FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Risikobasert tilsyn

Modul for operasjonell risiko

Evaluering av:
- Styring og kontroll
- Eksponering

DATO:
APRIL 2022

NUMMER:
2.0

SIST REVIDERT:
FEBRUAR 2016

FORFATTERANSVARLIG:
IRENE STØBACK JOHANSEN

SEKSJON/AVDELING:
BANKTILSYN

Innhold

1. INNLEDNING

Modulen for operasjonell risiko er en veiledning for Finanstilsynets vurdering av foretakenes operasjonelle risiko. Modulen benyttes av Finanstilsynet under stedlig tilsyn og i forbindelse med vurdering av foretakenes samlede risikoprofil og kapitalbehov (Supervisory Review and Evaluation Process – SREP).

Finanstilsynet definerer operasjonell risiko som "*risikoen for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil, eller eksterne hendelser*". Definisjonen omfatter juridisk risiko og atferdsrisiko, men ikke strategisk risiko som må vurderes særskilt. Selv om det er en sterk kobling mellom operasjonell risiko og omdømmerisiko operasjonelle hendelser kan eksempelvis påvirke foretakets omdømme, omfatter omdømmerisiko mer enn en konsekvens av operasjonell risiko og bør vurderes særskilt. Operasjonell risiko omfatter også styring og kontroll med utkontraktert virksomhet.

Operasjonell risiko er en risiko som griper inn på overordnet styring og kontroll og andre risikoområder, noe som kan gjøre det utfordrende å avgrense risikoområdet. Modul for operasjonell risiko skiller seg fra de øvrige modulene ved at den ikke er rettet mot et spesielt virksomhetsområde, men omfatter ulike kategorier av risiko og hendelser som kan påvirke flere deler av virksomheten. Utgangspunktet for modulen er at den i størst mulig grad skal være dekkende alene, noe som medfører at den på enkelte områder er overlappende med de andre modulene for styring og kontroll av risikoer.

Operasjonell risiko må hensyntas av alle finansforetak, og selv om veiledningen primært er utarbeidet med tanke på vurdering av større foretak, må risikoområdet vurderes og tillegges vekt i ethvert finansforetak. Styrings- og kontrollordningene samt retningslinjer og rutiner skal etter finansforetaksloven § 13-5 (3) imidlertid være tilpasset risikoen ved og omfanget av virksomheten i foretaket. Det vises til eget kapittel om forholdsmessighet i modul for evaluering av intern virksomhetsstyring.

I kapittel 2 til 6 med delkapitler omtales forskjellige momenter relatert til styring og kontroll av operasjonell risiko, mens eksponering omtales i kapittel 7. I vedlegg følger Baselkomiteens reviderte prinsipper for forsvarlig styring av operasjonell risiko[1]. I hvert av delkapitlene følger momenter som Finanstilsynet legger vekt på ved vurdering av foretakene. Vurderingsmomentene bygger på lov eller forskrift, Finanstilsynets rundskriv og internasjonale retningslinjer som eksempelvis Baselkomiteens prinsipper. Enkelte vurderinger er basert på Finanstilsynets erfaringer og observasjoner av beste praksis, herunder erfaringer fra tematilsyn.

Med utgangspunkt i momentene som følger av denne modulen, skal faktisk status for foretaket samt Finanstilsynets vurderinger, spørsmål og konklusjoner oppsummeres i et hjelpeskjema. Finanstilsynets interne vurderinger av status for foretakets styring og kontroll og vurdert nivå for foretakets risikoeksponering oppsummeres i en fire-delt gradering. Finanstilsynet benytter karakterer fra 1 til 4, som representerer beskrivelsen "god", "tilfredsstillende", "mindre tilfredsstillende" og "ikke tilfredsstillende". Klassifiseringen og hjelpeskjemaet benyttes ikke i den eksterne kommunikasjonen.

1.1. Relevante referanser

Lover og forskrifter

- Lov om finansforetak og finanskonsern (finansforetaksloven)
- Lov om tilsynet med finansforetak mv. (finanstilsynsloven)
- Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven)
- Lov om verdipapirhandel (verdipapirhandelloven)
- Forskrift om finansforetak og finanskonsern (finansforetaksforskriften)
- Forskrift om kapitalkrav og nasjonal tilpasning av CRR/CRD IV (CRR/CRD IV-forskriften)

[1] https://www.bis.org/bcbs/publ/d515.htm

- Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) (Forskrift om IKT-systemer i banker mv.)
- Forskrift om meldeplikt ved utkontraktering av virksomhet mv.
- Forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften)

Rundskriv

- Rundskriv 15/2009: Rapportering av IKT-hendelser til Kredittilsynet
- Rundskriv 12/2016: Finanstilsynets praksis for vurdering av risiko og kapitalbehov
- Rundskriv 4/2019: Retningslinjer for klagebehandling i bank-, finans-, forsikrings- og verdipapirverksemd
- Rundskriv 6/2019: Rundskriv om finansagenter
- Rundskriv 8/2019: Veileder til hvitvaskingsloven
- Rundskriv 10/2019: Finanstilsynets retningslinjer for gjenopprettingsplaner
- Rundskriv 7/2021: Veiledning om utkontraktering

Internasjonale retningslinjer (bl.a. EBA og Baselkomiteen)

- Baselkomiteen: Revisions to the Principles for the Sound Management of Operational Risk – March 2021
- Baselkomiteen: Principles for effective risk data aggregation and risk reporting - 2013 (BCBS 239)
- EBA Guidelines on common procedures and methodologies for the supervisory evaluation process (SREP) and supervisory stress testing (EBA/GL/2018/03)
- EBA Guidelines on institutions' stress testing (EBA/GL/2018/04)
- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)
- EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)
- EBA's Revised list of Risk Indicators and Methodological Guide
- EBA Report on Management and Supervision of ESG Risks for Credit Institutions and Investment Firms (EBA/REP/2021/18)

Annet

- Modul for evaluering av intern virksomhetsstyring

2. STRATEGI, OVERORDNEDE RETNINGSLINJER OG RISIKORAMMER

2.1. Strategi og overordnede retningslinjer

Formålet med dette kapittelet er å vurdere foretakets strategi og overordnede retningslinjer for operasjonell risiko, herunder at retningslinjene reflekterer strategien og at foretakets virksomhet drives i tråd med strategi og retningslinjer.

Foretaket skal drives forsvarlig og ha hensiktsmessige retningslinjer og rutiner for å identifisere, styre, overvåke og rapportere risiko foretaket er, eller kan bli, utsatt for, jf. finansforetaksloven § 13-5. Retningslinjene og rutinene for styring og kontroll av risiko skal omfatte operasjonell risiko, jf. CRR/CRD IV-forskriften § 36, herunder beredskapsplaner for å sikre drift og begrense tap ved driftsforstyrrelser.

Foretaket skal jevnlig vurdere og overvåke foretakets samlede risiko og kapitalbehov (ICAAP), herunder vurdere kapitalbehov knyttet til operasjonell risiko, jf. finansforetaksloven § 13-6.

Nedenfor følger aktuelle momenter.

Dokumentasjon og prosess

- Operasjonell risiko og annen ikke-finansiell risiko som eksempelvis omdømmerisiko bør inngå i foretakets ordinære rammeverk for risikostyring og kontroll.
- Foretaket bør ha et rammeverk for styring og kontroll av risiko som inkluderer en strategi for styring av operasjonell risiko, som dekker hele virksomheten, jf. finansforetaksloven § 13-5 (1) og Baselkomiteens prinsipp 2.
- Rammeverket bør i tillegg til risikostrategien inkludere rammer og retningslinjer for styring av operasjonell risiko, system for kontroller, registrering, oppfølging og rapportering. Rammeverket bør videre hensynta foretakets forretningsmodell, virksomhetsområder og konkurranseforhold, samt risikokultur.
- Rammeverket bør fastsettes og jevnlig revideres av styret i lys av endrede risikoforhold og rammebetingelser, makroøkonomiske utsikter, utviklingen innenfor strategiske satsningsområder, foretakets soliditet og økonomiske utvikling, jf. CRR/CRD IV-forskriften § 35 og Baselkomiteens prinsipp 3.
- Revisjoner av overordnede retningslinjer bør dokumenteres og endringer bør være sporbare.

Enkelte faktorer kan medføre økt operasjonell risiko, og vurderingen av rammeverket bør sees i lys av eksempelvis følgende:
- Har det vært gjennomført eller planlegges oppkjøp, fusjoner, fisjoner eller andre vesentlige endringer i foretakets forretningsmodell og/eller strategi?
- Har foretaket gjennomført eller planlegges nedbemanninger, omorganiseringer eller andre større organisatoriske endringsprosesser?
- Har foretaket gjennomført eller planlegges større endringer i IKT-systemet og/eller i andre produksjonsprosesser?
- Er foretakets strategi og/eller forretningsplan så ambisiøs at det kan påvirke foretakets operasjonelle risiko fremover?

Innhold

- I strategien bør styret tydelig definere sin operasjonelle risikoappetitt. Fastsettelsen av risikoappetitt bør definere nivået på operasjonell risiko som foretaket er villig til å akseptere, jf. Baselkomiteens prinsipp 4.
- Risikoappetitt bør stå i forhold til foretakets soliditet og lønnsomhet.
- Strategi og overordnede retningslinjer bør inneholde kvantifiserte måltall og rammer for eksponering på ulike områder og for ulike typer operasjonell risiko.

- Foretaket bør inkludere ESG-faktorer (ref. pkt. 4.4.6 under), herunder hvordan disse påvirker operasjonell risiko, i foretakets risikoappetitt, i strategien og i retningslinjene for operasjonell risiko. Strategien for operasjonell risiko bør være i samsvar med foretakets overordnede strategi for bærekraft, og tidshorisonten for strategisk planlegging bør utvides til minst 10 år, jf. EBA/REP/2021/18.
- Foretaket bør ha en systematisk tilnærming til definering og vurdering av sin risikoappetitt. Foretakets risikoappetitt bør være basert på relevant informasjon og dokumentasjon om operasjonell risiko. Foretaket bør i forbindelse med definering av risikoappetitt blant annet ha et bevisst forhold til terskler, triggere og risikoreduserende tiltak for operasjonell risiko.

2.2. Risikorammer

Formålet med dette punktet er å vurdere kvantitative risikorammer og måltall som er etablert for å styre operasjonell risiko.

Nedenfor følger aktuelle momenter:

- Styret skal med utgangspunkt i vedtatt risikoappetitt fastsette måltall og rammer for ulike områder for å sikre at foretaket har tilstrekkelig styring med den operasjonelle risikoen.
- Fastsatte rammer og måltall bør være målbare og ikke unødvendig komplekse.
- Rammestrukturen og måltallene bør være tilpasset aktivitets- og risikonivået i foretaket og dekke hele virksomheten.
- Risikorammer og måltall skal, som del av foretakets styrings- og kontrollordninger for operasjonell risiko, evalueres regelmessig, jf. finansforetaksloven § 13-6 (4). Normalt bør dette skje årlig.
- Foretakets risikorammer og måltall for styring og kontroll av operasjonell risiko bør være dokumentert og til enhver tid oppdaterte.
- Rammeutnyttelsen og indikatorer for operasjonell risiko bør overvåkes regelmessig opp mot måltallene styret har satt. Styret bør jevnlig motta rapporter om utnyttelsen av risikorammene.

Risikoappetitt og måltall kan for eksempel uttrykkes som maksimale beløp som aksepteres tapt pga. operasjonelle risikoforhold, operasjonelle tap i forhold til kapitalkrav i pilar 1 for operasjonell risiko, antall operasjonelle hendelser (både samlet, innenfor forskjellige områder og typer), indikatorer som måler oppetid eller driftsavbrudd, kundeklager, sykefravær, mm.

Finanstilsynet forventer at foretakene i forbindelse med fastsettelsen av rammer og måltall for styring av operasjonell risiko, bl.a. ser hen til foretakenes taps- og hendelsesdatabase. Se kapittel 4 Identifisering og vurdering – inkludert tapshendelseskategorier og kapittel 7. Eksponering under for mer om indikatorer på det operasjonelle risikonivået. Alle hendelser bør vurderes, men foretaket bør rette spesiell oppmerksomhet på hendelser med lav frekvens og høy konsekvens, dvs. ekstreme, men ikke usannsynlige hendelser som kan medføre store tap for virksomheten.

3. ORGANISERING, ANSVARSFORHOLD, UTKONTRAKTERING MV.

3.1. Styrets rolle og ansvar

Formålet med dette punktet er å vurdere styrets rolle og involvering i virksomheten, og styrets styring og kontroll med foretakets operasjonelle risiko, jf. finansforetaksloven § 8-6 og CRR/CRD IV-forskriften § 35.

Styret har ansvar for foretakets forvaltning og skal sørge for forsvarlig organisering av virksomheten, herunder påse at kravene til organisering av foretaket og etablering av forsvarlige styrings- og kontrollsystemer blir etterkommet, jf. finansforetaksloven § 8-6 (1).

Nedenfor følger aktuelle momenter. Det henvises for øvrig til modul for evaluering av intern virksomhetsstyring for mer utfyllende forventninger til styret.

- Styret skal fastsette og regelmessig vurdere strategier, risikoappetitt, planer og overordnede retningslinjer for å identifisere, styre, overvåke, kontrollere og rapportere operasjonell risiko, CRR/CRD IV-forskriften § 35.
- Styret har det overordnede ansvaret og bør etablere en sterk risikostyringskultur i hele organisasjonen, jf. Baselkomiteens prinsipp 1 og 9. "Tonen fra toppen" er avgjørende for risikostyringen i et foretak og arbeid med organisasjonskultur antas å gi positivt bidrag til operasjonell risikostyring.
- Styret skal sikre seg tilgang til risikoinformasjon ved å fastsette omfang, format og frekvens på rapporteringen, jf. etter CRR/CRD IV-forskriften § 35.
- Styret skal føre tilsyn med foretakets ledelse for å se til at overordnede retningslinjer, prosesser og systemer for styring av operasjonell risiko er effektivt implementert på alle beslutningsnivåer i organisasjonen, jf. finansforetaksloven § 8-6 og Baselkomiteens prinsipp 3.
- Styret bør påse at det eksisterer en sunn organisasjonskultur. Organisasjonskulturen (verdier, holdninger, etikk, mv.) i et foretak kan innvirke på operasjonelle hendelser. En usunn organisasjonskultur kan øke sannsynligheten for operasjonelle hendelser og konsekvensene eventuelle hendelser kan få for foretaket.
- Styret bør definere nøkkelfunksjoner, jevnlig vurdere nøkkelpersonrisikoen og ved behov iverksette risikoreduserende tiltak.
- Styret skal påse at foretaket har en tilfredsstillende internkontroll av foretakets operasjonelle risiko.
- Styret skal godkjenne internrevisjonens ressurser og planer på årlig basis.

3.2. Organisering, bemanning og kontroll

3.2.1. Ressurser, kompetanse og godtgjørelsesordninger

Formålet med dette kapitlet er å vurdere foretakets ressurser og kompetanse for styring og kontroll av operasjonell risiko, samt foretakets godtgjørelsesordninger.

Daglig leder skal sørge for at foretaket har ansatte som samlet har kvalifikasjoner og erfaringer som trengs for at virksomheten i foretaket drives på en forsvarlig måte, og at det etableres forsvarlige styrings- og kontrollsystemer, jf. finansforetaksloven § 8-11 (3). Foretakets godtgjørelsesordning, som skal fastsettes av styret, skal bidra til god styring og kontroll med foretakets risiko, motvirke høy risikotaking og bidra til å unngå interessekonflikter, jf. kapittel 15 i finansforetaksforskriften.

Nedenfor følger aktuelle momenter:

- Foretaket bør påse at medarbeiderne har nødvendig erfaring og kompetanse om operasjonell risiko, og at kompetansehevende tiltak tilbys.
- Antallet medarbeidere bør være tilpasset virksomhetens kompleksitet og omfang. Ressursene bør være tilstrekkelig til å dekke inn midlertidig fravær av nøkkelpersonell. Spesielt for mindre foretak kan nøkkelpersonellrisikoen være høy. Av særlige risikofaktorer kan nevnes sårbarhet ved tap av kompetanse, manglende kompetanse til å kontrollere spesialister i eget foretak, avhengighet av enkeltpersoner, svak arbeidsdeling og ikke tilstrekkelig uavhengig kontroll.
- Personell, både i støtte- og i uavhengige kontrollfunksjoner, bør ha god forståelse av aktuelle risikoer og ha myndighet til og ansvar for å belyse og vurdere handlinger utført av personell med resultatansvar.
- Uavhengige kontrollfunksjoners ressurser og kompetanse innen operasjonell risiko bør være tilpasset kompleksiteten og omfanget av virksomheten.
- Godtgjørelsesordninger som stimulerer til aggressivt handlingsmønster kan øke den operasjonelle risikoen i foretaket ved økt regelbrudd, kritikkverdig adferd og feil (atferdsrisiko). Se spesielt finansforetaksforskriften §§ 15-4 til 15-6 for regler om godtgjørelse til ledende ansatte, personer med vesentlig betydning for foretakets risikoeksponering og ansatte med kontrolloppgaver. Se for øvrig om godtgjørelsesordninger i modul for evaluering av intern virksomhetsstyring.

3.2.2. Organisering og ansvar for internkontroll i første linje

Formålet med dette punktet er å vurdere om foretakets organisering av styring og kontroll av operasjonell risiko er klar, dokumentert og tilpasset virksomhetens størrelse, kompleksitet og omfang.

Foretaket skal organiseres og drives på en forsvarlig måte og ha en klar organisasjonsstruktur, jf. finansforetaksloven § 13-5 første ledd. Risikohåndtering og internkontroll av operasjonell risiko bør integreres i foretakets overordnede rammeverk for risikohåndtering og internkontroll.

Nedenfor følger aktuelle momenter:

- Foretakets øverste administrative ledelse er ansvarlig for å utvikle en klar, effektiv og robust styringsstruktur med definerte, transparente og konsistente ansvarslinjer som godkjennes av styret, jf. finansforetaksloven § 8-11.
- Foretaket bør ha en styringsstruktur som effektivt iverksetter foretakets strategi for operasjonell risiko.
- Ledelsen er ansvarlig for å implementere og vedlikeholde retningslinjer, prosesser og systemer for styring av operasjonell risiko i hele virksomheten i samsvar med styrets definerte risikoappetitt, jf. finansforetaksloven § 8-11 og Baselkomiteens prinsipp 5.
- Foretaket skal ha retningslinjer for å sikre tilstrekkelig arbeidsdeling og for å unngå interessekonflikter, jf. CRR/CRD IV-forskriften § 35 annet ledd.
- Foretaket må sikre at det er tilstrekkelig uavhengighet og arbeidsdeling mellom enheter og personell med utøvende funksjoner og enheter og personell med ansvar for overvåking, rapportering og kontroll av operasjonell risiko.
- Stillingsinstrukser og arbeidsbeskrivelser bør foreligge for de mest sentrale medarbeiderne. Daglig leder skal etter finansforetaksloven § 8-11 (3) sørge for at det blir fastsatt instrukser som angir de ansattes arbeidsoppgaver og ansvarsforhold, samt rapporterings- og saksbehandlingsregler.

3.2.3. Uavhengige kontrollfunksjoner i andre- og tredje linje

Formålet med dette punktet er å kartlegge og vurdere mandat samt utøvelsen av ansvaret foretakets uavhengige kontrollfunksjoner er tildelt for operasjonell risiko. Dette innebærer blant annet å kartlegge og vurdere instrukser og retningslinjer, samt å vurdere omfang og innhold på arbeidet til uavhengige kontrollfunksjoner. Funksjonenes ansvar og generelle hovedoppgaver er også omhandlet i modul for intern virksomhetsstyring. Med uavhengig kontrollfunksjoner menes i denne sammenheng interne kontrollfunksjoner i andre linje og internrevisjonen i tredje linje.

Et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring og etterlevelse (compliance), samt internrevisjon, jf. finansforetaksloven § 13-5 (2). De uavhengige kontroll-funksjonene bør foreta relevante, dokumenterbare operasjonelle risikokontroller med høy faglig standard og må ha tilstrekkelig kompetanse og ressurser innen operasjonell risiko.

Interne kontrollfunksjoner skal jevnlig rapportere om risiko- og etterlevelse hva gjelder operasjonell risiko til ledelsen og styret for å gi en uavhengig vurdering av status, utvikling og mulige fremtidige risikoer på området.

Risikokontrollfunksjon

- Foretaket skal etter finansforetaksloven § 13-5 (2) ha en uavhengig risikokontrollfunksjon som skal ha tilstrekkelig kompetanse og ressurser for styring, overvåking og oppfølging av risiko, herunder operasjonell risiko, jf. CRR/CRD IV-forskriften § 38.
- Risikokontrollfunksjonen, som også har et ansvar for styring og kontroll av operasjonell risiko, skal være uavhengig av operative funksjoner, rapportere til daglig leder, kunne rapportere direkte til styret og ikke kunne avsettes uten samtykke fra styret, jf. CRR/CRD IV-forskriften § 38.
- Risikokontrollfunksjonen bør være involvert i diskusjoner om foretakets strategi og risikoappetitt for operasjonell risiko, og være involvert i utarbeidelsen av foretakets risiko-toleranse, risikostrategi og overordnede rammer for risikotagning. Risikokontrollfunksjonen skal være involvert i vurderinger som har vesentlig betydning for foretakets samlede risiko. Risikokontrollfunksjonen bør utfordre de operasjonelle risiko- og kontrollvurderingene av første forsvarslinje, samt overvåke implementeringen av passende kontroller eller utbedringstiltak, jf. Baselkomiteens prinsipp 7.
- Generelt sett endrer et foretaks operasjonelle risikoeksponering seg når foretaket iverksetter endringer, jf. Baselkomiteens prinsipp 7. Risikokontrollfunksjonen skal etter CRR/CRD IV-forskriften § 36 involveres i prosessen med å vurdere risiko i nye produkter, tjenester og andre nye aktiviteter som kan påvirke foretakets operasjonelle risiko.
- Risikokontrollfunksjonen bør foreta relevante kontroller og overvåke at foretakets internkontroll av operasjonell risiko er hensiktsmessig og effektiv.

Etterlevelsesfunksjon

- Foretaket skal etter finansforetaksloven § 13-5 (2) ha en uavhengig etterlevelsesfunksjon som skal ha tilstrekkelig kompetanse og ressurser for å kontrollere og regelmessig vurdere foretakets oppfølging av risiko, jf. CRR/CRD IV-forskriften § 39.
- Etterlevelsesfunksjonen bør gjennomføre tester for å verifisere at aktuelt eksternt og internt regelverk, herunder om hvitvasking og ESG-regelverk, etterleves. Rapporter vedrørende gjennomførte kontrollaktiviteter fra uavhengig kontrollfunksjon bør adresseres til og behandles av relevant nivå i organisasjonen.
- Etterlevelsesfunksjonen skal etter CRR/CRD IV-forskriften § 36 involveres i prosessen med å vurdere risiko i nye produkter, tjenester og andre nye aktiviteter som kan påvirke foretakets operasjonelle risiko.

Internrevisjon

- Foretak skal etter finansforetaksloven § 13-5 (2) ha en uavhengig kontrollfunksjon med ansvar for internrevisjon. Foretak som i mer enn de siste 12 måneder har hatt en forvaltningskapital som er lavere enn 10 milliarder kroner, har unntak fra kravet om internrevisjon. I foretak som ikke har internrevisjon, skal valgt revisor gi en årlig bekreftelse til styret om risikostyringen og internkontrollen.
- Internrevisjonen skal etter finansforetaksloven § 8-16 jevnlig kontrollere at virksomheten er organisert og drives på en forsvarlig måte og i samsvar med gjeldende krav. Undersøkelser bør blant annet omhandle kvaliteten på retningslinjer og rutiner for styring og kontroll av operasjonell risiko, og hvorvidt retningslinjer faktisk følges.
- Foretakets system for styring og kontroll av operasjonell risiko bør jevnlig evalueres av en uavhengig kontrollfunksjon. For foretak som benytter sjablongmetoden for beregning av kapitalkrav i pilar 1 skal systemet gjennomgås og bekreftes av en uavhengig funksjon regelmessig, jf. CRR/CRD IV-forskriften § 2, jf. CRR artikkel 320 (a).

3.3. Utkontraktering

Utkontraktering kan gi muligheter for bedre og mer kostnadseffektive prosesser og tjenester grunnet eksempelvis stordriftsfordeler og tilgang til ekspertise, og benyttes av de fleste finansforetak.

Utkontraktering av oppgaver kan samtidig medføre en mer kompleks organisering av den samlede virksomheten som kan øke den operasjonelle risikoen i foretaket. Endringer i forbindelse med etablering av utkontraktering kan i seg selv bidra til nye risikoer, risikoer som foretakets styre og ledelse må adressere, jf. Baselkomiteens prinsipp 7.

Foretaket skal sørge for at organisasjonen besitter tilstrekkelig kompetanse til å håndtere utkontrakteringsavtalen, jf. CRR/CRD IV-forskriften § 36.

Nedenfor følger aktuelle momenter:

- Oppgaver kan utkontrakteres, ikke ansvar. Foretaket er fullt ut ansvarlig for utkontraktert virksomhet, herunder risikostyring og internkontroll, jf. finansforetaksloven § 13-4 (3), CRR/CRD IV-forskriften § 36 og IKT-forskriften § 12.
- Styret må fastsette interne retningslinjer for utkontraktering. Retningslinjene bør inkludere rutiner for melding til Finanstilsynet før inngåelse av avtaler om utkontraktering, jf. finanstilsynsloven § 4c. Meldeplikten ved utkontraktering etter finanstilsynsloven gjelder avtaler om utkontraktering av virksomhet som er kritisk eller viktig for foretaket, jf. meldepliktforskriften § 3.
- Retningslinjene må bl.a. sikre at foretaket, før avtale om utkontraktering inngås, vurderer:
    - om det er begrensninger i adgangen til å utkontraktere de aktuelle oppgavene,
    - om avtalen er meldepliktig, og
    - hvilke risikoer utkontrakteringen vil innebære, og behovet for risikoreduserende tiltak.
- Utkontraktering forutsetter en skriftlig avtale som sikrer innsyn, kontroll og revisjon av den utkontrakterte virksomheten, også for Finanstilsynet.
- Avtaler om utkontraktering skal sikre rimelig rett til oppsigelse av avtalen under betryggende forhold til alternativ løsning er etablert.
- Avtaler om utkontraktering av IKT-systemer som er av betydning for foretakets virksomhet (og endringer i slike) skal behandles av styret, jf. IKT-forskriften § 2. En grundig risikovurdering skal inngå i grunnlaget for beslutninger om utkontraktering.
- Foretaket kan bare utkontraktere virksomhet dersom det anses forsvarlig. Foretaket må selv ha kompetanse til å vurdere om oppdragstaker utfører oppdraget tilfredsstillende. Oppdragsgiver må ha kapasitet og kompetanse til fortløpende å sikre nødvendig styring og kontroll med utkontraktert virksomhet, jf. finansforetaksloven § 13-4.
- Finansforetak kan ikke utkontraktere kjerneoppgaver. En bank kan eksempelvis ikke utkontraktere rentefastsettelsen eller fastsettelse av grunnlaget for innvilgelse av kreditt. For øvrig beror det på en konkret vurdering hva som anses som kjerneoppgaver.
- Foretakets risikovurdering må også vurdere muligheten til å terminere avtalen og flytte utkontrakterte funksjoner og data til andre tilbydere, alternativt ta oppgaven tilbake i foretaket, uten at det skaper vesentlige forstyrrelser i virksomheten.
- Foretaket skal ha en oppdatert oversikt over alle sine utkontrakteringsavtaler, jf. meldepliktforskriften § 1.

For mer informasjon, se rundskriv 7/2021 Veiledning om utkontraktering. Utkontraktering av oppgaver etter hvitvaskingsloven er omtalt i den generelle veiledning til hvitvaskingsloven i rundskriv 8/2019.

4. IDENTIFISERING OG VURDERING – INKLUDERT TAPSHENDELSESKATEGORIER

Formålet med dette kapitlet er å vurdere om foretaket har relevante systemer og prosesser for å identifisere, måle og vurdere operasjonell risiko.

Finansforetak skal til enhver tid ha oversikt over risikoer, herunder operasjonell risiko, som er knyttet til virksomheten. Vurdering av operasjonell risiko skal minimum gjøres årlig i forbindelse med foretakets vurdering av samlet kapitalbehov i forhold til risikoprofil (ICAAP[2]), jf. finansforetaksloven § 13-6.

Mangler og avvik påpekt av uavhengige kontrollfunksjoner som risikokontroll, etterlevelse og intern- og valgt revisor er viktige kilder til informasjon om den operasjonelle risikoen i et foretak. Dette bør vurderes og sees i sammenheng med foretakets egen taps- og hendelsesdatabase, risikovurderinger, stresstester og scenarioanalyser.

4.1. System for måling av operasjonell risiko i løpende drift

Foretaket bør ha system, prosesser og interne retningslinjer for å identifisere, måle og vurdere den operasjonelle risikoen i alle vesentlige produkter, aktiviteter, prosesser og systemer, jf. Baselkomiteens prinsipp 6.

4.1.1. Tapshendelser

Håndtering av hendelser utgjør et vesentlig element i styring og kontroll av operasjonell risiko, og hendelsesdata bør inngå som grunnlag når risikonivå og risikoappetitt skal vurderes. Hendelsesdata vil også kunne utnyttes for å identifisere potensielle risiko- og forbedringsområder. Foretak som har valgt å anvende sjablongmetoden for beregning av kapitalkravet for operasjonell risiko, må oppfylle kravene i kapitaldekningsregelverket (jf. CRR artikkel 320 samt pkt. 4.3 under). Blant annet skal foretaket registrere relevante opplysninger om operasjonell risiko, herunder opplysninger om betydelige tap.

Operasjonelle risikohendelser deles ofte inn i Baselkomiteens syv tapshendelseskategorier. Banker som benytter sjablongmetoden[3] må rapportere opplysninger om betydelige tap også som tilleggsinformasjon til kapitaldekningsrapporteringen (COREP C.17) i henhold til disse kategoriene:

1. Internt bedrageri
2. Eksternt bedrageri
3. Ansettelsesvilkår og sikkerhet på arbeidsplassen
4. Kunder, produkter og forretningspraksis
5. Skade på fysiske eiendeler
6. Avbrudd i drift eller systemer
7. Oppgjør, levering og annen transaksjonsbehandling

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.

[2] "Internal capital adequacy assessment process", ref. Rundskriv 12/2016 Finanstilsynets praksis for vurdering av risiko og kapitalbehov.

[3] For foretak som ønsker å søke om godkjennelse av avansert metode (AMA) forberegning av minstekrav til kapital for operasjonell risiko er det et krav at interne tapsdata tilordnes de samme tapshendelseskategoriene.

Beste praksis for måling av operasjonell risiko inkluderer et system for registrering av tapshendelser i en taps- og hendelsesdatabase, hvor hendelsene fordeles på tapshendelseskategorier med eventuelle underkategorier.

Nedenfor følger aktuelle momenter:

- Foretakenes taps- og hendelsesdatabase bør utformes slik at den tar vare på all relevant informasjon om hendelser. Informasjonen bør systematiseres på en måte som muliggjør læring og økt kunnskap, samt igangsetting av tiltak for å forhindre fremtidige uønskede hendelser. Bruk av interne beløpsterskler for registrering av hendelser kan redusere informasjonsverdien av taps- og hendelsesdatabaser.
- Alle operasjonelle hendelser, uavhengig av tap bør registreres. Også operasjonelle hendelser som resulterer i finansiell gevinst bør registreres i databasen(-e).
- Foretaket bør ha system og interne retningslinjer som sikrer at hendelser som medfører vesentlig reduksjon i funksjonalitet i IKT-systemer rapporteres til Finanstilsynet, jf. IKT-forskriften § 9 og rundskriv 15/2009.

For mer om vurdering av foretakets system for håndtering av hendelser, henvises det til rapport fra tematilsyn Operasjonell risiko – hendelser datert 11. juni 2017.

4.1.2. Egenevaluering, scenario-analyser mv.

Egenevalueringer av risiko bør videre jevnlig gjennomføres på forskjellige nivåer og deler av virksomheten. Vurderingene evaluerer typisk iboende risiko (risikoen før kontrolltiltak), effekten av kontrolltiltak og gjenværende risiko, vurdert ut fra sannsynlighet og konsekvens. Egenevalueringer bør være et supplement til løpende styrings- og kontrollinformasjon, som kan gi økt bevissthet og informasjon om foretakets operasjonelle risiko. En systematisk kartlegging av operasjonelle risikoer og tiltak for å følge opp områder med høyere risiko bør være en integrert del av styringen av virksomheten.

Scenarioanalyser er en metode for å identifisere, analysere og måle en rekke scenarioer, inkludert hendelser med lav sannsynlighet og høy alvorlighetsgrad, hvorav noen kan resultere i alvorlige operasjonelle tap. Scenarioanalyse involverer typisk workshop-møter med fageksperter, inkludert toppledelse, forretningsledelse og leder av operasjonell risikostyring og andre funksjonelle områder som etterlevelse (compliance), HR og IT-risikostyring, for å utvikle og analysere driverne og rekkevidden av konsekvenser av potensielle hendelser. Inndata til scenarioanalysen vil typisk inkludere relevante interne og eksterne taps- og hendelsesdata, informasjon fra egenvurderinger, rammeverket for internkontroll og sikkerhet, fremtidsrettede indikatorer, analyser av rotårsaker med mer. Scenarioanalyseprosessen kan brukes til å utvikle en rekke konsekvenser av potensielle hendelser, inkludert konsekvensvurderinger for risikostyringsformål, supplere andre verktøy basert på historiske data eller nåværende risikovurderinger. Det kan også integreres med gjenopprettingsplaner og beredskaps- og kontinuitetsplaner, og for bruk i testing av operasjonell motstandskraft. Gitt scenarioprosessens subjektivitet, er et robust styringsrammeverk og uavhengig gjennomgang viktig for å sikre integriteten og konsistensen i prosessen.

Benchmarking, komparativ analyse eller andre sammenlignende analyser kan videre øke forståelsen av bankens operasjonelle risikoprofil. Mangel på tilgjengelig og nøyaktig data innen operasjonell risikostyring gjør at sammenlignende analyser benyttes i mindre grad.

4.2. Operasjonell risiko i nye produkter, aktiviteter, prosesser og systemer

Nye produkter, aktiviteter, prosesser og systemer kan medføre store endringer i foretakenes operasjonelle risiko.

Nedenfor følger aktuelle momenter:

- Foretakets ledelse må sørge for at foretaket har retningslinjer for godkjenning og en klar godkjenningsprosess for nye produkter, aktiviteter, prosesser og systemer, jf. Baselkomiteens prinsipp 7 og CRR/CRD IV-forskriften § 36.
- Nye produkter, aktiviteter, prosesser og systemer av vesentlig betydning og/eller avvikende risikoprofil bør godkjennes av styret og/eller relevante organ på øverste ledelsesnivå.
- Nye produkter og tjenester skal særskilt vurderes ut fra risikoen for hvitvasking og terrorfinansiering før det tas i bruk, jf. hvitvaskingsloven § 7. Det samme gjelder der det tas i bruk ny teknologi.
- Foretaket skal ved endring eller etablering av produkter og rutiner av vesentlig betydning gjøre en risikovurdering, som må inkludere operasjonelle risikofaktorer, før virksomheten igangsettes, jf. CRR/CRD IV-forskriften § 36.
- Risikovurderingen bør klargjøre risikoreduserende tiltak, både tiltak som skal iverksettes før igangsetting og tiltak som kan iverksettes på kort og lang sikt dersom risikoen utvikler seg negativt.
- Styret bør sørge for at foretakets endringsprosesser har tilstrekkelige ressurser med klare ansvarslinjer og inkluderer kontinuerlige risiko- og kontrollvurderinger.

4.3. Måling av operasjonell risiko ved beregning av kapitalbehov

Etter dagens regelverk kan finansforetak anvende tre forskjellige metoder for beregning av kapitalkravet for operasjonell risiko i pilar 1: *basismetoden*, *sjablongmetoden* og *AMA-metoden*. Basismetoden og sjablongmetoden baserer seg på standardiserte prosentsatser for 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, jf. CRR/CRD IV-forskriften § 2, jf. CRR artikkel 320.

Norske foretak benytter basismetoden eller sjablongmetoden. Ingen norske foretak benytter per februar 2022 myndighetsgodkjente AMA-modeller. Foretakene skal i sin interne kapitalvurderings-prosess (ICAAP) minimum årlig vurdere sitt kapitalbehov for operasjonell risiko. I den forbindelse skal foretakene vurdere om beregnet regulatorisk kapital er tilstrekkelig sett i forhold til risikonivå, og vurdere om det er behov for et pilar 2-tillegg for operasjonell risiko.

Nedenfor følger aktuelle momenter:

- Foretaket bør ha rutiner og prosedyrer som sikrer riktig måling og beregning av regulatorisk kapital for operasjonell risiko.
- Beregnet regulatorisk kapital bør vurderes mot foretakets definerte risikoappetitt og faktiske historiske tap som følge av operasjonelle feil.

For foretak i vekst vil beregnet regulatorisk kapital bli for lavt – gitt alt annet likt – i et fremadskuende perspektiv. Også for foretak med ett eller flere år med uvanlig lave inntekter, vil beregnet regulatorisk kapital bli lavt. Den operasjonelle risikoen vil ikke nødvendigvis være redusert selv om inntektene går ned.

Baselkomiteen vedtok i 2017 nye, globale standarder for beregning av operasjonell risiko. Høsten 2021 publiserte Kommisjonen sitt forslag til implementering i EU/EØS[4]. Det nye rammeverket erstatter alle eksisterende beregningsmetoder med én ny revidert sjablongmetode som kalles standardmetode. Beregningsmetodikken for standardmetoden foreslås fortsatt å bygge på inntekter for de tre foregående årene. Basel-standarden åpnet for at beregningene også skulle inkludere tapshistorikk i foretakene, men i Kommisjonens forslag er denne valgmuligheten fjernet, slik at beregningene kun skal baseres på inntekter. Det som er nytt er at den foreslåtte metodikken skal baseres på størrelsen

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0664

på såkalte forretningsindikatorer, og at det legges til grunn bruttostørrelser, med unntak for renter hvor foretakene skal legge til grunn nettorenten. Bruk av bruttotall har den konsekvens at størrelse får større betydning sammenlignet med dagens regelverk som baserer seg på nettotall.

4.4. Enkelte underkategorier av operasjonell risiko

Det finnes flere underkategorier av operasjonell risiko. Formålet med dette kapittelet er å vurdere enkelte av disse risikoene som normalt er relevante for finansforetak og som kan ha vesentlig innvirkning på foretakenes virksomhet, og styring og kontroll av underkategoriene.

4.4.1. Modellrisiko

Modellrisiko kan relatere seg til forskjellige forhold:

1) Risiko for underestimering av kapitalbehov som følge av feil i utvikling, implementering og bruk av interne modeller, vanligvis IRB-modeller for beregning av kapital for kredittrisiko.
2) Risiko for tap som følge av utvikling, implementering og feilaktig bruk av modeller som brukes i foretakets beslutningsprosesser, eksempelvis til kredittvurdering, prising av produkter, evaluering av finansielle instrumenter, overvåking av risikorammer og måltall, mv.

Vedrørende pkt. 1) så er dette en risiko som vurderes som en del av spesifikke IRB-tilsyn og som dermed faller utenfor det ordinære tilsynet med operasjonell risiko. Denne risikoen hensyntas i hovedsak i pilar 1-kravet for kredittrisiko gjennom sikkerhetsmarginer i modellene.

Hva gjelder pkt. 2) er dette en risiko som faller inn under operasjonell risiko og som må vurderes under tilsyn av det aktuelle risikoområdet. Elementer som kan ha betydning er kvaliteten på foretakets prosesser for endringer av og nye produkter og tjenester (ref. kap. 4.2 over), valideringsprosesser mv. Modellrisiko kan i tillegg til å øke foretakets operasjonelle risiko også påvirke andre risikoer eller foretakets omdømme. Eksempelvis kan feil i eller feil bruk av en prisingsmodell føre til feil prising, som er en forretningsrisiko og som også kan påvirke foretakets strategiske risiko.

Finansforetakenes fokus på og økende bruk av digitalisering og automatisering, bruk av stordata og ny teknologi som eksempelvis kunstig intelligens, gir ikke bare økt modellrisiko, men også risiko for tap av omdømme og etiske utfordringer. Det er viktig at foretakene har god styring og kontroll med utvikling og bruk av ny teknologi, og påser at sikkerhet og kundevern (herunder personvern og etikk) er ivaretatt. Det forventes at foretakene har gjort grundige risikovurderinger før ny teknologi tas i bruk og at det iverksettes risikoreduserende tiltak der det er nødvendig. Økt tilgang til og bruk av store mengder data, både strukturert og ustrukturert, øker kravene til håndtering og bruk av dataene og datasikkerhet. Videre, bedre modeller har potensiale til å gjøre kundeseleksjon så treffsikker at større grupper kan ende opp uten tilbud om kreditt eller forsikring (finansiell eksklusjon). Etter hvert som algoritmene blir mer komplekse, øker kravene til forklarbarhet og åpenhet rundt beregninger og utfall (transparens).

4.4.2. Atferdsrisiko og kundevern

Internasjonalt er det en økende oppmerksomhet knyttet til risikoen for tap som følge av regelbrudd eller kritikkverdig adferd. Bøter, erstatningskrav og overtredelsesgebyr kan få store negative finansielle konsekvenser for enkeltforetak[5]. Kritikkverdig adferd kan også påvirke foretakets omdømme.

Organisasjonskulturen er nøkkelen til god og riktig adferd. For å få til sunn virksomhetsstyring er "tonen fra toppen" avgjørende og det er ledelsens ansvar å sørge for at den forplantes i virksomhetens verdier, organisasjonsstruktur og målsettinger. Kortsiktig kommersiell lønnsomhet må ikke prioriteres på bekostning av kundenes beste interesse.

I tillegg til å se til at finansforetak er solide og likvide – som sikrer at foretaket er i stand til å stå for sine forpliktelser overfor forbrukerne – er følgende momenter aktuelle og bør vurderes:

[5] Eksempelvis den såkalte "Røeggen-saken" fra 2013 eller "DNB Norge-saken" fra 2020.

Nedenfor følger aktuelle momenter for kundevern:

- Foretaket må ha interne retningslinjer og rutiner som sikrer en forsvarlig kredittpraksis og etterlevelse av utlånsforskriften, slik at forbrukerne ikke tar opp lån de senere ikke vil være i stand til å betjene.
- Foretaket bør ha interne retningslinjer som sikrer at forbrukerne får tilstrekkelig og pålitelig informasjon og god rådgiving om de produktene foretakene selger, og at kundenes interesser blir prioritert, og bør bl.a. omfatte utvikling og kvalitetssikring av dokumentasjon og markedsføringsmateriell, samt opplæring.
- Banker med verdipapirtillatelse skal ha interne retningslinjer som sikrer etterlevelse av kravene til investeringstjenester i tråd med verdipapirhandellovens bestemmelser (MiFID II/ MiFIR-reglene), jf. spesielt verdipapirhandellovens bestemmelser om investorbeskyttelse i §§ 10-9 – 10-25.
- Foretaket skal ha et register over finansagenter som skal gjøres offentlig tilgjengelig på foretakets egen nettside, jf. rundskriv 6/2019, og foretaket må ha egen avtale med alle agentene. Foretaket må ha retningslinjer for oppfølging av agentene.
- Foretaket skal ha skriftlige rutiner som sikrer grundig klagebehandling, herunder at alle kundeklager registreres i et eget register, og årlig rapportering av kundeklager til Finanstilsynet, jf. rundskriv 4/2019. Rutinene skal være offentlig tilgjengelig. Foretak skal videre løpende analysere klagene for å avdekke om årsakene til klagene gjelder systematiske eller grunnleggende problemer som indikerer en høyere operasjonell risiko hos foretaket.
- Foretaket skal sikre at avlønningssystemet (godtgjørelse) ikke premierer atferd som kan gå på bekostning av kundevernet.
- Foretaket skal påse at prinsippet om fritt valg av eiendomsmeglertjenester etterleves, jf. rundskriv 7/2016 og at interessekonflikter ved salg av regnskapstjenester overholdes, jf. rundskriv 4/2021.
- Foretaket må etterleve personopplysningsloven som gjennomfører EUs personvernforordning (GDPR). Regelverket forutsetter blant annet at foretaket har full oversikt over foretakets behandling av personopplysninger og iverksetter tekniske og organisatoriske tiltak som gjør at loven følges.

Bruk av eksterne distributører (forhandlere, agenter o.l.) samt salg av avanserte finansielle spareinstrumenter o.l. kan øke atferdsrisikoen.

I lavrenteregimer kan etterspørselen av alternative spareprodukter med potensiale for høyere avkastning (og høyere risiko) øke, noe som kan øke atferdsrisikoen i foretaket.

Produktpakker er i utgangspunktet forbudt og kan kun tilbys med mindre produktene er knyttet sammen på en måte som gjør det umulig å tilby produktet uten bruk av et annet eller de kan begrunnes med kostnadsbesparelser, jf. finansforetaksforskriften § 16-1.

Annen atferdsrisiko:

- For store banker kan det være en risiko for manipulering av referanserenter (eksempelvis Nibor[6]), kurser og indekser for å øke egen lønnsomhet.
- Egenhandel kan øke foretakets operasjonelle risiko da det øker risikoen for operasjonelle feil, posisjoner og adferd som ikke er i samsvar med foretakets risikoappetitt og innenfor definerte rammer. Videre svekker egenhandel i strid med verdipapirregelverket tilliten til foretakets omdømme og integritet spesielt og markedets integritet generelt.

[6] Norske Finansielle Referanser AS, etablert og heleid av Finans Norge, er ansvarlig administrator for Nibor. Kalkulerings- og lisensieringsagent er Global Rate Set Systems Ltd. (GRSS).

4.4.3. IKT-risiko

Finanssektoren i Norge baserer sin virksomhet på IKT-løsninger, og bruk av IKT er virksomhetskritisk. IKT-risikoen vurderes å være en av de største risikoene for foretakene og sårbarheten er stor, samt at den teknologiske utviklingen innen sektoren skjer raskt. Særlig er risikoen knyttet til digital kriminalitet, både mot foretakene selv og mot foretakenes kunder, økt betydelig.

Det vises til Finanstilsynets Risiko- og sårbarhetsanalyse (ROS)[7] på Finanstilsynets nettside for eksempler på spesifikke forhold som kan gi økt IKT-risiko og som er relevant for mange norske finansforetak.

Hva gjelder IKT-risiko, er IKT-forskriftens bestemmelser essensielle. EBAs retningslinjer om IKT-sikkerhet og -risiko[8] samt for utkontraktering[9] utdyper IKT-forskriftens bestemmelser og retningslinjene følges i Norge. Foretakene skal ha en IKT-strategi, det skal gjennomføres risikoanalyser, det skal fastsettes kvalitetsmål og utarbeides prosedyrer som sikrer systemene, for utvikling, anskaffelse, drift, avviks- og endringshåndtering, samt avtaler for utkontraktering. Videre stilles det krav til kontinuitet og kriseplan mv. Videre skal foretaket ha system og interne retningslinjer som sikrer at hendelser som medfører vesentlig reduksjon i funksjonalitet i IKT-systemer rapporteres til Finanstilsynet, jf. IKT-forskriften § 9 og rundskriv 15/2009.

I modulen er det lagt opp til en begrenset vurdering av IKT-risiko. Ved behov for en grundigere gjennomgang, eksempelvis på grunnlag av funn fra stedlig tilsyn eller andre tilsynsaktiviteter, vurderes IKT-risikoen i spesifikke IT-tilsyn hvor det anvendes egne moduler basert på bl.a. COBIT.

4.4.4. Risiko for feil i rapportering

Mange foretak finner det utfordrende å aggregere risikoeksponeringer og identifisere konsentrasjoner raskt og nøyaktig på foretaksnivå, på tvers av forretningsområder og mellom juridiske enheter. Det på grunn av eksempelvis mangelfulle IT-systemer, datakvalitet og/eller rapporteringsprosesser, noe som krever betydelig ressurser og er tidkrevende å forbedre. Det kan resultere i mangelfull kvalitet i intern- og ekstern rapportering, herunder myndighetsrapportering.

Baselkomiteens "Principles for effective risk data aggregation and risk reporting" (bcbs239) beskriver prinsipper som er vesentlige for å få på plass god aggregering av risikodata og praksis for risikorapportering. Finanstilsynet forventer at foretak tilstreber å etterleve prinsippene.

Nedenfor følger aktuelle momenter:

- Foretaket plikter å ha oversikt over risiko, herunder foretakets soliditets- og likviditetssituasjon, noe som forutsetter at datagrunnlaget som er nødvendig, er tilgjengelig.
- Foretaket bør ha interne retningslinjer som sikrer riktig, rettidig og konsistent intern- og ekstern rapportering.
- Bruk av utkontrakterte løsninger er uten innvirkning på foretakets rapporteringsplikter og -ansvar, jf. IKT-forskriften § 12 og finansforetaksloven § 13-4 (3).
- Rapporteringsfeil bør inngå i foretakets rapportering av operasjonelle hendelser.

4.4.5. Risiko for hvitvasking og terrorfinansiering

Formålet med hvitvasking er å skjule opprinnelsen til utbytte fra straffbare handlinger. Hvitvasking kjennetegnes ved at slikt utbytte integreres i den lovlige økonomien og dermed fremstår som legitimt. Terrorfinansiering er finansiering av terrorhandlinger, terrororganisasjoner eller individuelle terrorister. Bekjempelse og forebygging av hvitvasking og finansiering av terrorisme er viktig i arbeidet mot organisert kriminalitet og terrorisme. Banker og andre finansforetak er viktige aktører i kampen mot hvitvasking og terrorfinansiering.

Nedenfor følger aktuelle momenter:

[7] www.finanstilsynet.no/no/Venstremeny/Om-Finanstilsynet/Publikasjoner/Risiko--og-sarbarhetsanalyse/
[8] www.finanstilsynet.no/nyhetsarkiv/nyheter/2020/eba-har-fastsatt-retningslinjer-om-ikt-sikkerhet-og-risiko/
[9] www.finanstilsynet.no/regelverk/eba-retningslinjer/eba-retningslinjer/eba-har-fastsatt-nye-retningslinjer-for-utkontraktering/

- Foretaket må ha en klar organisering og tydelig ansvarsfordeling av sitt arbeid, bl.a. med en hvitvaskingsansvarlig i ledergruppen, jf. hvitvaskingsloven § 8 (5), og tilstrekkelig med ressurser og kompetanse på området.
- Foretaket må identifisere og forstå risikoen foretaket er eksponert for. Alle rapporteringspliktige må ha en overordnet risikovurdering, jf. § 7, som vurderer risikoen i foretakets egen virksomhet, produkter, tjenester og kundeforhold, type kunder og kundegrupper samt geografiske forhold.
- Styret skal fastsette interne rutiner som er konkret og dekkende og som sikrer etterlevelse av regelverket, jf. § 8. Det må være en tydelig sammenheng mellom risikovurderingen og rutinene.
- Banker, kredittforetak og finansieringsforetak skal ha et elektronisk transaksjonsovervåkingssystem som dekker hele virksomheten, jf. § 38.
- Foretaket skal gjennomføre risikobaserte kundetiltak og løpende oppfølging, jf. § 9, herunder:
    - Risikoklassifisering av kunder,
    - Gjennomføre kundetiltak, herunder bekrefte kundens identitet, identifisere reelle rettighetshavere, innhente opplysninger om formål og tilsiktet art, midlers opprinnelse og fastslå om kunden er en politisk eksponert person.
    - Dersom kundetiltak ikke kan gjennomføres, skal rapporteringspliktige ikke etablere kundeforholdet eller utføre transaksjonen, jf. § 21. Dersom kundetiltak som ledd i løpende oppfølging ikke kan gjennomføres, skal rapporteringspliktige avvikle kundeforholdet, jf. § 24.
- Foretak skal gjennomføre løpende oppfølging for å avdekke avvikende eller endret adferd fra kunder, herunder analysere kundens bruk av foretakets produkter og tjenester. Avvik fra forventet kundeadferd kan være en indikator på hvitvasking og terrorfinansiering og utløse undersøkelses- og rapporteringsplikt.
- Foretaket skal undersøke og rapportere mistenkelige forhold til Økokrim, jf. § 26.
- Foretaket skal oppbevare dokumentasjon og registrerte opplysninger, samt påse at dokumentasjon slettes etter at oppbevaringsplikten er omme, jf. § 30.
- Foretaket skal ha kontroll på bruken av tredjepartstjenester og utkontrakterte forpliktelser.

Se Rundskriv 8/2019 Veileder til hvitvaskingsloven for nærmere detaljer. I modulen er det lagt opp til en begrenset vurdering av risiko for hvitvasking og terrorfinansiering. Ved behov for en grundigere gjennomgang, eksempelvis på grunnlag av signaler, funn fra tilsyn eller fra andre kilder, skal seksjon Antihvitvasking og betalingsforetak varsles, som så vurderer behov for tiltak, herunder om det er behov for spesifikke hvitvaskingstilsyn hvor det anvendes egne moduler.

4.4.6. Bærekraftsrisiko, herunder klimarisiko

Bærekraftsrisiko[10] materialiserer seg gjennom de tradisjonelle kategoriene av finansielle - og ikke-finansielle risikoer, inklusiv operasjonell risiko. Klimarisiko er en undergruppe av bærekraftsrisiko.

Nedenfor følger aktuelle momenter:

- Foretaket må vurdere risikoen for at ESG-faktorer, som eksempelvis klimaforhold (f.eks. økt nedbør, flere flommer, hyppigere ras og stigende havnivå) på kort eller lengre sikt, medfører operasjonelle tap som følge av skade på foretakets fysiske eiendeler eller driftsavbrudd i virksomheten. Foretaket må også vurdere risikoen for avbrudd i leveransene fra utkontrakterte tjenesteleverandører og andre underleverandører.
- Foretakets atferd og forretningspraksis kan påvirkes av bærekraftsrisikoen. Konsekvenser av politiske beslutninger, den teknologiske utviklingen og endrede preferanser kan påvirke foretakets atferdsrisiko, juridisk risiko og etterlevelsesrisiko og påføre foretaket operasjonelle tap. Eksempelvis:

[10] ESG Risks: Environmental, Social and Governance Risks.

  - Endret regelverk og endrede forbrukerpreferanser kan eksempelvis medføre økt juridisk risiko og erstatningskrav hvis foretaket finansierer kontroversielle prosjekter og kunder.
  - Manglende etterlevelse av regelverket og standarder for bærekraft øker foretakets regulatoriske risiko. Foretaket må påse at det har tilstrekkelig kunnskap og forståelse av regelverk og standarder, samt å innhente tilfredsstillende data for å klassifisere/merke kundene og deres aktiviteter korrekt.
  - Ved feilaktig merking av bærekraft på foretakets produkter (utlån til kunder og egne utstedte papirer) kan foretaket få erstatningskrav (eksempelvis risiko for grønnvasking).
- Den sosiale dimensjonen i bærekraftsrisiko (S-en i ESG) bør også vurderes. Herunder om foretaket har identifisert og vurdert alvorlige brudd på menneskerettigheter, arbeidstaker-rettigheter, samt anstendige levekår både i egen virksomhet og hos underleverandører. Både skade og driftsavbrudd, hendelser som skyldes atferdsrisiko eller juridisk risiko samt manglende etterlevelse av regelverk, kan i tillegg til økt operasjonell risiko og operasjonelle tap, også skade foretakets omdømme.

5. OVERVÅKING, RAPPORTERING OG OFFENTLIGGJØRING AV INFORMASJON

I dette kapitlet kartlegges og vurderes om foretaket har relevante systemer for å overvåke, rapportere og følge opp operasjonell risiko, jf. CRR/CRD IV-forskriften § 36. Det skal kartlegges og vurderes hvilke rapporteringslinjer som følges, hvilke nivåer i organisasjonen som mottar ulik form for rapportering og om innholdet i rapportene er relevant og tilstrekkelig.

Det er viktig å kartlegge og evaluere de konkrete styringsrapportene som omhandler operasjonell risiko som produseres i foretaket og relevansen av innholdet i rapportene. Foruten selve rapportene vil tilhørende notater med analyser vurderes for å kartlegge hvilke vurderinger, konklusjoner og vedtak som fattes på bakgrunn av innholdet i rapportene.

5.1. Overvåking av operasjonell risiko

Formålet med dette punktet er å vurdere om foretaket har relevante systemer og prosesser for å overvåke operasjonell risiko, herunder bruk av stresstester.

Nedenfor følger aktuelle momenter:

- Foretaket bør ha enhetlige rutiner og prosedyrer som sikrer jevnlig overvåking av indikatorer for operasjonell risiko og vesentlige tapseksponeringer i hele virksomheten, jf. Baselkomiteens prinsipp 8.
- Foretaket bør ha rutiner og prosedyrer som sikrer jevnlig overvåking av etterlevelse av lov- og forskriftskrav samt interne retningslinjer og rutiner. Ved gjentatte brudd på regelverket må det vurderes om dette skyldes manglende respekt for regelverket og/eller at rutinene for overvåkningen ikke er tilfredsstillende.
- Foretaket bør benytte stresstester/sensitivitetsanalyser i overvåkingen og som underlag for framoverskuende vurderinger og strategiske beslutninger som vedrører operasjonell risiko.
  - Foretaket bør ta utgangspunkt i resultateffekten av operasjonelle hendelser, inkludert atferdsrelaterte hendelser. Foretaket bør videre vurdere hvilke effekter operasjonelle hendelser deretter kan få for omdømme eller andre risikoområder.
  - Stresstesting av operasjonell risiko bør være integrert i foretakets stresstest-rammeverk.
- Se EBAs veiledning om foretaks stresstesting EBA/GL/2018/04 for nærmere detaljer om stresstesting av operasjonell risiko.

5.2. Rapportering og oppfølging

Formålet med dette punktet er å vurdere om foretakets systemer og rutiner for håndtering og rapportering av risikodata, både internt og eksternt, er tilfredsstillende.

Nedenfor følger aktuelle momenter:

- Foretaket bør ha rapportering og oppfølging på de strategiske måltallene og rammene som er fastsatt i foretakets strategi/policy for operasjonell risiko.
- Hendelser og tap bør rapporteres jevnlig til ledelse og styret, både for siste periode og utvikling over tid, og spesielt alvorlige hendelser med rotårsak bør omtales særskilt.
- Banker som benytter sjablongmetoden må ha en rapporteringsstruktur til styret som sikrer at alle relevante funksjoner i banken gis nødvendig informasjon om operasjonell risiko, jf. CRR/CRD IV-forskriften § 2, jf. CRR artikkel 320 (c).
- Mottaker av rapporter bør være det organisatoriske nivå som har fastsatt strategi, policy, mål og rammer.
- Foretaket bør dokumentere hvilke rapporter som produseres, hvor ofte de produseres, hvem som er ansvarlig for innhold i rapportene, hvem som mottar hvilke rapporter og hvorledes informasjonen brukes og følges opp.
- Foretaket bør ha etablert rutiner for kvalitetssikring av rapporteringsdataene og systemene for rapportering, både for interne rapporter og for rapportering til myndighetene. Det bør foretas rimelighetskontroller og stikkprøver av dataene. Rapportenes form, innhold og frekvens bør revurderes jevnlig.

5.3. Internkontroll av operasjonell risiko

Formålet med dette avsnittet er å kartlegge og vurdere hvordan foretaket gjennom sitt system for internkontroll har avdekket eventuelle svakheter innenfor operasjonell risiko som krever iverksettelse av tiltak. Prinsipper for internkontrollen, hvilke prosesser som er etablert for å gjennomføre internkontrollen, samt kvaliteten på disse er tema som ivaretas av Finanstilsynets Modul for evaluering av intern virksomhetsstyring.

Nedenfor følger aktuelle momenter:

- Styret er ansvarlig for at det utvikles og vedlikeholdes robuste systemer for internkontrollen med hensiktsmessige interne kontroller som dekker operasjonelle risikoforhold i hele virksomheten, jf. Baselkomiteens prinsipp 9.
- Lederbekreftelsene bør være konkrete på hvilke operasjonelle risikofaktorer som er kontrollert og vurdert, hvilke kontrollhandlinger som er foretatt, resultatene av disse og utviklingen over tid, samt risikoreduserende tiltak som er iverksatt, jf. CRR/CRD IV-forskriften § 37.

5.4. Offentliggjøring av informasjon om operasjonell risiko

Formålet med dette punktet er å vurdere foretakets rutiner for kvalitetssikring av og offentliggjøring av informasjon om operasjonell risiko.

Nedenfor følger aktuelle momenter:

- Foretaket bør offentliggjøre tilstrekkelig med informasjon som gjør det mulig for interessenter å vurdere foretakets tilnærming til operasjonell risikostyring, jf. Baselkomiteens prinsipp 12.
- Foretaket skal ha interne retningslinjer og rutiner for å oppfylle sin informasjonsplikt innenfor operasjonell risiko (pilar 3), jf. CRR/CRD IV-forskriften § 2, jf. CRR del åtte.

- For operasjonell risiko skal foretaket minimum offentliggjøre informasjon om strategi og prosesser, organisering av risikostyringsfunksjonen, risikorapporterings- og målesystemet samt retningslinjer og rutiner for overvåking og bruk av sikkerhetsstillelse, jf. CRR/CRD IV-forskriften § 2, jf. CRR artikkel 435.

6. IKT-SYSTEMER, DRIFTS- OG FORRETNINGSMESSIG BEREDSKAP, KONTINUITET OG GJENOPPRETTING

Formålet med dette kapittelet er å vurdere om foretaket har etablert ordninger som synes hensiktsmessige for å styre, overvåke og forbedre effektivitet og pålitelighet i foretakets informasjons- og kommunikasjonssystemer og i beredskaps- og kriseplaner. Det for å sikre at driften kan videreføres og tap begrenses ved alle typer alvorlige driftsforstyrrelser og lignende. Vurderinger fra gjennomgangen av foretakets plan for å gjenopprette sin finansielle stilling når denne er betydelig svekket, vil også hensyntas i vurderingen av foretakets interne styring. For krav og vurderinger som vedrører foretakenes gjenopprettingsplaner, vises det til Finanstilsynets rundskriv 10/2019 med vedlegg.

Etter Finanstilsynets vurdering må alle foretak vurdere hva som kan skje, hvordan hendelser kan påvirke driften av foretaket, både driftsmessig og finansielt, og hvordan foretaket skal møte slike utfordringer. Disse elementene bør inkluderes i et helhetlig planverk for beredskap, kontinuitet og gjenoppretting.

I norsk regelverk stilles det eksplisitte krav til beredskapsplaner og lignende på følgende områder:

- *IKT-systemer:* Driftsløsningene i norske banker og finansieringsselskap er basert på informasjons- og kommunikasjonsteknologi. Foretakene bør implementere et robust rammeverk for styring og kontroll av IKT-risiko i samsvar med foretakets rammeverk for operasjonell risikostyring, jf. Baselkomiteens prinsipp 10. En detaljert vurdering av foretakets IKT-løsninger og kriseplaner knyttet til disse, jf. IKT-forskriften §§ 8 og 11, gjøres ved spesielle IT-tilsyn.
- *Likviditet/finansiering:* En detaljert vurdering av foretakets beredskapsplan for likviditetskriser, jf. CRR/CRD IV-forskriften § 14, gjøres ved likviditetstilsyn og det henvises til Modul for likviditetsrisiko – Evaluering av styring og kontroll[11].
- *Soliditet:* En kapitalplan for å kunne vurdere hvordan foretakets kapitalbehov på kort og lengre sikt kan tilfredsstilles, jf. finansforetaksloven § 13-6 (3). *Gjenopprettingsplaner:* Gjenopprettingsplanen har som formål å stabilisere og gjenopprette foretakets *finansielle* stilling i en alvorlig stressituasjon. Styret skal påse at foretaket har tilgjengelig effektive og relevante tiltak som kan gjennomføres i en stressituasjon, uten at det medfører vesentlig negative konsekvenser for kunder, andre finansforetak eller økonomien for øvrig. Krav til gjenopprettingsplaner fremgår av finansforetaksloven § 20-5, samt forskrift om utfyllende regler til finansforetaksforskriften kapittel 20 del 4. Finanstilsynet vurderer foretakenes gjenopprettingsplaner jevnlig, jf. Finansforetaksloven § 20-5 annet til fjerde ledd.

Nedenfor følger aktuelle momenter:

- Foretakets beredskapsplaner, både på overordnet nivå og for vesentlige virksomhetsområder, bør være dekkende for hele virksomheten inkludert utkontraktert virksomhet, sees i sammenheng og være basert på en oppdatert risikovurdering. Finanstilsynet forventer at

11 www.finanstilsynet.no/Global/Bank%20og%20Finans/Banker/Tilsyn%20og%20overv%c3%a5king/Tilsyn/Risikobasert%20tilsyn/Modul%20for%20likviditetsrisiko.pdf

foretakets beredskapsplaner godkjennes av styret. Foretakets gjenopprettingsplan og beredskapsplan for likviditet skal styregodkjennes.

- Beredskapsplanene skal oppdateres jevnlig og i lys av endrede rammebetingelser, utviklingen innenfor strategiske satsningsområder, mv.
- Beredskapsplanene må være tilgjengelige ved alle situasjoner. Alle medarbeidere i foretaket bør være inkludert i en beredskaps-/kriseplan og alle medarbeidere bør være kjent med aktuelle planer og sitt ansvar i en krisesituasjon.
- Foretaket bør gjennomføre opplæring regelmessig og beredskapsplanene bør testes jevnlig.
- Foretaket må sikre at IKT-systemene er effektive og pålitelige og at foretaket vil være i stand til å fremskaffe presise og fullstendige data fra sine fagsystemer slik at samlet risiko kan beregnes og rapporteres tidsaktuelt for både enkelte forretningsenheter og for hele foretaket, i så vel normale situasjoner som i situasjoner med stress.
- Planene bør omfatte forskjellige type scenarioer som kan påvirke foretakets driftssituasjon og finansielle situasjon vesentlig. Det kan være fysiske hendelser som eksempelvis brann, ran og flom, hendelser som medfører tap av omdømme og tillit i markedet som får finansielle konsekvenser, og hendelser knyttet til IKT-systemene som hacking, trojanerangrep og DDoS-angrep.
- Foretaket skal ha etablert retningslinjer, planer og hensiktsmessige verktøy, metoder og prosesser for å være best mulig forberedt på å håndtere ulike alvorlige forretnings- og driftsforstyrrelser som kan inntreffe, herunder planer for overgang til reserveløsninger på IKT-området, for utkontraktert virksomhet samt for gjenoppretting av kritiske funksjoner.
- Planene bør bl.a. inkludere retningslinjer og prosedyrer med tiltak, oversikt over roller og ansvarsforhold (beredskapsorganisasjon), og krav til intern og ekstern informasjon og kommunikasjon.
- Foretaket bør være i stand til raskt å kunne tilpasse seg nye behov for risikorapportering, herunder ad hoc forespørsler, herunder fra myndighetshold, som følge av endrede interne eller eksterne behov.
- Kriseplaner for foretakets IKT-systemer må tilfredsstille IKT-forskriftens krav i § 11.
- Beredskapsplaner for likviditetskriser må tilfredsstille CRR/CRD IV-forskriftens krav.
- Gjenopprettingsplaner skal tilfredsstille kravene som stilles i finansforetaksloven § 20-5, forskrift om utfyllende regler til finansforetaksforskriften kapittel 20 del 4, samt rundskriv 10/2019.

7. EKSPONERING

7.1. Virksomhetens iboende operasjonelle risiko

Operasjonell risiko henger tett sammen med foretakets forretningsmodell og virksomhet. Ved vurdering av operasjonell risiko bør foretakets iboende risiko først kartlegges og vurderes, det vil si den risiko som ligger naturlig i virksomheten, på bakgrunn av forretningsmodell, drift og integritet hos ledelsen og nøkkelpersoner. Følgende bør minimum vurderes:

- virksomhetens størrelse, omfang og kompleksitet,
- hvilke produkter og tjenester som selges,
- hvilke distribusjonskanaler som brukes,
- hvilken infrastruktur og tredjeparter foretaket er avhengig av i produksjon og distribusjon osv.

Enkelte faktorer kan medføre forhøyet operasjonell risiko, og spesielt vesentlige *endringer* bør vurderes særskilt. Vesentlige endringer av virksomheten er eksempelvis fusjoner, omorganiseringer, konverteringer av kjernesystemer mv., se pkt. 2.1. Foretakets bruk av underleverandører og samarbeidspartnere, samt styring og kontroll med utkontraktert virksomhet, nye og endrede produkter, aktiviteter, prosesser og systemer, er videre andre momenter som kan påvirke foretakets operasjonelle risiko. Videre kan nytt regelverk endre foretakets operasjonelle risiko, eksempelvis som følge av økt etterlevelsesrisiko eller risiko for at foretaket må bære mer tap.

Etter kartlegging og vurdering av foretakets iboende operasjonelle risiko vurderes foretakets styring og kontroll av risikoen, herunder rammeverk, kontrolltiltak og iverksatte risikoreduserende tiltak, for å avklare foretakets restrisiko. Det er det samlede restrisikonivået for operasjonell risiko som ligger til grunn for tilsynsvirksomheten, herunder vurdering av foretakenes samlede risikoprofil og kapitalbehov (SREP).

7.2. Måling av operasjonell risiko

Måling av faktisk operasjonelt risikonivå kan være utfordrende da det eksempelvis ikke finnes etablerte, ensartede kvantitative indikatorer – slik som er etablert for andre risikoområder – og siden tilgangen til ekstern data for sammenlignende analyser er begrenset. Måling og modellering av økonomisk tap som følge av operasjonell risiko er videre problematisk spesielt for sjeldne hendelser med store konsekvenser. Det finnes imidlertid alternative modelleringsverktøy for analyse av operasjonell risiko, eksempelvis bayesianske nettverk[12] som har tilslutning i enkelte miljøer. I vurderingen må foretakene også her se hen til kompleksiteten og omfanget av virksomheten.

Selv om det kan være utfordrende å gradere risikoeksponeringen betyr det ikke at det er lite hensiktsmessig å gjøre en vurdering av risikonivået. En slik vurdering kan gi verdifull informasjon i seg selv hva gjelder utvikling/trend, hvorfor risikoeksponeringen er som den er, hvilke forhold/komponenter som er viktige, hvordan forskjellige tiltak påvirker risikobildet mv.

Eksempler på faktorer som kan gi en indikasjon på nivået på operasjonell risiko i foretaket kan være:

- Antall tapshendelser, samlet og fordelt på forskjellige tapskategorier.
- Hvilken type tapshendelser som har oppstått og innenfor hvilke virksomhetsområder.
- Tap som skyldes operasjonelle hendelser, både faktisk tap og potensielt tap, samlet, samt fordelt på underkategorier.
- Omfanget av og merknader/påpekninger fra uavhengige kontrollfunksjoner og valgt revisor.

Under følger eksempler på tapshendelser, jf. Kap. 4 over, fordelt på tapshendelseskategoriene med indikatorer. Listen over eksempler og indikatorer er ikke uttømmende, og enkelte type hendelser kan

[12] Et bayesiansk nettverk er en metode for å estimere og oppdatere sannsynligheter for enkelthendelser ved hjelp av antagelser om sammenhenger mellom ulike hendelser.

kategoriseres i flere av kategoriene mens enkelte indikatorer kan gi indikasjoner på flere typer hendelser.

Type hendelse	Definisjon	Eksempler	Indikatorer
Internt bedrageri	Tap som følge av handlinger med sikte på uberettiget å tilegne seg midler eller omgå lovgivning eller virksomhetens mål unntatt hendelser knyttet til forskjellsbehandling.	- Korrupsjon - Underslag - Innsidehandling - "Rogue trading"	- Oversikt over saker meldt til politi/forsikringsselskap - Fullmaktsbrudd - Feriestatistikk (manglende ferieavvikling) - Oversikt over arbeidstider (avvikende arbeidstid, helge-/kveldsjobbing) - Antall varselsaker
Eksternt bedrageri	Tap som følge av handlinger som har til hensikt å bedra, uberettiget tilegne seg midler eller omgå lovgivningen, begått av en tredjepart.	- Svindel, bedrageri, inkl. kortsvindel, ID-tyveri - Dokumentforfalskning - Ran og annen volds-kriminalitet - Trusler mot ansatte - Hvitvasking - Terrorfinansiering - Hacking, phishing, ransomware	- Oversikt over saker meldt til politi/forsikringsselskap - Statistikk over mistenkelige transaksjoner; flaggede saker og meldinger til Økokrim - Statistikk over kortsvindelsaker - Statistikk over forsøk på å forsere brannmurer m.m.
Ansettelses-vilkår og sikkerhet på arbeidsplassen	Tap som følge av hendelser som er i strid med lovgivning, forskrifter og avtaler om arbeidsmiljø, utbetaling av erstatninger som følge av personskade eller andre forhold.	- Yrkesskader - Brudd HMS-regler - Diskriminering - Omorganisering - Nedbemanning	- Sykefravær - Personalstatistikk (turnover, overtid, kjønnsfordeling, fordeling etniske grupper mv.) - Medarbeidertilfredshets-undersøkelser - Varsler-saker - Statistikk behandlingstid/ ubehandlede saker/tapte anrop o.l.
Kunder, produkter og forretnings-praksis	Tap som følge av utilsiktede handlinger eller unnlatelser som medfører manglende oppfyllelse av en forpliktelse overfor bestemte kunder (herunder tillits- og egnethetskrav), eller som følge av produktets art eller utforming.	- Fullmaktsbrudd - Manglende prosesser for godkjennelse av nye produkter - Salg av uautoriserte produkter, produktpakker - Råsalg og salg av høy-risikoprodukter til feil kunder - Uautorisert innsyn i og misbruk av konfidensielle kundedata - Manipulering av referanse-renter o.l. - Manglende etterlevelse av hvitvaskingsregelverket mv.	- Statistikk kundeklager, inkl. klager behandlet i nemd - Statistikk over fullmaktsbrudd - Salgsstatistikk og porteføljе-analyser, fordelt på forskjellige distribusjonskanaler - Kundetilfredshetsundersøkelser - Rapporter/resultater bonus/ incentivordning
Skade på fysiske eiendeler	Tap som følge av skade på, eller tap av, fysiske eiendeler i naturkatastrofer eller andre begivenheter.	- Skade som skyldes brann, flom/oversvømmelser, snø - Ran og vandalisering - Terrorhandlinger (11. september/22. juli)	- Meldte forsikringssaker
Avbrudd i drift eller systemer	Tap som følge av driftsavbrudd eller systemfeil.	- IT-hendelser; både programvare og maskinvare - Strømbrudd/driftsstans - Brudd i telekommunikasjon	- Registrert nedetid på systemer - Regularitet i strømforsyning, telekommunikasjon og nettilgang - Statistikk over forsøk på å forsere brannmurer m.m. - Statistikk over rapporterte IT-hendelser til Finanstilsynet
Oppgjør, levering og annen transaksjons-behandling	Tap som følge av utilstrekkelig eller sviktende transaksjonsbehandling eller systemer for transaksjons-	- Feil i registrert data (tastefeil) og i systemer - Feil i intern og ekstern rapportering	- Transaksjonsstatistikk og feillogger - Rapportert fra internkontroll, compliance, revisor, tilsyn - Tilgangsoversikter

	behandling med handels-motparter og leverandører.	- Misforståelser og kommunikasjonssvikt - Feil systemtilganger - Feil i sikkerheters-dokumentasjon og manglende juridisk dokumentasjon - Tvister med andre motparter (ikke kunder) og leverandører - Tap relatert til utkontrakteringsavtaler - Tap relatert til transaksjons-monitorering	

En god analyse av foretakets operasjonelle risikonivå med utgangspunkt i analyse av registrerte tapshendelser forutsetter at systemet vurderes å være dekkende for hele virksomheten og at alle hendelser registreres på alle risikoområdene. Underrapportering av hendelser er en kjent problemstilling.

Videre er utviklingen over tid viktig. Det må vurderes om endringen skyldes endringer i rapporteringssystem og etterlevelser av interne rapporterings-retningslinjer eller om utviklingen skyldes endringer i det reelle, underliggende risikonivået. Utviklingen i hendelser og tap bør videre sees i sammenheng med andre faktorer som kan medføre økt operasjonell risiko over tid som endringer i strategi og forretningsmodell, organisatoriske endringer, systemkonverteringer og endringer i produksjonsprosesser mv.