



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Temarapport

Terrorfinansiering

Håndtering av risiko for terrorfinansiering i et utvalg banker
24. juni 2025



1. Innledning	3
1.1. Bakgrunn og formål.....	3
1.2. Oppsummering	3
2. Finanstilsynets observasjoner av bankenes håndtering av terrorfinansieringsrisiko	3
2.1. Risikovurdering	4
2.1.1. Rettslig grunnlag.....	4
2.1.2. Eksempler på god praksis	4
2.2. Risikoklassifisering.....	6
2.2.1. Rettslig grunnlag.....	6
2.2.2. Eksempler på god praksis	6
2.3. Regler i det elektroniske overvåkingssystemet.....	8
2.3.1. Rettslig grunnlag.....	8
2.3.2. Eksempler på god praksis	8

1. Innledning

1.1. Bakgrunn og formål

Etter lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven) skal rapporteringspliktige foretak forebygge og avdekke terrorfinansiering. For å sette økt fokus på forebygging og bekjempelse av terrorfinansiering startet Finanstilsynet høsten 2024 en kartlegging med dette som tema, blant annet for å gi veiledning til rapporteringspliktige ved å beskrive eksempler på god praksis.

Kartleggingen er basert på dokumentasjon fra syv norske banker og tre filialer av utenlandske banker (heretter samlet omtalt som "bankene").¹ Det er stor variasjon i bankenes størrelse, geografiske tilhørighet, produkter og kundegrupper.

Kartleggingen er avgrenset til å se på bankenes håndtering av risiko for terrorfinansiering i:

- den virksomhetsinnrettede risikovurderingen, jf. hvitvaskingsloven § 7,
- metoden for risikoklassifisering, jf. § 9,
- reglene i det elektroniske overvåkingssystemet, jf. § 38.

1.2. Oppsummering

Etter Finanstilsynets oppfatning innebærer god praksis blant annet at banken viser forståelse for de risikoelementene hvor risiko for terrorfinansiering skiller seg fra risiko for hvitvasking, at banken gjør konkrete vurderinger av hvordan foretaket er eksponert for risiko for terrorfinansiering, og er bevisst hvilke egenskaper ved kunder og transaksjoner som kan indikere risiko for eller mistanke om terrorfinansiering.

2. Finanstilsynets observasjoner av bankenes håndtering av terrorfinansieringsrisiko

Bankenes innsats for å forebygge og avdekke terrorfinansiering skal være risikobasert, slik det fremgår av hvitvaskingsloven § 6. Dette innebærer at risikoen for terrorfinansiering må hensyntas gjennomgående på lik linje med risiko for hvitvasking. Risiko for terrorfinansiering har mange likheter med, men også viktige forskjeller fra, risiko for hvitvasking. Derfor er det også enkelte forskjeller mellom indikatorer på terrorfinansiering og indikatorer på hvitvasking. Den viktigste forskjellen er fokuset på transaksjonens destinasjon fremfor midlenes opprinnelse.² Midlene kan stamme fra kriminalitet, men de kan også ha et legitimt opphav. En annen viktig forskjell er at transaksjonens størrelse har mindre betydning som indikator for terrorfinansiering, da terrorfinansiering ofte skjer ved bruk av små beløp.³ Videre kan ulike egenskaper ved kundemassen medføre forskjellig eksponering for henholdsvis risiko for hvitvasking og terrorfinansiering, som omtalt nedenfor.

Den virksomhetsinnrettede risikovurderingen danner grunnlaget for effektive tiltak for å forebygge og avdekke terrorfinansiering. En konkret vurdering av terrorfinansieringsrisiko er

¹ Sparebank 1 SMN, Sparebank 1 Sør-Norge, Nordea, Bank Norwegian, TF Bank, Eika Kredittbank, Skue Sparebank, Skagerrak Sparebank, Haugesund Sparebank og Sparebank 68 grader nord

² Økokrim Trusselvurdering 2024, s. 41

³ SNRA (2022) Commission staff working document, s. 39

en forutsetning for at risikofaktorer også blir fanget opp i risikoklassifiseringen og reglene i det elektroniske overvåkingssystemet.

2.1. Risikovurdering

2.1.1. Rettslig grunnlag

Rapporteringspliktige skal identifisere og vurdere risikoen for hvitvasking og terrorfinansiering knyttet til sin virksomhet, jf. hvitvaskingsloven § 7 første ledd.

Slik det fremgår av rundskriv 4/2022, skal terrorfinansieringsrisikoen alltid vurderes.

Rapporteringspliktige forventes å benytte eksterne kilder i forbindelse med kartleggingen og vurderingen, herunder "Nasjonal risikovurdering om hvitvasking og terrorfinansiering" fra politidirektoratet og Politiets sikkerhetstjeneste (PST) samt Finanstilsynets risikovurdering. Rapporteringspliktige skal også benytte kunnskap og erfaring fra egen virksomhet, jf. rundskriv 4/2022 punkt 2.2.4. Som et minimum må rapporteringspliktige i risikovurderingen ta i betraktning egen virksomhet (herunder virksomhetens art og omfang), produkter, tjenester og kundeforhold, type kunder, kundegrupper og geografiske forhold.

Risikovurderingen må oppdateres jevnlig for å kunne være et praktisk verktøy for rapporteringspliktige.

2.1.2. Eksempler på god praksis

Vurderinger av risiko for terrorfinansiering

God risikoforståelse gir banken mulighet til å identifisere og håndtere den konkrete terrorfinansieringsrisikoen banken er eksponert for.

Under kartleggingen fant Finanstilsynet eksempler på risikovurderinger som inneholder adskilte vurderinger av bankens eksponering mot henholdsvis risiko for hvitvasking og risiko for terrorfinansiering innenfor ulike risikoområder som produkt risiko, kunderisiko og geografisk risiko og innenfor bankens ulike forretningsområder.

Eksempelvis anså en av bankene iboende kunderisiko for terrorfinansiering å være høy i et forretningsområde, som følge av risikofaktorer som blant annet høy kontantandel og bruk av pengeoverføringstjenester. Banken tok med dette konkret stilling til dens iboende risiko for terrorfinansiering basert på en vurdering av risikoen innenfor de ulike risikoområdene og forretningsområdene. Videre tok banken stilling til restrisiko basert på en vurdering av kvaliteten på egne kontroller for å avdekke identifisert terrorfinansieringsrisiko.

Finanstilsynet fant også eksempler på eksplisitte vurderinger av risiko for henholdsvis hvitvasking og risiko for terrorfinansiering for hver enkelt risikofaktor innenfor de ulike risikoområdene, eksempelvis konkrete vurderinger av risiko for terrorfinansiering knyttet til hvert enkelt produkt, f.eks. ulike typer lån. Risikobeskrivelsen var i flere tilfeller likelydende for hvitvasking og terrorfinansiering, noe som er naturlig gitt risikoenes natur. Der terrorfinansieringsrisikoen var ansett å være forskjellig fra hvitvaskingsrisikoen, kom dette tydelig frem. Med denne metodikken tok bankene stilling til risikonivå for hvitvaskingsrisiko og terrorfinansieringsrisiko hver for seg, og på et detaljert nivå, selv om risikoen i mange tilfeller var ansett å være lik.

Enkelte banker hadde også dokumentasjon tilknyttet risikovurderingen som inneholdt konkrete eksempler på hvordan terrorfinansiering kan foregå, og tilhørende indikatorer for dette. Eksempelvis var det beskrevet hvordan frivillige organisasjoner kan misbrukes av terrororganisasjoner, og hvordan bruk av folkefinansiering kan representere en risiko for terrorfinansiering. Blant indikatorer som var nevnt, var høyt transaksjonsvolum med små

transaksjoner og donasjoner til veldedige organisasjoner uten kjent eller tydelig relasjon mellom avsender og det veldedige formålet.

Noen banker hadde en beskrivelse og vurdering av fremvoksende risikoer knyttet til terrorfinansiering som en integrert del av risikovurderingen. Dette var typisk utviklingstrekk eller hendelser som banken mente kunne endre trusselbildet, og der banken så behov for å følge med på hvordan dette påvirket risiko for terrorfinansiering. Et eksempel var eskaleringen av konflikten i Midtøsten, og radikalisering knyttet til dette. Et annet eksempel var økt bruk av kryptoeiendeler og betalinger gjennom sosiale plattformer, og potensialet dette har for å bli benyttet til terrorfinansiering.

Vurderinger av egenskaper ved kundemassen og bankens produkttilbud

Ved å identifisere ulike egenskaper ved kundemassen og bankens produkter som kan gjøre banken eksponert for risiko for terrorfinansiering, kan banken identifisere og håndtere den konkrete terrorfinansieringsrisikoen virksomheten er eksponert for.

Flere av bankene la i sine risikovurderinger særlig vekt på kundemassens tilknytning til høyrisikoland⁴ og enkelte andre land hvor tilknytningen kan anses å innebære høyere risiko for terror og terrorfinansiering. Dette gjaldt både kundens fødested, statsborgerskap etc. og hvilke land kundene hadde transaksjoner til eller fra.

I tillegg var det flere av bankene som vektla andre relevante risikofaktorer for terrorfinansiering knyttet til kunden, slik som hvilke produkter kunden benyttet seg av, eksempelvis kredittkort, eller om kunden var involvert i kryptohandel eller benyttet betalingsformidlere. Det var også noen av bankene som vektla bransjetilhørighet eller selskapsform, eksempelvis lag og foreninger eller ideelle organisasjoner.

Vurderinger av eksponering mot geografisk risiko for terrorfinansiering

Forholdene som gjør land aktuelle for transaksjoner som skal finansiere terror kan være forskjellige fra forhold som gjør land attraktive destinasjonsland for hvitvasking. Vurderinger av geografisk risiko for terrorfinansiering tilknyttet det enkelte land som banken har eksponering mot vil derfor være nødvendig for å kjenne denne risikoen.

Utover land som er listeført av EU og FATF, la flere banker også til grunn at land som er høyt rangert på Global Terrorism Index (GTI)⁵, utgjør høy risiko for terrorfinansiering. Enkelte banker gjorde også vurderinger av risiko for terrorfinansiering knyttet til andre land enn de som er rangert høyt på GTI, herunder land innenfor EØS.

Når det gjelder geografisk risiko for terrorfinansiering innenfor EØS, viser Finanstilsynet til at blant annet Etterretningstjenestens trusselvurdering⁶, og Europols TE-SAT⁷ beskriver eksempler på terrorfinansiering og terror i EU.

Forskjeller i risiko for terrorfinansiering knyttet til ulike ekstreme ideologier

Ulike typer ideologier kan innebære ulike indikatorer på terrorfinansiering og ulike risikoprofiler. Det kan eksempelvis være betydelige forskjeller mellom høyreekstreme og ekstreme islamister når det gjelder modus og indikatorer på finansiering av terror, blant annet ved at det kan brukes ulike plattformer for innsamling av midler eller ved at transaksjonene i kundeforholdet har ulike geografiske destinasjoner. En vurdering av bankens risikoeksponering som innbefatter ulike ideologier danner grunnlag for mer nyanserte

⁴ Slik de er definert av EU og FATF

⁵ Institute for Economics & Peace, Global Terrorism Index

⁶ Etterretningstjenesten, «Fokus 2024»

⁷ European Union Terrorism Situation and Trend Report (TE-SAT) 2024

indikatorer for terrorfinansiering, og gir dermed banken bedre forutsetninger for å forebygge og avdekke terrorfinansiering.

Enkelte av bankenes risikovurderinger ga uttrykk for en slik nyansert forståelse av risiko for terrorfinansiering. I disse ble ulike aktuelle ekstreme ideologier beskrevet og bankens eksponering mot disse vurdert, eksempelvis bankens eksponering gjennom kundemassen, mot høyreekstreme, venstreekstreme og ekstreme islamistiske miljøer.

Bruk av kilder

God kildebruk er viktig for å forstå og vurdere risiko for terrorfinansiering, og bruk av kilder utover de obligatoriske kildene som nevnes i rundskriv 4/2022, gir et bredere bilde av risikoen. Enkelte banker benyttet eksempelvis nasjonale risikovurderinger i de landene banken har eksponering mot. Noen kildelister inneholdt informasjon om hvorvidt den enkelte kilde belyste risiko for hvitvasking eller terrorfinansiering eller begge.

Etter Finanstilsynet oppfatning er også Etterretningstjenestens trusselvurdering, Europols TE-SAT eksempler på relevante kilder for å belyse risiko for terrorfinansiering.

Endring i risikovurdering som følge av hendelser

Trusselbildet er dynamisk, og eksterne hendelser kan få konsekvenser for hvilken eksponering banken har mot terrorfinansiering. Enkelte av bankene hadde i sin metodikk for risikovurdering adressert at det kan oppstå situasjoner hvor det er nødvendig å vurdere endring av terrorfinansieringsrisikoen utover den faste årlige oppdateringen av risikovurderingen. Behov for endringer kunne eksempelvis utløses av hendelser og konfliktsituasjoner internasjonalt eller av at nye trusler materialiserer seg.

2.2. Risikoklassifisering

2.2.1. Rettslig grunnlag

For å gjennomføre korrekte kundetiltak og løpende oppfølging av den enkelte kunde, må alle kunder risikoklassifiseres, jf. hvitvaskingsloven § 9 første ledd. Risikoklassifiseringen skal bygge på generelle vurderinger fra virksomhetens risikovurdering, i tillegg til konkrete forhold ved den enkelte kunde. Blant annet skal risikoen vurderes ut fra kundeforholdets formål og tilsiktede art, mengden kundemidler som skal inngå i kundeforholdet, transaksjoners størrelse, og regelmessigheten og varigheten på kundeforholdet.

Rapporteringspliktige kan anvende standardiserte risikoprofiler for kundene, jf. hvitvaskingsloven § 9 andre ledd. Risikoprofilene må tilpasses de konkrete risikoene i virksomheten. Rapporteringspliktige må kunne dokumentere hvorfor en kunde er klassifisert i en bestemt risikokategori. Rapporteringspliktige må påse at kundenes risikoprofiler er oppdaterte, slik at kundene endrer risikokategori dersom endringer tilsier det.

2.2.2. Eksempler på god praksis

Sammenheng mellom risikovurderingen og risikoklassifiseringen

En metodikk for risikoklassifisering som bygger på bankens forståelse for risiko for terrorfinansiering, som uttrykt gjennom risikovurderingen, og konkrete forhold ved den enkelte kunde, bidrar til at kundetiltak og oppfølging av kundeforholdet baseres på en forståelse av hvilken risiko for terrorfinansiering kundeforholdet representerer. Det samme vil en risikoklassifiseringsmetodikk som gjenspeiler en nyansert forståelse av risiko for terrorfinansiering, for eksempel med hensyn til ulike ideologier.

Finanstilsynet fant eksempler på at banker hadde stor grad av samsvar mellom risiko for terrorfinansiering som var beskrevet i risikovurderingen, og risikofaktorer som ble vektlagt i forbindelse med risikoklassifisering av kunden. Dette gjaldt særlig geografiske forhold, men også forhold knyttet til forventet og faktisk bruk av bankens ulike produkter, kundens befatning med kryptoeiendeler og kontanter, og for bedriftskunder også nærmere angitte høyrisikobransjer og selskapsformer.

Finanstilsynet fant at banker som gjorde konkrete vurderinger av risiko for terrorfinansiering i risikovurderingen, gjennomgående også ga uttrykk for et bevisst forhold til hvilke risikofaktorer som medførte forhøyet risiko for terrorfinansiering i kundeforhold.

Faktorer i risikoklassifiseringsmetodikken for å vurdere risiko for terrorfinansiering knyttet til kundeforholdet

For å kjenne bankens eksponering mot risiko for terrorfinansiering gjennom kundemassen kreves bevissthet om hvilke faktorer som kan indikere risiko for terrorfinansiering i tillegg til risiko for hvitvasking. Gjennom å inkludere slike faktorer i risikoklassifiseringsmetodikken, kan banken legge til rette for å fange opp risiko for terrorfinansiering der denne skiller seg fra risiko for hvitvasking.

Finanstilsynet fant eksempler på at banker var bevisst hvilke risikofaktorer som konkret innebærer forhøyet risiko for terrorfinansiering, eventuelt i tillegg til at de innebærer forhøyet risiko for hvitvasking. Hvilke risikofaktorer banken anså å utgjøre forhøyet risiko for terrorfinansiering sammenfalt naturlig nok i stor grad med faktorene som ble trukket frem ved vurdering av bankens eksponering for risiko gjennom kundemassen, som omtalt over.

Finanstilsynet fant også eksempler på at en kombinasjon av ulike faktorer med høy score gjorde at en kunde ble klassifisert med forhøyet risiko for terrorfinansiering. For eksempel vektla enkelte banker kundenes tilknytning til land med høy risiko for terrorfinansiering i kombinasjon med risiko for terrorfinansiering knyttet til produkter kundene benyttet seg av, og konkluderte med at det var forhøyet risiko for terrorfinansiering i kundeforholdet.

Eksempler på metodikk for å fange opp risiko for terrorfinansiering ved etablering av kundeforhold

For å kartlegge risiko for terrorfinansiering i kundeforhold er det nødvendig med bruk av ulike kilder. Finanstilsynet fant at bankene gjennomgående søkte å fange opp risiko for terrorfinansiering ved å gjennomføre søk mot internasjonale terror- og sanksjonslister. Flere av bankene opplyste også at de gjør søk i åpne kilder på kunder som har fått høy score i risikoklassifiseringssystemet, for blant annet å undersøke om kunden var omtalt i forbindelse med terrormiljøer eller radikalisering. Slike søk kan være god praksis, men Finanstilsynet vil bemerke at dersom det automatiske risikoklassifiseringssystemet ikke inneholder faktorer som knytter seg konkret til risiko for terrorfinansiering, og søk i åpne kilder kun gjennomføres for kunder med høy score, vil enkelte kunder med høy reell risiko for terrorfinansiering ikke bli fanget opp.

Hvordan identifiseres endringer i risiko for terrorfinansiering knyttet til kunden

Risiko for terrorfinansiering påvirkes og kan endre seg raskt som følge av endringer ved kunden, eller som følge av hendelser i verden. Invasjonen av Ukraina og eskalering av konflikten i Midtøsten er eksempler på hendelser som kan medføre endringer i risiko for terrorfinansiering i bankenes kundeforhold.

Flere banker i utvalget fanget opp endringer i risiko for terrorfinansiering som følge av endret kundeatferd, eksempelvis uventede eller hyppige transaksjoner til høyrisikoland eller endringer i bruk av kontanter.

Enkelte banker hentet jevnlig lister fra tredjepartsleverandører over personer og enheter med mulige koblinger til terrorisme eller terrorfinansiering. Listene var utarbeidet på grunnlag av for eksempel spesifikke landslister, negativ medieomtale eller rettsdokumenter og bankens kundelister ble screenet mot disse. Enkelte banker hadde også rutiner for å vurdere hvordan hendelser i verden, eksempelvis geopolitiske endringer eller terrorhendelser, påvirket bankens risikoeksponering, herunder på kundenivå.

Kunnskap om kundeforhold med høy risiko for terrorfinansiering

For at banken skal kunne ta til stilling til hvilken eksponering den har for risiko for terrorfinansiering gjennom kundemassen, er det nyttig å kunne trekke ut tall på hvor stor andel av kundemassen som er vurdert til høy risiko som følge av risiko for terrorfinansiering, og hvilke kundeforhold dette gjelder. Dette er kunnskap om egen virksomhet banken kan bruke i risikovurderingen.

Finanstilsynet ba i forbindelse med kartleggingen om informasjon om hvor stor andel av den enkelte banks kundemasse som var vurdert til høy risiko som følge av risiko for terrorfinansiering. Enkelte banker i utvalget hadde tall på dette.

2.3. Regler i det elektroniske overvåkingssystemet

2.3.1. Rettslig grunnlag

Foretaket plikter etter hvitvaskingsloven § 38 å ha elektroniske systemer for å avdekke forhold som kan indikere hvitvasking og terrorfinansiering. Videre følger det av hvitvaskingsforskriften § 7-3 at den elektroniske overvåkingen skal omfatte alle systemer for transaksjoner til eller fra rapporteringspliktiges kunder. Videre skal reglene i det elektroniske overvåkingssystemet være egnet til å avdekke forhold som kan indikere at midler har tilknytning til hvitvasking og terrorfinansiering, som identifisert i den rapporteringspliktiges risikovurdering.

2.3.2. Eksempler på god praksis

Separate regler ment for å avdekke terrorfinansiering

Ved å gjøre konkrete vurderinger av risiko for terrorfinansiering og omsette disse til scenarier og regler som er egnet til å adressere risikoen, blir bankene i bedre stand til å fange opp indikasjoner som konkret gjelder terrorfinansiering, også der disse skiller seg fra indikasjoner på hvitvasking. Reglene blir videre mer målrettet dersom de innrettes slik at de treffer på ulike stadier av terrorfinansiering, herunder innsamling, overføring og bruk av midler til terrorformål, og knyttes til ulike konkrete modus, eksempelvis innsamling via ulike plattformer, bruk av stråselkap og bruk av kurerer.

Gjennom kartleggingen fant Finanstilsynet eksempler på banker som hadde egne regler i det elektroniske overvåkingssystemet som var ment å avdekke indikasjoner på terrorfinansiering. Disse reglene hadde en innretning som var basert på scenarier beskrevet i bankenes risikovurderinger. Eksempler på dette var regler som fanget opp transaksjoner til eller i land med høy terrorfinansieringsrisiko. Reglene var utarbeidet i tillegg til regler som var ment å avdekke både hvitvasking og terrorfinansiering, og som dermed i mindre grad var rettet spesifikt mot terrorfinansiering.

Finanstilsynet fant generelt at det normalt var de bankene som hadde gjort konkrete og separate vurderinger av terrorfinansieringsrisiko for egen virksomhet, som også hadde regler i transaksjonsovervåkingen som kan anses egnet til å fange opp slik risiko.

Regler rettet mot produkter og kundetyper

Gjennom å hensynta variasjon i risiko som knytter seg til produkter, kundetyper etc., slik disse er vurdert i bankens risikovurdering, kan banken få bedre forutsetninger for at indikasjoner på terrorfinansiering faktisk fanges opp og håndteres.

Finanstilsynet fant eksempler på at banker hadde egne regler for spesifikke produkter, kundetyper og bransjer som i risikovurderingen var knyttet til forhøyet risiko for terrorfinansiering. For eksempel ble det funnet regler som rettet seg mot definerte kontantintensive bransjer og regler som rettet seg mot produkter som kredittkort, lån, e-handel og ulike typer utenlandstransaksjoner.

Finanstilsynet
Revierstredet 3
P.O. Box 1187 Sentrum
NO-0107 Oslo

Tel. +47 22 93 98 00
post@finansilsynet.no
finansilsynet.no

