FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Tematilsyn

Operasjonell risiko – hendelser

Rapport

DATO:
11.07.2017

Tematilsyn innen operasjonell risiko – hendelser

Innledning

I perioden 28. september til 17. november 2016 gjennomførte Finanstilsynet et stedlig tilsyn i syv banker[1]. Formålet med tematilsynet var primært å kartlegge og vurdere bankenes styring og kontroll av operasjonell risiko, med en særlig oppmerksomhet på identifisering og registrering av relevante opplysninger om operasjonell risiko, herunder opplysninger om betydelige tap, og hvordan hendelser brukes i bankenes planlegging, styring og kontroll av operasjonell risiko. Enkelte elementer knyttet til overordnet styring og kontroll av operasjonell risiko ble også diskutert under tilsynene.

Operasjonell risiko har fått økt oppmerksomhet i finansnæringen både i Norge og internasjonalt de siste årene. En av årsakene til dette er at operasjonelle hendelser har medført betydelige finansielle tap og tap av omdømme for enkelte foretak. Håndtering av hendelser utgjør et vesentlig element i styring og kontroll av operasjonell risiko, og hendelsesdata bør inngå som grunnlag når risikonivå og risikotoleranse skal vurderes. Hendelsesdata vil også kunne utnyttes for å identifisere potensielle risiko- og forbedringsområder.

Finansforetaksloven presiserer i § 13-5 (1) at foretak skal ha hensiktsmessige retningslinjer og rutiner for å identifisere, styre, overvåke og rapportere risiko foretaket er, eller kan bli, eksponert for, herunder operasjonell risiko, jf. CRR/CRD IV-forskriften § 27. Styring og kontroll av operasjonell risiko, herunder håndtering av hendelser, er i liten grad regulert i lov og forskrift. Bankene har siden innføringen av Basel II i 2007 rapportert kapitalkrav for operasjonell risiko etter enten basismetoden eller sjablongmetoden. Basismetoden og sjablongmetoden baserer seg på standardiserte prosentsatser i forhold til definerte inntektsbegreper. Kapitalkravet for basismetoden er 15 prosent av gjennomsnittlig inntekt de tre siste årene, mens sjablongmetoden baserer seg på forskjellige prosentsatser (fra 12 prosent til 18 prosent) avhengig av forretningsområde. Sjablongmetoden forsøker i større grad å gjenspeile risikoforskjeller i foretakets virksomhet, og bygger samtidig på at visse krav til risikostyringen må være oppfylt. Foretak som har valgt å anvende sjablongmetoden for beregning av kapitalkravet for operasjonell risiko, må oppfylle kravene i kapitalkravsforskriften kapittel 43. Blant annet skal foretaket registrere relevante opplysninger om operasjonell risiko, herunder opplysninger om betydelige tap. Opplysninger om betydelige tap skal også rapporteres som tilleggsinformasjon til kapitaldekningsrapporteringen. Tre av bankene i utvalget benytter basismetoden mens fire benytter sjablongmetoden for beregning av kapitalkravet for operasjonell risiko.

European Banking Authority (EBA) presiserer i sin "Guideline on common procedures and methodologies for the supervisory review and evaluation process (SREP)"[2] fra desember 2014 at operasjonelle tap og informasjon fra hendelsesdatabaser er en primær kilde til

[1] DNB Bank ASA, Skue Sparebank, SpareBank 1 Nord-Norge, SpareBank 1 SR-Bank ASA, Sparebanken Sør, Sparebanken Vest og Totens Sparebank.

[2] http://www.eba.europa.eu/documents/10180/935249/EBA-GL-2014-13+(Guidelines+on+SREP+methodologies+and+processes).pdf

informasjon om operasjonell risikoprofil for foretaket. I Basel-dokumentet "Principles for the Sound Management of Operational Risk"[3] fra juni 2011 vises det i prinsipp 6 til at sammenstilling og analyse av interne tapshendelser er ett av verktøyene som kan anvendes for å identifisere og vurdere operasjonell risiko. Både EBA og Basel-komiteen omtaler også øvrige elementer som bør inngå i en helhetlig styring av operasjonell risiko.

Samlerapporten bygger på innhentet dokumentasjon, gjennomføring av stedlige tilsyn og merknader til de syv bankene basert på Finanstilsynets foreløpige rapporter og bankenes svarbrev. Finanstilsynet har i samlerapporten angitt prinsipper for god praksis på området. Disse er fastsatt på bakgrunn av internasjonale prinsipper og retningslinjer, erfaringene fra tematilsynet og fra øvrig tilsynsarbeid.

Observasjoner fra tematilsynet og hovedpunkter fra tilbakemeldingene til bankene

Eksponering – faktiske hendelser

- Flere av bankene har et forbedringspotensial når det gjelder registrering og kvalitetssikring av hendelsesdata, samt systematisering og anvendelse av disse dataene.

  Dersom taps- og hendelsesdatabaser skal ha nytteverdi for bankene, bør hendelsesinformasjon registreres på en korrekt, helhetlig og systematisk måte. Opplysninger om hendelser kan gi viktig informasjon for bankenes arbeid med reduksjon av risiko, forbedringer og mulig effektivisering.

- Tematilsynet viser at underrapportering av hendelser er en utfordring for et flertall av bankene. Utdrag fra bankenes taps- og hendelsesdatabaser for alle registrerte hendelser i perioden 1. januar 2015 til 30. juni 2016, viste et lavt antall hendelser for flere banker.

  Alle operasjonelle hendelser, uavhengig av tap, bør registreres. Også operasjonelle hendelser som resulterer i finansiell gevinst bør registreres i databasene. Bruk av interne beløpsterskler for registrering av hendelser kan redusere informasjonsverdien av taps- og hendelsesdatabaser.

Styring og kontroll av operasjonell risiko – håndtering av hendelser

- Tematilsynet viser at det er forskjeller mellom bankene når det gjelder prioritering av og kultur for styring og kontroll av operasjonell risiko.

  Styret har det overordnede ansvaret for å etablere en sterk risikostyringskultur i hele organisasjonen. Holdninger fra styret og toppledelsen er avgjørende for risikostyringen i et foretak. Fokus på og arbeid med organisasjonskultur (verdier, holdninger, etikk, mv.) gir positivt bidrag til styring av operasjonell risiko. Styring og kontroll av operasjonell risiko berører alle nivåer i organisasjonen, og organisasjonskulturen i et foretak kan virke inn på operasjonelle hendelser, både risikoen for at hendelser oppstår og åpenhet rundt

[3] http://www.bis.org/publ/bcbs195.pdf

inntrufne hendelser. En forutsetning for en sterk kultur er at mellomledelsen viderefører og tydeliggjør holdninger fra toppledelsen.

- Enkelte av bankene har et forbedringspotensial når det gjelder strategi og/eller policy for operasjonell risiko og håndtering av hendelser, og mangler en tydelig definert risikotoleranse for operasjonell risiko.
- Bankenes overordnede rammeverk og styringsdokumentasjon (strategi, policy o.l.) for styring av operasjonell risiko bør tydeliggjøre bankenes ambisjonsnivå og risikotoleranse, bør inneholde kvantifiserte måltall/rammer og ulike risikoindikatorer for å kunne gi et godt og helhetlig syn på risikobildet, samt for å kunne illustrere utviklingen i risikoprofilen over tid.
- Rammeverket for styring av operasjonell risiko er i enkelte av bankene fragmentert og lite konkret, og operasjonell risiko sidestilles i stor grad med den overordnede risikostyringen og internkontrollen. Rammeverket bør gi et helhetlig perspektiv på styring og kontroll av operasjonell risiko, og bør inkludere vesentlige elementer som beredskapsplaner, utkontraktering, nye og endrede produkter og tjenester mv. Rammeverket bør fastsettes av styret og revideres jevnlig av styret i lys av endrede rammebetingelser, risiko og økonomisk utvikling.

- I flere av bankene har risikostyringsfunksjonen ansvar for styring og kontroll av operasjonell risiko, herunder håndtering av hendelser. Hos enkelte av bankene er compliance-funksjonen ansvarlig for håndtering av hendelser.

  Et flertall av bankene har etter Finanstilsynets vurdering ikke tilstrekkelige ressurser og kompetanse innen operasjonell risikostyring og håndtering av hendelser.
- Flere av bankenes rutiner og retningslinjer for håndtering av hendelser har mangler, og kun én av syv banker har en tydelig og ensartet definisjon av hva som er en hendelse og hva som vurderes som vesentlige tap. Seks av syv banker kategoriserer hendelser iht. Basel-komiteens syv hovedkategorier (jf. kapitalkravsforskriften).

  Bankene bør ha klare rutiner og retningslinjer for styring av operasjonell risiko inkludert hendelser. Disse bør blant annet beskrive hensikten og formålet med hendelsesregistrering, tydelig definisjon av hva som er en hendelse (uavhengig av kategorisering), hva som defineres som vesentlige tap, eventuelle interne terskler for registrering og myndighetsrapportering, kategorisering av hendelser, ansvar for registrering og håndtering av hendelser, kvalitetssikring samt intern rapportering.
- Bankene benytter forskjellige systemløsninger for registrering og oppfølging av operasjonelle hendelser, og systemløsningene er ofte ikke tilpasset bankenes behov. Tilgangen til databasene, både når det gjelder registrering og informasjon, varierer mellom bankene.

  Systemløsningene bør tilpasses og utformes slik at de er et hensiktsmessig verktøy for styring og kontroll av operasjonell risiko og slik at bankene effektivt kan utnytte en slik database. Alle ansatte bør kunne registrere hendelser i databasene. Tilgang til informasjonen i hendelsesdatabasene bør begrenses til de ansatte som har behov for det.
- Intern rapportering av operasjonell risiko og hendelser varierer mellom bankene.

Hendelser og tap bør rapporteres jevnlig til ledelse og styret, både for siste periode og utvikling over tid, og spesielt alvorlige hendelser bør informeres særskilt. De bankene som benytter sjablongmetoden må ha en rapporteringsstruktur til styret som sikrer at alle relevante funksjoner i banken gis nødvendig informasjon om operasjonell risiko (jf. kapitalkravsforskriften).

- Tematilsynet avdekket at enkelte av bankene som benytter sjablongmetoden til beregning av kapitalkrav for operasjonell risiko, etter Finanstilsynets vurdering ikke fullt ut etterlever kapitalkravsforskriftens krav for å anvende metoden. Det vises til vesentlige mangler i rammeverk, retningslinjer og organisering, underrapportering av hendelser og tap, samt manglende bekreftelse av uavhengig funksjon. Bankene har bekreftet i sine svar til Finanstilsynet på foreløpige rapporter etter inspeksjonene, at tiltak for å sikre etterlevelse vil bli iverksatt.
- Tematilsynet avdekket at enkelte av bankene har mangler eller feil i myndighets-rapportering av kapitalkrav for operasjonell risiko og tilleggsinformasjon (dvs. hendelsesdata). Finanstilsynet vil peke på viktigheten av korrekt myndighetsrapportering.
- Bankenes internrevisjonen har i liten grad hatt fokus på bankenes håndtering av hendelser og myndighetsrapportering av operasjonell risiko.

  Håndtering av hendelser er et viktig element i styring og kontroll av operasjonell risiko og bør dekkes av internrevisor i forbindelse med gjennomgangen og bekreftelsen av bankenes vurderings- og styringssystem iht. kapitalkravsforskriftens bestemmelser.

Organisering av risikostyring og compliance-funksjonen

- Organisering av compliance-funksjonen ble diskutert under inspeksjoner i banker hvor compliance er helt eller delvis ansvarlig for håndtering av hendelser. Hos flere av bankene er leder for compliance også leder for andre funksjoner, som risikostyring, juridisk og/eller forretningsutvikling. Etter Finanstilsynets vurdering er en slik organisering ikke i samsvar med kravene i finansforetaksloven § 13-5 og CRR CRD IV-forskriftens bestemmelser, jf. § 29 Risikokontroll og § 30 Kontroll av etterlevelse (compliance), bortsett fra i mindre foretak med mindre kompleks struktur, der forskriften åpner for at leder for kontrollfunksjonen kan ha andre ansvarsområder dersom interessekonflikter unngås.
- Finanstilsynet er av den oppfatning at foretak som er definert som systemviktige, samt store foretak, dvs. foretak med en forvaltningskapital (inkl. lån overført til kredittforetak) større enn 100 milliarder kroner, som er del av en konsernstruktur og med godkjenning for bruk av interne modeller (IRB-modeller), ikke kan påberope seg unntaksbestemmelsen som gjelder mindre foretak med mindre kompleks struktur. Finanstilsynet legger til grunn at gjeldende krav til risikostyring og kontrollordninger i foretak av denne type, tilsier at foretakene må ha egne kontrollfunksjoner for henholdsvis risikostyring og compliance med egne ledere som rapporterer til daglig leder, jf. CRR/CRDIV-forskriftens bestemmelser i § 29 og § 30, som har tilstrekkelige ressurser og kompetanse og som ikke kombineres med andre oppgaver. Finanstilsynet viser i denne sammenheng til finansforetaksloven § 13-5 tredje ledd som fastsetter at "Finansforetakets styrings- og kontrollordninger samt retningslinjer og rutiner skal være tilpasset risikoen ved og omfanget av virksomheten i foretaket".