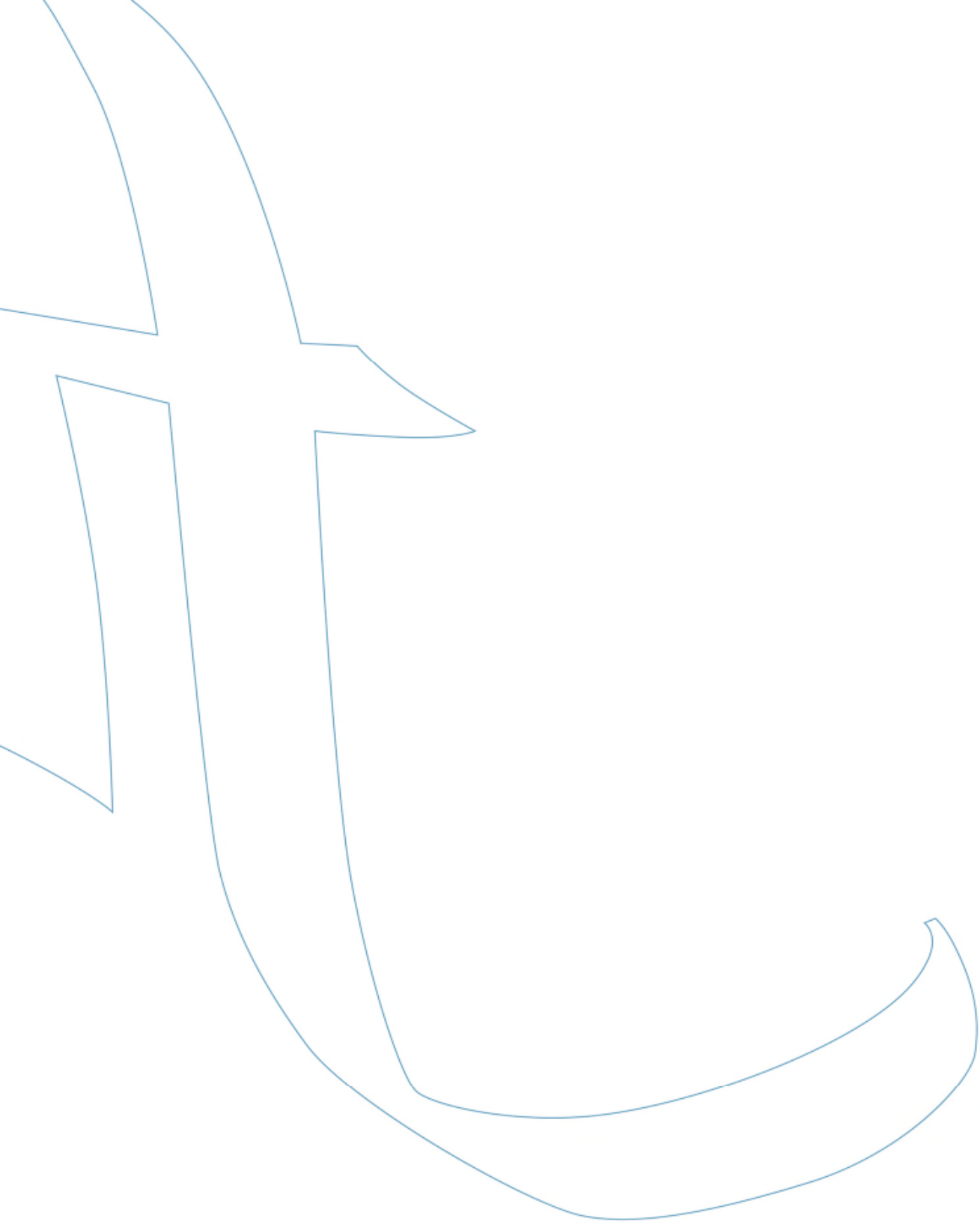
It-risker: Risker förknippade med personal, processer, system och externa faktorer som påverkar it-verksamheten.

It-strategi: Grundläggande vägval för it-verksamheten för att stödja [försäkrings]verksamhetens kritiska framgångsfaktorer.

It-verksamhet: Ett företags organisation, processer och personal för att hantera it-system

Molntjänst: It-tjänster som tillhandahålls med hjälp av så kallad *cloud computing*, det vill säga en teknisk infrastruktur och arkitektur som möjliggör enkel och flexibel tillgång till datorresurser genom att kapaciteten delas mellan många användare. Molntjänster kan bygga på olika typer infrastruktur:

- Public cloud: tillgänglig för allmänheten.
- Private cloud; enbart tillgänglig inom en institution.
- Community cloud: tillgänglig för medlemmar/deltagare.
- Hybrid cloud: en kombination av ovanstående.



Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
Fax +48 8 24 13 35
finansinspektionen@fi.se

www.fi.se