FI-tillsyn

Banker kan förbättra sin hantering av operativa risker

Nr 34
6 februari 2026

FI dnr 25-31134

Innehåll

FI-tillsyn

Finansinspektionen publicerar återkommande tillsynsrapporter i en numrerad serie. Tillsynsrapporterna tar upp undersökningar och annan tillsyn som FI utövar. I rapporterna informerar vi om våra iakttagelser, bedömningar och förväntningar i olika frågor. Rapporterna, som är en del av vår kommunikativa tillsyn, är tänkta att vara till stöd för företagen i deras verksamhet.

Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Sveavägen 44
Telefon +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

Sammanfattning

Genom att hantera operativa risker på ett effektivt sätt kan banker och kreditmarknadsbolag motverka sårbarheter i det finansiella systemet. Finansinspektionens (FI) fördjupade analys visar att företagen har processer och rutiner för att hantera sina operativa risker, men att de kan vidta ytterligare åtgärder för att minska riskerna.

FI har kartlagt hur 33 utvalda banker och kreditmarknadsbolag hanterar sina operativa risker. Syftet har varit att utforska hur branschen hanterar olika frågor samt analysera hur de tillämpar regelverken i praktiken, för att identifiera likheter och skillnader mellan företagen. Analysen visar att de granskade bankernas och kreditmarknadsbolagens processer för att hantera operativa risker i huvudsak framstår som ändamålsenliga. Samtidigt ser vi att det finns förbättringspotential inom alla typer av företag, både stora och små.

Ett förbättringsområde som berör många företag är dokumentation av processer som har väsentlig betydelse för verksamheten. Om aktuell processdokumentation saknas eller är ofullständig, kan det ge försämrade förutsättningar för att utveckla tillfredsställande kontinuitetsplaner. En bred och djup förståelse för it-system och aktiviteter i processerna, inklusive samband och beroenden, är en förutsättning för god kontinuitetsplanering. Det är nödvändigt att företagen har en robust styrning och kontroll över processer som är av väsentlig betydelse, samt att de har beredskap för att kunna hantera störningar.

Vid hantering av operativa risker är det även viktigt att bankerna och kreditmarknadsbolagen har ett genomtänkt riskramverk. Riskaptit, limiter och riskindikatorer bör återspegla de risker som företaget har identifierat i sin verksamhet. En del företag har exempelvis valt att sätta en riskaptit som framstår som subjektiv snarare än en som grundas på objektiva kriterier, som att riskaptiten för operativ risk är låg eller medium. Detta kan leda till att styrningen och uppföljningen blir otydlig.

Vidare behöver finansiella företag både analysera interna incidenter och bevaka händelser i omvärlden, eftersom dessa ofta kan vara tidiga varningssignaler om större problem. Vi har sett indikationer på att vissa företag ännu inte har fullt etablerade processer för att arbeta systematiskt med incidenter i syfte att minska risker. FI kan komma att följa upp hur enskilda företag arbetar med hantering av operativa risker, antingen i den löpande tillsynen eller genom separata undersökningar.

Tillsyn av operativa risker

FI:s föreskrifter och allmänna råd om hantering av operativa risker ställer krav på att företagen på ett strukturerat och systematiskt sätt identifierar, mäter och bedömer operativa risker. Syftet med föreskrifterna är att minska risken för händelser i företagens verksamhet som resulterar i stora förluster eller omfattande störningar. Genom att minska dessa risker bidrar företagen till att upprätthålla ett stabilt och väl fungerande finansiellt system med god beredskap för att kunna hantera störningar.

Prioriteringar i tillsynen

En av FI:s prioriteringar i tillsynen för 2025 var granskning av företagens förmåga att klara sina grundläggande uppgifter i en osäker omvärld. Banker och andra finansiella företag behöver kunna möta både dagens och morgondagens hot. Det gäller oavsett om riskerna är finansiella eller operativa. Genom en effektiv hantering av operativa risker kan sårbarheter i det finansiella systemet motverkas.

Om kartläggningen

Våren 2025 inledde FI en fördjupad analys av svenska bankers och kreditmarknadsbolags ramverk för hantering av operativa risker. Företagens skyldigheter inom området framgår bland annat av FI:s föreskrifter och allmänna råd, FFFS 2014:4 om hantering av operativa risker (operativa riskföreskrifterna) och FFFS 2014:1 om styrning, riskhantering och kontroll i kreditinstitut (SRK-föreskrifterna).

Kartläggningen omfattar 33 banker och kreditmarknadsbolag som är utvalda för att spegla sektorn som helhet. I urvalet ingår företag med varierande omsättning och verksamhetsinriktning, vilket sammantaget ger en bred täckning av branschen. Företagen har svarat på en enkät som omfattade centrala områden i deras ramverk för hantering av operativa risker.

Med operativ risk menas risken för förlust till följd av otillräckliga eller misslyckade interna processer, människor, system eller externa händelser. Undersökningsresultatet speglar hur förhållandena såg ut i företagen under slutet av det andra kvartalet 2025.

Kartläggningar är en viktig del av FI:s arbete för att verka för att finansiella företag följer reglerna. Baserat på resultatet av en kartläggning kan vi komma att följa upp enskilda företag i den löpande tillsynen eller starta separata undersökningar för att ta reda på om företaget har brustit i sin regelefterlevnad på ett sätt som motiverar ett ingripande.

Resultatet av analysen

FI:s fördjupade analys visar att bankerna och kreditmarknadsbolagen generellt lever upp till regelverkets krav. Men i många fall kan ytterligare åtgärder vidtas för att förbättra arbetet och minska riskerna.

Definition av operativ risk

De operativa riskföreskrifterna hänvisar till EU:s definition av operativ risk. Det kan konstateras att majoriteten av bankerna och kreditmarknadsbolagen i stora delar har definierat begreppet operativ risk i linje med tillsynsförordningen, om än inte alltid exakt så som det står i den reviderade förordningen[1], som lyder: *”Risken för förluster till följd av otillräckliga eller fallerade interna processer, människor och system eller yttre händelser, inbegripet, men inte begränsat till, legala risker, modellrisker och informations- och kommunikationsteknikrisker (IKT-risker), men med undantag för strategiska risker och anseenderisker”*.

Några företag har poängterat att de har valt att använda termen ”icke-finansiell risk” i stället för ”operativ risk” men med samma definition. En del förtydligar definitionen med att regelefterlevnadsrisk ingår i begreppet legal risk medan andra har valt att förklara vad som menas med legal risk. Vissa har kvar definitionen som den ursprungligen skrevs i förordningen, ibland med tillägg att it-risk inkluderas. Andra har uppdaterat definitionen helt i enlighet med revideringen av förordningen 2024 och förtydligat att även informations- och kommunikationsteknikrisker (IKT-risker) och modellrisk ingår.

Ibland har företag förtydligat definitionen med ännu mer detaljerade tillägg, som att penningtvättsrisker omfattas liksom finansiering av terrorism och övrig ekonomisk brottslighet, brister i hantering av personuppgifter, händelser orsakade av tredje part och störningar på betaltjänstområdet. I enstaka fall har företag gjort tillägg som inte är direkt förenliga med EU:s definition, då de till exempel valt att inkludera anseenderisk.

Enligt FI:s operativa riskföreskrifter betyder ”operativ risk” detsamma som i EU:s reviderade förordning. Genom att använda en gemensam definition går branschen mot en enhetlig syn på operativ risk. Även om många företag använder EU:s exakta definition har FI noterat att anpassningar förekommer.

Om företag gör egna anpassningar kan det leda till andra utmaningar i företagets riskramverk, till exempel att olika riskkategorier överlappar varandra. Det kan

[1] Europaparlamentets och rådets förordning (EU) 2024/1623 av den 31 maj 2024 om ändring av förordning (EU) nr 575/2013 vad gäller krav avseende kreditrisk, kreditvärdighetsjusteringsrisk, operativ risk, marknadsrisk och golvet för riskvägda tillgångar.

också skapa otydligheter i samband med att medarbetare ska inkludera operativa risker i kapitaltäckningsberäkningar. Om anseenderisk inkluderas i den interna definitionen kan det leda till osäkerhet inom företaget, om även det är en risk som ska kapitaltäckas.

Interna regler ska finnas

Det framgår av de operativa riskföreskrifterna att styrelsen ska besluta om interna regler som anger vilka operativa risker som företaget i huvudsak är exponerat för. Styrelsen ska också besluta om metoder och processer för att identifiera, mäta och hantera risker, samt rutiner för att fastställa och övervaka riskaptiten och limiterna.

I samtliga banker och kreditmarknadsbolag som omfattas av kartläggningen har styrelsen beslutat om interna regler, vanligen benämnt policy, som omfattar operativa risker. Företagens styrelser förefaller regelbundet se över och besluta om dessa styrdokument. Bara i ett fall är de interna reglerna beslutade för över ett år sedan.

Det ska även finnas interna regler för dokumentation av processer samt för hantering av legala risker och säkerhetsarbete. Mer detaljerade interna regler kan beslutas av den verkställande direktören. Oavsett om det är styrelsen eller den verkställande direktören som fattat beslut om de interna reglerna, ska de enligt SRK-föreskrifterna utvärderas regelbundet, eller minst årligen. Om det behövs ska de också uppdateras.

Det är vanligen den verkställande direktören som beslutar om mer detaljerade interna regler, ofta kallade instruktioner och riktlinjer. Även dessa verkar generellt uppdateras regelbundet. Bara i något enstaka fall är den verkställande direktörens styrdokument beslutat för mer än ett år sedan. I detta fall har företaget angett att uppdatering pågår och att dokumentet ska beslutas av den verkställande direktören inom kort. Tre företag har däremot angett att styrelsen fattar alla beslut om interna regler som berör operativa risker.

Risktaxonomi skapar struktur

Bankerna och kreditmarknadsbolagen som ingår i kartläggningen ombads dela sin så kallade risktaxonomi[2] för operativa risker.

Det finns inget krav i FI:s operativa riskföreskrifter på att företag ska ha en risktaxonomi för sina operativa risker. Däremot framgår det av föreskrifterna att företag ska identifiera operativa risker i sina produkter, tjänster, funktioner och processer.

[2] Risktaxonomi är en vanlig benämning för att kategorisera olika typer av operativ risk som har identifierats i verksamheten. Denna kategorisering kan bestå av en, två eller fler nivåer.

Syftet med en risktaxonomi är att skapa struktur, enhetlighet och tydlighet. Genom att ge en god överblick över de risker som företaget har identifierat, kan en risktaxonomi underlätta arbetet med att hantera och kontrollera risker.

Samtliga företag som ingick i kartläggningen skickade in en risktaxonomi men vi kan konstatera att taxonomierna skiljer sig mycket åt mellan företagen. Av de 33 företag som ingår i kartläggningen redovisade 18 företag en taxonomi för operativa risker i två nivåer, medan de övriga företagens risktaxonomier bestod av en nivå.

Den första nivån av företagens risktaxonomier bestod av 4–18 riskkategorier, med ett genomsnitt på åtta. Av de 18 företag som redovisade en risktaxonomi med två nivåer var skillnaderna i antalet riskkategorier i nivå två betydande. Som lägst fanns åtta och som högst fanns 64 olika underkategorier. Vi har observerat störst skillnader mellan mindre företag.

Det som också framgår i analysen är att företag med många kategorier i sin risktaxonomi i högre grad tenderar att ha överlappande kategorier. När det finns flera likvärdiga kategorier kan det bli oklart för medarbetare hur risker bäst ska kategoriseras, och det finns risk för att taxonomin uppfattas som otydlig. Detta kan i sin tur leda till att syftet med risktaxonomin, det vill säga att skapa tydlighet för att kontrollera identifierade risker, försvåras.

Händelser och orsaker

FI observerar att det bland banker och kreditmarknadsbolag med ett fåtal risker i risktaxonomin är relativt vanligt att företaget har valt en orsaksbaserad risktaxonomi med människor, processer, system och externa händelser som riskkategorier.

Mer vanligt är att företag har en händelsebaserad taxonomi med utgångspunkt i klassificeringen av de sju förlusthändelsetyperna i Europaparlamentets och rådets förordning (EU) nr 575/2013 (CRR) artikel 324[3]. Dessa händelsetyper är interna bedrägerier, externa bedrägerier, anställningsförhållanden och arbetsmiljö, kunder samt produkter och arbetsmetoder, skador på materiella tillgångar, avbrott i affärsverksamhet och systemfel, utförande samt leverans och processtyrning.

I tillägg till händelsetyperna som framgår av artikel 324 har EBA tagit fram ett förslag till teknisk standard (RTS) EBA/RTS/2025/03, som utöver de sju händelsetyperna presenterar 26 underkategorier (nivå 2). Ett slutgiltigt förslag av den tekniska standarden är antagen av EBA och skickad till EU-kommissionen för

[3] Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012.

godkännande. När EU-kommissionen godkänt förslaget träder standarden i kraft och kommer att publiceras i EU:s officiella tidning.

Flera företag har även satt upp en risktaxonomi som kombinerar orsaker och händelser. Det har även noterats att vissa banker har tagit inspiration från ORX referenstaxonomi. ORX är en internationell medlemsorganisation som verkar för kunskapsutbyte inom operativa risker.[4]

Identifiering och mätning av risker

Samtliga banker och kreditmarknadsbolag har angett att de mäter operativa risker genom att bedöma sannolikheten för att de inträffar och vilka konsekvenser de kan ge upphov till. Operativa risker ska mätas regelbundet enligt de operativa riskföreskrifterna.

I några fall är beskrivningen av vilka metoder som företaget använder i sitt löpande arbete med operativa risker mycket kortfattad. För dessa företag går det inte att, via enkätsvaret, utläsa hur det löpande arbetet med att identifiera och mäta risker utformats.

FI väljer i stället att återge hur de företag som har lämnat en mer utförlig beskrivning redogör för vilka metoder de använder för att identifiera och mäta operativa risker. För väsentliga processer beskriver många att de har en process där risker och kontroller utvärderas löpande eller minst årligen av verksamheten i den första försvarslinjen.

Vid självutvärderingen görs en bedömning av risker, inklusive sannolikheten för att de inträffar, och deras konsekvenser. Utvärderingen, inklusive planerade åtgärder för att hantera oönskade risker, dokumenteras i ett riskregister eller riskhanteringssystem. Arbetet samordnas och övervakas av den andra försvarslinjen (riskkontrollfunktionen).

Vissa företag beskriver även att de identifierar nya risker inom ramen för godkännandeprocessen, vid interna incidenter, sårbarhetsanalyser och penetrationstester (inom området informations- och kommunikationsteknik), processkartläggningar, omvärldshändelser och kontrollfunktioners iakttagelser. Då uppdateras också företagets riskregister löpande. Flera beskriver även att såväl identifierade operativa risker som incidenter klassificeras enligt den risktaxonomi som de har beslutat om.

Riskaptit för operativa risker

Det framgår av de operativa riskföreskrifterna att företag ska fastställa en riskaptit för sina operativa risker. Riskaptit definieras i SRK-föreskrifterna som en nivå och

[4] Operational Risk eXchange, https://orx.org.

inriktning på företagets risker som kan accepteras för att uppnå företagets strategiska mål.

Samtliga banker och kreditmarknadsbolag har svarat att styrelsen utvärderar och beslutar om riskaptit för operativ risk vid behov eller minst årligen. Ett företag har svarat att styrelsen gör detta halvårsvis.

En del styrelser har valt att enbart sätta en kvalitativ riskaptit, som att aptiten för operativ risk är mycket låg, låg eller medium eller att förluster på grund av händelser ska hållas låga. Ibland har kvalitativa mått för riskaptit satts för olika typer av operativa risker med varierande aptit beroende på om risken är kopplad till it-system, regelefterlevnad, personal eller processer.

FI kan konstatera att när styrelsen har kommunicerat riskaptit kvantitativt blir riskramverket som regel tydligare. Vanligtvis blir då även spårbarheten och kopplingen till limiter och riskindikatorer tydligare, det vill säga de riskmått som den verkställande direktören oftast har beslutat om.

Vi har också sett exempel på företag som har använt sig av en kombination av kvalitativa och kvantitativa mått för riskaptit. När endast en kvantitativ riskaptit har fastställts avser den oftast acceptabel kostnad för operativa incidenter. Analysen visar däremot att det är vanligare att flera riskaptiter har kommunicerats. Styrelsen har då förmedlat sin syn på risk i mer än en form till verksamheten och aptiten har uttryckts i olika mått beroende vilken typ av risk som ska styras och begränsas.

FI har fått in flera goda exempel där styrelsen har valt att tydligt specificera flera kvantitativa mått på olika riskaptiter. Det handlar då dels om att styrelsen har fastställt en beloppsgräns eller procentuell kvot för incidentkostnader, dels om att kompletterande riskaptiter har fastställts i strävan att kunder alltid ska ha god tillgång till tjänster. Kvantitativt uttryckta aptiter angivna i procent eller antal timmar finns då för tillgänglighet till system, alternativt för systemavbrott för kritisk verksamhet.

Det kan även handla om aptiter som anknyter till kontinuitet på annat sätt, som att upptäckta svagheter i kritiska it-system ska ha åtgärdats inom ett visst antal dagar eller att riskbedömningar för utkontrakteringsavtal ska ha gjorts under det senaste året. Ofta finns det även en specificerad aptit för försenade åtgärder med anledning av allvarliga iakttagelser som kontrollfunktioner har påtalat.

Risklimiter som är mätbara

Utgångspunkten när limiter fastställs ska enligt de operativa riskföreskrifterna vara företagets produkter, tjänster, funktioner, processer och it-system. Limiterna ska vara mätbara.

Av de 33 banker och kreditmarknadsbolag som ingår i kartläggningen har 25 svarat att den verkställande direktören utvärderar och beslutar om limiter årligen, eller årligen men oftare vid behov. Ett företag har svarat att den verkställande direktören utvärderar och beslutar om limiter kvartalsvis. Ett företag har svarat att de har en limitstruktur där vissa limiter beslutas på styrelsenivå och andra av den verkställande direktören, i båda fallen årligen. I fyra företag är det styrelsen som minst årligen fattar beslut om risklimiterna. I två företag finns ingen fastställd risklimit utan enbart riskaptit som beslutas av styrelsen. I båda dessa fall finns kvantitativa mått på riskaptiten.

När den verkställande direktören har satt en limit som exakt träffar samma mått som styrelsen har begränsat, ligger limiten med en betryggande marginal under styrelsens riskaptit. Precis som för riskaptiten, berör de kvantitativa måtten på limiter ofta maximalt accepterad förlust på grund av operativa incidenter, antingen som en fast beloppsgräns eller uttryckt som en procentuell andel av intäkter.

Dessutom har limiter ofta fastställts för driftsstörningar, alternativt tillgänglighet till system eller kunders tillgång till tjänster.

Oftast finns också fler specificerade limiter. Dessa utgör ibland ytterligare en begränsning i förhållande till den riskaptit som styrelsen satt. De kan även vara angivna på en annan detaljeringsgrad eller finnas inom fler områden än styrelsens aptit. Det förekommer att en beloppslimit har satts för enskilda incidenter, men det kan även handla om att varierande limiter har satts för olika risker i risktaxonomin, som bedrägeri eller avbrott i it-system.

Andra vanligt förekommande limiter som har fastställts berör exempelvis kundklagomål, anmärkningar från kontrollfunktioner, kundkännedom och identifierade högriskkunder i penningtvättsammanhang, sjukfrånvaro, personalomsättning, it-säkerhet samt andra it-relaterade risker eller risker med utkontraktering.

Det är dock stor variation mellan olika företag, både när det gäller antal limiter samt tydlighet och omfattning. Variationen förefaller ibland kunna förklaras av de tillfrågade företagens varierande storlek och komplexitet.

Vid sin hantering av operativa risker är det viktigt att företagen har en genomtänkt helhetsbild över riskerna. Företagens aptit, limiter och riskindikatorer bör återspegla alla, eller väl valda, kategorier som tas upp i företagens risktaxonomier.

Riskindikatorer ska ge en förvarning

Enligt de operativa riskföreskrifterna ska företag tillämpa lämpliga indikatorer och gränsvärden för sina operativa risker, som ger en förvarning om när riskerna har

ökat. Vid tillämpningen ska företagen ta hänsyn till verksamhetens art, omfattning och komplexitet.

Alla banker och kreditmarknadsbolag, utom ett, har svarat att de använder sig av riskindikatorer för att få en förvarning om eventuella ökningar av verksamhetens operativa risker. Företaget som inte använder sig av sådana indikatorer har i stället satt en struktur för risklimiterna med olika intervall och nivåer som ska visa om risken har ökat inom olika områden. Funktionaliteten blir då i allt väsentligt densamma som för indikatorer. Ett annat företag har svarat att det har tagit fram riskindikatorer, men att arbete kring datainsamling och att sätta gränsvärden pågår. Det företaget saknar ännu utfallsrapportering i rapporter till styrelse och verkställande direktör.

Vi kan konstatera att alla företag har riskindikatorer som berör alla eller flera av områdena som anges som exempel i FI:s operativa riskföreskrifter, det vill säga omorganisationer eller större verksamhetsförändringar, personalomsättning, vakanta tjänster, kundklagomål, incidenter och iakttagna brister från internrevisionen.

Därutöver noterar vi att merparten av alla företag har riskindikatorer som berör penningtvätt eller kundkännedom. Andra vanligt förekommande riskindikatorer berör systemtillgänglighet, rättsliga tvister, regelefterlevnadsfunktionens observationer och bedrägerier.

Rapportering till styrelsen

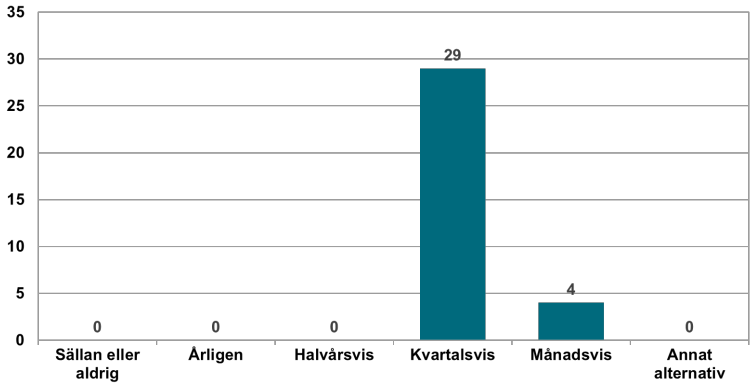
Enligt de operativa riskföreskrifterna ska företagen ta hänsyn till verksamhetens art, omfattning och komplexitet när de rapporterar operativa risker till styrelse och verkställande direktör, men indikatorer för operativa risker, överträdelser av riskaptit och risklimiter samt allvarliga incidenter är exempel på innehåll som ska ingå.

Enligt punkt 31 i EBA:s riktlinjer bör regelbunden intern rapportering även omfatta information om andra aspekter som är relevanta för bedömningen av en situation, risker och skeenden som påverkar eller kan komma att påverka företaget.[5]

Styrelsen får regelbundna skriftliga rapporter om operativa risker i alla tillfrågade företag, vanligtvis kvartalsvis men i några fall månadsvis (se diagram 1 nedan).

[5] European Banking Authority, Guidelines on Internal Governance (EBA/GL/2021/05).

Diagram 1
Hur ofta får styrelsen normalt en skriftlig rapportering om operativa risker?

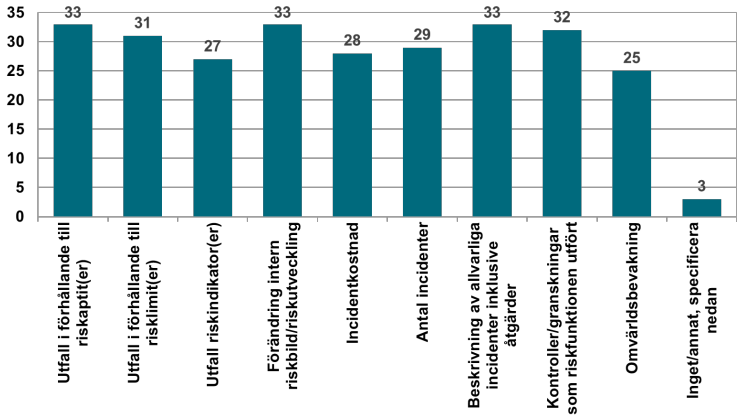


Innehållet i styrelserapporten varierar något, men vi kan konstatera att utfall i förhållande till riskaptit, beskrivning av allvarliga incidenter och åtgärder samt förändringar i den interna riskbilden eller riskutveckling ingår i rapporten hos alla företag (se diagram 2 nedan).

Hos nästan alla företag ingår även utfall i förhållande till risklimit och kontroller eller granskningar som riskfunktionen har utfört. Några företag har kommenterat att genomförda och pågående produktgodkännanden ingår i ”förändring intern riskbild”, medan några företag har specificerat att produktgodkännanden ingår under ”annat” i diagrammet nedan.

Hos cirka en fjärdedel av företagen ingår däremot inte någon omvärldsbevakning av operativa risker i rapporten till styrelsen.

Diagram 2
Vad innehåller rapporten till styrelsen kopplat till operativa risker?



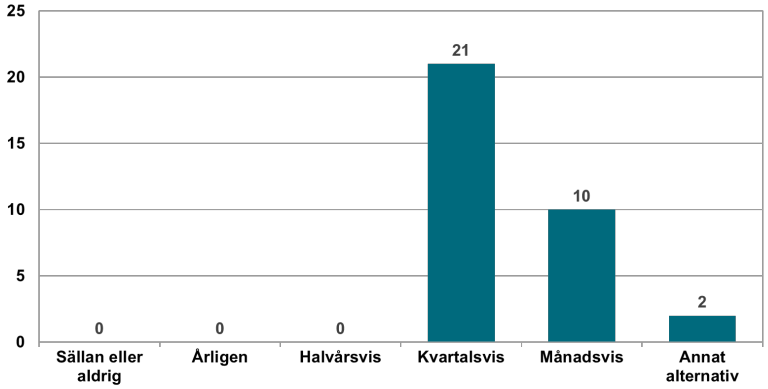
Rapportering till verkställande direktören

Den verkställande direktören får minst kvartalsvis skriftlig rapportering i alla tillfrågade företag. Cirka en tredjedel uppger att rapporteringen görs månadsvis (se diagram 3 nedan).

Andra alternativ som förekommer är att den verkställande direktören får rapporter åtta eller elva gånger per år (månadsvis, undantag i juli). Med andra ord får den verkställande direktören i många fall rapport om operativa risker med tätare intervall än styrelsen.

Det är logiskt att den verkställande direktören, som har ett operativt ansvar för att den dagliga verksamheten fungerar, kan ha behov av tätare regelbunden rapportering än styrelsen som brukar ha sammanträden mindre frekvent i sitt övervakande och strategiska ansvar.

Diagram 3
Hur ofta får verkställande direktör normalt en skriftlig rapportering om operativa risker?



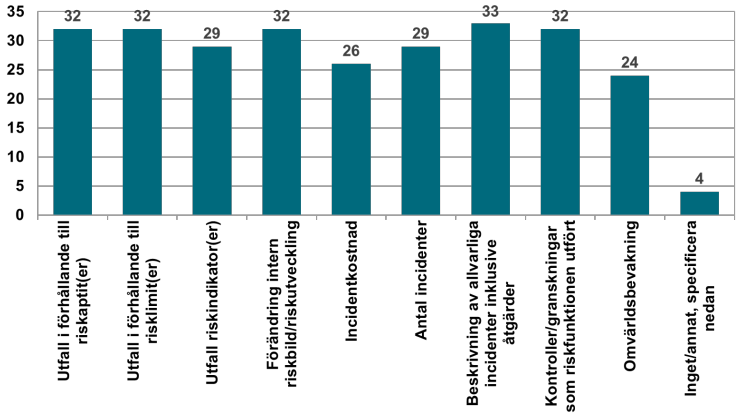
Innehållet i rapporten till den verkställande direktören är generellt detsamma som i rapporten till styrelsen. Beskrivning av allvarliga incidenter, inklusive åtgärder, ingår hos alla.

Nästan alla företag har även svarat att följande ingår: utfall i förhållande till riskaptit, utfall i förhållande till risklimit, förändringar i den interna riskbilden, samt kontroller eller granskningar som riskfunktionen har utfört (se diagram 4 nedan).

Specificerade kommentarer till ”annat” i diagrammet nedan handlar exempelvis om att produktgodkännanden ingår. Hos cirka en fjärdedel av företagen ingår däremot inte någon omvärldsbevakning av operativa risker i rapporteringen till

verkställande direktör. Det är som regel samma företag som inte heller har med det i styrelserapporteringen.

Diagram 4
Vad innehåller rapporten till den verkställande direktören kopplat till operativa risker?



Specialistkompetens inom operativ risk

En fråga i enkäten gällde om bankerna och kreditmarknadsbolagen har avsatt resurser med specialistkompetens för att arbeta med operativa risker. Syftet med frågan var att undersöka i vilken utsträckning det finns resurser som arbetar sammanhållande med interna riktlinjer, uppföljning och kontroller inom operativa risker.

Ett par mindre företag har angett att de inte har specialistkompetens för att arbeta med operativa risker. Men fler än de två företag som har svarat nekande förefaller inte ha sådana dedikerade resurser. Hos dem är operativt riskarbete i stället en arbetsuppgift bland andra. Några, främst mindre företag, har svarat att all personal som arbetar på avdelningar som säkerhet, juridik, penningtvätt, bedrägerier, regelefterlevnad och risk har specialistkunskap för att arbeta med operativa risker inom sitt område.

Storbankerna anger däremot att de har många heltidsanställda som är specialiserade på arbete med operativ risk fördelade mellan den första linjen (riskkoordinatorer, risksamordnare med flera) och den andra försvarslinjen (riskkontrollfunktion för operativ risk eller icke-finansiell risk).

Även medelstora företag har som regel minst en heltidsresurs i den andra försvarslinjen, vars arbetstid helt är avsatt för sammanhållande arbete med operativa risker. Ibland har även dessa medelstora företag en riskkoordinator eller en risksamordnare i den första försvarslinjen.

Systemstöd kan underlätta

Ett allmänt organisatoriskt krav är att företag ska ha it-system och rapporteringsrutiner som säkerställer att information om dess verksamhet och riskexponering är aktuell och relevant. Även kontrollfunktioner ska ha ändamålsenliga it-system och stöd till sitt förfogande enligt SRK-föreskrifterna.

Sju företag har svarat att de saknar systemstöd för arbetet med operativa risker. Det handlar främst om de mindre företagen. För några som angett att de har systemstöd, handlar det om lösningar eller egna modeller byggda i Microsoft, som Excel, Sharepoint, Forms eller Lists.

För övriga företag som har uppgett att de har systemstöd, handlar det om system som är inköpta från en extern part och som redan från början är specialanpassade för riskarbete.

När det gäller incidentrapportering har däremot bara två företag angett att de helt saknar systemstöd. På frågan vilket systemstöd som används för incidentrapportering är svaret ofta detsamma som för arbete med operativa risker, det vill säga, att vissa har Microsoft-lösningar, medan andra har inköpta system särskilt avsedda för incidentrapportering.

Väl anpassade systemstöd för arbete med operativa risker kan innebära att det blir enklare att identifiera, bedöma och följa upp risker på ett enhetligt sätt.

Nackdelar med specialbyggda system är ofta kostnader, komplexitet och risk för att systemet ger en falsk trygghet. Viktigt att förstå är att system är ett stöd och inte en garanti för god riskhantering. Det krävs en bra och stark riskkultur för att systemet ska ge mervärde. Systemet blir bara så bra som den information som rapporteras in och därefter behandlas.

Systemstöd för incidentrapportering kan däremot innebära att anställda enkelt kan rapportera incidenter via ett användarvänligt gränssnitt. Snabbare reaktioner på riskhändelser kan leda till att förlusterna begränsas. Om incidentdata dokumenteras konsekvent och systematiskt och finns väl samlat, underlättas möjligheten att analysera trender, mönster och grundorsaker, vilket kan bidra till ett bättre förebyggande arbete.

Incidenter som analyseras

Alla banker och kreditmarknadsbolag, utom ett, har uppgett att det fanns internt rapporterade incidenter under 2024. Det företaget har, trots att det är förhållandevis litet, satt en hög intern beloppsgräns för när incidenter behöver rapporteras. FI noterar att det inte är vanligt förekommande att sätta en intern beloppsgräns. Endast tre företag har uppgett att de har satt en beloppsgräns för när medarbetare behöver rapportera incidenter.

Spannet är stort när det gäller hur många incidenter som har rapporterats under 2024, liksom hur hög den totala, uppskattade incidentkostnaden är. Vi bedömer att det huvudsakligen beror på de tillfrågade företagens varierande storlek. Fem mindre företag har uppgett att deras totala uppskattade incidentkostnad är noll för verksamhetsåret 2024.

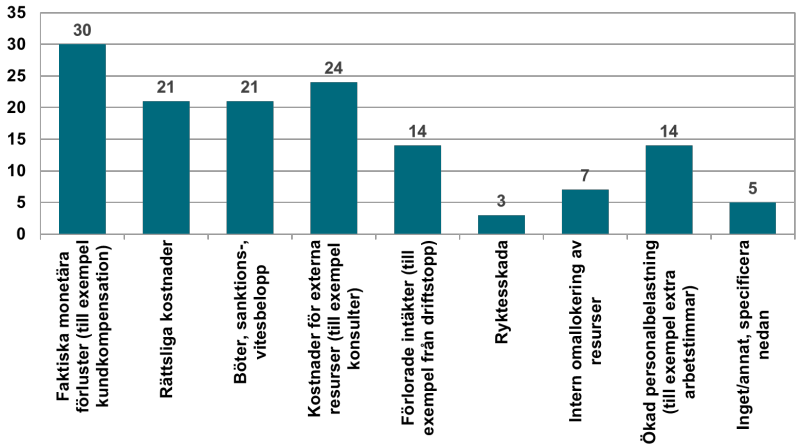
När det inträffar en incident ska finansiella företag dokumentera och analysera incidenten. Företaget ska, enligt de operativa riskföreskrifterna, även dokumentera de förluster som har uppstått i samband med incidenten.

FI anser att det är väsentligt för en sund riskhantering att alla incidenter – även de mindre – analyseras, eftersom de kan vara tidiga varningssignaler om större problem. Genom att systematiskt dokumentera och analysera incidenter kan mönster upptäckas, sårbarheter identifieras och framtida risker förebyggas.

Händelser som för företaget kan anses vara små och ha en liten finansiell påverkan, kan ändå vara betydande för den enskilda kunden. Påverkan på företaget kan därför vara liten på kort sikt, men kan på längre sikt påverka förtroendet för företaget och i förlängningen eventuellt även ge ett minskat förtroende för finansbranschen.

Vilken typ av kostnader som ingår vid beräknad förlust varierar mellan företagen (se även diagram 5 nedan). Direkta kostnader, till exempel kundkompensation, inkluderas som regel. Ett företag har angett att det inte fanns en etablerad process för att uppskatta kostnader under 2024 men att de implementerat detta under 2025. Det finns även exempel på företag som har angett att de inte har haft några kostnader under året och därför inte angett någon kostnadstyp. Det är endast ett mindre företag som svarat att alla kostnadstyper som fanns som förvalsalternativ i enkäten ingår i beräkningen av deras incidentkostnad.

Diagram 5
Vilken typ av kostnader ingår i beloppet ni har angett som en total förlust för incidenter?



Väsentliga processer behöver dokumenteras

Det framgår av FI:s operativa riskföreskrifter att företag ska fastställa och ange i en förteckning vilka processer i verksamheten som är av väsentlig betydelse. Förteckningen ska regelbundet ses över och uppdateras om det behövs. Processerna i förteckningen ska finnas dokumenterade. Därtill ska en ansvarig person eller funktion ha utsetts för varje väsentlig process.

Generellt har den verkställande direktören eller styrelsen fastställt vilka processer i verksamheten som är av väsentlig betydelse. I merparten av företagen har beslut fattats senast under 2024 eller 2025, vilket tyder på att det generellt finns en process för löpande översyn och beslut. Bara i ett fåtal fall har besluten fattats 2022 eller 2023.

Företagen ombads även skicka in sin förteckning över processer av väsentlig betydelse. Alla banker och kreditmarknadsbolag som ingick i kartläggningen bifogade en förteckning. Vi kan i analysen konstatera att de förteckningar som har bifogats över processer av väsentlig betydelse varierar mycket i utformning.

FI har fått in många förteckningar där det framgår att olika aspekter beaktats. Flera företag har till exempel en förteckning som anger om det är en affärsprocess, stödprocess eller en styrande process. Vissa har även specificerat huvudprocesser med tydliga underliggande delprocesser. Det finns även förteckningar som inkluderar information om processen innehåller kritisk eller viktig funktion enligt Doraförordningen[6].

På frågan om någon ansvarig person eller funktion utsetts för processer av väsentlig betydelse har företagen generellt svarat att ansvariga utsetts.

För många företag är det däremot en utmaning att upprätthålla processdokumentationen aktuell (se diagram 6). FI ser en risk att nödvändig processdokumentation inte alltid finns.

Enligt de allmänna råd som finns i de operativa riskföreskrifterna, bör företaget i processdokumentationen beskriva vilka regler som påverkar processens utformning, vilka de huvudsakliga aktiviteterna är inklusive deras samband, vilken information som används i aktiviteterna, vilka krav som ställs på kvalitet i informationen, vilka it-system som stödjer processen, när kontroller görs och beslut fattas, vilka intressenterna är, samt processens resultat.

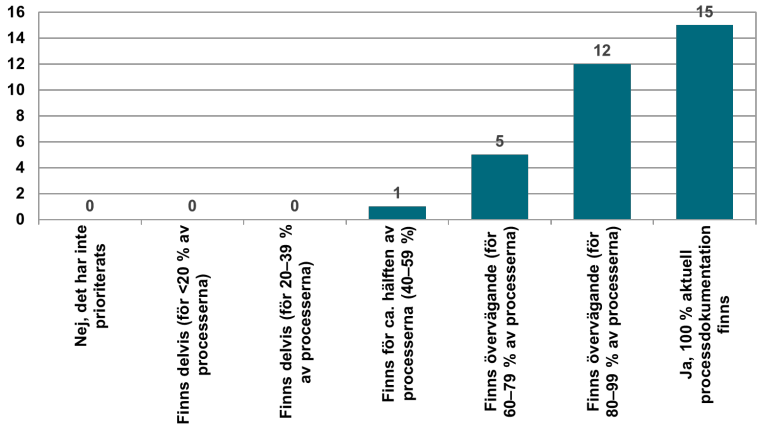
Att säkerställa att nödvändig dokumentation finns för processer av väsentlig betydelse för verksamheten är en viktig del i företagens hantering av operativa risker. I det nuvarande omvärldsläget är robust styrning, och kontroll över

[6] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn.

processer som är av väsentlig betydelse, nödvändigt för att ha beredskap för att kunna hantera störningar.

Om aktuell processdokumentation saknas eller är ofullständig, kan det leda till försämrade förutsättningar för att utveckla tillfredsställande kontinuitetsplaner. En bred och djup förståelse av system och moment i processerna, inklusive olika samband, är en förutsättning för god kontinuitetsplanering.

Diagram 6 Finns det aktuell processdokumentation för processer av väsentlig betydelse?



Slutsatser

Baserat på enkätsvar och insamlade underlag kan FI dra slutsatsen att banker och kreditmarknadsbolag överlag har processer och rutiner för riskhantering, men de kan förbättras.

Likheter, skillnader och utmaningar

Även om de analyserade bankerna och kreditmarknadsbolagen generellt följer regelverk och riktlinjer, har vi identifierat en förbättringspotential hos flera av företagen. Det gäller både större och mindre företag. Vi har inte funnit några tydliga skillnader mellan olika typer av företag, till exempel bankaktiebolag, sparbanker och kreditmarknadsbolag. Däremot visar analysen att företagens hantering är likartad på flera områden, exempelvis när det gäller frekvensen för rapportering till verkställande direktör och styrelse.

I andra avseenden finns det stora skillnader mellan företagen, exempelvis när det gäller hur riskramverket har utformats, inklusive riskaptiter och limiter. När företagen hanterar operativa risker är det viktigt att de har en genomtänkt helhetsbild. Riskaptit, limiter och riskindikatorer bör återspegla alla eller åtminstone väl valda kategorier som tas upp i risktaxonomin.

En del företag har valt att enbart ange en kvalitativ riskaptit, som att aptiten för operativ risk är låg eller medium, vilket kräver en subjektiv bedömning. Kopplingen till limiter och indikatorer kan då bli otydlig, vilket kan försvåra styrningen.

Det finns även indikationer på att metoderna för att löpande identifiera operativa risker i verksamheten kan behöva utvecklas hos vissa företag. FI vill betona vikten av att företagen regelbundet utvärderar sig själva samt att identifierade risker analyseras och hanteras på ett strukturerat sätt.

Det förefaller även finnas företag som inte har en väletablerad process för att arbeta systematiskt med incidenter. Många företag har också uppgett att de inte inkluderar någon omvärldsbevakning i sin interna rapportering av operativa risker. Vi anser att det är betydelsefullt att finansiella företag både analyserar interna incidenter och bevakar händelser i omvärlden, eftersom dessa ofta kan vara tidiga varningssignaler om större problem.

Därutöver har flera företag utmaningar när det gäller att dokumentera väsentliga processer. Vi ser en risk för att den interna styrningen och kontrollen av dessa processer inte alltid är tillfredsställande vilket kan påverka kontinuitetsplaneringen. I det nuvarande omvärldsläget är robust styrning och kontroll av processer som är av väsentlig betydelse nödvändigt för att ha beredskap och kunna hantera störningar.

Åtgärder utifrån analysen

FI kommer att återkoppla iakttagelser som vi har gjort inom ramen för den fördjupade analysen till respektive företag. Vi förväntar oss att finansiella företag löpande säkerställer att de följer reglerna och vidtar förbättringsåtgärder där det behövs. Det är också något som flera av de företag som ingår i analysen har skrivit att de har för avsikt att göra.

FI kan komma att följa upp hur enskilda banker och kreditmarknadsbolag arbetar med att hantera operativa risker, antingen i den löpande tillsynen eller genom separata undersökningar.

Den information som FI fått genom den här analysen kan vi även komma att använda i arbetet med att utveckla regelverk framöver.