FI-tillsyn

Bankernas kontinuitetshantering

Nr 18

9 juni 2020

9 juni 2020
Dnr 20-11770

INNEHÅLL

FI-tillsyn

Finansinspektionen publicerar återkommande tillsynsrapporter i en numrerad rapportserie. Tillsynsrapporterna är en del av FI:s kommunikation. De handlar om genomförda undersökningar och annan tillsyn som FI utför. I rapporterna informerar vi om vilka iakttagelser och bedömningar som FI har gjort och om våra förväntningar i olika frågor. Detta kan vara till stöd för företagen i deras verksamhet.

Sammanfattning

Finansinspektionens (FI) tillsyn visar att många banker arbetar aktivt med kontinuitetshantering och har genomfört viktiga åtgärder för att reducera risken för allvarliga avbrott i verksamheten. Samtidigt anser vi att bankerna behöver stärka sin kontinuitetshantering ytterligare. FI förväntar sig att bankerna fortsatt fokuserar på att stärka sin motståndskraft för sina kritiska funktioner.

När denna tillsynsrapport publiceras pågår fortfarande spridningen av det nya coronaviruset. De konsekvenser som pandemin har fått framhäver ytterligare vikten av bankernas kontinuitetshantering. Bankerna har sedan en tid tillbaka aktiverat sin krishantering. De uppdaterar löpande relevanta scenarier och planer för den rådande situationen. Detta har till stora delar fungerat, men uthålligheten över tid återstår att följa upp. Eftersom denna tillsynsrapport omfattar FI:s tillsyn för 2018 och 2019 behandlar den inte särskilt bankernas kontinuitetshantering i förhållande till pandemins effekter på verksamheten.

Många av bankernas produkter och tjänster fyller samhällsviktiga funktioner. Avbrott i dessa tjänster kan medföra stora konsekvenser för konsumenter. Allvarliga upprepade avbrott i bankernas tjänster kan även leda till ett minskat förtroende för det finansiella systemet och i värsta fall hota den finansiella stabiliteten.

Den ökande graden av digitalisering och globalisering samt ett förändrat konsumentbeteende har lett till att infrastrukturen för bankernas tjänster har blivit mer komplex. Många banker gör omfattande förändringar för att anpassa sin verksamhet och sitt tjänsteutbud i takt med att omvärlden förändras. FI bedömer att detta, åtminstone på kort sikt, kan leda till högre operativa risker i bankernas verksamheter, där en konsekvens kan bli allvarliga störningar. Under 2020 har även följderna av det nya coronaviruset ytterligare visat på vikten av beredskap för scenarier som kan anses osannolika inom samtliga sektorer, inte minst den finansiella.

Bankerna behöver därför ha en robust kontinuitetshantering på plats som är väl integrerad i verksamheten och motståndskraftig mot alla typer av händelser som kan orsaka allvarliga avbrott. Vår tillsyn visar att bankerna arbetar aktivt med sin kontinuitetshantering, samtidigt som det finns ytterligare behov av förbättring. Sammanfattat vill FI generellt gärna se förbättringar hos bankernas kontinuitetshantering inom följande områden:

- Stärka den interna styrningen och kontrollen av kontinuitetshanteringen, innefattat kontinuitetshanteringsstrategin, riskaptiten för operativ risk samt de oberoende kontrollfunktionerna.

- Vidareutveckla metoderna för konsekvensanalyser för att säkerställa att samtliga kritiska funktioner inklusive dess beroenden till varandra och till stödfunktioner identifieras.
- Tydliggöra innehåll och struktur för beredskapsplaner, kontinuitetsplaner och återställningsplaner.
- Säkerställa att ändamålsenliga kontinuitetstester genomförs för samtliga processer av väsentlig betydelse och de it-system som stödjer dessa processer.
- Förbättra rapporteringen av resultatet av utförda kontinuitetstester så att ledning och styrelse får relevant och meningsfull information.

FI:s tillsyn av kontinuitetshantering

I denna rapport redogör FI på ett generellt plan för slutsatserna av den tillsyn av bankernas kontinuitetshantering som gjordes under 2018 och 2019. I detta kapitel beskrivs varför kontinuitetshantering prioriteras i tillsynen, FI:s nuvarande syn på riskbilden och vilka regler som bankerna i huvudsak behöver följa när det gäller kontinuitetshantering.

VIKTEN AV KONTINUITETSHANTERING

Kontinuitetshantering kan beskrivas som processer och rutiner som syftar till att säkerställa att de mest kritiska aktiviteterna i en verksamhet kan upprätthållas på en acceptabel nivå när en allvarlig operativ störning uppstår. I kontinuitetshantering ingår också att verksamheten efter en sådan allvarlig störning ska kunna återställas till ett normalt läge. Vad som är kritiska aktiviteter och acceptabel nivå behöver ställas i relation till vilka konsekvenser en störning potentiellt kan få.

Många av bankernas produkter och tjänster fyller samhällsviktiga funktioner. Om det blir avbrott i dessa tjänster kan det medföra stora konsekvenser för konsumenter. Allvarliga upprepade avbrott i bankernas tjänster kan även leda till ett minskat förtroende för det finansiella systemet och i värsta fall hota den finansiella stabiliteten. Bankerna behöver därför ha en fungerande kontinuitetshantering som är väl integrerad i verksamheten och motståndskraftig mot alla typer av händelser som kan orsaka allvarliga avbrott.

Under 2020 har även följderna av coronavirusets spridning ytterligare visat på vikten av beredskap för scenarier som kan anses osannolika inom samtliga sektorer, inte minst den finansiella.

RISKER FÖR AVBROTT I VERKSAMHETEN

I och med den ökande graden av digitalisering och globalisering samt ett förändrat konsumentbeteende har infrastrukturen för bankernas tjänster blivit mer komplex. Många banker genomför stora förändringar inom sina verksamheter, inte minst i sina it-miljöer, för att förnya tjänsteutbudet och anpassa sig till nya regelverk. Det innebär bland annat att nya arbetssätt och it-system införs, samtidigt som arbete pågår för att fasa ut vissa äldre lösningar.

Detta förändringstryck kan leda till högre operativa risker hos bankerna, som bland annat kan orsaka avbrott i verksamheten. Ofta krävs det även en övergångsperiod från det att en ny lösning har införts till dess att en gammal lösning helt kan tas ur bruk, i de fall det alls är möjligt. Detta innebär att en ännu högre grad av komplexitet uppstår i verksamheten under denna period.

Vidare ska tjänsteutbudet med tillhörande processer och it-system löpande uppdateras och anpassas för att sedan snabbt nå marknaden. Detta innebär att det höga förändringstrycket numera är en ständig del av verksamheten. Därtill lägger bankerna i större omfattning ut delar av sin verksamhet till externa leverantörer, som många gånger är internationella företag med verksamhet i olika delar av världen. Dessa

företag kan i sin tur använda sig av underleverantörer, vilket gör att bankerna blir beroende av fler externa leverantörer.

Sammantaget är det FI:s bedömning att den ökande graden av komplexitet och förändringstryck inom bankernas verksamheter även har lett till högre risk för allvarliga avbrott i bankernas tjänster.

REGLER OCH STANDARDER FÖR KONTINUITETSHANTERING

De krav på kontinuitetshantering som ställs på banker utgår från reglerna om riskhantering som finns i 6 kap. 2 § lagen (2004:297) om bank och finansieringsrörelse. Till det har FI utfärdat följande föreskrifter och allmänna råd som preciserar lagkravet:

- Föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut.
- Föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker.
- Föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem.

Europeiska bankmyndigheten (EBA) har även gett ut riktlinjer[1] om kontinuitetshantering inom ramen för bland annat

- riktlinjer för intern styrning (EBA-GL-2017-11)
- riktlinjer för hantering av IKT-risker och säkerhetsrisker (EBA-GL-2019-04)
- riktlinjer för utkontraktering (EBA-GL-2019-02).

Det finns även en rad internationella standarder samt god praxis som helt eller delvis fokuserar på kontinuitetshantering, exempelvis följande:

ISO 22301:2012,

Societal security – Business continuity management systems,

Control Objectives for Information & Related Technology (COBIT),

The Business Continuity Institute Good Practice Guidelines (GPG) och

FSPOS Vägledning för Kontinuitetshantering.

Under senare år har branschorganisationer och tillsynsmyndigheter inom finansiell sektor arbetat vidare med begreppet operativ motståndskraft (Operational Resilience), detta är något som kan beskrivas som en vidareutveckling av kontinuitetshantering. Denna tillsynsrapport riktar dock in sig på den tillsyn som FI har utövat över kontinuitetshantering och kommer inte att ytterligare behandla operativ motståndskraft.

1 Riktlinjer utfärdade av EBA är att betrakta som allmänna råd.

Iakttagelser från tillsynen

Bankerna behöver ta hänsyn till sin storlek samt till verksamhetens art, omfattning och komplexitet i arbetet för att uppnå en tillräckligt ändamålsenlig och effektiv kontinuitetshantering. De behöver också ha processer och kontroller på plats, baserade på de regler som gäller[2].

STYRNING OCH KONTROLL

Strategi och riskaptit för kontinuitetshantering

FI föreskriver att bankerna ska ha en dokumenterad riskaptit som omfattar alla slag av risker, inklusive operativa risker[3]. FI föreskriver även att bankerna ska ha en riskstrategi. Riskstrategin kan ses som styrelsens och ledningens verktyg för att i rimlig grad säkerställa att bankens riskexponering är i linje med den fastställda riskaptiten.

Risk för allvarliga avbrott i verksamheten får anses vara en väsentlig operativ risk som bankernas styrelse och ledning behöver vara aktivt engagerade i. FI anser det därför lämpligt att denna risk omhändertas inom ramen för bankernas fastställda riskaptiter. Exempel på riskaptit i denna kontext kan vara vilka särskilda scenarier banken ska klara av i händelse av en allvarlig störning.

Vi ser gärna att kontinuitetshanteringen är en integrerad del i bankens riskstrategi, eftersom det är en avgörande komponent för hur robust och motståndskraftig bankens operativa verksamhet är vid allvarliga störningar. Faktorer som antal datahallar en bank använder sig av samt hur tillgängliga reservarbetsplatser och distansarbetslösningar är kan vara avgörande för hur väl en bank kan upprätthålla sina viktigaste funktioner i händelse av en allvarlig störning. I vilken utsträckning banken har identifierat och hanterat beroendet av nyckelpersoner bland de anställda kan också vara avgörande.

En bank behöver i detta avseende göra en mängd strategiska val. Det är viktigt att dessa val är väl grundade, medvetna och i linje med bankens riskaptit. Dessa strategiska val kan med fördel uttryckas genom en strategi för kontinuitetshantering. Det underlättar arbetet om strategin ger en tydlig bild av bankens önskade kapacitet och förmåga när det gäller kontinuitetshantering och vilka typer av scenarier banken har som målsättning att klara av, respektive accepterar att inte klara av. Exempelvis kan banken inom ramen för strategin redogöra för hur dess mest kritiska funktioner kan upprätthållas om en datahall fallerar (under förutsättning att banken driver sin verksamhet i två separata datahallar). Dock kan de mest kritiska funktionerna inte upprätthållas om båda datahallarna slås ut samtidigt, en risk som banken måste vara medveten om. FI anser att denna typ av konkreta

2 Bl.a. bestämmelserna i 6 kap. 2 § lag (2004:297) om bank och finansieringsrörelse, Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1), om hantering av operativa risker (FFFS 2014:4) och om informationssäkerhet, it-verksamhet och insättningssystem (FFFS 2014:5).

3 FFFS 2014:1

ställningstaganden är ett viktigt och inte minst, begripligt verktyg för bankens ledning och styrelse i styrningen av kontinuitetshanteringen. Vi anser det även lämpligt att bankens styrelse, som är ytterst ansvarig för bankens verksamhet, fattar beslut om kontinuitetshanteringsstrategin. På så sätt säkerställer man styrelsens kännedom om bankens operativa motståndskraft i händelse av en allvarlig störning och styrelsens engagemang i hur banken ska sköta sin kontinuitetshantering.

Erfarenheter från tillsynen av strategi och riskaptit för kontinuitetshantering

FI:s erfarenheter från tillsynen visar att bankerna kan bli bättre på att utforma och tydliggöra hur risken för allvarliga avbrott omhändertas i sin riskaptit. Vi anser också att bankerna kan tydliggöra sina strategier för kontinuitetshantering. Exempel på vad som behöver förtydligas:

- Vilka typer av händelser som verksamheten ska klara av och med vilka medel.
- Vilka delar av verksamheten som ska prioriteras och till vilken grad de prioriterade delarna ska upprätthållas.
- Vilka typer av händelser som verksamheten rimligen inte kan klara av, samt tydliggöra vilka risker banken därmed accepterar.

FI anser även att det finns utrymme för förbättring av i vilken utsträckning bankernas ledningar och styrelser engagerar sig i dessa frågor.

Organisation och ansvarsfördelning

Arbetet med kontinuitetshantering ska precis som all övrig verksamhet inom bankerna utföras utifrån principerna om de tre försvarslinjerna. Det innebär att den första försvarslinjen, verksamheten, äger riskerna inom sitt område och är ytterst ansvarig för att kontinuiteten kan upprätthållas i den grad som banken har beslutat om, i händelse av en allvarlig störning.

FI anser att samtliga delar av det operativa arbetet med en banks kontinuitetshantering ska utföras av funktionerna i första försvarslinjen. Med det operativa arbetet avses dels de olika processer och rutiner som ryms inom ramen för en banks ramverk för sin kontinuitetshantering. Exempel på processer och rutiner kan vara att göra konsekvens- och riskanalyser, upprätta kontinuitetsplaner och göra kontinuitetstester. I det operativa arbetet ingår även att leda och koordinera samt att fatta beslut inom de nämnda processerna och rutinerna. På så sätt tydliggörs verksamhetens yttersta ansvar för sin egen kontinuitetshantering.

Den andra försvarslinjen, som består av de oberoende kontrollfunktionerna för riskkontroll och för regelefterlevnad, ska övervaka och kontrollera det arbete som utförs av den första försvarslinjen. Syftet är att säkerställa att verksamhetens kontinuitetshantering är ändamålsenlig, effektiv och följer interna och externa regelverk. Dessa kontrollfunktioner kan även ha en rådgivande roll gentemot verksamheten. Med övervaka och kontrollera avses aktiviteter som exempelvis att upprätta, övervaka

och utvärdera mätetal och riskindikatorer som täcker bankens kontinuitetshantering. Det kan även innebära att utföra kontroller för att bedöma dels om processer och rutiner följs av verksamheten, dels om särskilda risker relaterade till allvarliga störningar hanteras effektivt. Rådgivande inslag från de oberoende kontrollfunktionerna kan även rymmas inom dessa aktiviteter. Det kan till exempel vara rekommendationer som ges av kontrollfunktionerna efter en genomförd kontrollaktivitet.

Den tredje försvarslinjen, funktionen för internrevision, ska i sin tur på ett riskbaserat sätt göra oberoende utvärderingar av både den första och den andra försvarslinjens arbete med kontinuitetshantering.

Erfarenheter från tillsynen av organisation och ansvarsfördelning
Erfarenheter från tillsynen visar att bankerna behöver förbättra sin organisation och ansvarsfördelning. Det finns några områden som FI särskilt vill lyfta fram.

De oberoende kontrollfunktionerna i andra försvarslinjen har i vissa fall haft ansvar för delar av kontinuitetshanteringen, vilket kan riskera att påverka dess oberoende negativt. Vi har funnit exempel på när kontrollfunktioner har det koordinerande ansvaret för bankens kontinuitetshantering och därmed driver det operativa arbetet med bankens kontinuitetshantering. Ett annat exempel är när en oberoende kontrollfunktion, i stället för verksamheten, fattar beslut om vilka praktiska kontinuitetsrelaterade lösningar som verksamheten i fråga ska använda.

FI anser även att de oberoende kontrollfunktionerna i andra försvarslinjen kan öka antalet av och förbättra de riskbaserade kontrollerna av kontinuitetshanteringen. Vi har i tillsynen noterat att dessa aktiviteter i vissa fall inte verkar vara tillräckligt djupgående och inte verkar belysa de faktiska riskerna i tillräcklig grad. Ett exempel på detta är att kontrollerna enbart har fokuserat på om verksamheten har fyllt i processens checklistor på ett korrekt sätt, i stället för att granska om verksamhetens kontinuitetshantering i praktiken är effektiv.

Vidare vill FI peka på vikten av att funktionen för internrevision i sina riskbedömningar utvärderar hur ändamålsenlig och effektiv bankens kontinuitetshantering är. Där ingår också att utvärdera om funktionen för riskkontroll och funktionen för regelefterlevnad har haft en tillräcklig och effektiv övervakning och kontroll av området. Funktionen för internrevision behöver utifrån denna bedömning anpassa omfattningen av och intensiteten i sina egna granskningar av bankens kontinuitetshantering.

FI vill även lyfta att det finns flera goda exempel när det gäller organisation och ansvarsfördelning. Vi har exempelvis sett att det har upprättats kommittéer eller forum bestående av beslutsfattare från samtliga verksamhetsområden inom banken, med särskilt fokus på kontinuitetshantering[4]. Ett annat gott exempel är att det har upprättats särskilda kontinuitetshanteringsfunktioner inom verksamheten som har det övergripande ansvaret för att koordinera bankens

4 En sådan kommitté har oftast skapats för att koordinera kontinuitetshanteringen på en strategisk nivå.

kontinuitetshantering. FI har även sett flera goda exempel på kontrollaktiviteter genomförda av oberoende kontrollfunktioner inom både den andra och tredje försvarslinjen. Exempel på detta är djupgående granskningar av hur ett särskilt verksamhetsområde har genomfört sin kontinuitetshantering i praktiken samt granskning av kontinuitetshanteringen för särskilt viktiga it-system.

KONSEKVENSANALYS

FI föreskriver att bankerna regelbundet ska göra konsekvensanalyser av avbrott eller större verksamhetsstörningar som kan inträffa inom verksamheten[5]. Analysen ska göras på alla affärsenheter och stödfunktioner.

Vi anser att konsekvensanalysen enkelt beskrivet handlar om att ”lägga alla korten på bordet”. Genom konsekvensanalysen har banken en möjlighet att inventera hela sin verksamhet och få en god överblick över samtliga aktiviteter. Banken ska i detta arbete ta hänsyn till de beroenden som aktiviteterna har till varandra. Beroenden kan exempelvis gälla leveranser från en annan aktivitet, personal och it-system. Konsekvensanalysen ska även omfatta utlagd verksamhet. Banken kan utifrån denna inventering systematiskt bedöma vad eventuella avbrott i varje aktivitet skulle kunna få för påverkan på banken. Med hjälp av konsekvensanalysen kan banken inom ramen för sin kontinuitetshantering prioritera de aktiviteter som motverkar de mest allvarliga konsekvenserna vid avbrott.

Enligt FI är det viktigt att konsekvensanalysen är väl dokumenterad och motiverad. Det ska tydligt framgå hur banken har resonerat och varför vissa aktiviteter prioriteras över andra, så att det framgår att aktiva och medvetna val har gjorts. Det är även viktigt att analysen görs på ett konsekvent sätt på bankens olika verksamhetsområden så att resultaten är jämförbara.

Konsekvensanalyserna ska användas som ett underlag för att rangordna bankens mest prioriterade aktiviteter. De ska uppdateras regelbundet för att säkerställa att de är aktuella och anpassade till verksamheten. Vi anser det lämpligt att de uppdateras åtminstone årligen och vid varje händelse inom verksamheten som väsentligen kan påverka de bedömningar som har gjorts inom konsekvensanalysen. Exempel på sådana händelser kan vara att ett nytt it-system har införts eller att en allvarlig incident har inträffat.

Att konsekvensensanalysen och identifieringen av väsentliga processer ska vara tätt sammankopplade framgår av FI:s föreskrifter som anger att banken inom ramen för sin kontinuitetshantering ska ange den längsta tillåtna tiden för avbrott för varje process av väsentlig betydelse. Av den anledningen anser vi att separata isolerade metoder för konsekvensanalys och identifiering av väsentliga processer försvårar kopplingen mellan dessa två processer.

Erfarenheter från tillsynen av konsekvensanalyser

FI har i tillsynen noterat att bankerna behöver förbättra sina konsekvensanalyser. Flera banker har initierat utvecklingsarbeten för att stärka sina konsekvensanalyser, vilket FI ser positivt på.

5 FFFS 2014:4.

Erfarenheter från tillsynen har bland annat visat att det inte alltid är tydligt om konsekvensanalyserna har omfattat samtliga berörda aktiviteter inom verksamheten. Det tycks finnas utmaningar i att identifiera samtliga viktiga beroenden till kritiska aktiviteter. Ytterligare exempel är fall där banken inte i tillräcklig grad har inkluderat utlagd verksamhet i sin konsekvensanalys. Detta kan leda till att banken gör sämre val och prioriteringar i kontinuitetshanteringen, eftersom informationen som prioriteringarna grundar sig på riskerar att vara inkomplett eller felaktig.

Utifrån erfarenheter från tillsynen anser vi även att bankerna överlag behöver förbättra dokumentationen av konsekvensanalyserna. FI har noterat att dokumentationen kan vara relativt begränsad och att möjligheten att spåra bankens motiveringar och resonemang därför också är begränsad. Detta kan försämra bankens egen förståelse för vilka bedömningar som gjorts. Det kan också påverka uppföljning och kontroll från andra och tredje försvarslinjen, extern revisor och FI:s möjligheter att utöva en effektiv tillsyn.

BEREDSKAPSPLANER, KONTINUITETSPLANER OCH ÅTERSTÄLLNINGSPLANER

FI föreskriver att banker ska upprätta beredskapsplaner, kontinuitetsplaner och återställningsplaner[6].

Planerna ska ta avstamp i konsekvensanalyser som banken har genomfört (se avsnittet *Konsekvensanalys*). De ska innehålla den information och de praktiska rutiner som behövs för att förbereda för, upprätthålla och återställa bankens verksamhet i händelse av en allvarlig störning. Enligt FI är kravet på att beredskapsplaner, kontinuitetsplaner och återställningsplaner ska upprättas, ett uttryck för att banken ska ta hänsyn till alla tre faser i sin kontinuitetshantering. Det finns inga hinder för att konsolidera informationen och rutinerna för faserna i en och samma plan[7]. Härefter används samlingsbegreppet *kontinuitetsplan* för alla tre typer av planer och faser.

FI anser att det är viktigt att kontinuitetsplanerna är användbara i praktiken och så enkelt utformade som möjligt. En kontinuitetsplan ska tydligt ange vilka rutiner och prioriteringar som gäller för verksamheten om ett allvarligt avbrott inträffar. Av planen ska det även framgå vilka roller som ansvarar för att utföra rutinerna och om det är tillämpligt, inom vilka tidsspann som de behöver utföras. Dessa tidsspann ska i relevanta fall vara i linje med den längsta tillåtna tiden för avbrott som nämns i avsnittet *Konsekvensanalys.*

Väl dokumenterade kontinuitetsplaner kan fungera som kvitto på att banken har arbetat aktivt med frågorna och noggrant tänkt igenom de förlopp som kan uppstå. Kontinuitetsplanerna ska precis som konsekvensanalyserna uppdateras regelbundet och med samma tidsintervall som konsekvensanalyserna, åtminstone årligen.

6 FFFS 2014:4.

7 FI har beskrivit detta i beslutspromemorian för FFFS 2014:4.

Erfarenheter från tillsynen av beredskapsplaner, kontinuitetsplaner och återställningsplaner
Erfarenheter från tillsynen visar att bankerna i allt väsentligt har infört kontinuitetsplaner för sina mest kritiska funktioner. Med andra ord finns reservresurser och reservrutiner på plats för dessa funktioner. Samtidigt anser FI att kvaliteten på planerna kan förbättras. Vi anser att planerna kan bli tydligare när det kommer till vilka faktiska åtgärder som ska prioriteras, prioriteringsordningen och vilka eventuella hålltider som verksamheten behöver ta hänsyn till. Även om det finns erfaren personal inom verksamheten i dag, som till stor del har den kunskap som krävs för att säkerställa kontinuitet vid allvarliga störningar, så anser FI att banken över tid varken kan ta personalen eller kunskapen för given. Av den anledningen behöver kontinuitetsplanerna vara tydliga och väl dokumenterade.

Vi har i tillsynen också noterat fall där antalet kontinuitetsplaner kan vara stort, exempelvis där flera funktioner har upprättat planer för samma aktiviteter på grund av att funktionerna tillhör olika delar av bankens organisation. En onödigt stor administrativ börda i hanteringen av kontinuitetsplaner kan leda till att planernas kvalitet och effektivitet försämras, i synnerhet om strukturen för planerna riskerar att ge upphov till överlappningar och dubbelarbete. FI ser gärna att bankerna fokuserar på att skapa så få, enkla och användarvänliga kontinuitetsplaner som möjligt genom att arbeta över de organisatoriska gränserna i bankens processer.

Erfarenheter från tillsynen har även visat att bankerna kan bli bättre på att regelbundet uppdatera sina kontinuitetsplaner. FI vill särskilt lyfta att många banker genomför omfattande förändringsinitiativ. Därför är det viktigt att de eventuella konsekvenser som förändringarna får för kontinuitetshanteringen även reflekteras i kontinuitetsplanerna.

KONTINUITETSTESTER

FI föreskriver att bankerna regelbundet ska testa sina kontinuitetsplaner. Kontinuitetsplaner för processer av väsentlig betydelse och it-system som stödjer dessa ska åtminstone testas årligen[8]. Bankerna behöver testa sina kontinuitetsplaner för att få en rimlig försäkran om att de är ändamålsenliga och effektiva. Testerna kan utformas och genomföras på olika sätt. För ett givet scenario blir ett test i regel mer resurskrävande, ju mer realistiska förutsättningarna för testet är. Samtidigt ökar graden av försäkran om bankens förmåga att bibehålla kontinuitet för ett givet scenario, ju mer realistiska förutsättningarna för testet är. FI:s förväntningar är att bankerna löpande vidareutvecklar sin testmetodik och utmanar sin verksamhets motståndskraft för allvarliga störningar inom ramen för sina kontinuitetstester. För bankernas mest kritiska funktioner får testerna gärna utformas på ett sätt som är så likt ett skarpt läge som möjligt. Vi vill även belysa vikten av att bankerna säkerställer att testernas utformning och därmed även grad av försäkran, överensstämmer med bankens riskaptit. Det är samtidigt viktigt att testerna inte skapar oacceptabla risker inom verksamheten som i sig skulle hota en banks kontinuitet.

8 FFFS 2014:4.

FI vill understryka vikten av att ha väl dokumenterade tester, där det tydligt framgår av dokumentationen vilka mål, premisser och avgränsningar testet har. Acceptanskriterier är viktiga att tydliggöra för varje testfall. Det är också viktigt att efter genomfört test utvärdera om acceptanskriterierna, målen och den längsta tillåtna tiden för avbrott har uppnåtts samt vilka eventuella brister som behöver åtgärdas. Testresultatet kan exempelvis visa att det finns behov av att uppdatera konsekvensanalyser och kontinuitetsplaner.

Erfarenheter från tillsynen av kontinuitetstester
FI har i tillsynen noterat att bankerna genomför kontinuitetstester av sina mest kritiska funktioner. Testerna kan i vissa fall vara omfattande och komplexa. Exempel på detta kan vara att i skarpt läge testa att flytta driften av stora delar av verksamheten till en enskild datahall. Bankerna kompletterar i vissa fall även skarpa övningar med skrivbordstester, bland annat för att även kunna förbereda sig för scenarier som inte är möjliga att simulera utan att utsätta verksamheten för oacceptabla risker. Vi ser positivt på dessa tester, men vill samtidigt lyfta vikten av att bankerna fortsätter att fokusera på att vidareutveckla sin testmetodik. Detta för att över tid kunna genomföra realistiska tester av samtliga materiella scenarier som bankerna kan exponeras för. FI vill betona vikten av att tester genomförs av samtliga processer av väsentlig betydelse och de it-system som stödjer processerna.

Vi anser även att det finns utrymme för förbättringar när det gäller testdokumentationen. I detta avseende behöver bankerna tydligare beskriva testfall, acceptanskriterier och resultat av genomförda tester.

RAPPORTERING

FI föreskriver att bankerna minst årligen ska informera styrelsen om resultatet från tester av kontinuitetsplaner.

Då test av kontinuitetsplaner som nämnts ovan är ett viktigt verktyg för att rimligen säkerställa effektiviteten i planerna, blir rapportering av testresultaten ett viktigt led i ledningens och styrelsens bedömning av bankens kontinuitetshantering[9]. Denna rapportering behöver vara välformulerad och innehålla meningsfull information om testerna, så att ledning och styrelse ska kunna få en god överblick över bankens sammantagna förmåga när det gäller kontinuitetshantering. FI anser att rapporteringen åtminstone behöver innehålla tydliga beskrivningar av de genomförda testernas mål och omfattning, samt vilka scenarier som har använts. Vi ser gärna att det även framgår i vilken utsträckning genomförandet var i linje med eventuella längsta tillåtna tid för avbrott samt eventuella väsentliga avvikelser som framkom under testerna. Det är också bra om det framgår om genomförda tester sammantaget visar att risker kopplade till allvarliga störningar inte anses vara inom bankens riskaptit.

Erfarenheter från tillsynen av rapportering
Erfarenheter från tillsynen visar att bankerna har utrymme att förbättra sin rapportering till ledning och styrelse av resultaten av kontinuitetstesterna. FI har noterat att rapporteringen i vissa fall består

9 Mer information om FI:s syn på rapportering finns i beslutspromemorian för FFFS 2014:4.

av begränsad information där mottagarna av informationen, i FI:s mening, inte kan göra någon meningsfull bedömning av vad testresultaten innebär. Exempel på det är när en bank endast informerar om att tester har genomförts och hur många de varit, utan att ge ytterligare beskrivning av testernas genomförande och resultat.

FI vill samtidigt nämna att även flera goda exempel har noterats i tillsynen. Bland annat har vi sett utförliga årliga rapporter till ledning och styrelse om kontinuitetshantering, som på ett pedagogiskt sätt har sammanfattat hela bankens arbete inom området under det gångna året.

Slutsatser

FI konstaterar att bankerna arbetar aktivt med kontinuitetshantering. Hos många banker finns strukturer och processer på plats som innebär att de driver kontinuitetshanteringen på ett systematiskt sätt. Bankerna har även vidtagit åtgärder för att reducera risken för allvarliga avbrott. Samtidigt anser FI att bankerna behöver fortsätta att utveckla och förbättra sin kontinuitetshantering för att ytterligare stärka sin motståndskraft mot allvarliga störningar.

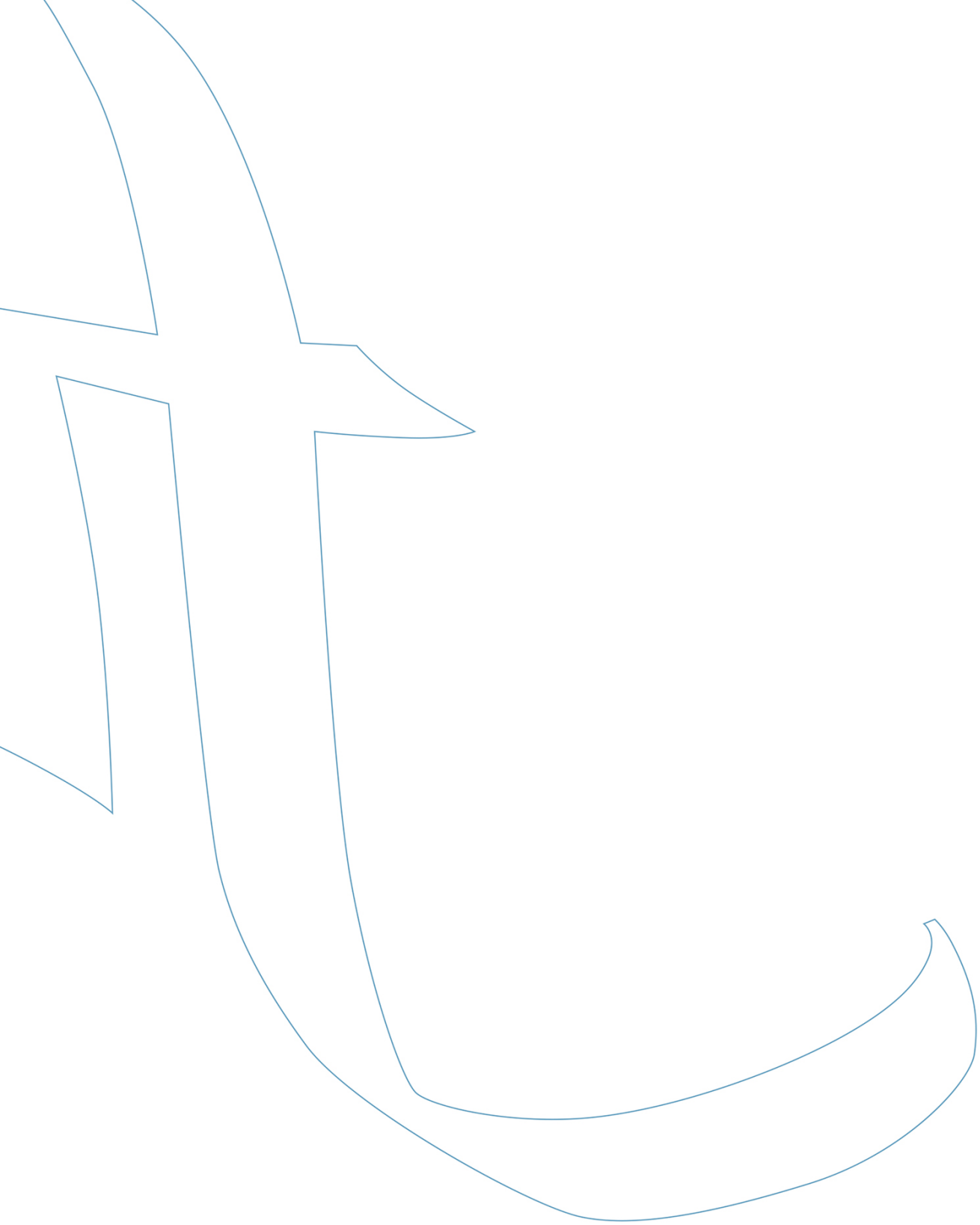
FI:s tillsyn visar att bankerna överlag har etablerat strukturer och processer för sin kontinuitetshantering. Ramverk och interna regler finns på plats, liksom utsedda funktioner som har ett särskilt ansvar för kontinuitetshanteringen. Bankerna gör regelbundet konsekvensanalyser av sina verksamheter. Vi ser positivt på att många banker driver kontinuitetshantering på ett systematiskt sätt.

FI:s tillsyn visar även att bankerna inom ramen för sin kontinuitetshantering har vidtagit åtgärder för att reducera risken för allvarliga avbrott i sina kritiska funktioner. Kontinuitetsplaner som beskriver reservresurser och reservrutiner finns på plats och dessa planer testas regelbundet. Bankernas ledning och styrelse informeras även i viss mån om resultatet av testerna.

Samtidigt anser FI att det generellt sett finns utrymme för bankerna att förbättra sin kontinuitetshantering ytterligare. Vi har redogjort för förbättringsbehoven i denna tillsynsrapport och sammanfattat avser de följande punkter:

- Stärka den interna styrningen och kontrollen av kontinuitetshanteringen, inklusive kontinuitetshanteringsstrategin, riskaptiten för operativ risk samt de oberoende kontrollfunktionerna.
- Vidareutveckla metoderna för konsekvensanalyser för att säkerställa att samtliga kritiska funktioner inklusive dess beroenden till varandra och till stödfunktioner identifieras.
- Tydliggöra innehåll och struktur för beredskapsplaner, kontinuitetsplaner och återställningsplaner.
- Säkerställa att ändamålsenliga kontinuitetstester genomförs av samtliga processer av väsentlig betydelse och de it-system som stödjer dessa processer.
- Förbättra rapporteringen av resultatet av genomförda kontinuitetstester så att styrelsen får relevant och meningsfull information.

FI kommer i tillsynen fortsätta att granska bankernas kontinuitetshantering och följa upp de förbättringsbehov som vi har identifierat.



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