ØKOKRIM

NASJONAL RISIKOVURDERING HVITVASKING 2026

Foto: iStock

NRA Hvitvasking 2026, Økokrim
Grafisk formgivning: Økokrim
1. opplag og trykk: 500x, Aksell

Nasjonal risikovurdering hvitvasking 2026

HOVEDPUNKTER

- **Utnyttelse av virksomhetsstrukturer er en hovedutfordring** fordi et selskap eller organisasjon kan brukes til mange forskjellige fremgangsmåter for hvitvasking. Selskapsstrukturer i form av enkeltpersonsforetak, aksjeselskap og multinasjonale komplekse strukturer utnytter ulike muligheter som handelsbasert hvitvasking, skjult eierskap, utnyttelse av muldyr og stråselskaper. I tillegg benytter profesjonelle tilretteleggere og organiserte kriminelle registermanipulasjon, falske dokumenter, fiktiv fakturering og id-tyverier.

- Virksomheter kan også benyttes i tilknytning til primærforbrytelser som **bedrageri av det offentlige, skattekriminalitet** og **miljøkriminalitet**, i tillegg til hvitvasking gjennom blant annet handelsbasert hvitvasking og eiendomskjøp.

- **Handelsbasert hvitvasking** er en hovedkategori for hvitvasking som det er begrenset kunnskap om. Sammenblanding med legal økonomi gjør det utfordrende å avdekke, men potensialet i både den grensekryssende vareflyten og tjenester er en viktig del av helhetsbildet for risikovurderingen.

- **Eiendomsmarkedet** påvirkes av særnorske forhold og mekanismer. Dette er også et område som kan inngå og brukes i mange forskjellige hvitvaskingsoperasjoner.

- Flere kriminalitetsformer har **høyt risikonivå**. Dette skyldes ofte at den kriminelle modellen fungerer. Kategoriene er også ganske overordnede og belyser ikke nødvendigvis spesifikke endringer som ikke har strategisk verdi eller forklaringskraft.

- **Kriminelle nettverk** er trusselaktører det over tid knyttes bekymring til. Kriminelle nettverk er fleksible og bruker et **bredt spekter av fremgangsmåter for hvitvasking av utbytte.**

- Mange sektorer har uendret risikonivå siden forrige NRA i 2022. Samtidig er risikovurderingen av flere sektorer **oppjustert**. Dette gjelder finansieringsforetak, e-pengeforetak, norske tilbydere av kryptovaluta, forsikringssektoren og eiendomsmeglere. Risikonivået for agenter for utenlandske betalingsforetak er **nedjustert**.

- Et høyt nivå på risikovurderingene knyttes ofte til teknologisk utvikling og tjenester, deriblant **heldigitale banker** og **digitale selvbetjente produkter**. **Kryptovaluta** oppleves også mer tilgjengelig og **sosiale medier** utvikler seg på siden av det finansielle systemet. **Kunstig intelligens** har senket terskelen for informasjonsdeling og kunnskap om bruk av metoder og produkter.

- Samtidig er fortsatt mange **primærforbrytelser** og fremgangsmåter for hvitvasking aktuelle utenfor det digitale domenet. Dette inkluderer blant annet fysisk oppmøte, manipulering, vold, kontanter, tyverier, narkotika, varer og naturressurser.

Risikoforståelse er et viktig fundament

Nye fenomen

Selv om den største risikoen fortsatt knyttes til tradisjonelle primærforbrytelser, fremgangsmåter og sektorer, er det nyttig å se på hva som representerer nye fenomen som kan få større betydning fremover.

Av **nye fremgangsmåter** er det bekymring knyttet til sosiale medier som kanal for overføringer av verdier. Virtuell IBAN, muligheter for rask flytting og tilsløring av kryptovaluta trekkes også frem. En **ny bransje** er datasentre. Det offentlige har lite kunnskap og erfaring med bransjen, noe som i seg selv er en alvorlig sårbarhet.

Kriminalitetsområder og primærforbrytelser av ny karakter inkluderer vipps-ran, tyveri av større mengder kryptovaluta, bedragerier i nye former deriblant investeringssvindel og CEO svindler med KI-hjelp, kjøp eller tyveri av eID, syntetisk narkotika og voldsoppdrag – også som menneskehandel. Enkelte fenomen står i fare for å gå under radaren eller falle mellom to stoler. Salg av overgrepsmateriale for å finansiere kriminalitet eller ekstremisme, er aktualisert, men kan fort kategoriseres som seksuallovbrudd uten at man gir de finansielle sporene nok oppmerksomhet.

Fra et **aktørperspektiv** er tilbydere av kriminelle tjenester aktuelle på nye markeder og produkttyper. Teknologisk ekspertise er fortsatt aktuelt, men også voldsoppdrag. Kriminelle aktører som ikke er voldelige unngår fokus, men kan hvitvaske store summer. Dette inkluderer aktører innen fiskeri- og sjømatnæringen og flere grupperinger innen organisert kriminalitet.

I **sektorperspektivet** er det også noe nytt. Låneformidling og tilbydere av virksomhetstjenester risikovurderes for første gang i denne rapporten. Klimakvoteregister har også slått fast at de skal rapportere til FIU ved mistenkelige forhold. Sistnevnte er beskrevet, men ikke risikovurdert.

Mistenkelig aktivitet har ikke åpenbart opphav. Det gjenspeiles i samfunnets tilnærming til **sammensatte trusler** og mistenkelig aktivitet mot samfunnskritiske funksjoner. Private aktører kan oppfatte mistenkelige forhold som kan gjelde hvitvasking, men det kan også være andre primærforbrytelser, sanksjoner, sanksjonsomgåelser, terrorfinansiering eller aktivitet tilknyttet statlige aktører.

for det nasjonale hvitvaskingsregimet

Oppsummering

Nasjonal risikovurdering av hvitvasking omhandler forskjellige sider ved hvitvasking, herunder utvalgte fremgangsmåter, kriminalitetsområder som generer økonomisk utbytte og rapporteringspliktig sektor som utnyttes i hvitvaskingshandlingene. Risikonivået vurderes gjennom analyse av elementene trussel, sårbarhet og konsekvens. Vurderingene tar utgangspunkt i indikatorsett tilknyttet hvert av disse elementene. Det er innhentet innspill og informasjon hos både private og offentlige aktører.

Kunnskap om hvitvasking er en av indikatorene for å vurdere sårbarhet. Overordnet har mange en snever forståelse både av hva hvitvasking er og aktørgrupper som inngår i situasjonsbildet. Mange knytter hvitvasking kun til kontanter og inkluderer dermed ikke helheten og kompleksiteten hvitvasking inngår i. Hvitvasking kan være nært knyttet til primærforbrytelsen og det økonomiske utbytte. Hvem som sitter igjen med utbyttet er ikke alltid tydelig eller i fokus.

Det knytter seg flere bevisste avveininger til ulike sårbarheter. For eksempel vil tillitsbaserte ordninger ofte være lønnsomt, tilsyn og kontroll koster penger og kontanter har en beredskapsfunksjon. Selv om vurderingen er skjerpet på flere områder er det flere positive faktorer de siste årene. Det gjelder blant annet nytt regelverk, restriksjoner, opprettelse av nye enheter, privat-offentlig samarbeid og konkrete satsinger på utsatte områder.

Hvitvasking via virksomheter er helt sentralt og vil fortsatt ha høy risiko. Samtidig er det indikasjoner på underrapportering av mistenkelige forhold om hvitvasking i virksomheter. Det er behov for mer kunnskap om enkelte sektorer, særlig der risikoen vurderes som betydelig eller høy, men rapporteringen fortsatt er lav. Eksempelvis bedriftsmarkedet i banksektoren, eiendomsbransjen og advokatsektoren.

Det er gjennomgående utfordringer knyttet til datakilder og mørketall. Eksempelvis er det informasjonshull knyttet til data som kan indikere både forekomst og økonomisk omfang i norsk kontekst for mange av temaene. Et bredt kildegrunnlag må kompensere for dette for å gi best mulig situasjonsforståelse for beslutningstagere i offentlige og private virksomheter.

Nasjonal risikovurdering hvitvasking 2026

INNHOLD

> Risiko vurderes gjennom å analysere trussel, sårbarhet og konsekvens

DEL 1

BAKGRUNN OG METODE

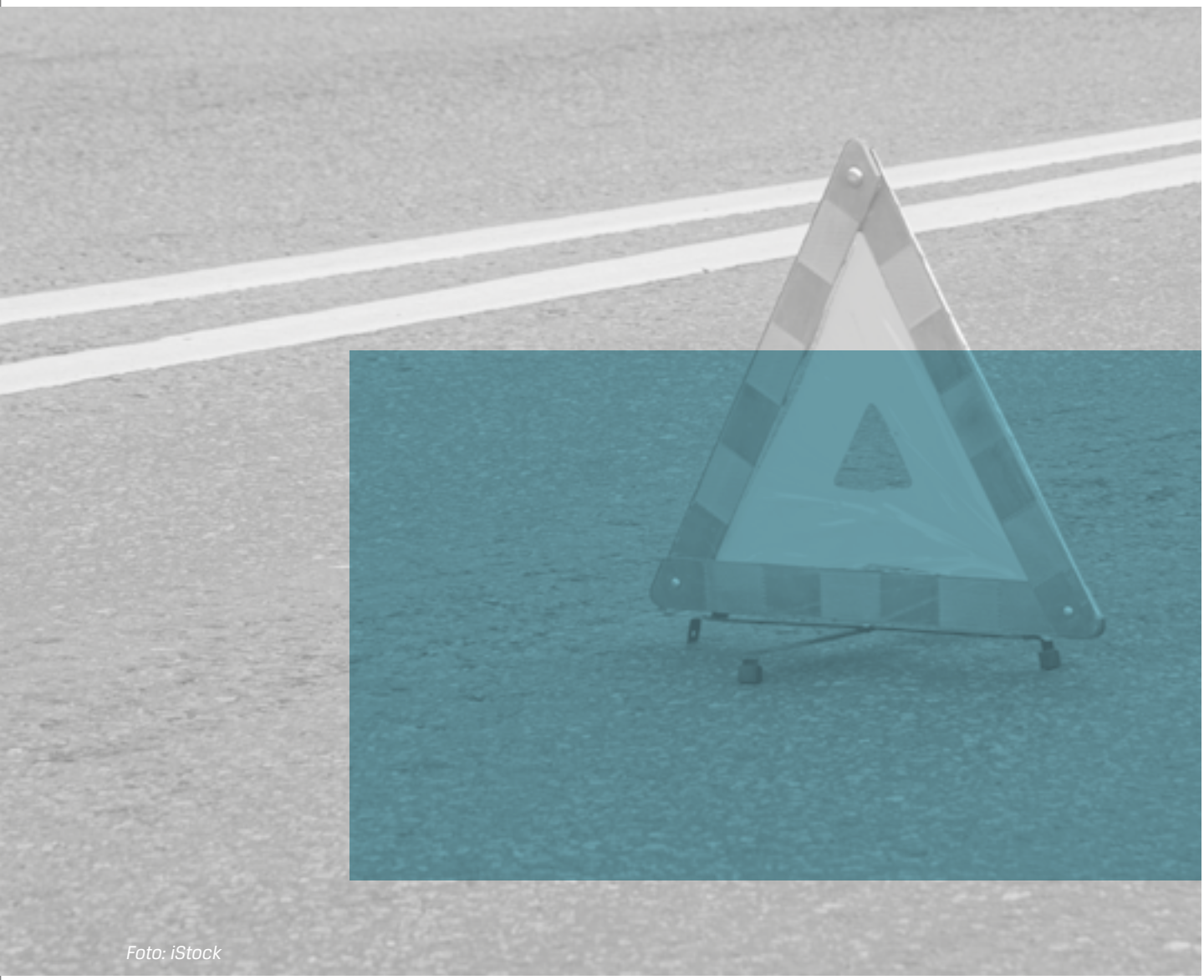


Foto: iStock

Innledning

Risikoforståelse er et viktig fundament for det nasjonale hvitvaskingsregimet. Formålet med rapporten er at den skal være et sentralt kunnskapsgrunnlag for å skape en felles forståelse for hvitvaskingsrisikoen i Norge, og for å gjøre riktige prioriteringer i innsatsen mot slik kriminalitet. Risikovurderingen danner også grunnlag for de rapporteringspliktiges arbeid.

Ifølge FATF standard skal landene identifisere, vurdere og forstå egne hvitvaskingsrisiko for å iverksette effektive sårbarhets- og risikoreduserende tiltak.[1] Det er behov for nasjonale tilpasninger i både tematikk, struktur og metode. Dette understrekes også i EUs sjette hvitvaskingsdirektiv. For å oppnå god risikoforståelse utarbeides jevnlig en helhetlig nasjonal risikoanalyse for hvitvasking. Nasjonal risikoanalyse (NRA) 2026 er Norges sjette samlede risikovurdering av hvitvasking. Den forrige ble utgitt i 2022. NRA 2026 bygger videre på NRA 2022 og har derfor de fire siste årene som referanseperiode, der ikke annet er presisert. Spesifikke endringer i denne perioden fremheves i rapporten.

Utarbeidelse av NRA 2026 er et oppdrag gitt av Justisdepartementet og Politidirektoratet. Økokrim har ansvar for hvitvasking og PST har ansvar for terrorfinansiering (TF). Risikovurderingene publiseres i to rapporter som må ses i sammenheng.

Endring og utvikling – tiltak siden NRA 2022

Stortingsmeldingen mot økonomisk kriminalitet «Felles verdier – felles ansvar» presenterer en rekke tiltak som skal bidra til effektiv bekjempelse av hvitvasking og terrorfinansiering.[2] I tillegg er det gjennomført en utredning, med påfølgende høringsrunde knyttet til implementering av EUs 6. hvitvaskingspakke.

Videre har det vært jobbet med informasjonsdeling og privat-offentlig samarbeid følger opp mange operative initiativ. I tillegg har det vært konkrete satsinger på utsatte områder som kriminelle nettverk, fiskerinæringen, korrupsjon og skattekriminalitet.

Advokattilsynet ble opprettet 1. januar 2025. Norsk politi fikk en dedikert bedragerienhet i oktober 2024, organisert under Økokrim. Det er også opprettet en korrupsjonsenhet under Økokrim og et inndragningsløft i norsk politi, ledet av Økokrim.

Det har også vært igangsatt lovgivningsarbeid for å innføre nye bestemmelser om forhåndsdeklarering ved inn- og utføring av betalingsmidler i forbindelse med reise. I denne sammenheng vil det også bli sett på FIU-ens tilgang til informasjon om valutadeklarasjoner fra Tolletaten.

1 FATF, *Money Laundering National Risk Assessment Guidance,* (FATF, 2024).
2 Regjeringen, Meld. St. 15 (2023–2024) – «Felles verdier – felles ansvar». Frigitt 22.03.2024 https://www.regjeringen.no/no/dokumenter/meld.-st.-15-20232024/id3031227/

Bakgrunn og metode

METODE OG DATAGRUNNLAG

NRA 2026 om hvitvasking bygger på metodikken fra de foregående NRA-ene. Det er imidlertid gjort noen strukturelle og metodiske endringer for å tilpasse rapporten til dagens situasjon og anbefalinger fra FATF[3,4]. Risikovurderingene bygger på analyse og vurdering av de tre elementene trussel, sårbarhet og konsekvens. Indikatorsett for trussel og sårbarhet er likt med NRA 2022, mens det er gjort endringer i indikatorene for konsekvens. I tillegg til å vurdere risikoen for hvitvasking innenfor de rapporteringspliktige sektorene, inkluderer rapporten også risikovurderinger for utvalgte fremgangsmåter for hvitvasking og utvalgte kriminalitetsområder (primærforbrytelser). Det benyttes en fire-delt skala for vurdering av risikonivå; lav, moderat, betydelig, høy.

Prinsippene beskrevet i Politiets etterretningsdoktrine har ellers vært rammeverket for rapporten. Det prioriterte etterretningsbehovet er:

Figur 1: Vurderingskala med fargekoder

«Hva er risikoene for hvitvasking i Norge og for at utbytte fra kriminalitet i Norge hvitvaskes i utlandet? Hvilke sektorer er (mest) utsatt?»

Data- og informasjonsgrunnlaget er innhentet fra relevante fagmiljø, offentlige etater, private aktører og akademia.

Viktige samarbeidspartnere har vært Skatteetaten, Tolletaten, Finanstilsynet, Advokattilsynet og Lotteritilsynet, i tillegg til Økokrim, Kripos og politiet for øvrig. Rapporteringspliktige og bransjeorganisasjoner har også bidratt. Rapporten bygger på et bredt utvalg dokumenter og rapporter, både nasjonale og internasjonale, som dekker ulike

3 FATF, *Money Laundering National Risk Assessment Guidance*, (FATF, 2024).
4 FATF, *Extended update to the ML NRA Guidance*, (FATF, 2025).

fenomen og aspekter. En del av disse er unntatt offentlighet. Navngitte kilder vil imidlertid kun være offentlige dokumenter.

Numerisk informasjon fra hvitvaskingsregisteret
Når det gjelder antall MF-rapporter (MFR) fordelt per sektor baserer tallene seg på uttrekk fra hvitvaskingsregisteret. Av systemtekniske årsaker og registreringskategorier, er det avvik mellom sektorkategorier i NRA og hvitvaskingsregisteret. Derfor har ikke alle sektorene i del seks egen virksomhetstype i denne listen. Det er rapporteringspliktige selv som velger virksomhetstype fra en forhåndsdefinert liste i rapporteringsskjema.

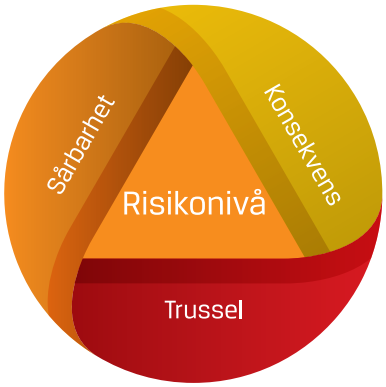
For å fange opp endringer er det gjort ordtellingssøk basert på uttrekk av utvalgte nøkkelord fra hvitvaskingsregisteret. Bakgrunn for bruk av ord kan variere, men kan gi en indikasjon på endringer i omfang av enkelte områder eller fenomen.

Risikotriangelet og indikatorer

Risiko vurderes gjennom å analysere trussel, sårbarhet og konsekvens. Det endelige risikonivået illustreres gjennom et risikotriangel, der vurderingene av de ulike elementene angis med respektive nivåer. På den måten kan man enkelt identifisere hvor hovedutfordringene ligger med tanke på hvor tiltak og innsats kan rettes. Trekanten som helhet uttrykker det samlede risikonivået.

Trussel defineres i denne rapporten som en person, objekt, grupper av personer eller aktiviteter som potensielt kan skade staten, samfunnet og økonomien. Trussel vurderes etter følgende indikatorer: (1) omfang knyttet til trusselaktør og primærlovbrudd; (2) omfang på kriminelt økonomisk utbytte; (3) utsatthet for internasjonale pengestrømmer og (4) aktørenes kapasitet. Omfanget knyttet til trusselaktører og primærlovbrudd kan handle om både hyppighet og antall personer involvert. Et viktig aspekt ved aktørers kapasitet er grad av organisering eller hvorvidt de er del av et kriminelt nettverk.

Sårbarhet defineres i denne rapporten som evnen til å begrense en trussel. Sårbarhet vurderes etter følgende indikatorer: (1) egenskaper som potensielt kan utnyttes som anonymitet eller



Figur 2: Risikotriangelet

Foto: iStock

tilgjengelighet; (2) juridisk rammeverk og reguleringer; (3) kompetanse og kunnskap om hvitvasking og hvitvaskingsarbeidet tilknyttet tema som vurderes («awareness»); (4) kontrollmekanismer og oppdagelsesrisiko.

Konsekvens defineres som skaden hvitvasking kan påføre, og inkluderer effekten av primærforbrytelsen. Konsekvens vurderes etter følgende indikatorer: (1) hvorvidt kriminaliteten undergraver samfunnsstrukturer og tillit; (2) økonomiske tap; (3) langsiktige/indirekte konsekvenser; (4) integritet, liv og helse. Økonomiske tap omfatter både private/personlige tap, bedrifters tap, i tillegg til samfunnets og fellesskapets økonomiske tap.

Datagrunnlag og datakvalitet

Statistiske og numeriske data er innhentet på områder der dette er tilgjengelig.

Politiets straffesakssystem (Strasak) og hvitvaskingsregisteret er sentrale datakilder, men denne informasjonen gir ikke nødvendigvis et fullstendig situasjonsbilde. Det er utfordringer knyttet til å estimere omfang – både hva gjelder utbredelsen av fenomen og økonomisk rekkevidde. Både hvitvaskingsregisteret og straffesaksregisteret kan være indikatorer når man skal estimere omfang, men krever tolkning. I 2025 var antallet opprettede hvitvaskingssaker i Strasak 431 og antallet registrerte MFR i hvitvaskingsregisteret 33 313. Disse tallene sier lite om omfang alene, men må forstås i sin kontekst.

Det har vært utfordrende å finne felles målepunkter. For både fremgangsmåter, kriminalitetsområder og sektorer, er det tilstrebet å finne numeriske datakilder som spesifikke og objektive indikatorer. Datagrunnlaget er imidlertid ofte mangelfullt. Ulike fagmiljøer er derfor bedt om å bidra med å peke ut relevante spesifikke indikatorer og samtidig vurdere usikkerheten knyttet til data og informasjonsgrunnlag etter følgende kriterier:[5]

- tilgang på relevante data og erfaringer
- forståelse av fenomenet som analyseres (kompetanse)
- grad av enighet blant ekspertene
- i hvilken grad endringer i forutsetninger påvirker nivåets gyldighet

Informasjon i publikasjoner og rapporter er også systematisert i henhold til indikatorene. Språkmodeller basert på kunstig intelligens har vært brukt som verktøy for å bryte ned enkelte offentlige rapporter. Det er også gjort en pengestrømsanalyse, i del tre av rapporten, men kildegrunnlaget oppleves for usikkert til å kunne gi tydelige konklusjoner.

Vurdering av data, informasjon og endringer

De overordnede indikatorene er som nevnt i stor grad en videreføring fra NRA 2022. Det gir et utgangspunkt for å vurdere hvor endringen treffer og vurdere hvilken påvirkning den har på risikobildet.

Både fremgangsmåter for hvitvasking, kriminalitetsområder og sektorer er forskjellige av natur, og datagrunnlaget varierer i kvalitet. I tillegg tolkes dataene på ulikt vis. Statistikk på anmeldt kriminalitet kan for eksempel indikere omfang og hyppighet for noen kriminalitetsområder, mens for andre områder tolkes som at det er lite kunnskap om typen kriminalitet, eller at det er lav oppdagelsesrisiko og store mørketall. Riksadvokatens og politiets prioriteringer påvirker også anmeldelsestallene. Narkotikakriminalitet og kriminelle nettverk er eksempler på kriminalitetsområder der anmeldelsestall påvirkes av politiets ressurser og innsats. Statistikk på anmeldt kriminalitet kan også påvirkes av hvordan påtalemyndigheten bygger sakskomplekser. For eksempel ved hvitvasking, vil primærforbrytelsene som midlene har sin opprinnelse fra, eller tilstøtende paragrafer påtalejuristen benytter eksempelvis korrupsjon og habilitet, menneskehandel, hallikvirksomhet eller sosial dumping i saker om arbeidslivskriminalitet, ha høyere strafferamme og være enklere å bevise. Ulike tema må derfor behandles ulikt.

For hvert tema er det lagt vekt på endringer fra forrige NRA. Hva endringen består i, hvilke indikatorer den påvirker, og om endringen påvirker nivået opp eller ned. Dette vil fremkomme i vurderingen. Det er imidlertid verdt å merke seg at en endring kan påvirke noen indikatorer positivt og andre negativt. Eksempelvis kan ny teknologi gjøre kriminelle mer kapable samtidig som den også styrker kontrollmuligheten og øker oppdagelsesrisiko. Vanskeliggjøring av enkelte hvitvaskingsmetoder kan føre til at kriminelle tar i bruk andre metoder.

Temaene inneholder mange underkategorier og store endringer kan bli

5 Kriteriene er hentet fra «*Fremgangsmåte for utarbeidelse av nasjonalt risikobilde*», (DSB, 2015).

helt eller delvis «nullet ut» i det store bildet. Indikatorene er heller ikke gjensidig utelukkende. Det vil være naturlig korrelasjon mellom noen av dem, blant annet trusselindikatoren, aktørers «kapabilitet» og sårbarhetsindikatoren, «tilgjengelighet». Det er derfor nødvendig å grave seg ned i lagene for å forstå mekanismene og hvor risikoen ligger. Dette gjenspeiles i rapportens oppbygging, hvor de ulike delene må ses i sammenheng.

Rapportens oppbygging

Del to av rapporten beskriver overordnet situasjonsbilde og drivere som påvirker utviklingen. Del tre og fire tar for seg pengestrømmer og hovedprinsipper for utvalgte fremgangsmåter for hvitvasking. I del fem vurderes hvitvaskingsrisikoen for utvalgte kriminalitetsområder og primærforbrytelser som genererer profitt. Del seks vurderer hvitvaskingsrisiko for rapporteringspliktige sektorer.

Hvert av temaene i del tre til seks har en introduksjon med beskrivelse og hvordan tematikken relaterer seg til hvitvasking. Videre fremheves spesifikke endringer siden NRA 2022 der det er relevant. Under vurderingene presenteres først samlet risikovurdering før vurderingene av trussel, sårbarhet og konsekvens beskrives.

I del 7 er alle risikovurderingene oppsummert i tabeller, etterfulgt av en begrepsliste. Ord markert i *kursiv* i teksten er forklart her.

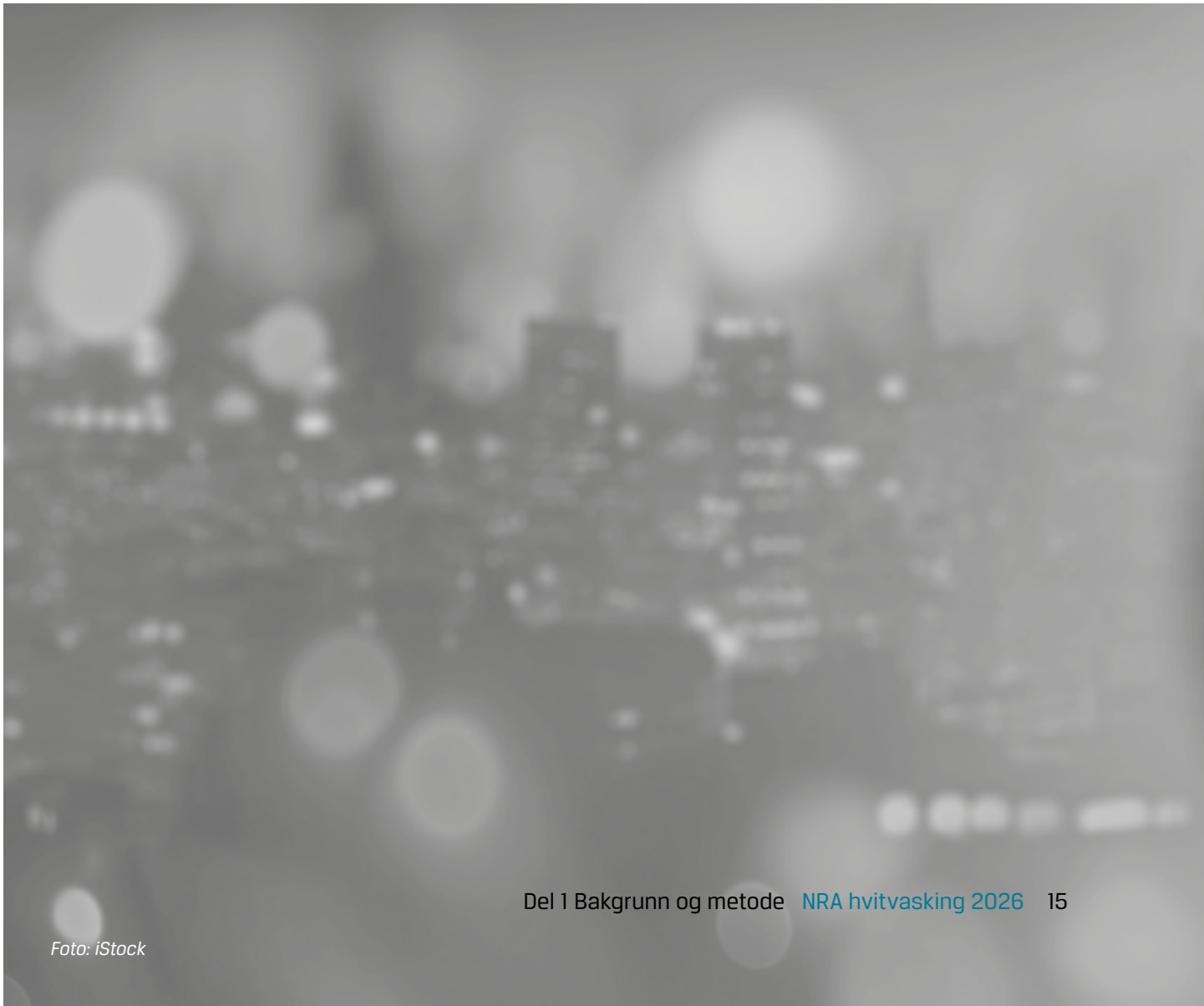


Foto: iStock

"Internasjonalt vurderes hvitvasking å være blant de alvorligste globale kriminalitetstruslene

DEL 2

OVERORDNET SITUASJONSBILDE

Foto: iStock

Innledning

Del to gir et overordnet situasjonsbilde for hvitvasking i norsk kontekst og danner grunnlag for de tematiske og sektorvise risikoanalysene i de neste delene av rapporten. I denne delen beskrives rammene for risikobildet, hvordan hvitvasking forstås i denne analysen, hvilke drivere som påvirker utviklingen, og hvordan det norske antihvitvaskingsregimet er innrettet. Denne delen danner et felles utgangspunkt for de mer detaljerte vurderingene i påfølgende deler.

Internasjonalt vurderes hvitvasking å være blant de alvorligste globale kriminalitetstruslene.[6] Kriminaliteten er i økende grad grensekryssende, kompleks og profesjonalisert. Europol beskriver hvitvasking som en del av fundamentet for organisert kriminalitet. De illustrerer hvordan den kriminelle maskinen holdes i gang av hvitvasking, som et av flere tannhjul, fordi det spiller en avgjørende rolle for å konvertere profitt fra kriminelle handlinger inn i den lovlige økonomien eller til å reinvestere i den kriminelle økonomien. Digitale tjenester, nye finansielle produkter og virtuelle verdier har gjort det enklere å flytte og skjule verdier på tvers av jurisdiksjoner.[7] Dette påvirker også risikobildet i Norge.

Faktaboks *Juridisk rammeverk*

I nasjonal lovgivning er hvitvasking straffesanksjonert i straffeloven:
§ 337 (simpel hvitvasking)
§ 338 (grov hvitvasking)
§ 339 (mindre hvitvasking)
§ 340 (uaktsom hvitvasking)
§ 341 (forbund om hvitvasking)

6 Europol, *The Other side of the Coin – Analysis of Financial and Economic Crime*, (Europol, 2023).
7 Europol, *Serious and Organised Crime 2025* (SOCTA), (Europol, 2025).

Overordnet situasjonsbilde

DET NORSKE ANTIHVITVASKINGSREGIMET

Faktaboks *Det norske antihvitvaskingsregimet*

Norges innsats mot hvitvasking og terrorfinansiering er bygget på anbefalinger fra Financial Action Task Force (FATF) og internasjonale standarder. Financial Intelligence Unit (FIU) i Økokrim er medlem av Egmont-gruppen, som er en global sammenslutning for finansiell etterretning. Lovverket i Norge sanksjonerer hvitvasking gjennom flere paragrafer i straffeloven, og hvitvaskingsloven definerer hvem som har rapporteringsplikt til myndighetene.

Rapporteringspliktige aktører skal sende meldinger om mistenkelige forhold til FIU i Økokrim, som analyserer og videreformidler informasjon. Flere etater har tilsynsansvar med rapporteringspliktig sektor. Herunder Finanstilsynet, Advokattilsynet og Lotteritilsynet. Riksadvokaten har det overordnede ansvaret for straffesaksbehandlingen. Politidirektoratet har ansvaret for at normer, krav, mål og prioriteringer gitt av riksadvokaten og statsadvokatene kan realiseres på en mest mulig effektiv og hensiktsmessig måte gjennom ressursallokering, organisering og kompetansehevende tiltak.

Kontrolletater som Skatteetaten og Tolletaten har også viktige ansvarsområder. Skatteetaten ved ansvar for utlikning og innkreving av skatt, merverdiavgift og særavgifter, og for folkeregistrering. I tillegg er Statens innkrevingssentral underlagt Skatteetaten. Tolletaten er en viktig aktør ved blant annet ansvar for å motvirke ulovlig inn- og utførsel av varer (smugling) og sørge for riktig deklarering, fastsettelse og rettidig innbetaling av toll og avgifter.

Norges innsats mot hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen koordineres i et tverretatlig Kontaktforum[8]. Privat sektor er observatører i Kontaktforum.

8 Kontaktforum består av Justis- og beredskapsdepartementet, Finansdepartementet, Utenriksdepartementet, Finanstilsynet, Politidirektoratet, Politiets sikkerhetstjeneste (PST), Riksadvokatembetet, Skattedirektoratet, Tolldirektoratet og Økokrim.

Overordnet situasjonsbilde

AVGRENSNING OG FORSTÅELSE AV HVITVASKING

Hvitvasking forstås som handlinger som har til formål å skjule eller tilsløre utbytte fra straffbare handlinger, slik at midlene fremstår som lovlige. Utbyttebegrepet omfatter ikke bare penger, men også andre former for økonomisk verdi, herunder besparelser, eiendeler, rettigheter og immaterielle verdier. Eksempler på besparelser kan være svart arbeid, verdiøkning gjennom økt standard eller miljøkriminalitet i form av sparte avgifter.

Det er ikke alltid et klart skille mellom primærforbrytelsen og hvitvaskingen. I mange kriminalitetsformer er hvitvasking integrert i selve forretningsmodellen, eksempelvis ved investeringsbedragerier, miljøkriminalitet, skattekriminalitet og arbeidslivskriminalitet.

Hvitvaskingsprosessen beskrives ofte gjennom tre faser: plassering, tilsløring og integrering. **Plassering** innebærer at utbyttet føres inn i det økonomiske systemet, ofte på måter som unngår effektiv kontroll. **Tilsløring** handler om å bryte sporbarheten, for eksempel gjennom *smurfing*, bruk av stråpersoner, utenlandsoverføringer eller komplekse selskapsstrukturer. **Integrering** innebærer at midlene bringes tilbake til den lovlige økonomien, eksempelvis gjennom kjøp og salg av eiendeler, investeringer eller bruk av ulike betalingsløsninger. I praksis kan disse fasene overlappe, og enkelte handlinger kan dekke flere faser samtidig.

Gjeldende hvitvaskingslov[9] dekker etter sin ordlyd ikke sanksjonsomgåelser eller sanksjonsbrudd. Heleri- og hvitvaskingsbestemmelsene i straffeloven avgrenser imidlertid ikke mot typen lovbrudd som har generert utbyttet, hvilket innebærer at også brudd på sanksjonsregelverket er et primærlovbrudd som vil kunne dekkes av disse straffebestemmelsene.

9 Fra 18. juli 2018.

Overordnet situasjonsbilde

DRIVERE FOR HVITVASKING

Utviklingen i kriminalitetsbildet og hvitvaskingsrisikoen påvirkes av flere overordnede drivere.

Teknologisk utvikling er en sentral driver. Kunstig intelligens, automatisering og digital infrastruktur gjør det enklere å begå komplekse lovbrudd og muliggjør mer avanserte hvitvaskingsmetoder. Samtidig gir teknologien også nye verktøy for forebygging og avdekking, både for private aktører og myndigheter. Enorme mengder data er lagret digitalt, og samfunnet fokuserer strengt på dataregulering. Mye har vært knyttet til personvern, men digital sårbarhet omfatter ikke bare privatpersoner, men også bedrifter og samfunnsinstitusjoner. Identitet blir en lukrativ vare enten den er stjålet, eller på andre måter blir kontrollert av kriminelle. Mye kriminalitet skjer utelukkende eller delvis via digitale kanaler.

Miljø- og klimarelaterte drivere kan skape nye kriminalitetsformer og hvitvaskingsmuligheter. Global oppvarming kan skape klimaendringer og ressursknapphet som igjen kan påvirke utfallet av ekstremvær og naturkatastrofer, og føre til migrasjon og konflikter. Endringene kan skape nye muligheter for kriminalitet og hvitvasking – eksempelvis handel med klimakvoter. Slike drivere kan dermed påvirke både trusselen fra hvitvasking, sårbarhet for hvitvasking og konsekvenser av hvitvaskingen.

Økonomiske drivere omfatter globalisering, migrasjon og økende økonomiske forskjeller. Endringer i kronekurs, arbeidsmarkedet og internasjonale kriser påvirker både lovlig og ulovlig økonomisk aktivitet. Større sosiale forskjeller bygger ned samhold, tillit og lojalitet til fellesskapet. Store økonomiske verdier

Bruken av KI kan påvirke trusselbildet både positivt og negativt

og høy kjøpekraft gjør Norge attraktivt for kriminelle aktører som ønsker å plassere eller integrere utbytte.

Sosiale og kulturelle forhold, herunder høy tillit til myndigheter og velferdsordninger, kan bidra til effektiv forvaltning, men også innebære risiko for misbruk. I Norge er det fortsatt et høyt tillitsnivå. Velferdsstaten aksepterer et visst nivå av bedrageri for effektivt å kunne tilby støtte og tjenester til befolkningen. Demografisk har Norge en aldrende befolkning. En aldrende befolkning kan bidra til økte digitale skiller i fremtiden, i tillegg vil det sette velferdsstaten på prøve og kunne bidra til økende sosial ulikhet.

Politiske drivere, som geopolitisk uro, proteksjonisme og svekket internasjonalt samarbeid, kan redusere effektiviteten i kontroll og rettshåndhevelse på tvers av grensene. Det politiske bildet preges av væpnede konflikter, allianser og et økende fokus på fiender. Maktfordelingen i verden utfordres, og Europa opplever økte trusler utenfra mot egen sikkerhet. Tilgang til knappe ressurser vil alltid være sentralt i politiske maktkamper. Internasjonalt samarbeid er tett knyttet til politisk klima. Finansmarkedet er internasjonalt, og kontrollmyndigheter må samarbeide på tvers for å stoppe kriminelle. Det er utfordrende at regelverk er fragmentert og tolkes ulikt. Internasjonalt samarbeid går sakte og kan enkelt nedprioriteres.

Juridiske drivere er forskjeller i regelverk, håndheving og praksis mellom land og tilpasning fra kriminelle aktører som utnytter smutthull og ulikheter i systemene. Enkelte stater legger til rette for utenlandske investeringer, investeringspass[10], hemmelighold og blir «skatteparadiser» eller på annen måte egnede oppsamlingspunkter for kriminelt utbytte. Kriminelle aktører har god oversikt over lov- og regelverk, og håndplukker land etter praksis og muligheter. Regelverk kan strammes inn, men det kan også åpnes, som da den amerikanske antikorrupsjonsloven Foreign Corrupt Practices Act (FCPA) ble satt på pause i 2025.

10 Fra engelsk: citizenship by investment.

Overordnet situasjonsbilde

SÆRTREKK I DET NORSKE HVITVASKINGSREGIMET

Norge har en åpen økonomi med omfattende internasjonale pengestrømmer. Norsk næringsliv er tett integrert i globale markeder, og mange norske virksomheter opererer i eller mot land med høyere korrupsjonsrisiko og svakere institusjoner. Norge har også høy levestandard, politisk stabilitet og et velfungerende finansielt system med høy tillit internasjonalt. Disse faktorene gjør Norge attraktivt både for legitime investeringer og for plassering av midler med ulovlig opphav.

Tilliten i samfunnet og de effektive digitale betalingsløsningene i den norske økonomien gir betydelige samfunnsgevinster, men innebærer også sårbarheter. Digitale løsninger muliggjør rask og grenseløs flyt av verdier, og tillitsbaserte ordninger kan utnyttes av aktører med vilje og evne til å begå økonomisk kriminalitet. Norge har også store og komplekse verdikjeder innen blant annet energi, sjømat, eiendom og bygg- og anleggsbransjen, som gir rom for skjult eierskap, kompliserte transaksjoner og tilsløring av utbytte.

Den finansielle og juridiske strukturen i Norge inneholder også sårbarheter. Det er et stort antall mindre banker i Norge noe som gjør det mulig for kriminelle å spre sine aktiviteter over flere bankforhold som kan opprettes raskt. I tillegg er det både enkelt og billig å opprette foretak og organisasjoner, en struktur som kriminelle nettverk aktivt misbruker.

Norge er grunnleggende et tillitsbasert samfunn med gode velferdsordninger, noe som utnyttes gjennom registermanipulasjon for å svindle til seg offentlige midler. Små sosiale forhold kan også være en sårbarhet; i kommuner kan tette bånd og rollekonflikter øke faren for korrupsjon, spesielt i planprosesser og tildeling av tillatelser.

Et moderne trekk er hvordan kriminelle aktører og nettverk aktivt benytter tilgang til media og sosiale plattformer for å merkevarebygge seg selv eller presentere sin versjon av saken for å påvirke opinionen og forhandlingsposisjoner.

Selv om det norske lovverket gir gode fullmakter til å følge pengesporet, er det utfordringer knyttet til den operative oppfølgingen. Mange saker henlegges på grunn av kapasitetsmangel eller manglende prioritering i politidistriktene.

Overordnet situasjonsbilde

RISIKOBILDET

Risikobildet for hvitvasking i Norge er sammensatt, endrer seg raskt og påvirkes av sterke koblinger mellom nasjonale og internasjonale forhold. Selv om Norge har et relativt robust antihvitvaskingsregime, er effekten i stor grad avhengig av evnen til praktisk gjennomføring, samhandling og prioritering i hele kjeden fra forebygging til straffereaksjon. Dette tilsier behov for fortsatt og forsterket risikobasert innsats, særlig rettet mot strukturelle sårbarheter og profesjonelle aktører som muliggjør hvitvasking i større skala.

Det er variasjoner fra lav til høy risiko innenfor rapporteringspliktig sektor samt ulike kriminalitetsområder og fremgangsmåter for hvitvasking.

Kriminelle aktører som har behov for å hvitvaske utbytte omfatter både organiserte kriminelle, hvitvaskingsnettverk, profesjonelle tilretteleggere og enkeltaktører som begår profittmotivert kriminalitet. Trusselaktørene kjennetegnes av høy tilpasningsevne, god markedstilgang og økende teknologisk kompetanse. Digitalisering, bruk av heldigitale banker, virtuelle verdier og grensekryssende betalingsløsninger gjør det mulig å flytte eller skjule verdier raskt og i stort omfang. Internasjonaliseringen av kriminalitet innebærer at utbytte fra lovbrudd begått i og utenfor Norge i økende grad blir forsøkt integrert i norsk økonomi.

Norge har en bred og voksende sårbarhetsflate. Den høye graden av digitalisering, komplekse verdikjeder og utstrakt bruk av tredjepartsleverandører gjør det krevende å ha full oversikt over hvordan verdier flyttes og hvor i systemene svakhetene oppstår. Nye teknologiske løsninger introduseres

raskere enn samfunnet klarer å forstå, regulere og kontrollere dem. Kunstig intelligens representerer i denne sammenheng en ny og mindre forstått sårbarhetsflate, både fordi teknologien kan brukes til å effektivisere kriminalitet og fordi den kan forsterke eksisterende svakheter.

Selv om det overordnede sårbarhetsbildet peker på sårbarheter i det norske hvitvaskingsregimet, betyr ikke det nødvendigvis at praksisen er uønsket. Ofte må flere hensyn balanseres og veies opp imot hverandre. Effektivitet og brukervennlighet i automatiserte og digitale søknader og prosedyrer, personvern og anonymitet, og beredskap, eksempelvis i forbindelse med kontanter er forskjellige legitime hensyn som kanskje utgjør en sårbarhet, men som likevel er ønsket i samfunnet.

Hvitvaskingsregimet skal som helhet forebygge, stoppe og reagere på hvitvasking for å hindre at kriminelle sitter igjen med økonomisk utbytte. For å oppnå dette er det nødvendig med effektiv samhandling og koordinering mellom offentlige og private aktører i tillegg til robuste systemer uten lovløse smutthull. Mekanismer for kontroll og iretteføring gir både reaksjon og virker avskrekkende. Samtidig er det identifisert sårbarheter knyttet til fragmentert ansvar, varierende kompetanse, begrensede analyse- og etterforskningsressurser og ulik forståelse av hvitvasking som fenomen.

Videre preges mange offentlige aktører av silotenkning og avgrensning av eget mandat. Dette kan gå ut over informasjonsdeling mellom etater. Manglende føringer fra tverrfaglig styrende organ svekker sjansen for endring.

Foto: iStock

Kunnskapshull er en annen viktig faktor som påvirker evnen til å avdekke hvitvasking. Evnen til å gjenkjenne metoder, aktører og mistenkelige forhold er god hos mange rapporteringspliktige og politiet, mens tilsyn blant annet har avdekket at den er svakere hos enkelte rapporteringspliktige. I tillegg er det også mer kunnskap om enkelte grupper og områder enn andre. Blant annet er kunnskapen om privatpersoner og kjente kriminelle nettverk bedre enn modus tilknyttet storbedrifter. Videre bidrar strukturelle endringer i bransjen til økt handlingsrom for kriminelle til å utnytte sårbarheter gjennom blant annet selvbetjeningsløsninger som tilbys gjennom offentlige registre.

Et stort antall rapporterte mistenkelige forhold presser analyseressursene. Manglende etterforskningskapasitet i politidistriktene er også kritisk for håndtering av økonomiske straffesaker.[11] Ofte prioriteres primærforbrytelsen fremfor hvitvasking, blant annet fordi beviskravene kan oppleves som lavere og strafferammene høyere.

Det offentlig-private samarbeidet er bra, imidlertid er det utfordringer knyttet til informasjonsdeling som følge av juridiske og praktiske hindringer. Denne problematikken er omtalt i en arbeidsgrupperapport fra mars 2026.[12] Private aktører bidrar også til å drive utviklingen i antihvitvaskingsarbeid fremover. De har blant annet tatt ansvar for rettslig avklaring i prinsipielle saker og systemer for informasjonsutveksling.

Hvitvasking undergraver tilliten til finanssystemet, offentlige institusjoner, næringslivet og rettsstaten. Det bidrar videre til å opprettholde og forsterke alvorlig kriminalitet. Økonomiske konsekvenser inkluderer tapte skatte- og avgiftsinntekter, konkurransevridning og feilallokering av kapital. De indirekte konsekvensene er betydelige og langsiktige, blant annet ved at kriminelle aktører kan etablere varige posisjoner i næringsliv og eiendomsmarked, samt påvirke samfunnsstrukturer og miljø gjennom korrupsjon, arbeidslivskriminalitet og utnyttelse av velferdsordninger.

11 Nettlenke, 10.02.2026: https://osloeconomics.no/wp-content/uploads/2024/05/0E-rapport-2024-25-Politiets-bruk-av-finansiell-etterretning.pdf

12 Regjeringen. Frigitt 17.03.2026: https://www.regjeringen.no/globalassets/departementene/jd/dokumenter/rapporter-planer-og-strategier/2026/rapport-ops_arbeidsgruppe_okokrim.pdf

Overordnet situasjonsbilde

FREMTIDSPERSPEKTIVER OG UTVIKLINGSTREKK

Dette kapittelet beskriver utviklingstrekk som kan påvirke hvitvaskingsrisikoen fremover. Bildet vil bli mer komplekst, men også mer mulig å forstå dersom data, kompetanse og samarbeid styrkes. Innsatsen bør først og fremst rettes mot de strukturene som muliggjør hvitvasking i stor skala.

Hvitvaskingsrisikoen i Norge vil de kommende årene påvirkes spesielt av rask teknologisk endring, økt geopolitisk og økonomisk usikkerhet, og et mer harmonisert og krevende regelverk. Samtidig vil de grunnleggende utfordringene bestå – kriminelle aktører vil fortsette å skjule utbytte gjennom virksomheter, eiendom, finansielle tjenester, digitale verdier, kontanter og internasjonale strukturer.

Utviklingen tilsier at innsatsen mot hvitvasking i større grad må være dynamisk, datadrevet og samordnet. Løsningen er ikke å bygge høyere gjerder rundt én sektor dersom kriminelle bare finner nærmeste åpne port i nabosystemet. Risikoen flytter seg raskt, og tiltak bør derfor vurderes på tvers av sektorer, metoder og kriminalitetsområder.

Geopolitikk, sanksjoner og grensekryssende verdiflyt

Geopolitisk uro, krig, sanksjoner og økt strategisk konkurranse vil fortsette å påvirke risikobildet. Internasjonale pengestrømmer, varestrømmer og eierskapsstrukturer kan brukes til å skjule både kriminelt utbytte, sanksjonsomgåelser og annen uønsket aktivitet. Dette gjelder særlig der verdier flyttes via tredjeland, komplekse selskapsstrukturer eller jurisdiksjoner med svakere innsyn og informasjonsdeling.

Norge er en åpen økonomi med høy tillit og omfattende internasjonal handel. Dette er en styrke, men også en sårbarhet. Fremover vil det være viktig å se hvitvasking, sanksjonsomgåelser, korrupsjon, skattekriminalitet og statlig påvirkning mer i sammenheng.

Foto: iStock

Regelverksendringer

EUs nye hvitvaskingspakke vil få stor betydning for det norske antihvitvaskingsregimet. Regelverket legger opp til økt harmonisering i EU/EØS, tydeligere krav til risikostyring, internkontroll og dokumentert effektivitet, samt klarere ansvarsplassering hos styre og ledelse. Det forventes også at det blir flere rapporteringspliktige med utvidede plikter for disse. Videre at FIU-en vil bli styrket med blant annet mer tilgang til data og tydeligere tilbakemeldinger til rapporteringspliktige.

Nasjonale prosesser

Det pågår også nasjonale prosesser som kan påvirke fremtidig risiko, blant annet oppfølgingen av stortingsmeldingen om økonomisk kriminalitet, vurderinger av informasjonsdeling, behov for nye hjemler, bedre tekniske løsninger og videreutvikling av offentlig-privat samarbeid. Et eksempel er Kartverket og Skatteetatens samarbeid om å kartlegge utfordringer ved eierskapsregistreringer til fast eiendom i Norge i dag. Det er levert en konseptvalgutredning (KVU) om hvordan det kan legges til rette for bedre registrering og oversikt over eierskap til fast eiendom.

Teknologi og kunstig intelligens

Teknologisk utvikling vil påvirke både trusselbildet og kontrollmulighetene. Kunstig intelligens, automatisering og digitale plattformer kan gjøre det enklere å produsere falsk dokumentasjon, manipulere identiteter, opprette trover-

dige selskapsstrukturer og gjennomføre bedragerier i større skala. Samtidig kan teknologien styrke analyse, transaksjonsovervåking, mønstergjenkjenning og prioritering av mistenkelige forhold.

Utfordringen fremover blir ikke bare å ta i bruk ny teknologi, men å forstå hvordan den endrer kriminaliteten. Kriminelle aktører trenger ikke nødvendigvis å være teknologiske eksperter dersom de kan kjøpe ferdige tjenester, verktøy og infrastruktur. Dette øker betydningen av å følge utviklingen i kriminelle tjenestemarkeder, digitale betalingsløsninger, kryptovaluta, syntetiske identiteter og plattformbaserte verdioverføringer.

Innsikt og datagrunnlag

Et gjennomgående funn i NRA 2026 er at datagrunnlaget på flere områder er mangelfullt. Det gjelder særlig økonomisk omfang, reelle aktører, utnyttelse av virksomhetsstrukturer og handelsbasert hvitvasking.

Fremover bør det arbeides mer systematisk med indikatorer, datakvalitet og analysegrunnlag. Dette omfatter bedre utnyttelse av MF-rapporter, pengestrømsdata, registerdata, tilsynsfunn, straffesaksinformasjon og informasjon til og fra rapporteringspliktige.

Våren 2026 ble det implementert et nytt rapporteringsskjema for rapporteringspliktige som sørger for mer strukturert data som gir bedre analysemuligheter.

Innføring av digitale anmeldelser for bedrageri er også noe som vil bidra til økt kriminalitetsforståelse. I tillegg er en helt ny analyseplattform i tilknytning til hvitvaskingsregisteret under utvikling. Den forventes å bli et kraftig verktøy for både operativ og strategisk analyse.

Samarbeid og gjennomføringsevne

Fremtidig risikoreduksjon vil i stor grad avhenge av gjennomføringsevne. Norge har et relativt robust antihvitvaskingsregime, men effekten svekkes dersom ansvar er fragmentert, informasjon ikke deles, eller saker stopper opp mellom forebygging, analyse, tilsyn, etterforskning og reaksjon.

Det bør derfor legges vekt på tettere samarbeid mellom offentlige myndigheter, rapporteringspliktige og relevante private aktører. Offentlig-privat samarbeid har allerede vist verdi, men bør videreutvikles med tydeligere prioriteringer og bedre operativ innretning. I denne sammenheng er det med bakgrunn i en arbeidsgrupperapport om offentlig-privat samarbeid, fremmet forslag om å opprette en pilot for en samvirkeenhet for offentlig-privat samarbeid høsten 2026.

> Når penger, varer og tjenester krysser landegrenser, blir det større avstand mellom det opprinnelige lovbruddet og midlene som senere brukes eller flyttes

DEL 3

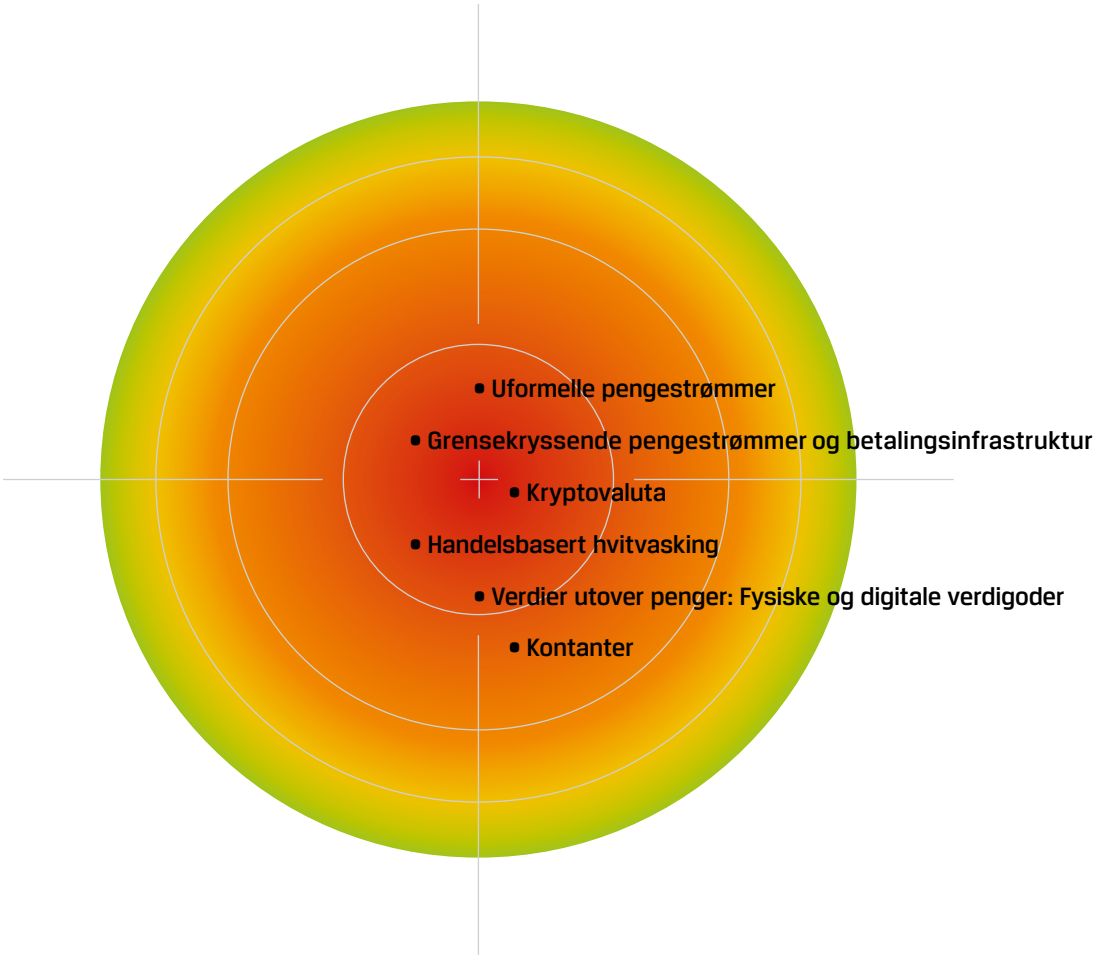
PENGESTRØMMER

Foto: Pexels

Innledning

Del tre av rapporten fokuserer på pengestrømmer ved å se på grensekryssende betalingsstrømmer samt andre typer grensekryssende verdiflyt som kontanter, kryptovaluta og varer gjennom handelsbasert hvitvasking. Sistnevnte markerer overgangen fra overordnede pengestrømmer og hvitvasking til del fire som beskriver mer spesifikke fremgangsmåter for hvitvasking.

FATF beskriver tre hovedmåter å hvitvaske på: (1) gjennom det finansielle systemet, (2) gjennom fysisk forflytning av kontanter, og (3) gjennom fysisk forflytning av varer, ofte omtalt som handelsbasert hvitvasking.[13] I tillegg kommer flyt av virtuelle verdier, som kryptovaluta, som i praksis fungerer som et fjerde spor.



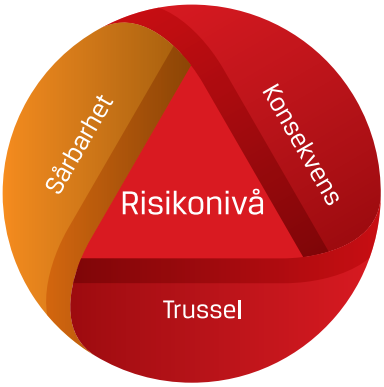
13 FATF, *Trade Based Money Laundering- Trends and Development*, (FATF, 2020).

Pengestrømmer

GRENSEKRYSSENDE PENGESTRØMMER OG BETALINGSINFRASTRUKTUR

Grensekryssende betalinger gir gode muligheter for hvitvasking. Når penger, varer og tjenester krysser landegrenser, blir det større avstand mellom det opprinnelige lovbruddet og midlene som senere brukes eller flyttes. Det gjør pengestrømmene vanskeligere å spore og lettere å skjule i store, legitime transaksjoner. I tillegg kan det utfordre politisamarbeid på tvers av jurisdiksjoner.

Tolletatens analyser[14] av perioden 2022–2025 viser at betalingsstrømmene til og fra Norge er større enn det som fullt ut kan forklares av registrert vare- og tjenestehandel. Dette kan ha legitime forklaringer som lån, investeringer, statistiske avgrensninger og andre finansielle midler til ikke-finansielle foretak.[15] Samtidig viser det at grensekryssende betalingsstrømmer gir et handlingsrom der ulovlige midler kan skjules. Hovedbildet er at Norden, EU og Europa for øvrig dominerer både betalinger, varehandel og tjenestehandel. Det er også identifisert betalinger til utlandet som ikke direkte kan knyttes til konkrete handelsoppgjør.



14 Analysene omfatter betalingsstrømmer fra private personer og ikke-finansielle foretak, samt tjenestehandel for ikke-finansielle foretak. I varehandelen er skip og energi holdt utenfor, mens sjømat er inkludert.

15 Ikke-finansielle foretak er i Statistisk sentralbyrås statistikk over utenriksregnskapet definert som foretak i andre næringer enn næring. Nettlenke, 22.01.2026: https://www.ssb.no/utenriksokonomi/utenriksregnskap/statistikk/betalingsstrommer-mellom-norge-og-utlandet

Digitalisering gjør grensekryssende transaksjoner raskere, enklere og mer oppdelte. Økt bruk av heldigitale banker, e-pengetjenester og internasjonale betalingstjenester kan gjøre det lettere eller skape behov for, å sende betalinger via tredjeland og mellomledd.[16] Dette øker kompleksiteten, gjør kontroll og etterprøving mer krevende.

Følgende forhold kan indikere skjulte pengestrømmer ut av Norge:

- overføringer fra norsk til utenlandsk bankkonto via digitale betalingstjenester, for eksempel Wise og Revolut
- overføringer til jurisdiksjoner med særskilte skattefordeler
- kontantbevegelser over grensen ved bruk av kurerer, agenter eller andre mellomledd
- beslag av biler, kontanter, gull, klokker og andre lett omsettelige verdigjenstander

Skjevheter mellom rapporterte betalinger og deklarert verdi på varer og tjenester må tolkes med varsomhet. Slike avvik kan være indikatorer på hvitvasking, for eksempel feilprising, sende via tredjeland eller mangelfull rapportering. De kan også ha legitime forklaringer. Datagrunnlaget alene er derfor ikke nok til å fastslå hvitvasking, men det peker på områder med forhøyet risiko.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking gjennom grensekryssende betalinger og pengestrømmer som HØY. Risikonivået påvirkes spesielt av stort volum av transaksjoner, tilgjengelighet og utenlandske aktører.

Trusselen for hvitvasking ved pengeoverføringer til utlandet vurderes som HØY. Sentralt for vurderingen er stort omfang og utsatthet for internasjonale pengestrømmer, noe som skaper handlingsrom for tilsløring.

Sårbarheten vurderes som BETYDELIG. Pengeoverføringer er svært tilgjengelig. Kompleksiteten i betalingskjeder og bruk av flere mellomledd øker sårbarheten for at ulovlige midler kan skjules i legitime strømmer. Særlig kan profesjonelle tilretteleggere utnytte kompleksiteten ved å tilby strukturer, konti eller betalingsløsninger som reduserer synlighet og gjør etterprøving mer ressurskrevende. Ordinære banktransaksjoner er likevel etterrettelig og regulert med system for anti-hvitvask og internasjonalt samarbeid. Dette reduserer sårbarheten.

Konsekvensnivået vurderes som HØYT i hovedsak fordi grensekryssende betalinger er helt sentralt i det finansielle systemet og tillit til systemet er viktig.

16 Behovet for å sende betalinger gjennom tredjeland og mellomledd er i tråd med utbygging av finansielle infrastruktur over hele verden. Behovet påvirkes av hvordan de ulike betalingsformidlerne har organisert seg eller strukturert sin pengeoverføringsinfrastruktur for å håndtere betalinger på tvers av jurisdiksjoner og regioner.

Pengestrømmer

KONTANTER

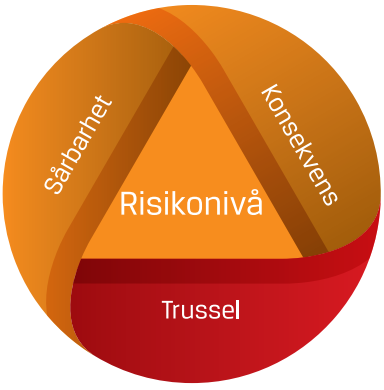
Kontantbeholdningen av norske kroner i omløp varierer gjennom året med økt etterspørsel i ferie- og høytidsperioder. Under pandemiutbruddet våren 2020 økte beholdningen midlertidig. I et langt perspektiv siden midten av 1990-tallet har beholdningen vært stabil, men fra rundt 2017 viser den tegn til nedgang. Ved utgangen av 2024 var rundt 36 milliarder kroner i kontanter i omløp i samfunnet. For fastlands-Norge var andelen kontanter av BNP på 0,9 prosent i 2024.[17]

Mengden kontanter i omløp sier ikke nødvendigvis noe om hvor mye kontanter faktisk blir brukt i betalinger, fordi kontanter både kan brukes til betaling og som verdioppbevaring. Samtidig gir utviklingen i kontantbeholdningen et grovt bilde av tilgjengelighet og potensial for kontantbaserte fremgangsmåter for hvitvasking.

Ifølge rapporten «Nå er det NOK» ble det årlig deklarert inn betydelige kontantbeløp til Norge, rundt 8-10 milliarder kroner, mens deklarert utførsel var betydelig lavere, rundt ti prosent av den deklarerte innførselen.[18] Differansen kan ha vært en indikasjon på at store kontantverdier ble smuglet ut uten deklarering. Dette ble underbygget av beslag i Norden av kontanter på vei sørover i Europa.[19]

Kontanter er et sentralt verktøy i hvitvasking fordi de gir høy anonymitet, er tilgjengelige, transaksjonen skjer umiddelbart og kan bryte pengesporet. Kontanter bærer ingen transaksjonshistorikk, kan oppbevares og brukes uten registrering hos tredjepart, og kan fraktes over lange avstander med relativt lite volum, særlig ved bruk av store valører. Kontantkurerer og mellomledd kan gjøre det krevende å identifisere reell eier.

I Norge er kontanter lite brukt som betalingsform ved store transaksjoner. Dette fører til at kriminelle i større grad må integrere kontantverdier i den digitale økono-



17 Norges Bank, *Det finansielle systemet 2024*, (Norges Bank, 2024).
18 Økokrim, *Nå er det NOK – kontanter i den kriminelle økonomien*, (Økokrim, 2023).
19 Nordic report, *Cashing out. Joint report by the Nordic countries on cross-border money laundering via cash transportation,* (Nordic report, 2024).

mien blant annet gjennom innskudd, veksling, kjøp av verdigjenstander eller konvertering til kryptovaluta.

Forbrukere kan betale på salgssteder med kontanter, betalingskort, mobil for eksempel Vipps, Apple Pay, eller faktura, og mellom privatpersoner typisk med kontanter, Vipps eller nettbank. Dette gir flere overgangspunkter der kontantmidler kan «digitaliseres». Det finnes også aktører som har spesialisert seg på digitalisering eller konvertering av kontanter for kriminelle der man unngår konvensjonelle banker. Disse tilbyr blant annet flere nye metoder for plassering og anvendelse av kryptovaluta.

Faktaboks *Kontanter*

Kontantbetaling over 40 000 kroner er forbudt for forhandlere av gjenstander (kontantforbudet[20]), og etter en endring gjeldende fra 1. oktober 2024 setter finansavtaleloven grensen for kontantbetaling til 20 000 kroner.[21]

Spesifikke endringer

Fra 2023 ble det innført restriksjoner og en praksis der kontanter som returnerer fra utlandet i liten grad tas imot uten dokumentasjon på midlenes opprinnelse. Dette har gjort hvitvasking via veksling av norske kontanter i utlandet betydelig vanskeligere.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking gjennom kontanter som BETYDELIG. Risikonivået påvirkes spesielt av at kontanter er anonyme og tilgjengelige, selv om det likevel er en noe regulert og upraktisk måte å håndtere verdier på. Volumet av hvitvasking er sannsynligvis mindre med kontanter enn med digitale penger og handelsbasert hvitvasking.

Trusselen vurderes som HØY. De kriminelles behov for å håndtere og hvitvaske kontanter vurderes fortsatt som stort, men modus endres. I Norge ser kontanter ut til å spille en større rolle i plasserings- og i tidlig tilsløringsfase av hvitvaskingen, før verdier flyttes ut gjennom andre kanaler for å kunne integreres og anvendes. Kriminelle nettverk benytter fortsatt kontanter i sin økonomi der hvitvasking er en del av økosystemet.

Aktuelle modus er blant annet kontantinnskudd utført av privatpersoner, kontantinnskudd etterfulgt av valutauttak eller kjøp av valuta, høye kontantinnskudd hos virksomheter, veksling til kryptovaluta, uregulert vekslingsvirksomhet, kjøp av verdigjenstander med kontanter og overføring til utlandet via betalingsforetak.

20 Hvitvaskingsloven kap.2 § 5.
21 Finansavtaleloven § 2-1.

Foto: iStock

Sårbarheten vurderes som BETYDELIG. De nye restriksjonene på innførsel av kontanter, kan ha ført til redusert utførsel av norske kontanter, og derfor til økt trykk på kontantinnskudd i Norge. Når norske kroner ikke like lett kan veksles i utlandet, blir det også mer attraktivt å konvertere kontanter til andre verdier før utførsel for eksempel gjennom utenlandsk valuta, gull, klokker, kryptovaluta eller biler. Det gir også et marked for å tilby tjenester for håndtering og konvertering av kontanter, deriblant «kontant til krypto»-tjenester. Kontanter er fortsatt en aktuell metode for å bryte spor, men med økt betydning av koblingspunkter mot digital økonomi som konto, kort, betalingsforetak, kryptovaluta og verdigjenstander.

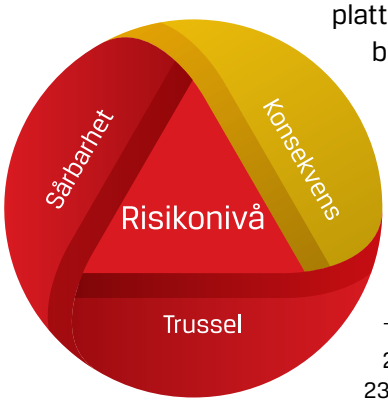
Konsekvensnivået vurderes som BETYDELIG. Med utgangspunkt i hvor stor andel av økonomien som er kontant og «gapet» på innførsel av norske kroner frem til 2023, er omfanget av hvitvasking av norske kontanter mindre enn områder som digitale penger og handelsbasert hvitvasking.

Pengestrømmer

KRYPTOVALUTA

Kryptovaluta benyttes i hvitvasking fordi den har global rekkevidde og tillater hurtige transaksjoner på tvers av landegrenser og pseudoanonymitet. I praksis brukes kryptovaluta både som betalingsmiddel i kriminelle markeder, som oppgjørsform i svindel og som verktøy for tilsløring av verdiers opprinnelse gjennom kjedede transaksjoner.

Kjernen i fremgangsmåten er ofte rask forflytning av verdier mellom aktiva og plattformer. Midler kan flyttes fra bank til kryptovaluta, også via bankkort, byttes til *stablecoins*, sendes via *broer*[22] mellom *blokkjeder* og deretter videre til høyrisikobørser, *P2P-kanaler* eller *OTC-ledd*[23]. *Pengemuldyr* og identitetsmisbruk gir tilgang til kontoer og kort som gjør første ledd mindre synlig. *Stablecoins* beskrives som særlig attraktive i bedragerisaker på grunn av stabil pris og lav friksjon, mens *privacy coins* i større grad brukes selektivt som anonymitetsforsterker, ofte ved mindre beløp eller i tidlig fase. Norske ofre for kriminalitet eksponeres særlig via digitale plattformer, og investeringssvindel pekes ut som en dominerende driver internasjonalt. På cyberområdet beskrives en utvikling der *løsepengevirus* og større *hacks* inngår i mer komplekse betalingsløp.



22 På engelsk: bridges.
23 Over the counter.

Datagrunnlaget for Norge omtales som begrenset, og det legges derfor vekt på internasjonale indikatorer og trendbeskrivelser. Internasjonale kilder viser at volumet for svindel internasjonalt sank fra i underkant av 17 milliarder USD i 2022 til i underkant av 11 milliarder USD i 2024, og at Nord-Korea tilskrives omtrent 35 prosent av hackerelatert utbytte, om lag 800 millioner USD, i de refererte tallene.[24]

Ifølge Skatteetaten oppga 73 000 skatteytere kryptoverdier i skattemeldingen 2024, med en samlet formue på ca. 40 milliarder.[25] Det faktiske beløpet på verdier plassert i kryptovaluta er formentlig større, og viser hvor vanlig det har blitt.[26]

Spesifikke endringer

Siden 2022 beskrives et skifte fra utstrakt bruk av sentraliserte *miksere* til mer modulære teknikker som inkluderer *token-swaps*, *brotransaksjoner* og *kjedehopping*[27]. Dette øker tempoet og gjør sporing vanskeligere fordi midler fragmenteres og flyttes mellom *blokkjeder.*

EUs regelverk for kryptoaktiva, -utstedere og -tjenesteleverandører, «Markets in Crypto-Assets» (MiCA), ble innført i Norge gjennom kryptoeiendelsloven. Regler om *stablecoins* ble innført i juni 2024, og de fleste reglene ble innført i løpet av 2025.

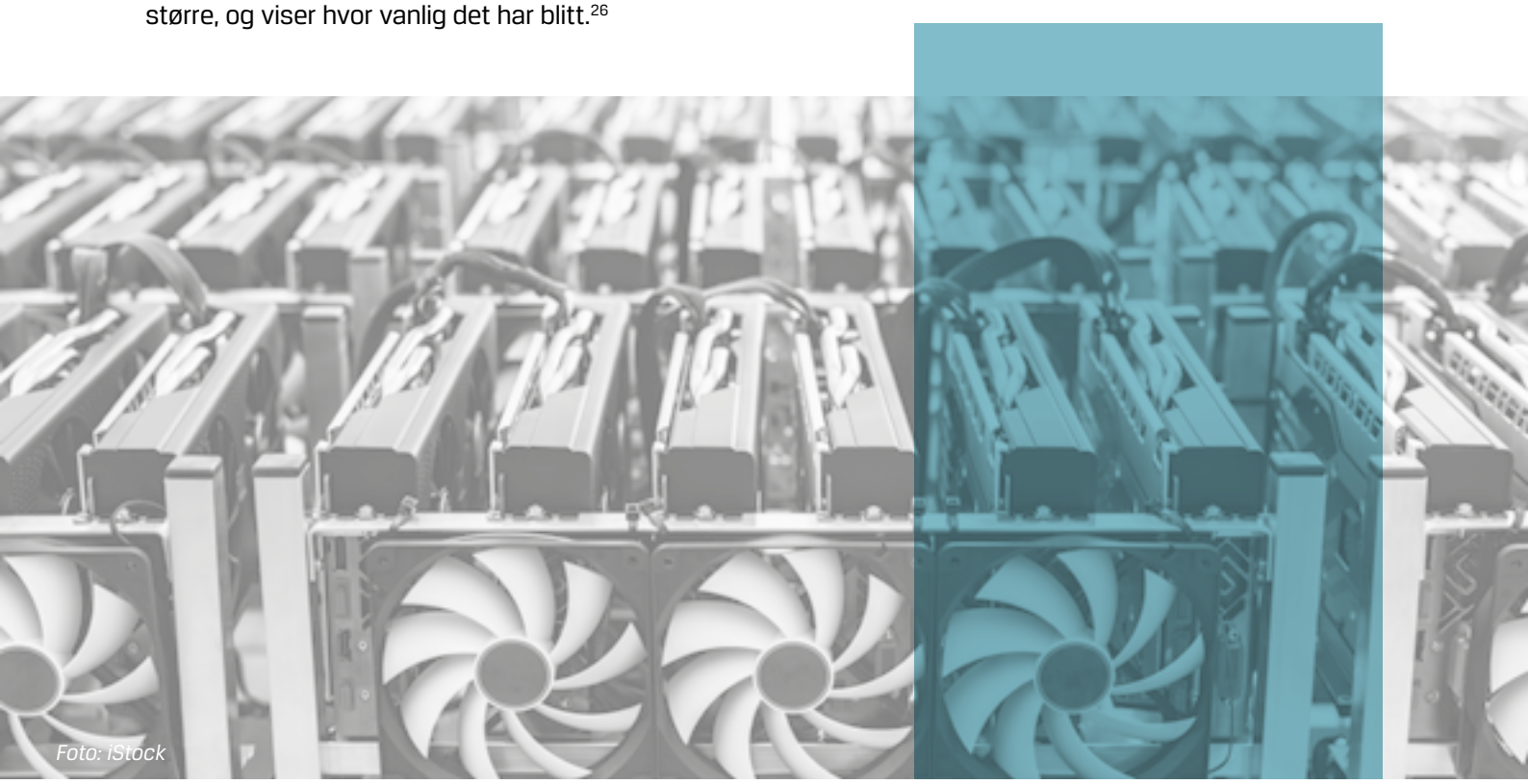


Foto: iStock

24 TRM Labs, *Crypto Crime Report February 2025*. Nettlenke, 06.01.2026: https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report

25 Nettlenke, 28.10.2025: https://e24.no/boers-og-finans/i/1Mgz1q/krypto-boom-nordmenn-hadde-40-milliarder-i-verdier

26 Skatteetaten. Frigitt: 28.10.2025, Pressemelding: *Økning i antall som rapporterer krypto i skattemeldingen* - Skatteetaten.

27 På engelsk: chain hopping.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking med kryptovaluta som HØY. Risikonivået påvirkes spesielt av stort volum, at kryptovaluta er mer tilgjengelig enn tidligere, og at kapasitet blant kriminelle på metoden er stor. Selv med bedre regelverk og kontroll gir kryptovaluta fortsatt mulighet for anonymisering. Kriminalitet som tjeneste[28]-aktører tilbyr tjenester for både plassering, tilsløring og integrering til og fra kryptoverdier og andre verdityper. Både straffesaker og annen informasjon underbygger at kriminelle nettverk bruker kryptovaluta som metode for hvitvasking.

Trusselen vurderes som HØY, særlig fordi teknologien muliggjør rask og grenseløs forflytning av verdier, og fordi profesjonelle flerlags nettverk kombinerer kryptovaluta med tradisjonelle kanaler som bankkonto, kort, foretak og varer. Statlige og halvstatlige aktører bidrar til økt tempo og kompleksitet.

Tiltak som frysing av kryptovaluta, sanksjoner og bedre analyseverktøy har effekt, men trusselaktører har høy kapasitet og omstiller seg raskt gjennom for eksempel plattformbytte, kjedebytte, bruk av høyrisikojurisdiksjoner eller *P2P-kanaler*.

Sårbarheten vurderes som HØY. For Norge fremheves en særlig utfordring med at eksponering importeres gjennom utenlandske virtuelle tjenestetilbydere[29], heldigitale banker og *fintech-plattformer*. Dette kan svekke nasjonal synlighet og gjøre informasjonsinnhenting og samarbeid mer krevende. Samtidig er kunnskap og kunnskapsdeling hos kontrollorgan og samarbeidende aktører god. Det er økende rapportering til hvitvaskingsregisteret og det etterforskes flere straffesaker hvor det er gjort beslag og inndragning.

Konsekvensnivået vurderes som MODERATE. I Norge er ikke virtuell valuta en sentral del av det finansielle systemet. Det er likevel et økende volum og betydelige midler plassert i virtuelle valuta eller andre virtuelle verdier.

28 På engelsk: crime-as-a-service (CaaS).
29 På engelsk: virtual asset service providers (VASP).

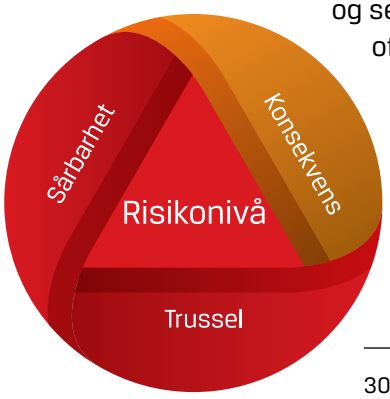
Foto: iStock

Pengestrømmer

VERDIER UTOVER PENGER: FYSISKE OG DIGITALE VERDIGODER

Hvitvasking handler ikke bare om kontanter, kontooverføringer og kryptovaluta. Flere verdityper kan fungere som bærere av verdi som kan skjules, flyttes og senere omsettes til penger eller andre verdier. Eksempler er gull, kjøretøy, kunst, eiendom, gavekort og luksusvarer som blant annet design, merkeklær eller klokker.

Digitale verdier kan omfatte *NFT-er*[30], *skins* og virtuelle gjenstander i spill, digitale annonser, apper og andre digitale tjenester. Slike verdier kan kjøpes og selges på tvers av plattformer, ofte med begrenset prisgjennomsiktighet.



Det er også informasjon som peker på at tjenester og andre «fordeler» kan ha økonomisk verdi i hvitvaskings- og korrupsjonskontekst, for eksempel posisjoner, styreverv eller tilgang til beslutningstakere og informasjon.

Enkelte verdigoder blir omhandlet spesielt i del fire, deriblant eiendom og gull.

Spesifikke endringer

Når enkelte kanaler blir vanskeligere, eksempelvis veksling av norske kontanter i utlandet, øker insentivet til å benytte mer portable og omsettelige verdier, særlig der kontroll- og rapporteringsregimer er svakere.

Digitalisering og fremvekst av nye produkter som *tokeniserte* verdier, digitale plattformer og markedsplasser kan skape nye muligheter for verdiflytting og prismanipulasjon, samtidig som etterprøvbarheten kan være lav.

30 Non-Fungible token.

Foto: iStock

Nye markeder kan få relevans, som handel med klimakvoter, der verdier kan flyttes gjennom komplekse aktør- og kontraktskjeder.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til ikke-monetære verdier som HØY. Det er stor variasjon mellom verditypene, men det er sårbarheten som påvirker risikoen spesielt. Den øker når verdier er flyttbare, globale, lett omsettelige og prisfleksible eller vanskelig å verdsette, svakt regulerte eller i liten grad rapportert av aktører som håndterer transaksjonene.

Trusselen for at verdigoder blir brukt i hvitvasking vurderes som HØY. Omfanget er usikkert, men det er godt kjent at kriminelle nettverk bruker gjenstander, eksempelvis dyre klokker, istedenfor penger. Det kan være som betaling til kurerer, bestikkelser eller hvitvasking for eksempel ved at kjøp og salg av verdigjenstander dokumenterer midlenes opphav og på den måten gi dem et legitimt preg. Enkelte varegrupper kan stige i verdi, som også er gunstig ved legitimering av midlene.

Sårbarheten vurderes som HØY. Mange typer verdigoder kan bytte hender uten noen form for registrering og er derfor både anonymt og tilgjengelig. Mange verdigoder egner seg også for prismanipulasjon. Det er vanskelig å avdekke transaksjoner av ting - både for rapporteringspliktige og kontrollinstanser. Blant annet fordi det kan gjemme seg i globale handelsstrømmer som har enorme volumer.

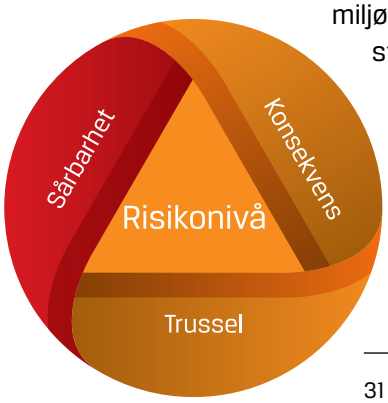
Konsekvensnivået vurderes som BETYDELIG. Nivået varierer etter hvilke verdigoder som benyttes. Noen markeder, eksempelvis eiendom har en grunnleggende funksjon i samfunnsstrukturen. Andre markeder vil lide tillitstap som går ut over driften til seriøse aktører, eksempelvis i kunstmarkedet.

Pengestrømmer

UFORMELLE PENGESTRØMMER – FRA DELINGSØKONOMI TIL ILLEGAL BANKVIRKSOMHET

Ved siden av det formelle finansielle systemet finnes et bredt spekter av uformelle og halvformelle kanaler. Mange er i utgangspunktet legitime delings- og plattformøkonomier: kjøp og salg via Finn.no, Facebook eller Tise, pengeinnsamling via Spleis/GoFundMe, abonnement og gaver via Patreon/OnlyFans, utleie via Airbnb eller Finn osv. Slike kanaler kan brukes til å splitte opp betalinger, kamuflere formål eller skape tilsynelatende legitime transaksjoner mellom privatpersoner og mange små mottakere.

Illegal bankvirksomhet[31] omtales som betalingssystemer som opererer ved siden av formelle institusjoner innen sektoren betalingsforetak. Hawala er et kjent begrep som knyttes særlig til miljøer med svak finansiell infrastruktur, der oppgjør kan skje via kontanter eller digitale overføringer gjennom mellommenn. I Norden er også kinesisk illegal bankvirksomhet aktuelt.



31 På engelsk: underground banking.

Spesifikke endringer

Vekst i digitale plattformer og økt tilgjengelighet av finansielle plattformer som opererer på tvers av grenser, gjør at uformelle kanaler lettere kan kobles til formelle betalingsmidler som kort, e-penger og kryptovaluta, og at volum på transaksjoner kan øke uten tilsvarende økning i myndigheters innsyn.

Der enkelte aktører har konsesjon eller opererer i gråsoner, kan det oppstå en fragmentert etterlevelse av hvitvaskingsregelverket og varierende kvalitet på kundetiltak, noe som utnyttes av aktører som ønsker å gå under radaren og oppnå anonymitet overfor rapporteringspliktige institusjoner. Handel via sosiale medier og bruk av gavekort og funksjoner for digitale verdier gjør *smurfing* mulig også uten tradisjonelle bankoverføringer.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking gjennom uformelle pengestrømmer som HØY. Risikonivået

> Uformelle kanaler brukes ofte i kombinasjon med andre metoder

påvirkes spesielt av endring i rapportert omfang og potensialet knyttet til systemenes sårbarheter.

Trusselen vurderes som HØY. Omfanget av hvitvasking ved bruk av uformelle plattformer er økende. Metoden omfatter ofte internasjonale betalingsstrømmer samt store plattformer kontrollert av internasjonale kommersielle aktører. Illegal bankvirksomhet fremstår som svært godt organisert, i mange tilfeller av organiserte nettverk eller samarbeidspartnere.

Sårbarheten vurderes som HØY. Metodene oppleves ofte tilgjengelige for relevante grupper og gir en viss grad av anonymitet. Sårbarheten ligger særlig i at rapporteringspliktige kan se en overføring til en plattform, men ikke endelig mottaker eller hele transaksjonskjeden. Plattformene kan samtidig være registrert i jurisdiksjoner med begrenset informasjonsdeling.

Uformelle kanaler brukes ofte i kombinasjon med andre metoder som kontanter, foretak og kryptovaluta. Det gjør at tiltak rettet mot ett ledd kan føre til tilpasning og forskyvning til andre ledd snarere enn bortfall av risiko. Transaksjonene berøres ofte kun indirekte av rapporteringsplikt. Effektiv håndtering kan bli krevende hvis det er nødvendig med både risikobasert tilsyn og praktisk samarbeid med plattformer og betalingsformidlere, inkludert tilgang til relevante transaksjonsdata ved mistanke.

Konsekvensnivået vurderes som BETYDELIG. Bruk av uformelle kanaler er ofte en av flere måter å hvitvaske på, men omfanget er svært usikkert. Bruk av tjenester innen delingsøkonomi, for eksempel Finn.no og Spleis, er utbredt. Det vil skade tilliten vesentlig om denne typen tjenester blir utnyttet til hvitvasking.

Illegal bankvirksomhet er utenfor myndighetskontroll og undergraver formelle kanaler. Det kan kobles til ulike hvitvaskingsmetoder som for eksempel handelsbasert hvitvasking med alvorlige konsekvenser.

Pengestrømmer

HANDELSBASERT HVITVASKING

Alle land i verden er involvert i handel og handelsbasert hvitvasking foregår på tvers av et bredt spekter av jurisdiksjoner. Handelsbasert hvitvasking er blant de mest komplekse hvitvaskingsmetodene og er en global utfordring.[32,33] Handelsbasert hvitvasking er prosessen der utbytte fra kriminalitet skjules og legitimeres ved å flytte verdier gjennom handelstransaksjoner. FATF beskriver flere teknikker for hvitvasking, blant annet over- eller underprising av varer og tjenester, fiktive eller overprisede tjenester og manipulasjon av handelsdokumenter.[34] Varer som er mest utsatt for å bli brukt til tilsløring av utbytte, kjennetegnes gjerne ved at de er gjenstand for hyppig omsetning og likviditet, varierer mye i pris, er minimalt regulert, og omsettes på tvers av grenser.

Rundt 80–90 prosent av varetransporten internasjonalt går sjøveien.[35] I EU håndteres rundt 90 millioner containere årlig, mens myndighetenes kapasitet til kontroll anslås å dekke mellom to og ti prosent av volumet. I tillegg kan havner også generelt være sårbare for bestikkelser og innsidebistand, ifølge Europol.[36]

Handelsbasert hvitvasking og annen misbruk av vareflyt kan gjelde både varer og tjenester. Siden tjenester er «immaterielle», kan det være særlig krevende å vurdere om tjenesten faktisk er levert, om prisen og den påståtte

32 National Enhed For Særlig Kriminalitet, Temarapport fra Hvidvasksekretariatet: *Handelsbaseret hvidvask,* (National Enhed For Særlig Kriminalitet, 2022).
33 TI, Global Financial Integrity, Fedesarrollo, *Trade based Money laundering: A global Challenge*. (Transparency International Kenya and ACODE. 2023).
34 FATF, *Trade Based Money Laundering- Trends and Development*, (FATF, 2020).
35 World Bank, 2025. Nettlenke 26.02.2026: https://www.worldbank.org/en/topic/transport/brief/sustainable-development-in-shipping-and-ports
36 Europol, *Criminal Networks in EU ports. Risk and challenges for law enforcement*, (Europol, 2023).

etterspørselen er troverdig. Dette kan gjelde tjenester innen formidling, rådgivning, og IKT-tjenester.

Dersom betalingsoppgjør skjer etter at varen er levert, kan det vanskeliggjøre kontroll av sammenheng mellom vare og betaling i sanntid. Der kontrollregimer for vareførsel, merverdiavgift og finansielle transaksjoner ikke er tett koordinert, kan aktører utnytte «hull» mellom systemene.

Oppdagelse er krevende fordi den internasjonale vareflyten er svært stor. En stor andel av transporten går til sjøs, og kontrollkapasiteten er begrenset. For å avdekke handelsbasert hvitvasking må vareforsendelser, tolldeklarasjoner, faktura og betaling sammenholdes, ofte på tvers av etater og jurisdiksjoner. Det er indikasjoner på handelsbasert hvitvasking blant kriminelle nettverk i Norge, imidlertid mangler data og informasjon fra andre kontrolletater og rapporteringspliktige som kan berike og styrke funnene.

Spesifikke endringer

Digitalisering av banktjenester, fremvekst av heldigitale banker og økt bruk av grensekryssende vekslingstjenester påvirker hvordan betalinger for handel gjennomføres og rutes, og kan øke kompleksiteten i pengestrømmen knyttet til vareflyt.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til handelsbasert hvitvasking som HØY. Risikonivået påvirkes spesielt av omfang og en kombinasjon av fragmentert kompetanse, kontroll og koordinering hos ansvarlige myndigheter.

Trusselen vurderes som HØY. Det er særlig volum og omfang av internasjonal handel og handlingsrommet det medfører, utsattheten for internasjonale pengestrøm og kapasiteten aktørene besitter i sine bransjer som vektlegges.

Sårbarheten vurderes som HØY. Handelsbasert hvitvasking kjennetegnes av lav oppdagelsesrisiko og høyt potensial for verdiflytting gjennom få transaksjoner. Samtidig er datagrunnlag og kompetanse ofte fragmentert mellom toll, politi, banker og andre rapporteringspliktige. I tillegg er det begrenset mulighet for rapporteringspliktige til å verifisere varepriser og handelsdokumenter i sanntid.

Konsekvensnivået vurderes som HØYT. Handelsbasert hvitvasking kan føre til forvrengte økonomiske data, tapte skatteinntekter, konkurransevridning og at Norge brukes som transittland for verdier knyttet til straffbar handling.

"Utnyttelse av virksomhetsstrukturer er en hovedutfordring

DEL 4

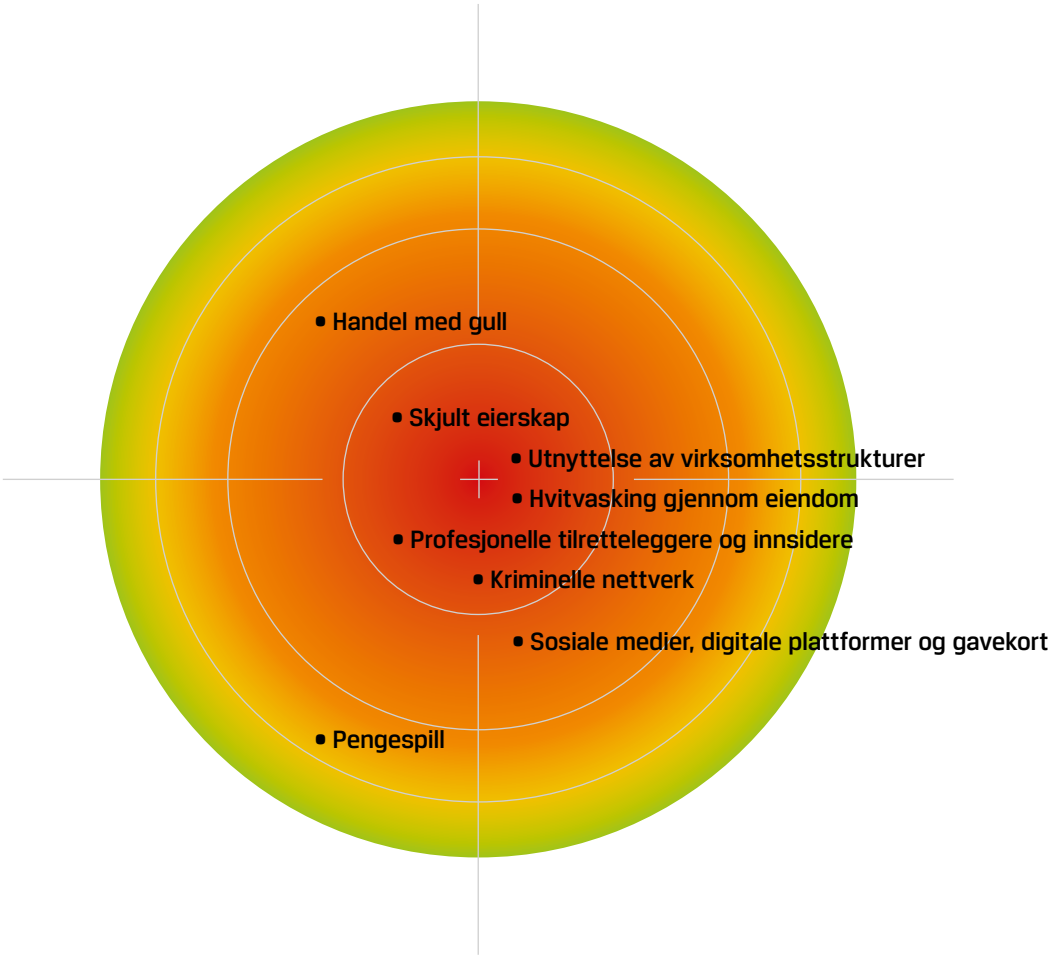
UTVALGTE FREMGANGSMÅTER FOR HVITVASKING

Foto: iStock

Innledning

Del fire av rapporten tar for seg ulike perspektiver og utvalgte fremgangsmåter for hvitvasking og risikovurderer disse.

Fremgangsmåter for hvitvasking kan vurderes fra ulike perspektiver. Et perspektiv er å se på overordnede prinsipper som er felles for flere fremgangsmåter for hvitvasking. Et aktørperspektiv tar utgangspunkt i roller ulike aktører har enten som del av selve hvitvaskingsoperasjonen eller i forbindelse med primærforbrytelsen. Et siste perspektiv er hvitvasking av utbytte generert gjennom kriminalitet i utlandet.



Utvalgte fremgangsmåter for hvitvasking

UTNYTTELSE AV VIRKSOMHETSSTRUKTURER

Lovlige virksomhetsstrukturer kan brukes til å gi ulovlige midler et tilsynelatende legitimt opphav. Dette kan skje gjennom etablering av foretak, bruk av stråpersoner, komplekse eierstrukturer og skjult eierskap i flere jurisdiksjoner. Teknologisk utvikling muliggjør lengre og mer sofistikerte fakturakjeder, der tilsynelatende troverdig dokumentasjon kombineres med reelle banktransaksjoner. Dette kan øke kvaliteten på opphavstilsløringen og gjøre avdekking mer ressurskrevende.

Fiktiv fakturering er en særlig relevant fremgangsmåte i arbeidslivskriminalitet, men kan også inngå i nesten alle typer kriminalitet som omfatter foretak. For eksempel kan en aktør med reelt arbeidsgiveransvar motta fakturaer fra en underleverandør som ikke faktisk har levert tjenestene det faktureres for. Pengestrømmen preges av store, raske overføringer, ofte til utlandet, og det benyttes stråpersoner i styrende roller.

Et dokumentasjonsbasert eksportregime innebærer at kontrollen i stor grad bygger på oppgitte opplysninger, fremfor fysiske kontroller av varepartiene. Dette kan redusere sannsynligheten for å avdekke handels- og dokumentasjonsbasert hvitvasking.

Det skilles også mellom lovlig internprising, som er en form for skatteplanlegging, og handelsbasert hvitvasking. Internprising er i utgangspunktet et lovlig verktøy for multinasjonale konsern, men kan i noen tilfeller misbrukes dersom formålet er å skjule eller omdanne utbytte fra kriminalitet til å fremstå som lovlige midler.

Sårbarheter i ulike organisasjonsformer

Aksjeselskap – AS – egner seg til hvitvasking primært for å skape legitimitet og fordi ansvaret for AS-ets handlinger ikke er personlig, med noen unntak. Det er forholdsvis billig, særlig siden aksjeinnskuddet hos kriminelle kan fungere som et kortsiktig lån de tapper ut med det samme AS-et er registrert.

Enkeltpersonsforetak – ENK – er mest brukt ved arbeidslivskriminalitet fordi det er lave kostnader ved å opprette, mindre formelle krav ved registrering og rapportering, og overfører ansvar fra arbeidsforhold til selvstendig næringsvirksomhet. ENK kan innebære en personlig risiko, men kan også utnyttes av personer som ikke har til hensikt å være i Norge eller ved misbruk av annen persons ID. ENK vil ofte fremstå mindre seriøst enn AS, men vil gi kriminelle et skinn av legitimitet, blant annet i form av eget organisasjonsnummer. I praksis kan ENK brukes uavhengig av personen registrert som innehaver.

Norskregistrert utenlandsk foretak – NUF – gir muligheter for komplekse hvitvaskingsmodus fordi det er under en utenlandsk jurisdiksjon. NUF ble særlig brukt tidligere for å unngå kapitalinnskudd og revisjonsplikt. Nå er det heller ikke revisjonsplikt i Norge for små AS og med lavt kapitalinnskuddet er forskjellene fra AS mindre.

Foreninger/lag/innretning – FLI – er en enhetstype hvor det er sårbarheter knyttet til hvitvasking, inkludert lite kunnskap i kontrollorganer. Hvor utstrakt hvitvasking er i tilknytning til denne organisasjonsformen er ukjent. Enhetstypen har flere egenskaper som kan gi handlingsrom for hvitvasking. De mottar blant annet organisasjonsnummer og gir en fasade av legitimitet. I tillegg har de andre formål enn næringsvirksomhet og er ikke underlagt tilsyn. Siden det er mange FLI, er det enkelt å gjemme seg i mengden. Fra et trusselperspektiv er det kjent at flere kriminelle aktører har roller i FLI. I tillegg har FLI vært brukt i uformelle betalingstjenester som for eksempel hawala.

Informasjonsboks
Kriminelle nettverk og selskapsstrukturer

Kriminelle nettverk og selskapsstrukturer

Det er informasjon om at kriminelle nettverk bevisst etablerer selskaper innen en bestemt næringskode. Dette gir dem mulighet til å opptre som underleverandører for større, seriøse tilbydere av samfunnskritiske produkter og tjenester. Ved å få innpass hos disse aktørene får de tilgang til sensitiv informasjon om potensielle ofre, noe som setter dem i stand til å målrette kriminalitetsutøvelsen. Denne informasjonen brukes deretter til alvorlig økonomisk kriminalitet, herunder grov hvitvasking, fiktiv fakturering, misbruk av stønadsordninger, stråpersonvirksomhet, bedrageri og svart arbeid. I en rekke av tilfellene er det indikasjoner på at aktørene er knyttet til kriminelle nettverk med internasjonale forgreininger og betydelig voldspotensial.

Spesifikke endringer

Ingen spesifikke endringer siden NRA 2022.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking gjennom virksomhetsstrukturer som HØY. Risikonivået påvirkes spesielt av omfang og utstrekning. Det har også knytninger til handelsbasert hvitvasking, og er i tillegg en inngangsport til flere ulike modus. Videre er selskapsstrukturer en viktig del av økonomien som gjør konsekvensene av å bruke selskaper til hvitvasking alvorlig.

Trusselen vurderes som HØY. Kompleksiteten i og kapasiteten for hvitvasking gjennom virksomheter varierer mellom aktuelle bransjer og forretningsmodeller. Hvilke selskapsformer som brukes, varierer også ut fra modus. Transaksjoner og generell aktivitet gjennom foretak blir i samfunnet oppfattet som mer legitimt. Bruk av foretak gir økt trussel ved at foretak er egne subjekter som gir avstand mellom aktiviteten som utøves i foretakets navn, og dem som reelt misbruker foretaket. Denne avstanden forsterkes så av å sette inn stråpersoner som eiere og rollehavere.

Sårbarheten vurderes som HØY. Virksomhetsstrukturer og dokumentasjonsbasert hvitvasking gir kriminelle mulighet til å fremvise kontrakter, lån og fakturaer som skaper tvil om midlenes opprinnelse, selv der den underliggende aktiviteten er fiktiv eller manipulert. Dette kan redusere sannsynligheten for oppdagelse og øke ressursbruken i kontroll og etterforskning. Sårbarheten forsterkes når de som vokter inngangen til de lovlige systemene, såkalte portvoktere, som for eksempel bank,

Foto: iStock

revisor, regnskapsfører, advokat eller betalingsforetak, ikke har tilstrekkelig innsikt i den reelle aktiviteten, eller når informasjon om reelle rettighetshavere er vanskelig tilgjengelig på grunn av utenlandske strukturer.

Konsekvensnivået vurderes som HØYT. Virksomheter er en viktig del av samfunnsstrukturen og misbruk kan undergrave systemet og skade tilliten. De ulike organisasjonsformene treffer på ulike konsekvensindikatorer. Det samme gjelder hva bruken av virksomheten omfatter. Eksempelvis kan konkurs og tømming av foretak treffe på flere indikatorer. Foretak kan brukes til innfasing av midler, til å oppnå kreditt eller likviditet og utføre uttak, før ansvar skyves over på stråpersoner. Det kan få personlig konsekvenser hvis sårbare personer og arbeidstakere utnyttes. Det kan også gi økt økonomisk skade og belastning på kontroll- og straffesakskjeden.

Utvalgte fremgangsmåter for hvitvasking

SKJULT EIERSKAP

I et forenklet hvitvaskingsperspektiv kan utenlandske jurisdiksjoner og skjult eierskap knyttes til de tre fasene (1) plassering, for eksempel ved oppsamling og sikring av utbytte, (2) tilsløring gjennom skallselskaper, truster og distanse, og (3) integrering gjennom investeringer, eiendom, betalingskort, nye betalingstjenester.

Ulike jurisdiksjoner har ofte ulike roller. Større forvaltningssteder kan brukes til forvaltning av midler, mens andre ofte brukes i plasserings- eller tilsløringsfasen gjennom etablering av skallselskaper og komplekse eierskapsstrukturer. Når opphavet er tildekket, kan integrering skje gjennom investeringer og forbruk i normalskatteland.

Verktøy som kan redusere informasjonsinnholdet i betalingssporet, er blant annet virtuelle IBAN-løsninger, kryptovaluta og engangskort. Videre kan også agenter for utenlandske betalingsforetak legge til rette for at kun samletransaksjoner blir synlige slik at reell avsender eller mottaker blir skjult uten direkte innhenting av kontoutskrifter.

Spesifikke endringer

Internasjonale standarder for informasjonsutveksling og registre over reelle rettighetshavere har gitt økt innsyn i eierkjeder og finansielle konti.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking gjennom skjult eierskap som HØY. Risikonivået påvirkes spesielt av omfanget, bruken av profesjonelle tilrettelegge-re, sårbarheten i offentlige registre og innrapporter-ingsordninger. Dette er et kjent fenomen, hvor det knytter seg moderat usikkerhet til vurderingen. Den største usikkerheten knytter seg til hvilke nye verktøy som

tas i bruk for å skjule eierskap, og hvor effektive og utbredte de er.

Trusselen vurderes som HØY. Det er potensialet i det økonomiske omfanget, bruken av profesjonelle tilretteleggere og teknologiske løsninger som kan skjule spor som trekker trusselen opp. Det finnes også profesjonelle tilretteleggere som i tillegg tilbyr krypteringsløsninger, både innenfor kommunikasjon, datalagring og betaling – i tillegg til en rekke andre verktøy som kan opprettholde anonymitet.

Sårbarheten vurderes som HØY. Til tross for informasjonsutveksling og registre over reelle rettighetshavere kan likevel komplekse eierkjeder tilbys av profesjonelle tilretteleggere som et aktuelt verktøy for å skjule hvem som er reell eier av verdier. Det kan blant annet skje gjennom jurisdiksjoner som har en mangelfull oppfølging av internasjonale standarder innen antihvitvasking og informasjonsutveksling. Manglende transparens i eierstrukturer og mangelfull oppfølging av internasjonale standarder i enkelte jurisdiksjoner gjør det utfordrende å avdekke reelle forhold og begrense hvitvasking. Dette øker sårbarheten. Sårbarheten forsterkes ytterligere av at nye metoder og verktøy stadig utvikles i takt med mottiltakene, noe som stiller store krav til både kontrollmekanismer og internasjonalt samarbeid.

Norske registre har også vesentlige sårbarheter. Eierskapsregistrene gir ikke klar oversikt over utenlandske eiere, og det er vanskelig å følge eierskap ut av landet – særlig når flere ledd er involvert.[37] I tillegg oppdateres det norske aksjonærregisteret kun en gang i året. Slike svakheter kan utnyttes både av norske rettighetshavere for å skjule utbytte fra skattekriminalitet, og av utenlandske aktører for å omgå sanksjoner.

Konsekvensnivået vurderes som HØYT. Sakene gjelder ofte store beløp og hvitvasking kan føre til omfattende økonomiske konsekvenser. Skjulte verdier dreier seg både om verdier i Norge som eies gjennom en kompleks eierstruktur, og verdier i utlandet, i såkalte skatteparadiser. Forskning viser at omfanget av verdier i skatteparadiser ikke har blitt redusert, og at en stor andel av rapporterte finansielle konti eies gjennom komplekse eierstrukturer.[38] Det store omfanget av profesjonelle tilretteleggere og tjenester for hemmelighold indikerer at dette fortsatt er en sårbarhet som utnyttes i betydelig grad og kan undergrave tilliten til systemet.

37 Skatteetaten og Brønnøysundregistrene, *Konseptvalgutredning eierskapsopplysninger aksjer*, (Skatteetaten og Brønnøysundregistrene, 2024). Se også Kartverket, *Konseptvalgutredning eierskap til fast eiendom*, (Kartverket, 2025).

38 Boas et al, Did Automatic *Exchange of Information End Bank Secrecy? Evidence from Aggregate Administrative Data*, (Boas et al, 2026).

Utvalgte fremgangsmåter for hvitvasking

MULDYR OG IDENTITETSMISBRUK

Pengemuldyr, stråpersoner i foretak og misbruk av andres kort og identiteter er metoder for å bruke tredjepart til å redusere synlighet og flytte risiko fra bakmenn til utskiftbare ledd. Muldyr kan rekrutteres med lovnad om enkel profitt. Rekruttering kan skje blant ungdom, familiemedlemmer og utlendinger som har lite forutsetninger for å forstå systemet.

Rekruttering av sårbare personer som muldyr, og bruk av stråpersoner i styrende roller i foretak fremstår som sentralt for å skalere opp kapasiteten og redusere risikoen for kjerneaktørene.

Identitetsmisbruk kan gi tilgang til bankforhold, lån, etablering av foretak og abonnementer som senere inngår i hvitvaskingskjeder. Dette er relevant for lånebedragerier, opprettelser av ENK og andre strukturer som kan gjenbrukes i flere moduser. En bakenforliggende årsak til at «personer» hjelper eller blir misbrukt av kriminelle, er hvordan identiteter blir skapt. Kilden til identiteter er ofte utenlandske personer som er midlertidige arbeidsinnvandrere eller personer på studentvisum. Disse blir registrert i folkeregisteret og tildelt en eID. Når personer hentes til Norge ved hjelp av kriminelle, vil det ofte være den kriminelle «arbeidsgiveren» og kontaktpersoner som i realiteten kontrollerer eID-en. Disse eID-ene benyttes så i samme kriminelle miljø eller tilbys andre som en *kriminell tjeneste*[39].

Det er en utvikling der sosiale medier blir brukt til rekruttering av muldyr. Lite endringer knyttet til metoden viser hvor effektiv den er.

Forebygging krever både tekniske tiltak som transaksjonsovervåking, identitetskontroller, mønstergjenkjenning og målrettede tiltak mot rekruttering, innsidetrusler og profesjonell medvirkning.

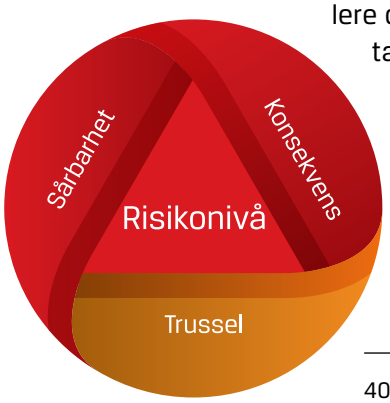
I et risikoperspektiv bør slike aktørroller vurderes som muliggjørende faktorer på tvers av flere metoder, ikke som et eget isolert fenomen.

39 På engelsk: crime-as-a-service (CaaS).

Utvalgte fremgangsmåter for hvitvasking

PROFESJONELLE TILRETTELEGGERE OG INNSIDERE

Profesjonelle tilrettelegger og innsidere kan for eksempel være regnskapsførere, bankrådgivere og advokater. Disse kan muliggjøre hvitvasking ved å åpne kontoer, tilby klientkonto, tilrettelegge for lån eller «lukke øynene» i portvokterroller. Attester, bekreftelser, godkjenninger og vedtak kan også muliggjøre hvitvasking, eksempelvis gjennom legeattester ved forsikringsutbetalinger. Ulike aktører kan opptre som profesjonelle tilrettelegger og tilby kriminelle tjenester. Eksempelvis kan teknologiske tilrettelegger tilby løsninger som gir anonymitet, manipulere dokumenter eller skjuler digitale spor. Tilrettelegger gjør det enklere for flere å bruke avanserte metoder uten spesiell fagkompetanse.



Politiets trusselvurdering 2026 peker på at bank- og finansnæringen er særlig utsatt for innsidevirksomhet. Ansatte kan utsettes for bestikkelser eller press fra kriminelle aktører som har vilje og evne til å benytte seg av personer i nøkkelposisjoner til å gjennomføre kriminelle handlinger. Imidlertid kan ansatte selv også tilby disse tjenestene eller ha tett knytning til kriminelle nettverk. Europol trekker frem at også offentlige ansatte kan være utsatt for samme mekanismer.[40] Tilretteleggeres involvering finnes i mange former og kan beskrives i et spenn fra «helt uvitende», «burde ha skjønt», «lukker øynende» eller «medvirker bevisst til kriminalitet» til at noen er eller blir del av kriminelle nettverk.

Spesifikke endringer

Det er vanskelig å si om omfanget profesjonell tilrettelegging reelt har økt, men flere forhold er avdekket de siste

40 Europol, *The changing DNA of serious and organised crime,* (Europol, 2025).

årene og oppdagelsesrisikoen kan ha økt som følge av bedre kunnskap og oppmerksomhet i offentlig og privat sektor. Samtidig beskrives en utvikling der hvitvasking i større grad settes sammen som «økosystemer» med flere ledd, som øker behovet for kriminelle tredjeparter og spesialiserte tjenester.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking ved bruk av profesjonelle tilretteleggere som HØY. Risikonivået påvirkes spesielt av aktørenes kapasitet, myndighetenes mangel på informasjon og alvorlige konsekvenser som svært ødeleggende for tillit til samfunnsstrukturer. Usikkerheten i vurderingen knytter seg særlig til manglende informasjonsgrunnlag og mørketall.

Trusselen vurderes som BETYDELIG. Selv om mange saker er avdekket, er det mistanke om at problemet er mer utbredt enn det som er avdekket. Kriminelle nettverk har kapasitet til å benytte profesjonelle tilretteleggere ved bruk av nettverk, insentiver eller press. Innsidere kan ha løse eller sterke knytninger til nettverkene. Det er også mulig for kriminelle nettverk å ha langsiktige strategier for å ha egne folk i passende posisjoner.

Teknologisk utvikling gir profesjonelle aktører mulighet til å gjennomføre langt større og mer avanserte handlinger enn tidligere, noe som øker omfanget og gjør avdekking vanskeligere.

Sårbarheten vurderes som HØY. I Norge har arbeidstakere ofte høy grad av autonomi som kan gi handlingsrom for innsidere. I tillegg vil et selskap ikke nødvendigvis tape penger på at det finnes innsidere blant ansatte i ulike roller. Kriminelle som innvilges lån i hvitvaskingsøyemed, er ikke nødvendigvis dårlige kunder så lenge de betjener lånet. Det samme gjelder kjøpere og selgere av eiendom. Det kan tvert imot lede til både økonomiske tap og omdømmetap for arbeidsgiver å avsløre utro tjenere.

Manglende informasjonsgrunnlag gjør det vanskelig å avdekke tilretteleggeres involvering. Sårbarheten forsterkes av at komplekse strukturer og tidlig tilrettelegging ofte går under radaren, samtidig som risikoen for avsløring oppleves som lav.

Konsekvensnivået vurderes som HØYT. Utbredt hvitvasking ved hjelp av innsidere vil ha alvorlige konsekvenser for samfunnet. Tilretteleggere utgjør en usynlig, men avgjørende infrastruktur for den kriminelle økonomien. Deres tjenester binder sammen lovlige og ulovlige aktiviteter og gjør det mulig for kriminelle nettverk å operere effektivt. Dette bidrar til økt omfang av kriminalitet og svekker tilliten til samfunnsstrukturer.[41]

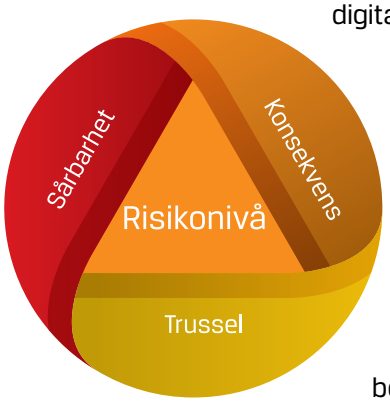
Sosiale plattformer muliggjør ikke bare kommunikasjon, men også overføring av verdier. Noen plattformer tilbyr direkte betaling, mens andre benytter virtuelle eiendeler som kan konverteres til penger. Dette kan brukes til legitime formål, men kan også utnyttes til tilsløring av midlenes opphav og ulovlig betalingsformidling.

41 EOS, *Svarta siffror – en ESO-rapport om den kriminella ekonomins omfattning* - ESO - Expertgruppen för studier i offentlig ekonomi. (EOS, 2026).

Utvalgte fremgangsmåter for hvitvasking

SOSIALE MEDIER, DIGITALE PLATTFORMER OG GAVEKORT

Digitale plattformer, inkludert sosiale medier med betalingsfunksjoner, kan benyttes til hvitvasking. En utfordring er at når midler overføres til en plattform, har rapporteringspliktige begrenset innsyn i videre transaksjonskjede og endelig mottaker; plattformen opptrer som mellomledd. Eksempler på slike tilslørende mellomledd og produkter som kan inngå i samme modus er TikTok, heldigitale banker, Google Pay, gavekort, refundering og annullering av kjøp, utbetalinger fra spillselskaper og andre former for digitale verdiløkker.



Spesifikke endringer

Antallet MF-rapporter som nevner «TikTok» er økende, fra 18 rapporter i 2022 til 89 rapporter i 2024. Antall transaksjoner til TikTok beskrevet i MF-rapporter i materialet økte i perioden 2022–2024 fra rundt 2 600 til 13 000. Undersøkelser i valutaregisteret underbygger også økningen.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking gjennom sosiale medier, digitale plattformer og gavekort som BETYDELIG. Risikonivået påvirkes spesielt av tilgjengelighet, manglende transparens og avgrenset rapporteringsregime.

Trusselen vurderes som MODERAT. Potensialet er stort, men så langt er det ikke avdekket vesentlige summer, selv om enkeltpersoner kan ha høye samlede beløp overført til plattformen. Enkelte av disse er også omtalt i flere MF-rapporter. Digitale plattformer er utsatt for internasjonale pengestrømmer.

Sårbarheten vurderes som HØY. De fleste sosiale medier er lett tilgjengelige. Transaksjoner tilbyr en viss form for anonymitet, i hvert fall for relasjonen mellom avsender og mottaker. Sårbarheten ligger i manglende transparens og begrenset rapporteringsregime. Plattformer kan være utenfor rapporteringsplikt eller etablert i jurisdiksjoner som ikke nødvendigvis utleverer data effektivt. Dette kan gjøre det krevende å identifisere reell mottaker, formål og koblinger til kriminalitet.

Veksten i rapporterte transaksjoner og informasjon fra hvitvaskingsregisteret, indikerer at plattformer i økende grad inngår i mistenkelige betalingsmønstre, særlig der utbytte fra bedrageri kan formidles videre gjennom virtuelle eiendeler og små, hyppige transaksjoner.

Veksten i slike MF-rapporter indikerer at rapporteringspliktige har kunnskap om metoden. Det kan være relevant å avdekke modus som kombinerer banker, kortbetalinger og plattformtransaksjoner i håndteringen av svindelutbytte. Restriktiv informasjonsdeling mellom plattformer, betalingsforetak og myndigheter kan være en sårbarhet også på dette feltet.

Konsekvensnivået vurderes som BETYDELIG. Sosiale medier og delingsplattformer har blitt viktige verktøy for mange. Svekket tillit til disse plattformene vil kunne berøre mange. Foreløpig er omfanget av hvitvasking i disse kanalene lite kjent, men utviklingen fremstår som bekymringsfull.

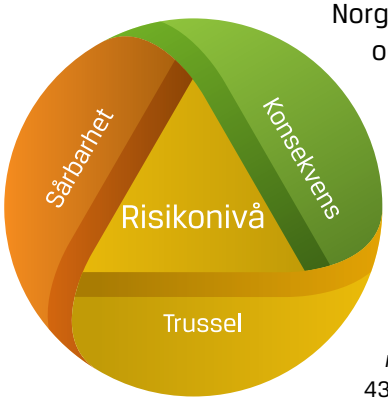
Foto: iStock

> Det er et stort marked av utenlandske pengespill

Utvalgte fremgangsmåter for hvitvasking

PENGESPILL

Lotteritilsynet estimerer at det uregulerte pengespillmarkedet utgjorde mellom 1,7 og 2,0 milliarder kroner i 2025, noe som tilsvarer ca. 13 prosent av det norske pengespillmarkedet.[42] Utenlandske pengespill har ikke de samme taps- og innsatsbegrensningene som norske spillselskap, og vil dermed være mer attraktive å benytte til hvitvaskingsformål. Det er et stort marked av utenlandske pengespill som kasino, poker og oddsspill på internett, som ikke har lov å tilby pengespill i Norge, men som er tilgjengelige og rettet mot Norge.



Spillselskaper som tilbyr pengespill på nett i Norge uten tillatelse, er oftest selskaper som også tilbyr de samme pengespillene i andre land. De fleste nettstedene Lotteritilsynet påla norske internettilbydere å blokkere i 2025, hadde adresse på øya Curaçao. Hos en del av nettstedene kan kryptovaluta eller *skins* benyttes som innskudd.[43]

Norske banker og andre betalingstjenester i Norge har ikke lov til å formidle innsats og utbetaling i pengespill som tilbys av pengespillselskaper uten tillatelse i Norge. For å omgå dette forbudet blir utenlandske betalingsløsninger, blant annet heldigitale banker, benyttet. Det kan også foregå samarbeid mellom spillere for å omgå bankenes kontroll og få utbetalt gevinster på vegne av ulovlige selskaper. Det er også noen spillsel-

42 Lotteritilsynet, *Ansvarligheit og kanalisering hos Norsk Tipping og Norsk Rikstotto, mars 2026*, (Lotteritilsynet, 2026).

43 Lotteritilsynet, *Blokkering av ulovlige pengespillsider 2025*, (Lotteritilsynet, 2025).

skaper som oppretter kontoer i spillernes navn i utlandet for å kunne overføre penger. Spillere risikerer dermed å ha en konto i sitt navn i utlandet, som de ikke har kontroll over.

Spesifikke endringer

Ingen spesifikke endringer siden NRA 2022.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til pengespill som MODERAT. Risikonivået påvirkes spesielt av utenlandske pengespill og bruk av tredjepartsløsninger for overføring av penger og omgåelse av bankenes kontrollmekanismer. Det mangler imidlertid datagrunnlag for markeder som ikke er underlagt hvitvaskingsloven i Norge. Sektorkunnskap, data fra tilsyn og internasjonalt samarbeid viser imidlertid generelt forhøyet risiko for økonomisk kriminalitet hos aktørene som tilbyr pengespill uten tillatelse.

Trusselen vurderes som MODERAT. I Norge er det sportspill, spillterminaler, bingo (hovedspill), lotteri, fysisk kasino og NM i turneringspoker, som er underlagt hvitvaskingsreglene. Poker med lave innsatser i vennelag og andre lavrisikospill, som basarer og foreningslotterier, er ikke underlagt hvitvaskingsregelverket. Det eksisterer i tillegg ulovlige pokerklubber i Norge med høy omsetning. Videre er det de fire siste årene mottatt rundt fire hundre meldinger i hvitvaskingsregisteret fra Malta om nordmenn, hvor de fleste gjelder pengespill. Lotteritilsynet mottar også tips fra spillere som i stor grad videreformidles til politiet dersom det er informasjon om at det er høy omsetning og annen kriminalitet.

Sårbarheten vurderes som BETYDELIG. Lotteritilsynet fører ikke hvitvaskingstilsyn med pengespillaktører som opptrer uten tillatelse i det norske markedet. Det er myndighetene i det landet der spillselskapet har lisens, dersom de har lisens i hele tatt, som har ansvar for å følge opp spillselskapets etterlevelse av hvitvaskingsregelverket. Derfor vil det i praksis være bankene som kan avdekke og sikre at innskudd og gevinster fra utenlandske pengespill ikke har tilknytning til hvitvasking. Det forsterker sårbarheten at det er enkelt og tilgjengelig å omgå regelverket og kontrollmekanismer.

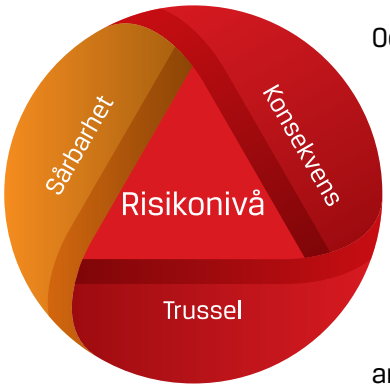
Konsekvensnivået vurderes som LAVT. Det er små samfunnsmessige tap, mens de økonomiske tapene vil for det meste ramme enkeltpersoner.

Foto: iStock

Utvalgte fremgangsmåter for hvitvasking

EIENDOM

Eiendomsmarkedet er attraktivt for plassering og integrering av kapital på grunn av verdistigning over tid, god avkastning, at sektoren er kapitalintensiv, har gunstige skatteordninger og muligheter for skjult eierskap gjennom selskaper, stråpersoner eller utenlandske strukturer. Kjøp og salg av eiendom som metode for hvitvasking gir ofte muligheten til å flytte store summer. Det kan skje ved å blande kriminelt utbytte med lovlige midler, gjennom sammenblanding av privat- og selskapsøkonomi eller ved at hele kjøpet dekkes av midler som stammer fra kriminelt utbytte.



Også samarbeid om uriktig prising kan bidra til hvitvasking, i tillegg til lånebedragerier. Eiendom kan leies ut, faktisk eller fiktivt, og gi legitim inntekt og forklaring på midlenes opprinnelse. Selv om det er mulig å ettergå slike opplysninger er det arbeidskrevende. Hvitvasking kan også skje ved nedbetaling av lån med kriminelt utbytte, oppussing med utbytte fra kriminalitet eller *flipping*.

Kriminelt utbytte fra utlandet plasseres i eiendom i Norge. Omvendt er eiendomsinvesteringer i utlandet en kjent metode for plassering og oppbevaring av kriminelt utbytte fra Norge. Det rapporteres også mistenkelige forhold der midlenes opprinnelse forklares med salg av eiendom i utlandet.

Spesifikke endringer

Ingen spesifikke endringer siden NRA 2022.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking gjennom eiendom som HØY. Eiendom representerer store summer i norsk økonomi, og kan brukes til hvitvasking av kriminelt utbytte gjennom en rekke fremgangsmåter. Det kan også

Foto: iStock

involvere korrupsjon og bruk av profesjonelle tilretteleggere. Risikoen forsterkes av at flere av metodene brukes av kriminelle nettverk.

Trusselen vurderes som HØY. Eiendom knyttes til utbytte fra mange kriminalitetsområder. Det er kjent at kriminelle nettverk bruker eiendom til hvitvasking. Kjøp av eiendom i utlandet, for eksempel Dubai, er også utbredt. I tillegg er det kjent at enkelte tilbyr hjelp eller fasilitering av kjøp av eiendom i utlandet. De siste årene har det vært flere saker med innsidere og korrupsjon knyttet til eiendomskjøp. Videre kan lån eller gevinst knyttet til eiendom også brukes til å finansiere kriminalitet som kjøp av større mengder narkotika.

Sårbarheten vurderes som BETYDELIG. Eiendomsmarkedet er i utgangspunktet regulert og lite anonymt. Likevel er det informasjon om at kriminelle utnytter muligheter som finnes ved bruk av blanko-skjøte og skjult eierskap. Dette forsterker sårbarheten.

Skatteetaten har også identifisert utfordringer knyttet til skattekriminalitet. De viser blant annet til en konseptvalgutredning om eierskap til fast eiendom som Kartverket publiserte i 2025. Der peker de både på manglende kvalitet i registrene og fragmenterte og lite tilgjengelige opplysninger. De mener også at sårbarheter i nasjonale registre utnyttes av kriminelle aktører og at aktører finner nye svakheter hvis kjente modus lukkes.

Konsekvensnivået vurderes som HØYT. Store summer går gjennom eiendomsmarkedet årlig. Dette markedet er også en viktig del av norsk samfunnsstruktur, som i vesentlig grad vil få svekket tillit om det misbrukes til kriminalitet.

Foto: Pexels

Utvalgte fremgangsmåter for hvitvasking

UTBYTTE FRA KRIMINALITET I UTLANDET

Utbytte fra kriminalitet begått i utlandet kan være krevende å avdekke og tolke for rapporteringspliktige. Eksempelvis går en økende andel av utbetalinger fra Skatteetaten til utenlandske bankkonti. Offentlige utbetalinger i ett land, vil ofte fremstå som lovlige i et annet land og det kan være vanskelig å avsløre illegitim opprinnelse for pengene. Videre kan det være begrensninger knyttet til informasjonsutveksling med utlandet.

Norge fremstår ikke som spesielt attraktivt for hvitvasking sammenlignet med andre land. Det har likevel vært noen større saker med hvitvasking av midler fra kriminalitet i utlandet. Fellestrekk er at sakene ofte involverer selskaper og store summer. At hvitvaskingen gjøres via strukturer i Norge synes litt tilfeldig og baserer seg tilsynelatende på faktorer som blant annet bekjentskap.

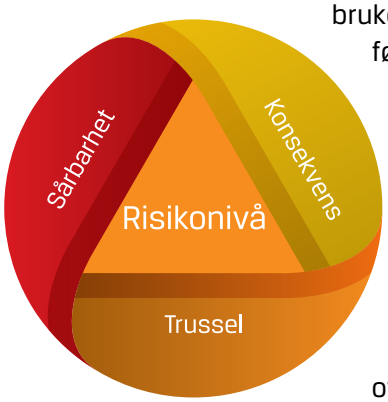
Et eksempel på utbytte fra kriminalitet i utlandet som hvitvaskes via Norge, er Windmill-saken. I 2024–2025 skrev VG om hvordan en slovakisk partitopp skal ha overført minst 90 millioner kroner fra Dubai til telefonsalgfirmaet Windmill på Jessheim. Pengene skal ha hatt et uklart opphav og forsøkt dokumentert som senere ble avslørt som fiktive. Deler av midlene ble brukt til blant annet kjøp av en luksusvilla på den franske rivieraen.[44]

44 Nettlenke, 13.05.2025: https://www.vg.no/nyheter/i/730L68/oekokrim-aksjon-etter-vg-avsloeringer-to-siktet-for-hvitvasking

Utvalgte fremgangsmåter for hvitvasking

HANDEL MED GULL

Gull fremheves som særlig attraktivt i hvitvasking fordi det er globalt akseptert, har høy verdi per volum og kan omsettes relativt lett. Det egner seg både som investeringsobjekt og som oppgjørsmiddel. Handel kan skje med høy grad av anonymitet, blant annet gjennom kontanttransaksjoner. Gull kan inngå i handelsbasert hvitvasking ved at pris, kvalitet eller kvantitet under- eller overrapporteres ved import/eksport, eller ved at fiktive fakturaer brukes til å legitimere pengeoverføringer uten reell vareflyt. *Smurfing* omtales som en sentral metode også her, både ved å spre verdier på flere personer og ved å bruke flere moduser for å gjøre koblingen til kriminalitet mindre synlig. Andre modus kan være veksling, overføringer, kontantuttak og kjøp av varer. Gull kan også smeltes og omformes, noe som gjør det vanskelig å spore.



Spesifikke endringer

Endret praksis i 2023 som vanskeliggjorde veksling av norske kontanter i utlandet, kan ha økt insentivet til å kjøpe og selge gull som alternativ kanal for tilsløring av midlenes opprinnelse og verdiflytting.

Tolletatens tall beskriver betydelige deklarerte volum. For perioden 2022–2024 ble det deklarert innførsel av gullmynter for i underkant av 1,6 milliarder kroner, mens deklarert utførsel var på om lag 322 millioner kroner. For smykker og gullskrap var deklarert innførsel og utførsel i samme periode på henholdsvis i underkant av 7,5 og 7 milliarder kroner. Et fåtall aktører hadde rundt 80 prosent

av markedsandelen for import/eksport av gullmynter.

For 2021 til juli 2025 har antallet beslag økt. Det ble avdekket om lag 300 saker med udeklarert innførsel av gullvarer av privatpersoner, der rundt 80 prosent av beslagene skal være gjort i 2024 og 2025. Estimert verdi er 40–50 millioner kroner.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking ved handel med gull som BETYDELIG. Risikonivået påvirkes spesielt av muligheten for anonymitet samt fraværet av rapporteringsplikt og kontroll.

Trusselen vurderes som BETYDELIG. Gull fremstår som en «bro» mellom kontanter og internasjonal verdiflytting fordi verdien kan konverteres, bæres og realiseres i andre jurisdiksjoner, og dermed kan erstatte kontantutførsel som metode når norske kontanter blir vanskeligere å veksle i utlandet. Kombinasjonen av høy pris per volum, global likviditet og muligheten for anonymitet gjør gull til et høyrelevant verdiobjekt i hvitvaskingsvurderinger, både alene og i kombinasjon med handelsbasert hvitvasking.

Med utgangspunkt i Tolletatens tall fremstår omfanget som ikke ubetydelig, men det er mindre enn flere andre metoder for hvitvasking, eksempelvis kontanter. Noen kriminelle nettverk bruker gullhandel som en av flere hvitvaskingsmetoder.

Sårbarheten vurderes som HØY. At gullforhandlere ikke er rapporteringspliktige utgjør en betydelig sårbarhet fordi det ikke foregår noen kontroll av midlenes opprinnelse. Det er særlig sårbart der kontanter kombineres med kjøp og videresalg av gull.

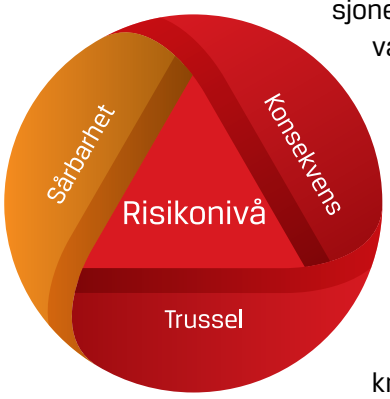
Konsekvensnivået vurderes som MODERAT. Det er formentlig noe økonomisk tap for samfunnet. Slik hvitvasking kan gå utover ryktet og tilliten til bransjen, men fremstår ikke som en viktig del av den finansielle strukturen.

> Gull kan inngå i handelsbasert hvitvasking

Utvalgte fremgangsmåter for hvitvasking

AKTØRPERSPEKTIVET: KRIMINELLE NETTVERK OG HVITVASKING

Organiserte kriminelle og andre grupper bruker en rekke forskjellige fremgangsmåter for å hvitvaske kriminelt utbytte. I dette kapitlet avgrenses nettverksbegrepet til aktører innenfor politiets spesielle satsing mot kriminelle nettverk. Utvalget aktører omtales likevel som stort, med over tusen personer som kjennetegnes av stor organiseringsevne, høy fleksibilitet og i flere tilfeller betydelig voldskapasitet. Tradisjonelt har utbytte og hvitvasking vært tett knyttet til narkotikahandel og kontantintensive strukturer. Det er imidlertid indikasjoner på en endring mot bransjer og kriminalitet med høy profitt og lavere oppdagelsesrisiko, herunder ulike former for bedrageri og cyberstøttet kriminalitet.



En beskrivelse som går igjen i analysene fra hvitvaskingsregisteret, er at hvitvasking i økende grad organiseres som sammensatte økosystemer. Eksempelvis kan kontanter innfases i foretak gjennom fiktive oppdrag og fakturaer. Foretaket kan bygge opp tilsynelatende likviditet, og midler kan tas ut via fiktive lån eller fakturaer før de blir flyttet videre via heldigitale banker eller konvertert til kryptovaluta for utførsel.

Det er informasjon om at mange prioriterte kriminelle nettverk aktivt benytter heldigitale banker og kryptovaluta som del av sin økonomi. Kriminelle kan benytte kryptovaluta for å flytte midler raskt over landegrenser, ofte via flere lommebøker og såkalte *mikse-tjenester* for å redusere sporbarheten. Selv om transaksjoner på *blokkjede* i utgangspunktet er sporbare, forsøker aktørene

å utnytte tekniske muligheter og gå gjennom mange ledd som egen sikkerhetsmekanisme.

Alternative investeringsobjekter som gull, kunst, luksusvarer, klokker og digitale eiendeler kan kjøpes og selges med relativt begrenset kontroll sammenlignet med handel hos tradisjonelle finansinstitusjoner. Manglende regulering av enkelte varehandlere, for eksempel gullforhandlere, gjør disse aktørene til attraktive alternative kanaler for hvitvasking. Det er informasjon om at slike investeringer fortsetter å være høyaktuelle.

Hvitvasking gjennom kjøp av eiendom er en utbredt metode som beskrevet i kapittelet om hvitvasking gjennom eiendom. Informasjon viser at flere store kriminelle nettverk aktivt investerer i eiendom i utlandet som et ledd i å hvitvaske midler.

Profesjonelle tilretteleggere spiller ofte en rolle. Dette kan være regnskapsførere, rådgivere eller mellommenn. Disse aktørene kan noen ganger være uvitende, og andre ganger bevisst involvert. De tilbyr verdifull kompetanse som gir nettverkene bistand til selskapsopprettelser, fiktiv fakturering eller komplekse transaksjonskjeder.

Når utbytte plasseres i foretak og eiendom og sendes gjennom internasjonale betalingskanaler, tilsløres midlenes opprinnelse. Det er derfor viktig med tidlig identifisering av midlene før de når jurisdiksjoner med lavere innsyn eller blir konvertert til vanskelig sporbare verdier. Indikatorer på slik hvitvasking kan være foretak som skifter pengestrømsmønster, foretak som har lån og likviditet uten reell drift, utgående pengestrøm til heldigitale banker eller andre mottakere i utlandet, konvertering til kryptovaluta eller *stablecoins*, samt kjøp av høymobile verdigjenstander.

Oppsummert bruker kriminelle nettverk et bredt spekter av metoder for hvitvasking, og de er aktuelle innenfor de fleste kriminalitetsområdene beskrevet i denne rapporten. Kriminelle nettverk bruker nettopp nettverket og tredjeperson til hvitvasking. Det kan være gjennom muldyr, innsidere eller profesjonelle tilretteleggere. De bruker også hverandre for å forklare midlers opprinnelse eller destinasjon, siden de er hverandres arbeidsgivere, leietakere, kunder, attestanter og lignende.

Informasjonsboks
Profesjonelle hvitvaskingsnettverk

Profesjonelle hvitvaskingsnettverk

Kriminelle nettverk har profesjonalisert hvitvaskingsmetodene og opererer i stor grad med uoffisielle og ulovlige finansielle systemer, hvor penger overføres utenom det ordinære banksystemet. Hvitvaskingen håndteres ofte av egne nettverk som kun spesialiserer seg på å tilby et bredt spekter av hvitvaskingstjenester. Dette er godt organiserte og profesjonaliserte hvitvaskingsnettverk med spisset kunnskap og høy kompetanse. De kan ha representanter i Norge, men jobber ofte i internasjonale klustre, og kan håndtere store pengebeløp effektivt. Profesjonaliseringen gjør det ofte svært krevende for myndighetene å avdekke hvitvaskingen. I tillegg til profesjonaliserte hvitvaskingsnettverk benytter kriminelle nettverk i Norge seg i høy grad av hvitvasking gjennom foretak, heldigitale banker, *pengemuldyr*, kryptovaluta, *smurfing*, eiendom og verdigjenstander. Det er også avdekket at kriminelle nettverk oppretter datterselskap i utlandet og har flere utenlandske bankkontoer og *wallets* spredt i flere land. I tillegg kjøper de eiendom og verdier i utlandet, ofte i land hvor juridisk samarbeid er lite utviklet.

Spesifikke endringer

Det er endringer i primærkriminaliteten og hvordan denne begås. Blant annet, er det en bekymringsfull utvikling innen bestilling av voldsoppdrag og rekruttering av mindreårige til grove voldshandlinger. Selv om dette ikke direkte omfatter økonomisk utbytte av betydning, innebærer det alvorlige konsekvenser for samfunnet og får derfor økt prioritet.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til kriminelle nettverk som HØY. Det er svært alvorlig hvis dette får utvikle seg. Bakmenn som tjener seg rike på kriminalitet vil få mye makt til å påvirke samfunnet negativt, også utover nettverket. Det påfører samfunnet store tap, men skaper også frykt, utrygghet og lovløse rom. Kriminelle nettverk knyttes til primærforbrytelser med stort omfang over tid, både i antall og summer.

Trusselen vurderes som HØY. Kriminelle nettverk kombinerer høy kapasitet, tilpasningsevne og tilgang på et bredt spekter av metoder for å hvitvaske utbytte fra kriminalitet. Utbyttene beløper seg til store summer både for enkeltnettverk og nettverkene til sammen. Alle de prioriterte nettverkene opererer på tvers av grenser både ved gjennomføring av primærforbrytelsen, blant annet ved transport av varer som narkotika og fisk, og ved hvitvasking av utbytte.

Sårbarheten vurderes som BETYDELIG. Kriminelle nettverk bruker komplekse kombinasjoner av metoder. Myndigheter og rapporteringspliktige må derfor kunne se sammenhenger på tvers av ulike ledd og ulike land. Selv med mye kunnskap om fenomen og aktører er det krevende å iverksette tiltak og gi reaksjoner. Kartlegging av nettverket er viktig for å straffeforfølge og stanse disse kriminelle aktørene. Personvernregler hindrer informasjonsflyt knyttet til kriminelle nettverk. Det forsterker sårbarheten. Der utbytte er skaffet til veie i utlandet eller føres ut av Norge, kan samarbeid med utenlandske jurisdiksjoner være avgjørende. Samtidig kan treghet eller lite utviklet juridisk samarbeid med enkelte jurisdiksjoner gjøre tidlig inngripen og frys av midler mer utfordrende.

Konsekvensnivået vurderes som HØYT, fordi hvitvasking tilknyttet kriminelle nettverk kan undergrave samfunnsstrukturer og tillit, og fordi utbyttet reinvesteres i ny kriminalitet. Store pengestrømmer kan føre til korrupsjon og maktmisbruk som undergraver rettsstaten og demokratiet. Skatteunndragelser påfører samfunnsøkonomiske tap som gir dårligere finansiering av velferdstjenester. Investering av ulovlig midler i eiendom kan være med på å skape kunstige priser og økt etterspørsel som ikke skyldes et reelt boligbehov, men at eiendom benyttes til verdioppbevaring. Kriminelle nettverk har ofte et voldspotensial, er involvert i voldslovbrudd og spiller på frykt. Dette får negative konsekvenser for folks liv, helse og integritet.

Foto: iStock

> Hvitvasking kan være nært knyttet til primærforbrytelsen og det økonomiske utbytte

DEL 5

KRIMINALITETSOMRÅDER

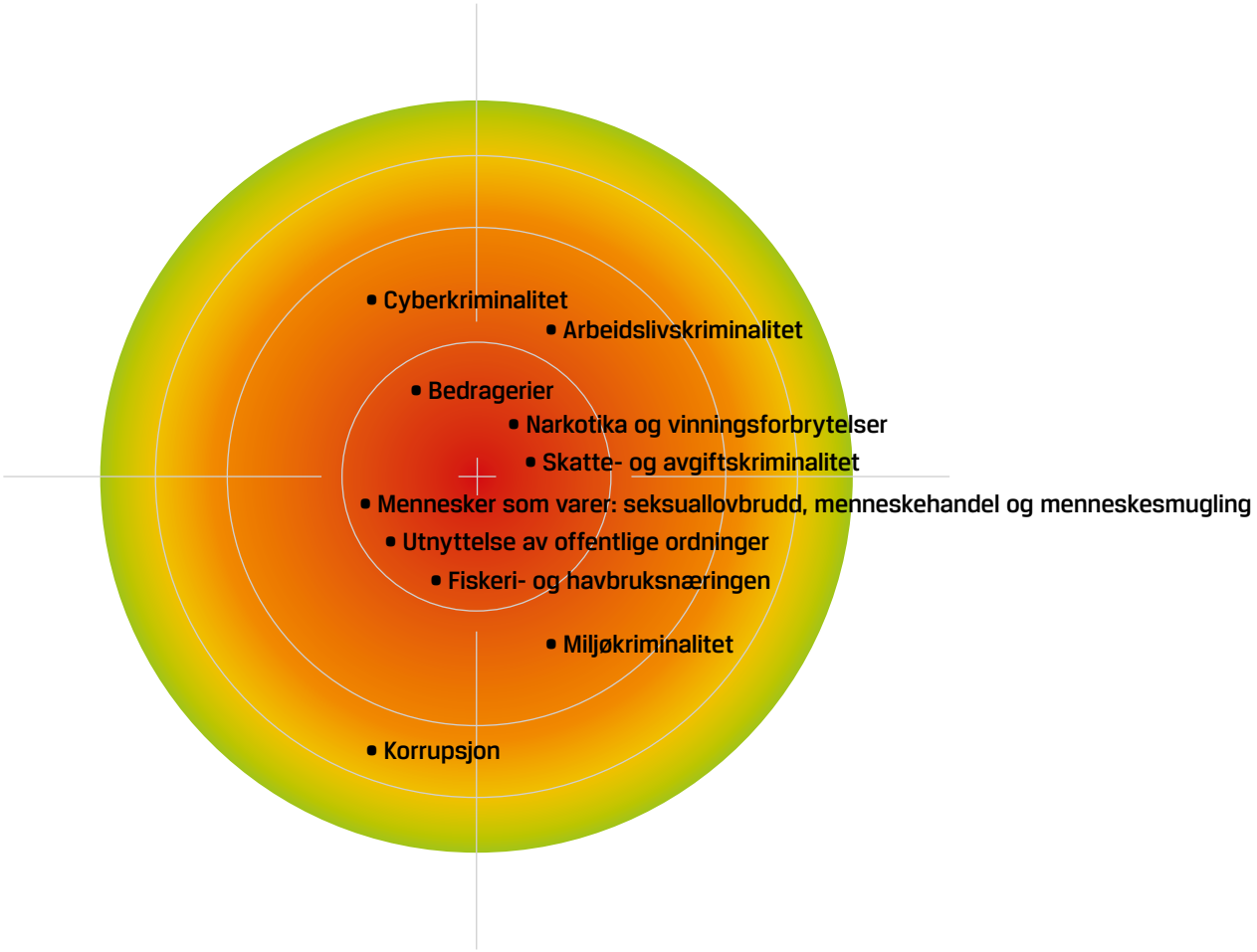
Foto: iStock

Innledning

Formålet med del fem er å beskrive forholdet mellom primærforbrytelsen og hvitvasking. Det kan i en del tilfeller også være vanskelig å skille primærforbrytelsen fra hvitvaskingshandlingen fordi den kan være en del av den kriminelle forretningsmodellen.

Det vurderes i hvilken grad kriminalitetsområdet genererer profitt som må hvitvaskes. Ofte identifiseres primærforbrytelsen før eller samtidig med hvitvaskingen. Hvert kriminalitetsområde inneholder en beskrivelse, før det foretas en overordnet vurdering av hvitvaskingsrisikoen, basert på trussel, sårbarhet og konsekvens. I vurderingen legges det særlig vekt på NRAs indikatorer for omfang.

Til slutt i del fem beskrives hvitvasking i utvalgte bransjer.



Kriminalitetsområder

BEDRAGERIER

Statistikk *Bedragerier*

Strasak
31 464 anmeldte lovbrudd totalt i 2025 – økning hvert år de fire siste årene.

Hvitvaskingsregisteret
Varianter av ordene bedrageri og svindel er nevnt i rundt 5 000 MFR i 2025.
En økning på 76 prosent fra rundt 2 800 MFR i 2022.[45]

Det har de siste tjue årene vært et skifte fra klassiske vinningsforbrytelser som tyveri fra person, butikk og bankran til økonomisk kriminalitet og bedragerier rettet mot personer, banker og bedrifter. Når mye av kommunikasjonen og aktiviteten foregår digitalt på nettet gir det et godt utgangspunkt for kriminalitet i form av bedragerier. Privat kjøp og salg har blitt vanligere gjennom digitale plattformer som blant annet Finn.no, Facebook og disse er sårbare for bedrageri. ID-tyverier i ulike former kan også ha blitt begått med bedrageri som formål.

Trusselaktørene er alt fra enkeltaktører til organiserte nettverk. Det er ofte internasjonale forgreininger. De vanligste typene bedragerier er investerings-, identitets-, relasjons- og fakturabedragerier. De foregår hovedsakelig digitalt, og det er innslag av sosial manipulasjon og fysisk kontakt. Et kjennetegn er

45 Basert på ordtellingssøk i hvitvaskingsregisteret.

også at modus endres og tilpasses raskt. Hvitvasking skjer blant annet gjennom privatkonti, *pengemuldyr*, heldigitale banker og videre overføring til kryptovaluta.

I perioden 2020–2025 økte antallet digitale bedragerier betraktelig. Økokrim har anslått at utbyttet fra bedragerier har vokst fra 860 millioner i 2020 til to milliarder kroner i 2024. Det er grunn til å anta at det reelle tallet er større. Den svenske rapporten «Svarta siffror» anslår at kriminelle transaksjoner knyttet til bedragerier omfatter rundt 40 milliarder svenske kroner årlig. Total profitt anslås til 39 milliarder svenske kroner årlig.[46]

Spesifikke endringer

Tiltak i finanssektoren har redusert omfanget av enkelte modus, men aktørene tilpasser seg raskt gjennom nye plattformer og betalingsløsninger. Et eksempel på tiltak er da teletilbyderne i 2024 innførte et spoofing-filter som i stor grad stopper bedrageriforsøk hvor bedragerne får det til å se ut som de ringer fra politiet eller banken.[47]

I 2024 ble det opprettet en egen bedragerienhet i Økokrim, og i 2025 ble det åpnet for digitale anmeldelser til politiet.

Vurderinger

Samlet sett vurderes **risikoen** knyttet til bedrageri som HØY. Risikonivået påvirkes spesielt av omfang i kombinasjon med tilgjengelighet og store økonomiske tap, noe som forsterker risikoen.

Trusselen vurderes som HØY. Omfanget er høyt, med over 31 000 anmeldelser i 2025. Dette utgjorde 86 prosent av alle økonomiske straffesaker i 2025.[48] Mange bedragerier er både enkle å gjennomføre og svært lønnsomme. Kriminelle nettverk har særlig god evne og vilje til å utføre dem. Dette trekker trusselnivået opp.

Sårbarheten vurderes som HØY. Mange metoder for bedragerier er svært tilgjengelige og krever lite kunnskap for gjennomføring. Oppdagelsesrisikoen er lav i forhold til det store omfanget. Dette forsterker sårbarheten. På den andre siden er oppmerksomheten i næringslivet høy, dette, sammen med opprettelsen av en egen bedragerienhet i Økokrim reduserer sårbarheten.

Konsekvensnivået vurderes som HØYT. De økonomiske tapene er store for både bedrifter og enkeltpersoner, og omfanget bidrar til generell svekkelse av tillit i samfunnet. For privatpersoner kan bedragerier oppleves dramatisk, være invaderende og krenkende på samme måte som innbrudd.

---

46 EOS, *Svarta siffror – en ESO-rapport om den kriminella ekonomins omfattning* - ESO - Expertgruppen för studier i offentlig ekonomi (EOS, 2026).

47 Nettlenke, 31.01.2026: https://www.telenor.no/privat/artikler/sikkerhet/mindre-svindelanrop-med-spoofing-filter/?srsltid=AfmBOorHBz6H-b3B_Qelps2eDePGmTjMpqapHQ7wdHSQvPGx-n2eMzLGZ

48 Tall fra politiets straffesaksregister.

Kriminalitetsområder

UTNYTTELSE AV OFFENTLIGE ORDNINGER

Hvert år går rundt to tredjedeler av statsbudsjettet til utbetalinger innen anskaffelser og ulike tilskudd, støtte- og refusjonsordninger. Velferdsmodellen er i stor grad finansiert gjennom skatter og avgifter på inntekt, forbruk og formue. Utnyttelse av offentlige ordninger er en samlebetegnelse og inkluderer blant annet misbruk av refusjons- og velferdsordninger, anskaffelser, tilskudds- og støtteordninger. Misbruket kjennetegnes ofte av uriktige, mangelfulle eller bevisst villedende opplysninger. Digitalisering og ny teknologi gjør at denne type kriminalitet skjer i et annet tempo og i en større skala enn tidligere.[49]

I nasjonale og europeiske trusselvurderinger beskrives kjente modus som fiktive søknader og grunnlag for utbetalinger, urettmessige tilbakebetalinger, kreditorsvik og registermanipulasjon.

I Sverige estimeres bedrageri og utnyttelse av offentlige ordninger å gi mer profitt til kriminelle nettverk enn narkotikahandel.[50]

Ulike offentlige etater rammes av bedrageri og misbruk av velferds- og refusjonsordninger. Velferdsbedrageri rammer Nav. Mange av de største utbetalingene fra Nav bygger på opptjening av rettigheter basert på opplysninger fra a-ordningen. Feilrapportering av inntekt eller arbeid er dermed med på å muliggjøre slike bedragerier. Misbruk av refusjonsordninger rammer Skatteetaten gjennom blant annet urettmessige MVA-refusjoner. Skatteunndragelse og bedrageri i forbindelse med merverdiavgift er eksempler på økonomisk kriminalitet som påfører staten store økonomiske tap. I mange

49 Nettlenke, 06.01.2026: https://www.skatteetaten.no/presse/nyhetsrommet/skatteetaten-med-67-mva-anmeldelser

50 Nettlenke, 22.01.2026: https://eso.expertgrupp.se/wp-content/uploads/2024/10/ESO-rapport-2026_1_svarta-siffror_webb.pdf

saker avdekkes at fiktiv dokumentasjon blir brukt for å legitimere MVA-refusjon for virksomheter som ikke har reell drift. Misbruk av refusjonsordninger rammer også HELFO-refusjoner knyttet til helsetjenester og medisiner. En rekke andre ordninger med subsidier og støtte innen ulike bransjer rammes også. Eksempler på slike tjenester er subsidier og støtte til innovasjon, utdanning og forskning, som støtte fra SkatteFUNN, kunst og kultur, og frivillige organisasjoner.

Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) har de siste årene satt søkelyset på hvordan kriminelle utnytter sårbarheter i de offentlige systemene. De har blant annet fremhevet hvordan registermanipulasjon muliggjør en rekke metoder for hvitvasking og bedragerier. Metodene som benyttes er blant annet bruk av falske dokumenter, ID-misbruk, manipulasjon av digitale søknadsprosesser og registeropplysninger. Faren for misbruk er særlig stor i forbindelse med ordninger med lite kontroll og som i stor grad er tillitsbaserte. Effektivisering av digitale systemer og forvaltningsprosesser kan skape større brukervennlighet, men også gjøre det enklere å begå kriminalitet.[51]

Spesifikke endringer

Ingen spesifikke endringer siden NRA 2022.

Vurderinger

Samlet sett vurderes **risikoen** knyttet til utnyttelse av offentlige ordninger som HØY. Risikonivået trekkes spesielt opp av handlingsrommet som skapes gjennom kjente systemsårbarheter i kombinasjon med de kriminelles grad av organisering, økonomiske konsekvenser og undergraving av tillit. Det knytter seg liten usikkerhet til vurderingen.

Foto: iStock

51 Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES), Registermanipulasjon, (NTAES, 2024).

Kjente systemsårbarheter muliggjør utnyttelse av offentlige ordninger

Trusselen vurderes som BETYDELIG. Det er særlig aktivitet fra kriminelle nettverk og deres grad av organisering som trekker trusselen opp. Kriminelle nettverk er tydelig integrert i den legale økonomien. Samarbeid dem imellom og tilgang til ressurser og spesialistkompetanse gjør dem bedre til å utnytte offentlige ordninger. Nav anmeldte blant annet trygdemisbruk for 86 millioner kroner i 2025. De peker på mer komplekse og sammensatte saker. I tillegg at enkeltsaker kan ha koblinger til kriminelle nettverk med mer systematisk utnyttelse av velferdsordninger som kan inngå som finansiering av annen kriminalitet.[52]

Kriminelle nettverk har rettet betydelig oppmerksomhet til området som en kilde til profittmotivert kriminalitet. Utviklingen forsterkes av umodne digitale løsninger i offentlig og privat sektor og digitale verktøy som muliggjør gjennomføring i langt større omfang, hurtigere og med mindre bruk av ressurser. En viktig komponent er misbruk av elektroniske identiteter og registrering av utenlandske personer med norske elektroniske identiteter med formål om å bruke disse til kriminalitet.

Sårbarheten vurderes som HØY. Kjente systemsårbarheter muliggjør utnyttelse av offentlige ordninger. Systemene er tillitsbaserte, og flere kriminelle nettverk er tydelig integrert i den legale økonomien gjennom virksomheter som kan utnytte dette. Registrene er sårbare for manipulasjon, og når digitalisering, brukervennlighet og hurtighet prioriteres fremfor kontroll, skaper dette mulighetsrom for kriminelle. Ulik tolkning av taushetsplikt og delingsadgang samt andre praktiske hindringer fører til mindre utveksling av informasjon mellom institusjonene for effektiv forebygging. Sårbarheten forsterkes i tillegg av manglende totaloversikt og samordning.

Konsekvensnivået vurderes som HØYT. Kriminalitet mot det norske velferdssystemet har alvorlige konsekvenser for økonomien og undergraver tilliten til velferdsstaten. Det kan igjen gå utover de som trenger velferdsstaten. Faktisk tap er ikke beregnet, men sakseksempler viser et omfattende potensial, og det er store mørketall.

52 Nav, 2026. Nettlenke 25.03.2026. https://www.nav.no/no/nav-og-samfunn/statistikk/flere-statistikkomrader/trygdemisbruk

Kriminalitetsområder

SKATTE- OG AVGIFTSKRIMINALITET

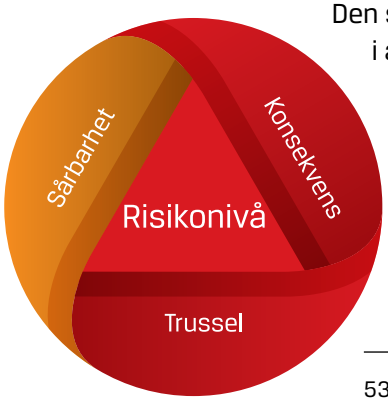
Statistikk *Skatte- og avgiftskriminalitet*

Strasak
821 anmeldte lovbrudd totalt i 2025, økning hvert år siden 2022.

Hvitvaskingsregisteret
Varianter av ordene skattesvik og skatteunndragelser er nevnt i rundt 7 600 MFR i 2025. En økning på 154 prosent fra rundt 3 000 MFR i 2022.[53]

Skatte- og avgiftskriminalitet er et samlebegrep for tilsiktede eller grovt uaktsomme handlinger som bryter med skattelovgivningen, og omfatter både strafferettslig og forvaltningsmessige lovbrudd, samt medvirkning til slike.

Den straffbare handlingen består i å gi uriktige eller ufullstendige opplysninger, eller helt unnlate å gi opplysninger, når dette kan føre til en skattemessig fordel. Ofte er manglene i opplysningsplikten også ledsaget av brudd på bokførings- og regnskapslovgivningen.



Den ulovlige aktiviteten kamufleres ved å kombinere informasjonsskjevheter og digitale sårbarheter for å skjule den reelle skattbare aktiviteten. Aktiviteten kjennetegnes av bruk av stråpersoner som rollehavere og eiere i foretak, oppsplitting av virksomhet i komplekse foretaksstrukturer og systematisk bruk av unøyaktige eller manipulerte opplysninger i registre og rapportering til

53 Basert på ordtellingssøk i hvitvaskingsregisteret.

skattemyndighetene. Virksomheten kan fremstå legitim, enten gjennom faktiske økonomiske transaksjoner, blanding av reelle og fiktive bilag eller tilfeller der kun enkelte deler av driften blir rapportert.

Alvorlig skattekriminalitet omfatter dels nettverkskonstellasjoner som ofte omfatter multikriminelle miljø, dels mer sofistikerte former for unndragelser blant internasjonale konsern og velstående personer. I omfattende unndragelser er det ofte tilretteleggere som tilbyr støttefunksjoner, tekniske tjenester eller kunnskap om hvordan skattesystemet kan misbrukes gjennom juridisk omgåelse eller ved å skjule de faktiske forhold.

Skattekriminalitet kan også være å tilegne seg utbetalinger gjennom skattesystemet basert på fiktive refusjonskrav, for eksempel MVA-meldinger, og uriktige grunnlag i ordninger. Mange metoder brukt i skattekriminalitet er også relevante for hvitvasking. Det kan for eksempel være fiktiv fakturering, bruk av stråpersoner, registermanipulasjon og skjult utbytte i utlandet. Det er ofte glidende overganger mellom skattesvik og hvitvasking. Skatteetatens betalings- og innkrevingsprosesser utnyttes til å legitimere midler med ukjent eller kriminell opprinnelse, for eksempel gjennom tredjepartsbetalinger, overbetaling og tilbakebetaling, eller refusjon av avgifter. Slike transaksjoner kan gi ulovlige midler et legitimt preg.

Spesifikke endringer

Skatteetaten forventer at skattekriminalitetsbildet i økende grad vil være preget av grenseoverskridende strukturer og tjenestetilbydere som muliggjør større informasjonsasymmetri mellom myndigheters registre, systemer og de faktiske økonomiske forholdene. Bruken av utenlandske selskaps- og tjenestestrukturer bidrar til fragmentert sporbarhet, lengre avstand mellom reelle aktører og rapporterte opplysninger. Det gir derfor økt rom for å utnytte både jurisdiksjonsforskjeller og svakheter i informasjonsutvekslingen. Denne utviklingen forsterkes av profesjonelle tilretteleggere som gjør det enklere å skjule eierskap, inntekter og pengestrømmer.

Samtidig muliggjør teknologiske verktøy en betydelig oppskalering av skattekriminalitet gjennom masseproduksjon av fiktive grunnlagsdata, automatisert bilagsgenerering og målrettet manipulasjon av rapporteringsløsninger og registre. Dette skjer parallelt med et tydeligere innslag av kriminelle nettverk i næringslivet, hvor skattekriminalitet inngår som en integrert del av bredere vinningsmotivert virksomhet. Nettverksaktører utnytter virksomheter, stråpersoner og digitale identiteter for å øke handlingsrommet, redusere oppdagelsesrisikoen og sikre at skatteunndragelser kan hvitvaskes.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til skatte- og avgiftskriminalitet som HØY. Risikonivået påvirkes spesielt av kriminalitetens omfang og tillitstapet dette påfører viktige samfunnsstrukturer. Det knytter seg moderat usikkerhet til vurderingen som følge av usikkerhet rundt mørketall.

Trusselen vurderes som HØY. I forhold til antatt omfang er antall anmeldte lovbrudd relativt lite. Bankene anslår at en stor andel av MF-rapportene gjelder skattekriminalitet enten direkte eller indirekte. Flere rapporterte foretak og personer har også en antatt gevinst på mange millioner. Videre er det observert høy grad av profesjonalisering, både for å få skattekriminaliteten til å fremstå lovlig og for å skjule skattbar inntekt og formue. Kriminelle nettverk begår også skattekriminalitet, gjerne gjennom virksomheter. Pengene som unndras kan brukes til å finansiere ny kriminalitet.

Sårbarheten vurderes som BETYDELIG. Komplekse regelverk med gråsoner og begrenset kontrollkapasitet forsterker sårbarheten. Digitalisering har økt effektiviteten ved all slags rapportering, men også sårbarheten ved at feil grunnlagsdata kan misbrukes systematisk.

Konsekvensnivået vurderes som HØYT. Den svarte økonomien utgjør tapte skatteinntekter og store tap for fellesskapet, i tillegg er det konkurransevridende. Skattesystemet er en viktig pilar i samfunnsstrukturen, og tap av tillit til dette systemet veier tungt i negativ retning for konsekvensvurderingen.

Foto: iStock

Kriminalitetsområder

KORRUPSJON

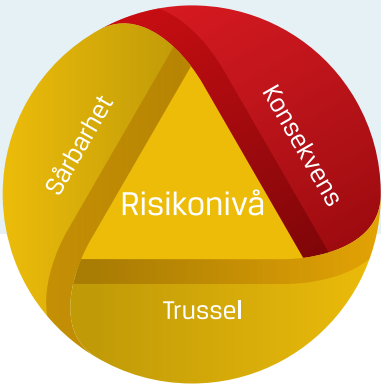
Korrupsjon fungerer både som egen profittkriminalitet og som tilrettelegger for hvitvasking. Det kan innebære bestikkelser, utilbørlige fordeler og misbruk av posisjoner i offentlig og privat sektor. Fordeler en ønsker å oppnå gjennom korrupsjon kan være tjenester eller immaterielle fordeler, som køsniking og urettmessige avgjørelser i offentlig eller privat virksomhet, for eksempel tildeling av kontrakter, byggetillatelser ved utbygging, stønader eller løyver. Det kan også dreie seg om at noen gir eller får urettmessig lån eller kreditt. Fordeler som oppnås gjennom interessekonflikter kan være utilbørlige og dermed også brudd på korrupsjons-bestemmelsene.

Hvitvasking av denne typen utbytte er i liten grad synlig gjennom rapporter om mistenkelige forhold. Tjenestepersonen som er korrupt, kan motta fordeler som bestikkelser og *returprovisjon*[54]. Andre eksempler på korrupsjon er underslag / økonomisk utroskap, urettmessig påvirkning, nepotisme eller riggede anskaffelser.

Statistikk *Korrupsjon*

Strasak
41 anmeldelser totalt i 2025 (korrupsjon og påvirkningshandel). Dette er en økning fra 35 anmeldelser i 2024.

Hvitvaskingsregisteret
Varianter av ordene korrupsjon og bestikkelser er nevnt i rundt 109 MFR i 2025.[55]



54 På engelsk: kick-back.
55 Basert på ordtellingssøk i hvitvaskingsregisteret.

Både sårbarheter og konsekvenser knyttet til korrupsjon er godt dokumentert. Omfanget av faktiske hendelser og aktører er det knyttet større usikkerhet til. Mange tror det forekommer i «smarte former» – samtidig er antallet straffesaker lavt. Det er også eksempler på at kriminelle nettverk bestikker relevante personer på innsiden av systemene. Det knytter seg stor bekymring knyttet til omfanget av profesjonelle tilretteleggere som tar betalt eller lar seg bestikke.[56] Kriminelle som har behov for å hvitvaske utbytte, vil bestikke aktører som muliggjør hvitvasking. I SOCTA 2025 er korrupsjon et av nøkkelementene i DNA-et til organisert kriminalitet da det bidrar til å bygge ned tillit og destabilisere samfunnet.[57]

Det er også en del forhold som grenser til korrupsjon som faller utenfor den juridiske definisjonen, men som likevel har samme funksjon, eksempelvis habilitetsspørsmål i politikk. Norge har mange små bygder, samfunn og miljøer. Vennetjenester kan også ha forventninger om motytelser på sikt. Korrupsjon muliggjør tilsløring i hvitvaskingsprosessen.

Måtene korrupsjon gjennomføres på, fortsetter å gjenspeile den teknologiske og samfunnsmessige utviklingen. For eksempel brukes kryptovaluta, ifølge Europol, i økende grad til å betale korrupte tjenestepersoner og til hvitvasking av penger. I tillegg vil digitaliseringen føre til at enkeltpersoner i større grad blir mål, enten fordi de kan manipulere prosesser og beslutninger i digitale systemer eller på andre måter gi tilgang til verdifull informasjon i offentlig forvaltning og privat næringsliv. Det er også trukket frem at det kan være forhøyet risiko for korrupsjon knyttet til forretnings- og næringslivet, eller der det offentlige og det private møtes.

Foto: iStock

56 Nettlenke, 31.01.2026: https://samfunnsokonomisk-analyse.no/publikasjoner/uetisk-atferd-korrupsjon-og-velferdskriminalitet-i-kommuner-og-fylkeskommuner

57 Europol, *Serious and Organised Crime 2025* (SOCTA)., (Europol, 2025).

> Risikoen for innsidere er tilstede både i det private og i det offentlige

Internasjonale undersøkelser av korrupsjonsutsatte bransjer eller næringer, indikerer at norsk næringsliv, selskaper og ledere er utsatt. I bransjer der bedriftene er avhengige av lisenser, kvoter eller konsesjoner for å kunne drive virksomhet, foreligger det vedvarende korrupsjonsrisiko. Dette gjelder særlig olje- og gassnæringene i inn- og utland, fiskeri- og oppdrettsvirksomhet, våpenproduksjon og forsvarsindustrien.[58] Det har også vært saker knyttet til ressurssterke personer som innehar stillinger med høy status og sentrale posisjoner i lokalmiljøet eller bransjer. Korrupsjonsrisikoen eksisterer tilsvarende der det offentlige gir lån og tilskudd.

I Transparency International's (TI) gjennomgang av korrupsjonsdommer i Norge fremkommer det at flere av dommene gjelder aktører i finansbransjen, og omfatter både korrupsjon og hvitvasking. I dommene omtales også pengespor, banktransaksjoner og overføringer mellom banker i inn- og utland, samt koblinger til andre økonomiske verdier. Dette illustrerer at banker og andre aktører i finansmarkedet kan inngå i nasjonale og internasjonale korrupsjonskjeder.[59]

Spesifikke endringer

Fra 2023 til 2024 rykket Norge ned fra en score på 84 til 81 på Transparrency's international sin korrupsjons indeks fra 0–100. Dette var det laveste nivå på 10 år. Scoren var uendret i 2025, og Norge er rangert som topp fire. Danmark toppet listen med en score på 89.[60]

I 2025 beordret president Donald Trump en pause og omprioritering i håndhevingen av den amerikanske antikorrupsjonsloven Foreign Corrupt Practices Act (FCPA). Loven, som har vært en hjørnestein i USAs innsats mot bestikkelser i internasjonal handel siden 1977, forbyr amerikanske selskaper å bestikke utenlandske embetsmenn for å sikre kontrakter og avtaler. Presidenten oppga at loven skaper store utfordringer for amerikanske selskaper i utlandet. Dette kan øke mulighetsrommet for

58 Transparency International Norge og Advokatfirmaet Erling Grimstad, *Hva hindrer politiets etterforskning av korrupsjonssaker*, (TI Norge, 2023).

59 Transparency Interntional. Frigitt: 30.01.2023: https://static1.squarespace.com/static/6336b296b65a960446be756c/t/63eb9485dacd206160d7008d/1676383366446/Domssamling2023_web_3.pdf

60 Nettlenke, 10.02.2026: https://www.transparency.org/en/cpi/2020/index/nor og https://fn.no/Statistikk/korrupsjon?country=42264

korrupsjon og legitimering av korrupte handlinger inkludert hvitvasking i internasjonal handel.[61]

Vurderinger

Samlet sett vurderes **risikoen** knyttet til korrupsjon som MODERAT. Risikonivået påvirkes spesielt av at det er lavt omfang i et internasjonalt perspektiv og at Norge er rangert blant de beste av TI, men at skadepotensialet er svært høyt. Konsekvensene for tilliten til institusjoner er alvorlige. Risikoen for innsidere er tilstede både i det private og i det offentlige der betydelige verdier forvaltes. Risikoen øker også der det er små forhold, svake kontrollmekanismer og tette bånd mellom aktører, og der øvrige ansatte har for høy tillit til leder eller mellomledere. Risikoen for korrupsjon og press oppleves i kommunal sektor som størst som innen offentlige anskaffelser, plan- og byggesaker.

Trusselen vurderes som MODERAT, blant annet fordi det i et internasjonalt perspektiv er få saker knyttet til korrupsjon i Norge. I 2025 var flere bankansatte under etterforskning for å ha gitt lån på uriktig grunnlag, lekket sensitiv informasjon og misbrukt tilganger til bankenes systemer.[62] Korrupsjon blant finansmarkedets aktører generelt har et stort skadepotensial.[63] Ifølge Europol benytter om lag 60 prosent av kriminelle nettverk korrupsjon i en eller annen form, og det er en integrert del av nesten all organisert kriminalitet.[64] I Sverige viser undersøkelser at organiserte kriminelle jobber målrettet for å skaffe seg innsidere i banknæringen.[65]

Korrupsjon knyttes til flere metoder for hvitvasking og andre kriminalitetsformer der en innsider eller profesjonell tilrettelegger er nyttig, eksempelvis utnyttelse av offentlige tilskudd. Erfaringen fra Sverige er at kriminelle stadig blir flinkere til å utnytte svakheter i kontrollsystemer og myndighetenes arbeidsmetoder. Kompliserte selskapsstrukturer og utfordringer med å fastslå reelle rettighetshavere i utenlandske selskaper kan også være noen blant flere indikatorer på korrupsjon. I tillegg gir digitalisering og kryptovaluta nye muligheter for skjult verdioverføring.

Sårbarheten vurderes som MODERAT. Internasjonale evalueringer har påvist svakheter i Norges oppfølging av internasjonale forpliktelser i antikorrupsjonsarbeidet. I 2025 viste OECD og GRECOs gjennomganger av norske forhold vedvarende strukturelle man-

61 US Dep. of Justice. Frigitt, 09.06.2025: https://www.justice.gov/dag/media/1403031/dl?inline
62 DN, *Etterforsker minst syv saker med utro banktjenere i Norge*, (Dagens Næringsliv, 28.11.2024).
63 DNB, *Finansiell trygghet: Når virkeligheten utfordres – trender og trusler fra et DNB-perspektiv*, (DNB, 2026).
64 Politiet, *Politiets trusselvurdering 2025,* (Politiet, 2025).
65 Europol, *The Other side of the Coin – Analysis of Financial and Economic Crime,* (Europol, 2023).

gler. Rapportene trekker frem manglende systematisk arbeid mot korrupsjon, fraværende konsekvenser ved interessekonflikter på politisk toppnivå og liten vilje til å sikre åpenhet rundt lobbyisme rettet mot statens mektigste. Dette forsterker sårbarheten fordi det kan bidra til at det juridiske rammeverket åpner for et visst handlingsrom for korrupsjon og hvitvasking. I tillegg er det i ulike sammenhenger fremhevet at terskelen for å få dom i korrupsjonssaker oppleves som høy, og at sakene derfor heller subsumerer forholdet under andre straffebud enn korrupsjon.[66] Det reduserer imidlertid sårbarheten at Økokrim i 2025 opprettet en korrupsjonsenhet der forebygging og irretteføring er to primærstrategier.

Konsekvensnivået vurderes som HØYT. Det som kjennetegner korrupsjon – og til dels skiller det fra annen økonomisk kriminalitet – er de sterkt samfunnsskadelige effektene. Det svekker særlig borgernes tillit til myndighetene og personer med makt både i offentlig og privat sektor. I tillegg kan korrupsjon ha andre mer håndfaste skadelige effekter som skade på mennesker[67] og natur[68], eller den kan utgjøre en risiko for nasjonal sikkerhet[69].

Korrupsjon kan også skade økonomisk vekst, ettersom det skaper usikkerhet for næringslivet og påfører det ekstra kostnader. Slik det oppsummeres i forarbeidene til straffeloven utgjør korrupsjon «en trussel mot rettsstaten, demokratiet, menneskerettighetene og sosial rettferdighet, og kan også hindre økonomisk utvikling og virke konkurransevridende».

Foto: iStock

66 Transparency International Norge og Advokatfirmaet Erling Grimstad, *Hva hindrer politiets etterforskning av korrupsjonssaker,* (TI Norge, 2023).

67 Eksempelvis brukes bestikkelser overfor personer som skal kontrollere at sikkerhetskrav er oppfylt. Et nybygg godkjennes selv om ikke skulle vært det, og bygningen raser sammen og folk blir skadet eller dør.

68 Eksempelvis en ansatt hos tilsynsmyndighetene bestikkes for å se gjennom fingrene på utslipp av farlig avfall.

69 Eksempelvis bestikker en ansatt for å få tilgang til hemmelig informasjon, jf. tiltalen i ambassade-saken, der en sikkerhetsvakt er tiltalt bla for å ha mottatt bestikkelser fra fremmed etterretning for å dele sensitiv informasjon.

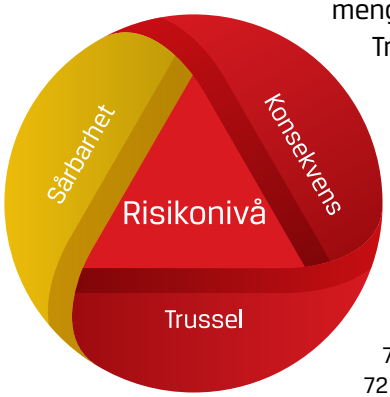
Kriminalitetsområder

NARKOTIKA OG VINNINGSFORBRYTELSER

Statistikk *Narkotika og vinningsforbrytelser*

Strasak
17 727 narkotika anmeldelser totalt i 2025. Nedgang fra 19 351 i 2024.
122 492 anmeldte vinningslovbrudd totalt i 2025, hvorav 1 292 ran.

Hvitvaskingsregisteret
Varianter av ordet narkotika er nevnt i rundt 1 540 MFR i 2025. En økning fra rundt 390 MFR i 2022.[70]



Dette kapittelet omhandler tradisjonell mengdekriminalitet. Ifølge Politiets Trusselvurdering 2026 dominerer vinningsforbrytelser fortsatt store deler av kriminalitetsstatistikken, med 35 prosent av alle anmeldte lovbrudd i 2025.[71] Politiet ser en økning i tyveri fra person på offentlig sted, brukstyveri av bil og såkalte «ungdomsran» utført av unge gjengangere de siste årene.[72] Det samlede økonomiske tapet som følge av vinningskriminalitet vurderes å være i milliardklassen.

70 Basert på ordtellingssøk i hvitvaskingsregisteret.
71 Politiet, *Politiets trusselvurdering 2026,* (Politiet, 2026).
72 Politiet, *Politiets trusselvurdering 2025*, (Politiet, 2025).

Narkotikakriminalitet genererer store inntekter, ofte i form av kontanter. Disse verdiene hvitvaskes så ved at de brukes til kjøp av verdigjenstander, sluses inn i foretak, veksles i annen valuta, benyttes videre til kjøp av lovlige varer osv. Stadig oftere vaskes de gjennom digitale betalingsmidler og kryptovaluta. Politiets trusselvurdering 2026 trekker frem at tradisjonell narkotikakriminalitet fortsatt er den vanligste aktiviteten blant kriminelle nettverk i Norge.

I noen markeder opererer mange kriminelle nettverk etter en *kriminalitet som tjeneste*-modell, der de kjøper transport- og distribusjonstjenester av hverandre. Narkotikaen smugles ofte kamuflert blant ordinær last via landeveien eller sjøveien i fraktcontainere. Andre markeder, eksempelvis for syntetisk narkotika, opererer i stor grad på digitale flater og følger andre betalings- og handelsmønstre.

Spesifikke endringer

Siden NRA 2022 er det endringer som beskrives i trusselvurderingen.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til narkotika- og vinningsforbrytelser som HØY. Risikonivået påvirkes spesielt av både antall hendelser, gjerningspersoner og samlet utbytte, i tillegg til at det er en hovedkilde til økonomisk utbytte for kriminelle nettverk med voldspotensiale.

Trusselen vurderes som HØY. Narkotika og vinningsforbrytelser preges av økt profesjonalisering, digitalisering og tette koblinger til internasjonale nettverk. Det norske narkotikamarkedet kjennetegnes av høy tilgjengelighet og et bredere utvalg av stadig mer potente stoffer. Etter flere år med nedgang, har antallet økt fra 2022 til 2024, men falt noe fra 2024 til 2025. Internasjonale kriminelle nettverk, inkludert svenske gjengmiljøer, ekspanderer i Norge fordi gatesalgsprisene og profittmulighetene er høyere her.

Sårbarheten vurderes som MODERAT. Sårbarheten forsterkes av tilgjengelighet og utbytte i flere ledd. Det er for øvrig god kunnskap om narkotikakriminalitet i kontrolletater noe som trekker sårbarheten ned.

Konsekvensnivået vurderes som HØYT. Omfanget er fortsatt stort, med betydelige samfunnsmessige konsekvenser. Narkotika- og vinningsforbrytelser er ofte koblet til vold og annen alvorlig kriminalitet, som rammer ofre for kriminaliteten. Narkotikabruk gir også samfunnet utgifter knyttet til fravær av deltakelse i arbeidslivet, helse- og sosialtjenester. Narkotika har i tillegg store personlige konsekvenser for de som utvikler avhengighet og rusmisbruk.

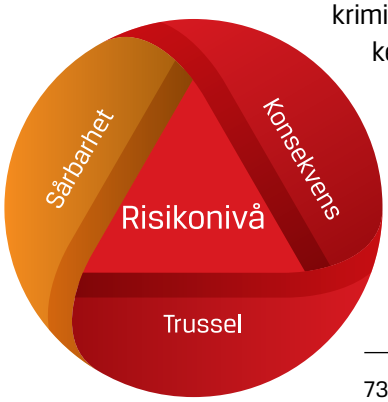
Kriminalitetsområder

MENNESKER SOM VARER: SEKSUALLOVBRUDD, MENNESKEHANDEL OG MENNESKESMUGLING

Statistikk *Mennesker som varer: seksuallovbrudd, menneskehandel og menneskesmugling*

Strasak
7 111 anmeldte seksuallovbrudd totalt i 2025
26 anmeldte menneskesmuglingssaker
24 anmeldte menneskehandelssaker

Hvitvaskingsregisteret
Varianter av ordene seksuallovbrudd, menneskehandel og menneskesmugling er nevnt i rundt 1 110 MFR i 2025. En økning fra rundt 340 MFR i 2022.[73]



Mennesker som varer omhandler kriminalitetsområder der mennesker er til salgs. Det er et globalt marked, med god profitt og høy grad av organisering. Bakmenn tjener store penger som må hvitvaskes.

Til deres fordel er det ofte «kunden» eller kjøperen av eksempelvis overgrepsmaterialet som løper den største risikoen for kontroll og straffeforfølgning.

Menneskehandel kan grense mot hallikvirksomhet, arbeidslivskriminalitet og sosial dumping. Ved menneskesmugling

73 Basert på ordtellingssøk i hvitvaskingsregisteret.

Foto: iStock

behandles også mennesker som vare. Grad av medvirkning varierer. Barn har ingen innflytelse på valgene familien gjør, mens voksne, gjerne i svært vanskelige situasjoner, tar selvstendig risiko ved å betale smuglere.[74]

Det er et kommersielt marked for kjøp og salg av overgrepsmateriale og seksuelle tjenester samt direkteoverføring av seksuelle overgrep mot barn (DOBO). Store deler av kriminaliteten er organisert, er av profesjonell karakter og foregår på tvers av landegrenser. Det er ulike kategorier overgrep som selges i dette markedet, og som avdekkes gjennom finansielle spor. På tre år er det opprettet ca. 50 politianmeldelser som har sitt utspring i mistenkelige transaksjoner i hvitvaskingsregisteret. Cyberstøttede overgrep skjer i stort volum og blir derfor vektlagt tyngst i vurderingen. I 2025 registrerte politiet 3 212 straffesaker som omhandler seksuallovbrudd mot barn. I underkant av 1 900 av disse sakene er knyttet til digitale modus.[75]

Spesifikke endringer

Salg og formidling av cyberstøttede seksuallovbrudd har økt på ende-til-ende-krypterte meldingsplattformer. Dette utfordrer politiets evne til å skille mellom norske og utenlandske gjerningspersoner.

74 Kripos, Cyberkriminalitet 2025, (Kripos, 2025).
75 Ibid.

Det har vært en kraftig økning i tips om nordmenn med befatning med *syntetisk overgrepsmateriale*[76], med 9 060 tips i 2025 mot 1 561 i 2024.[77]

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til kriminalitet med mennesker som varer som HØY. Risikonivået påvirkes spesielt av grad av organisering og av at bakmannsapparatet ofte er i utlandet, og at kriminaliteten gir høy profitt og opererer i et grenseløst marked. Kriminaliteten rammer liv, helse og integritet hos sårbare ofre.

Trusselen vurderes som HØY. Kriminelle bakmenn drar nytte av et grenseløst marked. De organiserte kriminelle sitter i andre land som Filippinene og Tyrkia. Nettverkene er godt organiserte. Kriminell profitt kan finansiere annen kriminalitet eller ekstremisme.

Sårbarheten vurderes som BETYDELIG. Kriminelle som ønsker å tjene penger på salg av overgrep eller menneskehandel er avhengig av rekruttering i sårbare grupper. Sammenlignet med mange andre former for kriminalitet er det noen begrensninger med hensyn til tilgjengelighet. Bildemateriale og betalinger kan spores selv om det er gjort grep for anonymisering, det reduserer sårbarheten noe. Oppdagelse av lovbrudd avhenger av utstrakt samarbeid på tvers av landegrenser. Samarbeid med fornærmede i overgreps- og menneskehandelsaker og asylsøkere i menneskesmuglingssaker kan være utfordrende. Det forsterker sårbarheten.

Konsekvensnivået vurderes som HØYT. Overgrep mot barn i andre land får ingen kostnad her hjemme. Konsekvensene bæres av ofrene, gjerne barn og marginaliserte. Belastningen ved å bli utsatt for digitale seksuelle overgrep kan være svært stor. Konsekvensene kan være langvarige. KI kan re-aktualisere gammelt overgrepsmateriale, noe som påfører voksne som ble utsatt for overgrep som barn, ny belastning.[78]

76 KI-generert overgrepsmateriale.
77 Kripos, *Cyberkriminalitet 2026,* (Kripos, 2026).
78 Kripos, *Cyberkriminalitet 2025,* (Kripos, 2025).

Kriminalitetsområder

UTPRESSING

Seksuell utpressing («sextortion») er cyberstøttet profittmotivert kriminalitet.

I Kripos rapport om cyberkriminalitet fra 2025 ble det antydet at norske fornærmede betalte til sammen omtrent 7,6 millioner kroner til utpressere i perioden 1. januar 2023 til 31. oktober 2024. Voksne betaler i snitt 10 000 kroner per utpressingssak, mens barn betaler i snitt 2 800 kroner. Nesten 2 000 tilfeller av utpressing mot norske gutter og menn skal ligge til grunn for analysen.[79]

Seksuell utpressing med profittmotiv mot norske fornærmede forekommer fra land som Filippinene, Nigeria og Elfenbenskysten.[80]

Som i mange andre typer bedragerier er de som begår seksuell utpressing, gode på sosial manipulasjon. Det kan være vanskelig å erkjenne at man er lurt, be om hjelp og rapportere lovbruddet.

De samfunnsøkonomiske kostnadene av cyberstøttede seksuallovbrudd og seksuell utpressing kan indirekte knyttes til blant annet manglende deltakelse i utdanning og yrkesliv. Håndteringen av slike lovbrudd krever også store ressurser fra helsevesenet, politiet og rettsvesenet.[81]

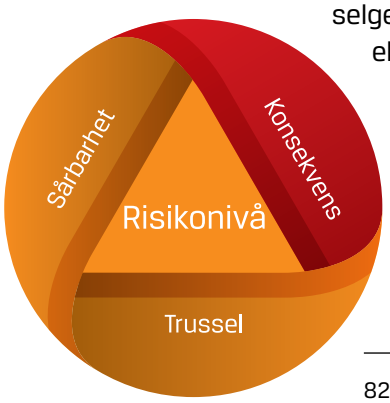
79 Ibid.
80 Ibid.
81 Ibid.

Kriminalitetsområder

CYBERKRIMINALITET

Kripos' rapport «Cyberkriminalitet 2026» omhandler et bredt spekter av lovbrudd. Disse kategoriseres langs en skala fra cyberrettet kriminalitet, som datainnbrudd, *løsepengevirus* og tjenestenektangrep, til cyberstøttet kriminalitet der teknologi fungerer som et sentralt verktøy for tradisjonelle lovbrudd. Sentrale kriminalitetstyper er digitale bedragerier og seksuallovbrudd som seksuell utpressing, DOBO og befatning med overgrepsmateriale.[82] Kryptovaluta er ofte sentralt i betalings- og hvitvaskingsleddet.

Ifølge Kripos er profittmotiverte kriminelle som bruker cyberdomenet en mangfoldig aktørgruppe. Kommersielle aktører opererer ofte i gråsonen ved å selge tjenester som overvåking eller digital infrastruktur som tilslører kriminell virksomhet, mens utpressere har profesjonalisert seg gjennom «utpressing som handelsvare» (USH), der de kombinerer datatyveri og kryptering for å kreve løsepenger fra både virksomheter og privatpersoner.



Profittmotiverte seksuallovbrytere får utbytte fra DOBO, seksuell utpressing og salg av overgrepsmateriale. Salg av overgrepsmateriale kan også være en inntektskilde for radikale nettsamfunn som kan berike enkeltpersoner eller brukes til å finansiere annen kriminalitet. Vold som handelsvare (VSH) er et annet fenomen som er muliggjort gjennom teknologiske plattformer. Samlet sett utnytter disse aktørene det cyberkriminelle økosystemet og digitale muliggjørere for å effektivisere sin ulovlige drift, maksimere profitt og redusere risikoen for å bli oppdaget.

Cyberstøttet kriminalitet blir omtalt i flere andre kapitler, særlig bedragerier og mennesker som varer. Cyberrettet kriminalitet som *løsepengevirus* og datainnbrudd er utgangspunkt for vurderingene i dette kapitlet.

82 Kripos, *Cyberkriminalitet 2026*, (Kripos, 2026).

Spesifikke endringer

Det ble registrert 349 straffesaker om innbrudd i datasystemer i 2025, en økning fra 245 saker i 2024 og 251 i 2023. En mørketallsundersøkelse fra 2024 viste at kun 24 prosent av virksomhetene som opplevde datainnbrudd og datatyveri, anmeldte forholdet.[83]

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til cyberrettet kriminalitet som BETYDELIG. Risikonivået påvirkes spesielt av rask teknologisk utvikling og profesjonalitet ved trusselaktørene. Høy kompetanse og høyt fokus på beskyttelse og mottiltak reduserer sårbarheten noe, mens alvorligheten knyttet til hvordan kriminaliteten kan ramme og lamme samfunnet veier tungt i negativ retning.

Trusselen vurderes som BETYDELIG. Utviklingen innen KI og digital infrastruktur utvider de kriminelles rekkevidde, og senker språklige, kulturelle og teknologiske barrierer. Dette kan gjøre at norske interesser blir mer utsatt for cyberkriminalitet fra aktører som tidligere fokuserte på andre land.

Kriminalitet som handelsvare gjør det lettere for mindre kyndige aktører å begå kriminalitet på egen hånd. Det har blitt lettere for profittmotiverte kriminelle å forbedre verktøy, skaffe kompetanse eller endre handlingsmønster. Dette profesjonaliserer alle ledd i cyberkriminaliteten. Kriminelle er avhengige av tilretteleggere med spesialistkompetanse for spesifikke oppgaver i cyberdomenet eksempelvis skadevarebyggere, hvitvaskere og økonomiansvarlige.

Sårbarheten vurderes som BETYDELIG. Kriminelle benytter anonymiseringsteknologi som VPN, proxy-tjenester og Tor for å skjule identitet og redusere risikoen for å bli tatt. Mange kriminelle benytter kryptovaluta til økonomiske transaksjoner. Bruk av kryptokort muliggjør en omgåelse av tradisjonelle finansielle systemer med regulatoriske rapporteringskrav, og gir en viss anonymitet i transaksjonene. Kriminelle kan også utøve kriminalitet fra land uten utleveringsavtale med Norge.

Kriminelle utnytter gapet mellom den raske teknologiske utvikling og samfunnets tregere evne til å utvikle effektive mottiltak. Samtidig har offentlige og private bedrifter god kunnskap om egne sårbarheter, og de har iverksatt beskyttelsestiltak mot digital kriminalitet. Dette reduserer sårbarhetsnivået.

83 Ibid.

Konsekvensnivået vurderes som HØYT. Angrep mot *OT-avhengige*[84] virksomheter, eksempelvis ved *løsepengevirus*, kan føre til produksjonsstans og nedetid i bedrifter og påføre ofrene store økonomiske kostnader. Aksjefall og tap av publikums tillit kan også være en konsekvens.[85] På samfunnsnivå kan det føre til bortfall av kritiske samfunnsfunksjoner og fysisk skade på utstyr, miljø og menneskeliv.[86] Det kan både medføre økonomiske tap og skade tilliten til kritisk samfunnsstruktur.

For eksempel har *løsepengevirus*angrep mot helseforetak ført til forstyrrelser i utlevering av resepter, utsettelse eller kansellering av operasjoner og blodmangel.

Sensitiv data på avveie som personopplysninger eller forretningshemmeligheter, kan utgjøre en trussel mot enkeltpersoner, virksomheter og nasjonale sikkerhetsinteresser. Konsekvensene av kompromittert informasjon kan vare i over flere tiår.[87]

Foto: iStock

84 OT = operativ teknologi.
85 Kripos, *Cyberkriminalitet* 2025, (Kripos, 2025).
86 Ibid.
87 Ibid.

Kriminalitetsområder

MILJØKRIMINALITET

Statistikk *Miljøkriminalitet*

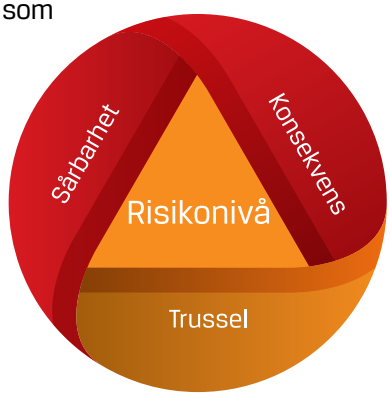
Strasak
2 298 anmeldte miljølovbrudd totalt i 2025.

Hvitvaskingsregisteret
Varianter av ordet miljøkriminalitet er nevnt i rundt 70 MFR i 2025. En økning fra rundt 60 MFR i 2022.[88]

Miljøkriminalitet omfatter ulovlig forurensning, nedbygging av natur og brudd på ressursforvaltning. Kriminaliteten skjer ofte i gråsonen mot lovlig virksomhet. Tolkninger eller overskridelser av tillatelser er særlig relevant for flere typer miljøkriminalitet. Miljøkriminalitet kan være svært lønnsomt. I flere bransjer blir miljøregler nedprioritert når de kolliderer med sterke økonomiske interesser. Profitten kan være i form av besparelser, konkurransefortrinn eller tillatelser innvilget på uriktig grunnlag. Hvitvasking knyttes særlig til selskapsstrukturer og bakes inn i lovlig virksomhet.

Økokrims trusselvurdering på miljøkriminalitet for 2025 tar for seg tolv kriminalitetsutfordringer fordelt på fire kriminalitetsområder: natur- og faunakriminalitet, havbruks- og fiskerikriminalitet, forurensningskriminalitet og miljøkriminalitet i et globalt marked. Kriminalitetsutfordringene har også blitt mer relevante som følge av økt handel på tvers av landegrenser, digitalisering og økende avfallsmengder.

Import av falske eller ikke godkjente produkter er en utfordring. Volumet og potensialet for profitt er stort.



88 Basert på ordtellingssøk i hvitvaskingsregisteret.

Miljødirektoratet har i kontroller avdekket avvik på mer enn 70 prosent av kontrollerte varer. Eksempelvis ble det ved kontroll avdekket ulovlig import av falske Swims-sandaler til en verdi av rundt 100 millioner kroner. Volumet indikerer høy grad av organisering.

Ulovlig deponering av avfall og masser på land utføres både av enkeltpersoner og foretak. Flere aktører som er omtalt i politiets systemer for involvering i ulovlig dumping er også registrert som involvert i økonomisk kriminalitet. Ulovlig avfallsdumping kan ha alvorlige miljøkonsekvenser. Ved et avfallsdeponi i Møre og Romsdal, hvor det var dumpet over 1000 tonn med avfall, ble opprydningsarbeidet estimert til å koste mer enn 129 millioner kroner. Eksempelet viser nivået på økonomiske konsekvenser. I andre europeiske land rapporteres det om at handel med avfall og dumping av avfall i økende grad er en attraktiv bransje for kriminelle nettverk, og Europol peker på at avfallskriminalitet ofte er organisert.[89]

Utrangerte kjøretøy og annet avfall har også fått oppmerksomhet i Norge. Syv aktører ble anmeldt av Tolletaten i 2024. Utrangerte kjøretøy har store mangler, kort gjenværende levetid og er svært forurensende, men eksporteres ofte til Vest-Afrika hvor eksportørene får stor gevinst. Det er kartlagt over 40 norske kjøretøyeksportører som har dette som hoved- eller biinntekt. De bruker gjerne samme tilretteleggere og shippingselskaper. Én aktør har vært registrert med nærmere 6 000 kjøretøy på seg og sine enkeltpersonsforetak de siste 15 årene.

Unndragelse av skatter og avgifter, ulovlig arbeid, utnyttelse av sårbare arbeidstakere, bedrageri og hvitvasking sees ofte i kombinasjon med miljøkriminalitet og forsterker den økonomiske gevinsten.

Spesifikke endringer

Det er stadig endringer i regelverk relatert til miljøkriminalitet. Dette er noen eksempler:

- Regjeringen har vedtatt omfattende tiltak for å redde fiskebestandene i Oslofjorden. Fra 1. januar 2026 blir det innført tre nullfiskeområder, inkludert indre Oslofjord og de marine nasjonalparkene ved Færder og Ytre Hvaler. Tiltakene innebærer et tiårig forbud mot både yrkes- og fritidsfiske.
- Villaksbestanden i Norge er under sterkt press etter rekordlave fangsttall i 2024. Miljødirektoratet har derfor innført de strengeste reglene noensinne og slår hardt ned på tjuvfiske, særlig ulovlig garnbruk.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til miljøkriminalitet som BETYDELIG. Risikonivået påvirkes spesielt av omfanget av kriminaliteten selv om det er vanskelig å anslå. Ut fra enkeltsaker i Norge og internasjonale estimater utløser slik kriminalitet både stor profitt og store økonomiske tap. Komplekse lover og regelverk gir dessuten rom for misbruk og lav oppdagelsesrisiko. Konsekvensene er langsiktige og alvorlige for miljø og samfunn.

89 Europol, *The Changing DNA of Serious and Organised Crime*, (Europol, 2025).

Trusselen vurderes som BETYDELIG. Det er usikkerhet knyttet til omfanget utover sakseksempler og internasjonale estimater. Enkelte bransjeaktører kan ha nettverk, kriminell historikk og kunnskap for å utnytte mulighetene. En del former for kriminalitet under paraplyen miljøkriminalitet er aktuelle for internasjonale pengestrømmer og for hvitvasking av kriminalitet begått i utlandet.

Sårbarheten vurderes som HØY. I Økokrims trusselvurdering er det skissert noen sårbarheter i kontrollsystemet som kan utnyttes av trusselaktører. Miljøkriminalitet skjer ofte innenfor ellers lovlige rammer. Forurensning, avfallskriminalitet og ulovlig nedbygging av natur skjer ofte på steder der det allerede finnes en tillatelse, men der man overskrider rammene for den tillatelsen som er gitt. I fiskerinæringen skjer legitime og ulovlige aktiviteter side om side. Ulovlig fangst og feilrapportering kan lett blandes inn i den lovlige virksomheten. Når kriminaliteten skjer i tilknytning til en ellers lovlig virksomhet, synker risikoen for å bli oppdaget. Og risikoen blir enda lavere når overtredelsene skjer i avsidesliggende områder, eller når konsekvensene ikke blir synlige før langt senere. Enkelte ordninger åpner for misbruk, som forskuddsbetaling i avfallssektoren, der man får betalt før jobben er gjort. Da er det lettere for avfallet å «forsvinne» eller havne på ulovlige eksportreiser.

Kompetansen er mangelfull hos både tilsynsmyndigheter og politiet med ansvar for oppfølging av miljøkriminalitet. Dette fører blant annet til lang saksbehandlingstid og at mange saker sendes tilbake til forvaltningen. Manglende oppfølging og prioritet hos politiet kan bidra til at forvaltningen unnlater å anmelde selv alvorlige lovbrudd. Dette forsterker sårbarheten. Videre er forvaltningens oppfølgning av miljøregelverket ressurskrevende, og sårbarheten øker av at det er få tilsyn. En stor mengde tips og bekymringsmeldinger vurderes hvert år som relevante, men bare få av disse følges opp med tilsyn eller saksbehandling. På flere områder baseres tilsynsvirksomheten i tillegg på egenrapportering. Dette medfører en sårbarhet ettersom aktører kan tilpasse og tilbakeholde informasjon.

For å avdekke aktører som begår lovbrudd på tvers av områder og landegrenser, kreves god samordning mellom etatene og politiet. Sårbarheten forsterkes av at fragmenterte systemer og ulike digitale løsninger svekker muligheten til å se helheten i kriminaliteten. Også manglende informasjonsdeling, innenfor allerede lovregulerte rammer, skaper handlingsrom for aktører i grenselandet mellom ulike myndigheters ansvarsområder. Sårbarheten trekkes også opp av at for tette bånd eller rollekonflikter kan føre til at beslutninger fattes på uriktig grunnlag. Dette øker risikoen for korrupsjon, dokumentforfalskning eller uriktig forklaring til offentlig myndighet.

Konsekvensnivået vurderes som HØYT. Avhengig av kriminalitetsformen kan lovlige bedrifter, forsikringsselskaper, samfunnet og privatpersoner sitte igjen med tap. Naturødeleggelser kan gi indirekte konsekvenser som kan resultere i både samfunnsmessige og personlige tap påført for eksempel gjennom forurensning, farlige produkter, mangelfull flomsikring, støy og nedbygging av natur. Kriminaliteten kan også gå ut over liv og helse og skadene kan i mange tilfeller være uopprettelig.

Kriminalitetsområder

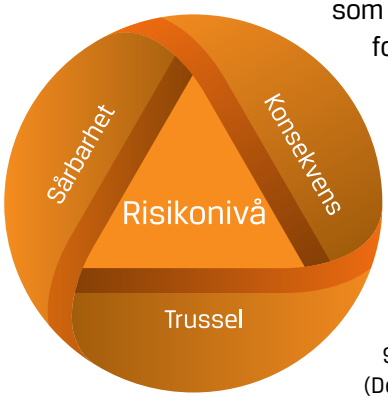
ARBEIDSLIVSKRIMINALITET

Statistikk *Arbeidslivskriminalitet*

Strasak
2 298 arbeidsmiljølovbrudd totalt. Det er ikke egen kategori i Strasak for arbeidslivskriminalitet.

Hvitvaskingsregisteret
Varianter av ordet arbeidslivskriminalitet er nevnt i rundt 700 MFR i 2025. En økning fra rundt 300 MFR i 2022.[90]

Arbeidslivskriminalitet er en samlebetegnelse for ulike former for økonomisk motivert, ofte organisert, kriminalitet i arbeidslivet. Eksempler er ulike handlinger som bryter med norske regelverk for lønns- og arbeidsforhold, trygd, skatter og avgifter, utnyttelse av arbeidstakere og handlinger som virker konkurransevridende og undergraver samfunnsstrukturen.[91] Arbeidslivskriminalitet utøves ofte av organiserte aktører som misbruker foretak og selskapsstrukturer eller oppretter slike. Modus inkluderer fiktiv fakturering, utnyttelse av sårbare personer, misbruk av digital ID, falske identiteter og misbruk av offentlige ordninger. Foretakene brukes som ledd i hvitvasking av utbytte fra annen kriminalitet.



90 Basert på ordtellingssøk i hvitvaskingsregisteret.
91 Departementene, *Handlingsplan mot sosial dumping og arbeidslivskriminalitet*, (Departementene, 2025).

Foto: iStock

En særlig relevant modus i arbeidslivskriminalitet er fiktiv fakturering. Dette kan gjøres ved at en aktør med reelt arbeidsgiveransvar mottar fakturaer fra en underleverandør som ikke faktisk har levert tjenestene det faktureres for. Ved hjelp av uriktig og villedende regnskapsdokumentasjon unndrar den reelle arbeidsgiveren seg fra forpliktelser til å betale arbeidsgiveravgift samt at de uriktige fakturaene kan benyttes som uriktig grunnlag for merverdiavgiftsrefusjon og reduksjon av skattepliktige inntekter. Pengestrømmen preges av store, raske overføringer, ofte til utlandet, og bruk av stråpersoner i styrende roller. Pengestrømmene benyttes ofte til svart avlønning av ansatte. På denne måten gjennomføres både skattesvik og hvitvasking samtidig.

Spesifikke endringer

Økt myndighetsinnsats har avdekket utbredt bruk av slike strukturer som del av større kriminelle økosystemer. Deling av aktørinformasjon mellom relevante etater for å forebygge og avverge kriminalitet, gjør etablering og avvikling rask og lite kostbar.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til arbeidslivskriminalitet som BETYDELIG. Risikonivået påvirkes spesielt av grad av organisering, begrenset kontrollvirksomhet og undergraving av samfunnsstrukturer. Det knytter seg moderat usikkerhet til vurderingen som følge av antatte mørketall.

Trusselen vurderes som BETYDELIG. Grad av organisering og knytninger til kriminelle nettverk samt at kriminaliteten er gjentakende og systematisk forsterker trusselen.

Sårbarheten vurderes som BETYDELIG. Mange små foretak og begrenset tilsyn forsterker sårbarheten. Uklart regelverk, usikkerhet rundt tolkninger av regelverket, og ulik forståelse blant ulike etater av hvilke lovbrudd som inngår i arbeidslivskriminalitet, påvirker samarbeidet på tvers av etatene, og øker også sårbarheten.

Konsekvensnivået vurderes som BETYDELIG. Sosial dumping og tapte skatteinntekter er alvorlige konsekvenser som rammer både enkeltpersoner og samfunnsstrukturer. I tillegg kommer konkurransevridning og tap av tillit.

Kriminalitetsområder

HVITVASKING I UTVALGTE BRANSJER

Transport, bygg og anlegg, bil og restaurantnæringen er eksempler på bransjer som er utsatt for hvitvasking på grunn av komplekse strukturer, knytninger til kriminelle nettverk og at store verdier håndteres. Noen bransjer har også internasjonale knytninger gjennom eierskap eller markeder.

Eksempelvis er det i transportbransjen muligheter for fiktive oppdrag eller drift. Hvitvasking i bilbransjen kan skje ved import og eksport av biler fordi biler kan ha stor verdi, og er ofte avgiftsbelagt. Bygg og anlegg er en arbeidsintensiv bransje. De kriminelle utnytter strukturer med mange underselskaper og utenlandske arbeidstakere. I restaurantbransjen er det muligheter for opprettelse av mange foretak. Slik kan de bli hvitvaskingsfabrikker med stor gjennomstrømning av penger. Bransjen egner seg for kontanter, men også andre betalingsformer.

Datasentre

Datasentre er en nyere bransje med potensiale for høy hvitvaskingsrisiko. Mangel på erfaring og kunnskap hos myndighetene er en viktig sårbarhet. Dette påvirker myndighetenes evne til kontroll som igjen påvirker oppdagelsesrisikoen. Internasjonale aktører og komplekse eierstrukturer er i tillegg en indikator som øker handlingsrommet. Datasentrene kan gi stor økonomisk profitt, noe som gjør det attraktivt for hvitvasking av store summer. Det gjelder også for utbytte fra kriminalitet begått i utlandet. Tilsvarende fører det til betydelig tap for samfunnet hvis bransjeaktørene bryter loven for å maksimere utbytte.

Olje- og gassektoren

Olje- og gassektoren er Norges største og viktigste næring. Beskrivelsen og vurderingene av denne sektoren er i stor grad uendret siden NRA 2022. Bransjen er sterkt regulert, og dette antas å påvirke oppdagelsesrisikoen. Sektoren er likevel sårbar for misligheter hos leverandører og underleverandører, blant annet i forbindelse med innleie av arbeidskraft. Komplekse eierstrukturer og internasjonale investeringer er en sårbarhet. I til-

legg kan det grønne skiftet og tilhørende støtte- og insentiv ordninger skape nye muligheter for misbruk.

Energibransjen

I Norge produseres fornybar energi først og fremst ved vannkraft, som står for 88 prosent av den totale energiproduksjonen. Vindkraft står for 10 prosent, mens 2 prosent kommer fra termisk kraft og solkraft. NVE har i sin langsiktige kraftmarkedsanalyse for 2025 anslått at energiproduksjonen i Norge vil øke vesentlig fra rundt 2030, og at den vil basere seg på vindkraft på land, vindkraft til havs og solkraft. Det ligger også an til store investeringer i nettkapasitet etter 2030.

Hvitvasking vil i fornybarsektoren kunne skje gjennom leverandører av varer og tjenester knyttet til investeringer i ny produksjons- og nettkapasitet, som involverer en rekke underleverandører fra inn- og utland.

Risikoen for hvitvasking på investorsiden antas å være høyest i eierstrukturer med et skjult eierskap. Noen av eierstrukturene innenfor vindkraft og småkraft er kompliserte, og det er utfordrende å identifisere hvem som til syvende og sist står bak den utenlandske investeringen.

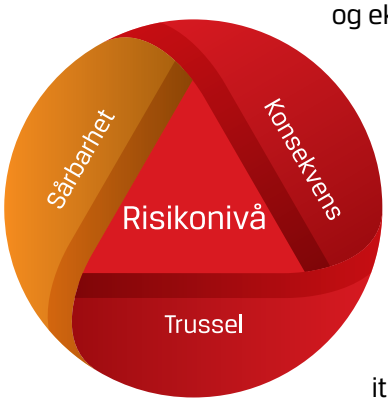
Det er både offentlige, private og utenlandske private eierskap i energibransjen. Etter innføring av grunnrenteskatt på vindkraft var det flere utenlandske eiere som solgte seg ut, og graden av utenlandsk eierskap innenfor vindkraft gikk noe ned.

Grunnrenteskattesystemet for vannkraft har en utbetalingsordning for skatteverdien av nyinvesteringer. Dette innebærer at rundt 58 prosent av investeringer i nye driftsmidler dekkes av staten i det inntektsåret investeringene gjøres. Ordningen kan tenkes utnyttet til hvitvasking for å oppnå raskere gevinst fra de innskutte midler enn hva som kan oppnås i andre typer virksomheter. Ordningen kan også tenkes utnyttet som et rent bedrageri ved å rapportere uriktige opplysninger som danner grunnlag for utbetaling.

Kriminalitetsområder

FISKERI- OG HAVBRUKSNÆRINGEN I NORGE

Fiskerikriminalitet kan foregå i hele verdikjeden, fra fangst til landing, videreforedling, salg og eksport. Kriminaliteten er ofte profittmotivert, konkurransevridende og svekker både ressursforvaltningen og statens inntekter fra skatter og avgifter. Det er også risiko for omgåelser av regelverket ved kjøp av fiskefartøy med kvote. Under- og feilrapportering av fangst på sluttseddel er en sentral fremgangsmåte. Det er også avdekket risiko for fiskerikriminalitet hos selskaper med integrert verdikjede, ved at fartøy og mottak har samme eier. Egenleveransene skaper muligheter for å skjule fiskerikriminalitet. Uregistrert fisk kan bli hvitvasket gjennom bearbeiding og videreforedling, og gjennom salg, transport og eksport ut av landet.



Havbrukskriminalitet kan foregå i hele verdikjeden, fra drift og fôrproduksjon til slakting, videreforedling, salg og eksport. Eksempler på slik kriminalitet er produksjon av mer fisk enn tillatt, overskridelse av lokalitetsgrenser, ulovlig bruk av legemidler, dårlig dyrevelferd, forurensende utslipp, rømning av oppdrettsfisk osv. Slike brudd truer miljøet, skader villfiskbestandene og undergraver tilliten til oppdrettsnæringen. Manipulering av rapporteringer og merking foregår også. I perioden 2024–2025 har kriminalitet knyttet til ulovlig eksport av produksjonsfisk vært utbredt, og inntjeningspotensialet er stort. Det er informasjon om at død fisk eller selvdøende fisk, som ikke er egnet for konsum, også har blitt eksportert ulovlig som matfisk til forbrukere i utlandet. Dette truer tilliten til norsk sjømat og matsikkerheten.

Fiskeri- og havbruksnæringen egner seg for hvitvasking ved å skjule midlenes opprinnelse. Indikatorer kan være store betalinger som overstiger vareverdien, selskap uten tydelig rolle i handelen, prisnivå som avviker fra markedet, selskap uten drift eller ansatte, men som samtidig har høy finansiell aktivitet.

Spesifikke endringer

I fiskeriene har handlingsrommet blitt strammere, med lavere kvoter og flere

reguleringer, særlig der fiskebestanden er alvorlig belastet.

Havforskningsinstituttets kvoteråd for 2026 viser svært kraftige innstramminger for torsk. Blant annet er det iverksatt tiltak som nullfiskeområder og helårlig torskeforbud i Oslofjorden. Når marginene blir mindre og begrensningene flere, kan insentivet til å tøye regelverket øke, for eksempel gjennom under- og feilrapportering av fangst. Utviklingen med reduserte kvoter utpeker seg også innen det pelagiske fiskeriet, der makrell er den mest verdifulle arten. Det internasjonale havforskningsrådet (ICES) anbefaler den laveste makrellkvoten i moderne tid for 2026.[92]

I havbruk har fiskevelferd fått økt oppmerksomhet. Mattilsynets systemrevisjoner i 2024 og 2025 peker på brudd og svakheter hos enkelte aktører.[93] Temaet har også fått mer offentlig fokus, blant annet gjennom Brennpunktserien «Lakselandet», som satte søkelys på fiskevelferd, ulovlig håndtering og ulovlig eksport av produksjonsfisk til land som Kasakhstan, som også kan være en indikasjon på sanksjonsomgåelser.

Vurderinger

Samlet sett vurderes **risikoen** for hvitvasking knyttet til fiskeri- og havbruksnæringen som HØY. Risikonivået påvirkes spesielt av grad av organisering, mangel på kontroll i kombinasjon med kompleksitet og uoversiktlige verdikjeder samt store samfunns- og miljøkonsekvenser.

Trusselen vurderes som HØY. Aktørene har stor kapasitet fordi de kjenner bransjen, er godt organisert og er involvert i flere ledd i verdikjeden. Fiskeri- og havbruksnæringen er sårbar for profesjonelle tilretteleggere i forskjellige roller og det internasjonale aspektet handel på tvers av landegrensene legger også mulighetene til rette for hvitvasking.

Sårbarheten vurderes som BETYDELIG. Fiskeriforvaltningen er kompleks. Den involverer flere kontrollorgan og næringsaktører i tillegg til at regelverket er komplisert. Videre er muligheten for oppdagelse lav, og det gjennomføres få fysiske kontroller av lasterom ved eksport fordi hygienekrav gjør slike inspeksjoner ressurskrevende og avhengige av godkjente kontrollfasiliteter.

Kontrollen består gjerne kun av en dokumentgjennomgang, noe som gjør systemet sårbart for manipulasjon, feilrapportering eller dokumentforfalskning.

Konsekvensnivået vurderes som HØYT. Samfunnet lider store økonomiske tap, bransjen utsettes for konkurransevridning, og handlingene kan ha langsiktige og alvorlige miljøkonsekvenser.

---

92 Fiskeribladet, 2025: *Havforskerne ber om laveste makrellkvote i moderne tid*. Nettlenke, 30.09.2025: https://www.fiskeribladet.no/forskning/havforskerne-ber-om-laveste-makrellkvote-i-moderne-tid/2-1-1878587.

93 Mattilsynet, 2026: *Samlerapport for systemrevisjoner av oppdrettsaktører 2024–2025*. Nettlenke, 03.02.2026: https://www.mattilsynet.no/fisk-og-akvakultur/oppdrettsanlegg/systemrevisjon-av-oppdrettsselskapene/samlerapport-for-systemrevisjoner-av-oppdrettsaktorer-2024-2025.

> Åpne økonomier med velfungerende finanssystemer anses attraktive for plassering og lagring av utbytte fra kriminalitet, også når den underliggende kriminaliteten skjer utenfor landets grense

DEL 6

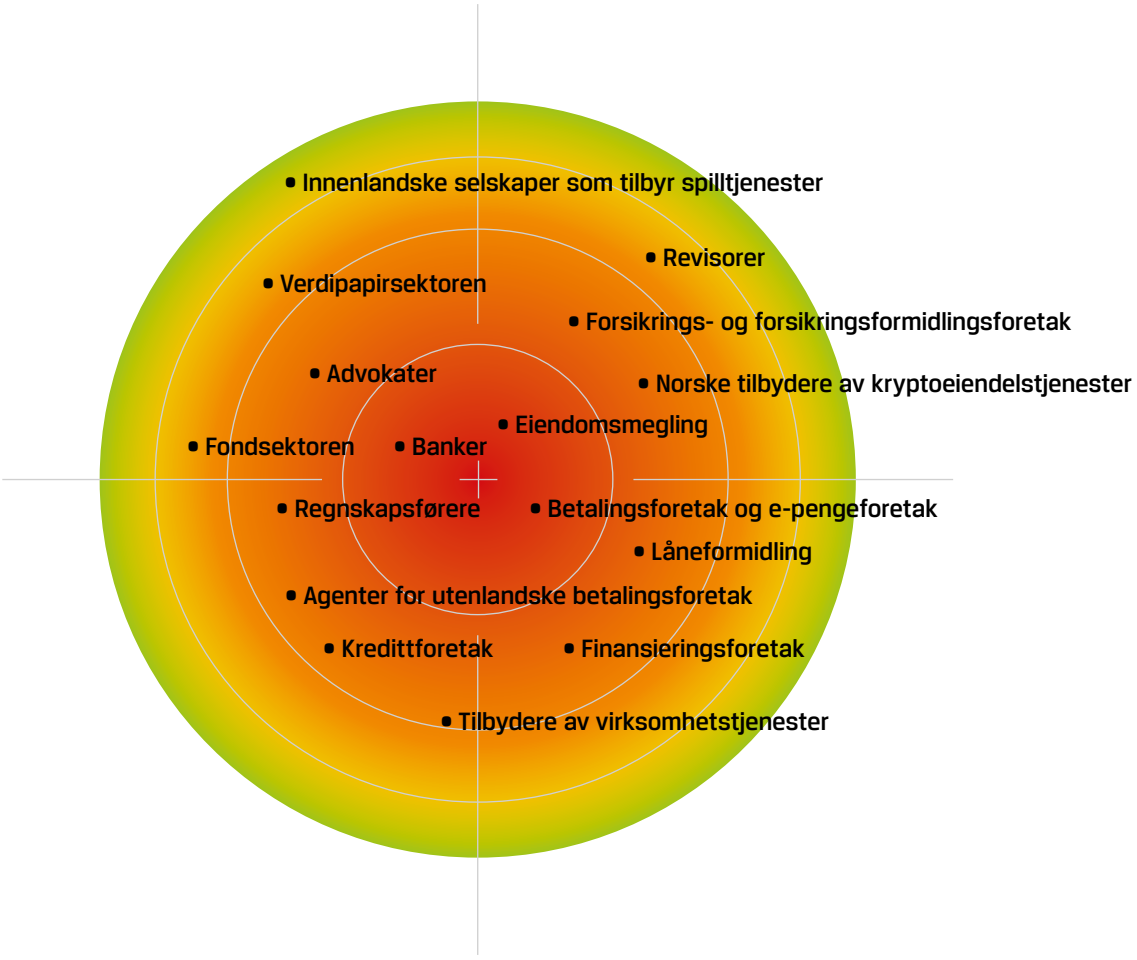
RISIKO FOR HVITVASKING I RAPPORTERINGSPLIKTIG SEKTOR

Foto: iStock

Innledning

I denne delen risikovurderes rapporteringspliktig sektor. Før den enkelte sektor blir presentert, gis en beskrivelse av fellestrekk og forhold som går igjen i flere av sektorene og som derfor også ligger til grunn for risikovurderingene.

Alle kapitlene starter med en generell sektorbeskrivelse etterfulgt av en kort presentasjon av risikonivå sammenlignet med NRA 2022. Videre trekkes spesifikke endringer frem, før vurderingene av trussel, sårbarhet, konsekvens og endelig hvitvaskingsrisiko utdypes. Faktaboksene inneholder tall som beskriver den enkelte sektorens størrelse og antall MF-rapporter de har sendt i 2023–2025.[94]



94 Av systemtekniske årsaker og registreringskategorier, er det avvik mellom sektorkategorier i NRA og hvitvaskingsregisteret. Det er derfor ikke antall MF-rapporter i faktaboks for enkelte sektorer.

Fellestrekk for sektorer

Utviklingen av heldigitale banker og betalingstjenester med grensekryssende virksomhet har tiltatt. Slike forretningsmodeller gir effektive kundetjenester, men kan samtidig svekke foretakets kundekjennskap, skape utfordringer for myndighetenes tilsynsoppfølging og redusere oversikten over pengestrømmer.

EU- og IMF-analyser, særlig for Norden og Baltikum, fremhever grensekryssende betalinger, samt komplekse strukturer og transaksjonsmønstre som sentrale risikofaktorer.[95] Dette, i kombinasjon med bruk av virtuelle IBAN (vIBAN) som er kjent internasjonalt, øker risikoen for manglende transparens om sluttbruker og midlers faktiske opprinnelse.

Siden forrige NRA har den teknologiske utvikling, og bruken av KI spesielt, skutt fart. Bruken av KI kan påvirke risikobildet både positivt og negativt. Det skaper på en side et større handlingsrom som følge av økt profesjonalisering av kriminaliteten som kan gjøre det vanskeligere å avdekke. På den andre siden kan KI også være en del av rapporteringspliktiges antihvitvaskarbeid (AHV).

Effekten av slike løsninger er avhengig av både kvaliteten på løsningen, men også styring og kompetanse hos institusjonene, ettersom feil bruk av *RegTech* og KI også kan skape nye sårbarheter.[96]

Det er variasjoner innad i mange av sektorene, de er sammensatt både når det gjelder foretakenes størrelse, omsetning, produkter, tjenester, kundemasse, forretningsmodeller og geografiske eksponering. Felles risikovurdering av en hel sektor er derfor utfordrende og nivået for hvitvaskingsrisiko for enkeltdeler kan være både høyere eller lavere enn den samlede vurderingen.

Det som i stor grad skiller konsekvensnivået er ikke (bare) omfanget av primærforbrytelsen og utbyttet som hvitvaskes, men hvor store pengestrømmer som går igjennom sektoren og hvor viktig posisjon sektoren har i norsk samfunnsstruktur. Det siste vil være avgjørende for hvor alvorlig det er hvis tilliten til sektoren blir svekket. Bank- og forsikring er bærende sektorer i det norske finansielle systemet, mens eksempelvis kryptovaluta er mindre viktig for selve finanssystemet – tross store pengestrømmer av både legale verdier og hvitvasking.

95 International Monetary Fund, *IMF Nordic-Baltic Regional report no 23/320*, (IMF, 2023). Nettlenke: https://www.imf.org/-/media/files/publications/cr/2023/english/1eurea2023003.pdf

96 European Banking Authority, *Risk Assessment Report of the European Banking Authority, December 2023,* (EBA, 2023).

Risiko for hvitvasking i rapporteringspliktig sektor

BANKER

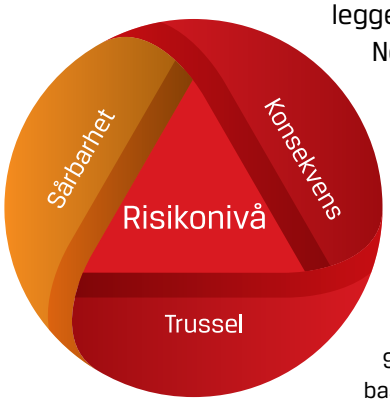
Statistikk og faktaboks *Banker*

Banksektoren omfattes av hvitvaskingsloven § 4 (1) bokstav a.

Antall foretak
Ved utgangen av 2025 hadde 91 norske foretak konsesjon som bank, og 37 utenlandske banker hadde grensekryssende virksomhet gjennom filial i Norge. I tillegg meldte 410 utenlandske banker om grensekryssende virksomhet inn til Norge, uten etablering av filial.[97]

Antall MF-rapporter 2023–2025[98]

Antall MFR	2023	2024	2025
Bank	17 869	23 043	23 231
Totalt alle	23 703	30 658	33 313



Bankene leverer majoriteten av grunnleggende finansielle tjenester i Norge til både privatpersoner og næringsliv. De har en sentral rolle i det finansielle systemet, både som inngangsport til finansielle tjenester og som formidler av store, komplekse pengestrømmer nasjonalt og internasjonalt. Bankene varierer betydelig i størrelse, produkttilbud, kundesammensetning og geografisk eksponering. Sektoren anses

97 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1.

98 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

attraktiv for utnyttelse til hvitvasking fordi produktene og tjenestene muliggjør rask og effektiv flytting av verdier mellom personer, foretak og jurisdiksjoner samt håndtering av komplekse transaksjoner gjennom ulike betalings- og oppgjørsstrukturer.[99] Produkter og tjenester som innskudd, betalingsformidling, internasjonale overføringer, korrespondentforbindelser, kontanter, handelsfinansiering, kreditter, «privat banking» og formuesforvaltning, anses å være særlig egnet til å misbrukes til hvitvasking.

Bankene er innslagspunkt for det meste av utbytte fra kriminalitet som plasseres i finanssystemet. Produktenes og tjenestenes natur gjør dem egnet for hvitvasking, og sektoren anses derfor attraktiv i alle tre fasene av hvitvasking – plassering, tilsløring og integrering.[100]

Risikoen for hvitvasking i banksektoren vurderes som HØY. Dette er uendret fra NRA 2022.

Spesifikke endringer

Endringer i regelverket for blant annet kapitalkrav, soliditet og virksomhetsstyring i banker og innføringen av et mer harmonisert EØS-rammeverk mot hvitvasking innebærer økte krav til intern styring, risikostyring og dokumentert effektivitet av iverksatte kontroller.[101] Hvitvaskingsrisiko forstås i økende grad som en del av operasjonell risiko og virksomhetsstyring, med tydelig ansvar tillagt styre og ledelse.[102]

Innføringen av meldingsstandarden ISO 20022 innebærer mer detaljerte data i betalinger. Dette kan styrke sporbarhet og mulighetene for analyse, blant annet gjennom bedre kvalitet på avsender- og mottakerinformasjon. Samtidig kan økt datamengde og kompleksitet stille høyere krav til systemer, datakvalitet og kompetanse. Mangelfull utnyttelse eller feil implementering av meldingskravene kan minske den reelle risikoreduserende effekten og i enkelte tilfeller skape nye sårbarheter.

---

99 Norges Bank, *Det norske finansielle systemet 2025*, (Norges Bank, 2025).
100 Finanstilsynet, *Risikovurdering 2023*, (Finanstilsynet, 2023).
101 Det vises her til EØS-relevant regelverk (forkortet hhv. CRR/CRD) som blant annet minstekrav til ansvarlig kapital, risikoeksponering og likviditet som regulerer virksomhetsstyring, tilsynsprosesser og utbyttepolicy i banker. Dette er gjennomført i norsk rett.
102 Finansdepartementet (EU) 2024/1623). https://www.regjeringen.no/no/dokumenter/forskrift-om-endring-i-forskrift-6.-desember-2024-nr.-2952-om-endring-i-forskrift-om-kapitalkrav-og-gjennomforing-av-crrcrd-regelverket-ikrafttredelse-av-forordning-eu-20241623/id3090311/.

Revidert forordning om opplysninger som skal følge pengeoverføringer (TFR II) innebærer strengere og mer harmoniserte krav til informasjon som skal følge betalinger. Dette inkluderer overføringer av kryptoeiendeler. Regelverket skal styrke transparens og sporbarhet i grensekryssende transaksjoner og redusere muligheten for anonym overføring av midler. Samtidig medfører TFR II økt operasjonell kompleksitet, operativ kunnskap og behov for tilpasning i bankenes systemer og kontrollprosesser, særlig i grenseflatene mot betalingstjenesteytere og kryptoaktører.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for banksektoren som HØY. Risikonivået påvirkes spesielt av omfang, variasjoner i etterlevelse av hvitvaskingsregelverket, modenhet og kvalitet i AHV-arbeidet i sektoren. Konsekvensene ved svekket tillit vil være store siden banksektoren er en viktig del av det finansielle systemet og samfunnsstrukturen.

Trusselen vurderes som HØY. De fleste former for kriminalitet er aktuelle for forsøk på hvitvasking gjennom banksektoren. Hvitvaskingen kan også bidra til å opprettholde og styrke organisert kriminalitet, korrupsjon og annen alvorlig kriminalitet, både nasjonalt og internasjonalt. Gjennom MF-rapportering gjenspeiles blant annet det store omfanget av bedragerier som er beskrevet i del fem. Det trekker også trusselnivået opp at Norge benyttes som transittland eller oppbevaringssted for midler som stammer fra kriminalitet begått i utlandet. Åpne økonomier med velfungerende finanssystemer anses attraktive for plassering og lagring av utbytte fra kriminalitet, også når den underliggende kriminaliteten skjer utenfor landets grenser.[103]

Videre forsterkes trusselen av økende bruk av selskaper i hvitvaskingsoperasjoner. De foregår ofte gjennom hyppige og til dels sirkulære overføringer mellom banker, sammenblanding av privat- og selskapsøkonomi samt bruk av komplekse eier- og kontrollstrukturer på tvers av selskaper og landegrenser. For bankene anses derfor særlig bedriftssegmentet som utsatt for hvitvasking. I tillegg har utviklingen av grensekryssende heldigitale banker økt de siste årene. Heldigitale banker i kombinasjon med økt bruk av løsninger som vIBAN, bidrar til bedre og raskere service for kundene i det finansielle systemet. Det kan imidlertid komplisere AHV-arbeidet, siden det gir kriminelle større muligheter for å skjule midlenes opprinnelse.

Sårbarheten vurderes som BETYDELIG. Mange banker har investert både ressurser og gjennomført omfattende tiltak mot hvitvasking. Fremdeles varierer etterlevelsen av hvitvaskingsregelverket innad i sektoren. Dette skaper handlingsrom for kriminelle som aktivt kan identifisere banker med svakere AHV-etterlevelse og bytte til disse.

Det øker også sårbarheten at regelverket oppleves som komplekst og til dels krevende å navigere i. Dette gjelder blant annet grensedragningen mellom tillatt informasjonsdeling og avslørings-

103 EU COM, *Supranational Risk Assessment 2022*, (EU COM, 2022).

forbudet. Ulik tolkning og praktisering mellom institusjoner bidrar også til fragmentert informasjonsflyt i eksempelvis undersøkelser etter hvitvaskingsloven. Dette fører til at informasjon som i utgangspunktet kunne vært delt for å forebygge og avdekke hvitvasking, i praksis ikke deles. Samtidig reduseres sårbarheten av at det eksisterer og videreutvikles initiativer for samarbeid og informasjonsutveksling mellom banker og relevante aktører.

Sårbarheten vurderes å være større i bedriftssegmentet enn hos personkunder. Bedriftssegmentet kjennetegnes av mer komplekse kundeforhold, høyere transaksjonsvolum, bruk av mellomledd og ofte grensekryssende strukturer. Det forsterker sårbarheten at det fortsatt er en utilstrekkelig forståelse av reelle rettighetshavere, komplekse eier- og kontrollstrukturer, samt begrenset transparens i internasjonale strukturer. Slike forhold kan føre til at det blir mer krevende for bankene å monitorere og identifisere tilsløring og integrering av utbytte.

Sårbarheten forsterkes også av at tilsynsvirksomheten med sektoren fremstår å være noe begrenset, antallet tilsyn sett i forhold til antallet banker og omfanget av sektoren. Begrenset tilsynsintensitet kan bidra til at svakheter i sektorens interne kontrollsystemer opprettholdes. Videre er det eksempler på mangler i sektorens vurderinger av egne ansattes skikkethet. Slike forhold kan undergrave ellers robuste kontrollsystemer og bidra til at hvitvasking ikke avdekkes.

Banker benytter eksterne leverandører til å foreta transaksjonsovervåkning. I mange tilfeller mangler bankene systemkompetanse, mens leverandøren mangler regelverkskompetanse. Dette forsterker sårbarheten siden systemene som konsekvens ikke i tilstrekkelig grad fanger opp indikasjoner på hvitvasking.

Konsekvensnivået vurderes som HØYT. Det begrunnes særlig i sektorens sentrale rolle i det finansielle systemet og at den fungerer som navet i betalingsformidling, kredittgivning og kapitalflyt. Det økonomiske tapet for samfunnet og sektoren, men også enkeltpersoner, er svært stort siden en stor andel av all hvitvasking foregår via banker. Det kan undergrave tilliten til finanssystemet, offentlige institusjoner og myndighetenes evne til å forebygge og bekjempe økonomisk kriminalitet. Tillit er en grunnleggende forutsetning for finansiell stabilitet, og gjentatte eller alvorlige hvitvaskingssaker kan gi varige skadevirkninger.

Norge er en åpen økonomi med høy grad av internasjonal integrasjon og et velfungerende finanssystem. Mangelfull håndtering av hvitvasking i banksektoren kan svekke Norges omdømme internasjonalt, men også påvirke tilliten hos utenlandske myndigheter, finansinstitusjoner og investorer. Flere internasjonale vurderinger viser at land med sterke finansielle sentre samtidig står overfor alvorligere konsekvenser dersom sektoren misbrukes.

Risiko for hvitvasking i rapporteringspliktig sektor

KREDITTFORETAK

Statistikk og faktaboks *Kredittforetak*

Kredittforetak omfattes av hvitvaskingsloven § 4 (1) bokstav b.

Antall foretak
Ved utgangen av 2025 hadde 27 norske foretak konsesjon som kredittforetak. Ingen utenlandske kredittforetak hadde grensekryssende virksomhet verken i eller inn til Norge.[104]

Antall MF-rapporter
Kredittforetak har ikke egen kategori under virksomhetsområde i hvitvaskingsregisteret og sorterer under ulike kategorier for bank.[105]

Kredittforetak yter kreditt og stiller garantier for egen regning, men skiller seg fra bankene ved at de ikke kan ta imot innskudd eller tilby betalingstjenester.

I Norge utgjør boligkredittforetak hovedtyngden av sektoren, hvor banker har flyttet hele eller deler av boliglånsvirksomheten til egne selskaper. Administrasjon, kredittvurdering, utlånsvur-

104 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

105 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste. Avvik kan forekomme fordi hvitvaskingsregisterets virksomhetskategorier ikke fullt ut samsvarer med sektorinndelingen i NRA.

dering og annen tilknyttet virksomhet utføres normalt av bankene eller andre selskap i konsernet.[106]

Disse foretakene har gjennomgående en enkel produktsammensetning, lav kundekompleksitet og variasjon, i tillegg til begrenset geografisk eksponering.

Øvrige kredittforetak tilbyr blant annet statsstøttede og markedsbaserte eksportkreditter, lån til kjøretøy og maskiner, usikrede forbrukslån, lån til kommunesektoren, mellomlange og langsiktige lån til sparebanker samt næringslån til næringsbygg og -eiendom. Disse produktene kjennetegnes av begrenset transaksjonsintensitet sammenlignet med andre finansielle produkter, men kan innebære økt risiko der utlån kombineres med komplekse selskapsstrukturer, høye lånebeløp eller eksponering mot høyrisikobransjer slik som eiendom og internasjonal virksomhet. Kredittforetak er særlig attraktive i tilslørings- og integreringsfasen av hvitvasking.

Risikoen for hvitvasking gjennom kredittforetak vurderes som MODERAT. Dette er uendret fra NRA 2022.

Spesifikke endringer

Siden forrige NRA har kredittforetakene i Norge vært preget av økt digitalisering, nye distribusjonskanaler og mer spesialiserte forretningsmodeller. Utviklingen øker tilgjengelighet og effektivitet.

Det er gjort endringer i EØS-regelverk[107] som omfatter blant annet kapitalkrav, risikoeksponering og likviditet.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for kredittforetak som MODERAT. Risikonivået påvirkes spesielt av at foretakene i all hovedsak har enkel produktsammensetning med lav geografisk eksponering. Sektoren håndterer store verdier og betydelige pengestrømmer, men har samtidig en mer avgrenset funksjon i det finansielle systemet enn banker, særlig når det gjelder betalingsformidling og løpende kontotjenester.

Trusselen vurderes som MODERAT. Kredittforetak kan benyttes til hvitvasking av utbytte fra straffbare handlinger, særlig gjennom nedbetaling av lån. Det flyter store pengestrømmer gjennom sektoren. Verdier flyttes gjennom ulike produkter og tjenester, herunder boliglån, kredittstillelse og sikkerhet ved kjøp av næringseiendom og annen eiendomsfinansiering. Dette kan gjøre sektoren attraktiv for aktører som søker å stabilisere eller sikre verdier over tid. Samtidig er transaksjonsmønstrene ofte mer forutsigbare og mindre hyppige enn i banksektoren, noe som samlet sett bidrar til et lavere trusselnivå.

Trusselen vurderes som lavere for boligkredittforetak enn for øvrige kredittforetak. Dette begrunnes særlig i at boligkredittforetak i hovedsak mottar lavrisikolån, og at virksomheten i stor grad er begrenset til refinansiering og forvaltning av eksisterende porteføljer. Denne strukturen reduserer handlingsrommet for kriminelle aktører sammenlignet med kredittforetak som tilbyr mer

106 Norges Bank, *Det norske finansielle systemet 2025*, (Norges Bank, 2025).
107 Henholdsvis CRR/CRD.

Foto: Pexels

komplekse eller fleksible finansieringsprodukter.

Sårbarheten vurderes som MODERAT. I mange tilfeller vil sårbarheten i kredittforetak speile etterlevelsen av hvitvaskingsregelverket i morselskapet. Det gjelder særlig der kredittforetaket er tett integrert i bankkonsern når det gjelder styring, kontrollfunksjoner, kundetiltak og transaksjonsovervåking.

Videre varierer sårbarheten ut fra forretningsmodell og kundegruppe. Kompleksitet og manglende innsikt i kundenes økonomiske disposisjoner trekkes frem som sentrale sårbarhetsdrivere. Samtidig forsterkes sårbarheten av begrenset tilsynsaktivitet rettet mot sektoren. Dette kan medføre at svakheter i etterlevelsen i mindre grad avdekkes og korrigeres. I tillegg kan det gi kriminelle aktører et økt handlingsrom, særlig der kredittforetak inngår som del av mer komplekse hvitvaskingsoperasjoner i samspill med banker.

Konsekvensnivået vurderes som MODERAT. Vurderingen reflekterer at kredittforetak i mindre grad enn banker har en systemkritisk funksjon i det finansielle systemet, men samtidig håndterer store verdier og langsiktige finansielle eksponeringer som kan benyttes til integrering og legitimering av kriminelt utbytte. Misbruk av kredittforetak til hvitvasking kan medføre økonomiske tap, både for det enkelte foretak og for tilknyttede finansinstitusjoner. Selv om slike tap normalt ikke vil være av et omfang som alene truer den finansielle stabiliteten, kan de i enkelttilfeller være betydelige og bidra til svekket tillit til foretaket og sektoren.

Risiko for hvitvasking i rapporteringspliktig sektor

FINANSIERINGSFORETAK

Statistikk og faktaboks *Finansieringsforetak*

Finansieringsforetak omfattes av hvitvaskingsloven § 4 (1) bokstav c.

Antall foretak
Ved utgangen av 2025 hadde 25 norske foretak konsesjon som finansieringsforetak. Ingen utenlandske kredittforetak hadde grensekryssende virksomhet gjennom filial i Norge. Ett utenlandsk finansieringsforetak meldte grensekryssende inn til Norge, uten etablering av filial.[108]

Antall MF-rapporter
Finansieringsforetak har ikke egen kategori under virksomhets område i hvitvaskingsregisteret.[109]

108 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

109 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste. Avvik kan forekomme fordi hvitvaskingsregisterets virksomhetskategorier ikke fullt ut samsvarer med sektorinndelingen i NRA.

Finansieringsforetak omfatter foretak med konsesjon til å drive finansieringsvirksomhet uten å ta imot innskudd. Sektoren kjennetegnes av varierte forretningsmodeller. Disse yter i hovedsak kortsiktige og mellomlange lån innen leasing, *factoring*, forbrukslån og gjeldsbrevlån til næringslivet. I tillegg tilbyr de valutaveksling og annen finansieringsrelatert aktivitet.

Ifølge Norges Bank utgjør utenlandske foretak etablert i Norge rundt 30 prosent av sektoren målt i utlånsvolum, noe som kan øke kompleksiteten og risikoprofilen for grensekryssende virksomhet.[110] Produkter med høy transaksjonsintensitet, kort løpetid og svakere tilknytning til realaktiva, herunder valutaveksling og enkelte forbrukskreditter, fremheves i nasjonale og europeiske risikovurderinger som særlig utsatt for misbruk i hvitvaskingens tidlige faser.

Finansieringsforetak anses som attraktive i plasserings- og tilsløringsfasen av hvitvasking, særlig der kontantnære eller valutarelaterte tjenester inngår. Samtidig kan leasing- og factoringvirksomhet også benyttes i integreringsfasen, ved at midler reinvesteres eller gis et legitimt preg gjennom finansiering av eiendeler og næringsvirksomhet.

Risikoen for hvitvasking gjennom finansieringsforetak vurderes som BETYDELIG. Dette er en oppjustering fra moderat i NRA 2022.

Foto: iStock

110 Norges Bank, *Det norske finansielle systemet 2025*, (Norges Bank, 2025).

Virksomheter knyttet til valuta og kontanter trekker trusselen opp

Spesifikke endringer

Endringene og utviklingstrekkene i regelverk som er relevante for bank- og kredittforetakssektoren, er også relevante for finansieringsforetak.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for finansieringsforetak som BETYDELIG. Risikonivået påvirkes spesielt av at sektoren håndterer store verdier og tilbyr produkter som kan benyttes til å integrere utbytte fra kriminalitet i lovlig økonomisk aktivitet, særlig gjennom finansiering, leasing og valutavirksomhet.

Trusselen vurderes som BETYDELIG. Det er imidlertid variasjoner innad i sektoren hvor virksomheter knyttet til valuta og kontanter, herunder valutaveksling, trekker trusselen opp. Finansieringsforetak kan benyttes til hvitvasking ved at ulovlig ervervede midler brukes for å betjene lån eller leasingavtaler. Gjennom regelmessige betalinger kan midlene gis et skinn av legitimitet og kanaliseres inn i næringsvirksomhet eller eiendeler. Når lånet er tilbakebetalt, eller leasingobjektet er kjøpt ut, fremstår verdiene i større grad som lovlig ervervet. Det foreligger ikke konkrete indikasjoner på at utenlandske aktører systematisk benyttes i stedet for norske finansieringsforetak som følge av norske rapporteringspliktiges tiltak.

Sårbarheten vurderes som BETYDELIG. Sektoren er preget av produkt- og kontanteksponering, varierende kompetanse i AHV-arbeidet og begrenset helhetlig kundekunnskap. Disse forholdene utnyttes av kriminelle aktører, særlig når finansieringsforetak benyttes som ledd i mer sammensatte hvitvaskingsoperasjoner på tvers av sektorer, eksempelvis banker og andre finansielle aktører. Sårbarheten vurderes som høyere for valutaaktører enn for øvrige finansieringsforetak, særlig der virksomheten omfatter valutaveksling og kontanthåndtering. For øvrige finansieringsforetak antas det at usikret kreditt og finansiering rettet mot næringsvirksomhet er ekstra sårbare tjenester.

Konsekvensnivået vurderes som BETYDELIG. Finansieringsforetak håndterer store verdier, langsiktige finansielle forpliktelser og eiendeler. Konsekvensene kan derfor medføre vesentlige økonomiske tap for både virksomheter og enkeltpersoner. Selv om konsekvensene vil være mindre systemkritiske for betalingsformidlingen enn for bankene, kan de i enkeltsaker være alvorlige og få betydelig økonomisk og samfunnsmessig betydning. I tillegg skades samfunnets tillit til sektoren.

Risiko for hvitvasking i rapporteringspliktig sektor

BETALINGS- OG E-PENGEFORETAK

Statistikk og faktaboks *Betalings- og e-pengeforetak*

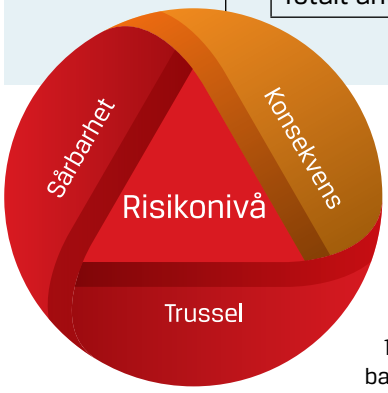
Betalings- og e-pengeforetak omfattes av hvitvaskingsloven §4 (1) bokstav g og e.

Antall foretak
Ved utgangen av 2025 hadde 20 norske foretak konsesjon som betalingsforetak, og fem utenlandske betalingsforetak hadde grensekryssende virksomhet gjennom filial i Norge. I tillegg meldte 265 utenlandske betalingsforetak om grensekryssende virksomhet inn til Norge, uten etablering av filial.[111]

Ved utgangen av 2025 hadde ni norske foretak konsesjon som e-pengeforetak, og ingen utenlandske betalingsforetak hadde grensekryssende virksomhet i Norge. I tillegg meldte 195 utenlandske e-pengeforetak om grensekryssende virksomhet inn til Norge, uten etablering av filial.[112]

Antall MF-rapporter 2023–2025[113]

Antall MFR	2023	2024	2025
Betalingsforetak	1 620	2 126	1 953
E-pengeforetak	294	732	2 306
Totalt antall	23 703	30 658	33 313



111 Det er flere betalingsforetak i EU/EØS som nå tilbyr betalingstjenester med e-pengetokens og som også grensekrysser disse inn til Norge.
112 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1
113 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

Sektorene omfatter et bredt spekter av produkter og tjenester, herunder pengeoverføringstjenester, digitale lommebøker, mobil- og nettbaserte betalingsløsninger, gavekort, forhåndsbetalte instrumenter og selvbetjenings- og betalingsløsninger. Disse er i rask og kontinuerlig endring. Blant aktørene inngår både globale betalingsformidlere som tilbyr betalingstjenester i Norge, og norske foretak innen blant annet billettformidling, dagligvarehandel, lojalitets- og betalingsprogrammer. I tillegg omfattes regulerte tilbydere av gavekort og betalingsløsninger knyttet til kryptotjenester, der betalingstjenester benyttes som ledd i kjøp, salg eller oppbevaring av digitale verdier.

Enkelte betalings- og e-pengeforetak har betalingstjenester som sin kjernevirksomhet, men en betydelig andel av foretakene tilbyr slike tjenester som et supplement til annen virksomhet, der ikke alle tjenestene omfattes av sektorregelverket. Dette kan omfatte digitale plattformer, handel og tjenesteytere samt teknologiselskaper der betalingstjenester inngår som en integrert del av hovedproduktet. Betalings- og e-pengeforetak er attraktive for hvitvasking, særlig i plasserings- og tilsløringsfasen.

Risikoen for hvitvasking gjennom betalings- og e-pengeforetak vurderes som HØY. Nivået er uendret fra forrige NRA for betalingsforetak, mens e-pengeforetak er oppjustert fra betydelig til høy.

Spesifikke endringer

Den nye kryptoreguleringen gjennom MiCA[114] som er gjennomført i norsk rett gjennom kryptoeiendelsloven, har betydning for betalings- og e-pengeforetaksektoren. Regelverket innebærer blant annet at foretak som utsteder e-pengetokens som hovedregel må ha konsesjon som bank eller e-pengeforetak. Samtidig åpner regelverket for enkelte unntak, som kan innebære at enkelte utstedere ikke blir konsesjons- eller rapporteringspliktige. Dette kan skape regulatoriske gråsoner og ulik risikohåndtering i markedet.

Det har over tid blitt færre tilbydere av pengeoverføringstjenester, særlig for overføringer til tredjeland. En sentral årsak er at slike tilbydere har utfordringer med å etablere og opprettholde bankforbindelser i Norge. Tilsvarende utfordringer gjelder for utenlandske foretak som tilbyr grensekryssende betalingstjenester i Norge gjennom agenter. Dette kan redusere konkurransen, men også føre til at etterspørselen etter slike tjenester flyttes til mindre regulerte eller uformelle kanaler.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for betalings- og e-pengeforetak som HØY. Det er imidlertid stor variasjon innad i sektorene. Risikoen påvirkes i stor grad av hvilke produkter og tjenester som tilbys, graden av digitalisering, foretakenes rolle i transaksjonskjeden og om virksomheten innebærer lagring, overføring eller aggregering av kundemidler. I tillegg øker risikonivået spesielt av lite kontroll og uklart regelverk med mulighet for ulik tolkning. Etterlevelsen av hvitvaskings-regelverket er tidvis mangelfull.

114 Markets in Crypto-Assets.

Sektorene omfatter et bredt spekter av produkter og tjenester

Foretak med tjenester og produkter som innebærer kryptoeiendeler påvirker også risikoen, spesielt for e-pengeforetak. Selv om mekanismene er tydelige, er det stor usikkerhet knyttet til omfanget av hvitvasking i sektoren. Risikoen påvirkes også av høy transaksjonsfrekvens, rask flytting av midler, bruk av digitale løsninger med begrenset kundekontakt og i grensekryssende betalinger.

Trusselen vurderes som HØY. Nivået påvirkes spesielt av sektorens høye transaksjonsvolum, raske og fleksible betalingsløsninger, økt bruk av agenter og uformelle kanaler. I tillegg er det indikasjoner på omfattende ulovlig virksomhet og mørketall. Trusselaktørene omfatter både organiserte kriminelle nettverk og profesjonelle tilretteleggere som utnytter både regulerte og uregulerte deler av betalingsmarkedet.

Trusselnivået forsterkes videre av at det har blitt færre foretak med tillatelse til å tilby pengeoverføringstjenester, samtidig som det knytter seg bekymring til at en større andel av pengeoverføringstjenestene skjer via agenter eller utenfor det regulerte markedet. Denne utviklingen skaper økt handlingsrom ved at kriminelle kan utnytte svakere kontrolledd, uregistrerte aktører eller uformelle betalingskanaler.

E-pengetjenester kan være særlig attraktive for hvitvasking fordi de er lett tilgjengelige samtidig som omsetning og bruk i betalingskjeden foregår raskt. Slike tjenester kan gi kriminelle aktører rask tilgang til betalingsinfrastruktur, redusere behovet for kontanter og legge til rette for lagdeling av midler gjennom flere ledd og produkter.

En særlig relevant trussel er knyttet til ulovlig hawala-virksomhet og andre uformelle verdioverføringssystemer, hvor uregulerte pengeoverføringer tilbys utenfor etablerte kontroll- og rapporteringsmekanismer. Slike betalingstjenester kan blant annet tilbys gjennom agenter for utenlandske betalingsforetak som ikke er korrekt innmeldt eller registrert i henhold til regelverket. De kan også benyttes til å flytte verdier over landegrenser med begrenset sporbarhet. Disse omtales i neste kapittel.

Sårbarheten vurderes som HØY for betalings- og e-pengeforetak. Nivået påvirkes spesielt av manglende stedlig tilsyn over tid, varierende kompetanse om forpliktelser etter hvitvaskingsregelverket og etterlevelse av dette i kombinasjon med teknologisk kompleksitet og rask utvikling. Sårbarheten varierer avhengig av foretakenes størrelse, forret-

ningsmodell og hvilke typer betalings- og e-pengetjenester som tilbys. Dette samsvarer med funn i rapporter fra European Banking Authority, som indikerer at betalings- og e-pengeforetakssektoren samlet sett ikke har optimal etterlevelse av hvitvaskingsregelverket sett opp mot risikoen hos det enkelte foretak. Sårbarheten forsterkes av at mange raske og grensekryssende betalingsstrømmer kan gjøre løpende oppfølging og etterkontroll krevende. Dette gjelder både formelle betalingsløsninger og mer uformelle eller hawala-lignende mekanismer for verdioverføring, hvor sporbarheten kan være begrenset og midlene raskt flyttes mellom jurisdiksjoner.

Regulatorisk usikkerhet kan føre til at enkelte foretak tolker seg inn under unntaksbestemmelser og dermed unnlater å etterleve rapporteringsplikten. Når det gjelder grensekryssende virksomhet uten etablering, forsterkes sårbarheten ved at det i hovedsak er hjemstatsmyndigheten som har tilsynsansvaret, mens tjenestene tilbys i vertslandet. Dette kan medføre at den grensekryssende virksomheten følges opp i mindre grad, enten fordi tjenestene er geografisk og regulatorisk «langt unna», eller fordi det foreligger uklarhet om ansvar og oppfølging mellom tilsynsmyndigheter.

Konsekvensnivået vurderes som BETYDELIG. Det er potensielt store økonomiske tap. Dette kan i vesentlig grad undergrave systemet og tilliten til det, siden sektoren har en sentral rolle i betalingsinfrastrukturen, høye transaksjonsvolum og funksjon som bindeledd mellom kontanter, digitale betalingsløsninger og det ordinære finanssystemet.

Foto: iStock

Risiko for hvitvasking i rapporteringspliktig sektor

AGENTER FOR UTENLANDSKE BETALINGSFORETAK

Statistikk og faktaboks *Agenter for utenlandske betalingsforetak*

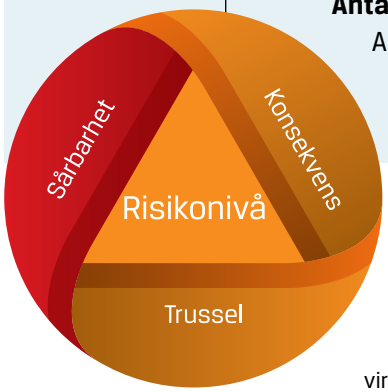
Agenter for utenlandske betalingsforetak omfattes av hvitvaskingsloven §4 (6) bokstav g, jf. Hvitvaskingsforskriften § 1-2.

Antall foretak

Ved utgangen av 2025 var det 184 agentforhold fordelt på 131 unike foretak for utenlandske betalingsforetak. Dette var fordelt på syv utenlandske betalingsforetak, hvorav ett har vesentlig annerledes forretningsmodell. I tillegg var det 26 agentforhold, alle med unike foretak, for utenlandske e-pengeforetak. Disse var fordelt på 2 utenlandske betalingsforetak. Ingen var grensekryssende.[115]

Antall MF-rapporter

Agenter for utenlandske betalingsforetak har ikke egen kategori under virksomhetsområde i hvitvaskingsregisteret.[116]



115 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

116 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste. Avvik kan forekomme fordi hvitvaskingsregisterets virksomhetskategorier ikke fullt ut samsvarer med sektorinndelingen i NRA.

Agenter av utenlandske betalingsforetak er foretak etablert i Norge som på vegne av betalingsforetak med konsesjon i andre EØS-land tilbyr betalingstjenester til kunder i det norske markedet.

Agentene kan utføre betalingstransaksjoner, herunder pengeoverføringer, kontanttjenester og andre betalingsformidlingstjenester, og er rapporteringspliktige etter hvitvaskingsregelverket.

Transaksjonsmønsteret i sektoren er preget av en betydelig overvekt av grensekryssende betalinger, ofte til mottakere i utlandet. Dette kan bidra til å svekke sporbarheten og vanskeliggjøre myndighetenes oppfølging. I hvitvaskingsøyemed benyttes agenter av utenlandske betalingsforetak særlig til å overføre utbytte fra kriminalitet ut av Norge. Sektoren er spesielt attraktiv for hvitvasking i plasserings- og tilsløringsfasen fordi midler raskt kan flyttes videre til andre jurisdiksjoner.

Risikoen for hvitvasking gjennom agenter for utenlandske betalingsforetak vurderes som BETYDELIG. Dette er en nedjustering fra forrige NRA, da risikoen var vurdert som høy.

Spesifikke endringer

Antallet agenter av utenlandske betalingsforetak i Norge er nedadgående, og antallet transaksjoner i valutaregisteret har sunket gjennom flere år. I 2021 var det i underkant av 880 000 transaksjoner, mens det i 2024 var sunket til i overkant av 620 000. I slutten av oktober 2025 var antallet sunket ytterligere til 479 915 transaksjoner.

Det kan være flere årsaker til nedgangen, men det er rimelig å anta at behovet for internasjonal pengeoverføring ikke har gått ned. Nedgangen kan være knyttet til nedgangen i pengeoverføringsaktører med norsk konsesjon. De utenlandske foretakene melder selv at digitale flater øker på bekostning av fysiske. De digitale kanalene er ofte tjenester tilbudt grensekryssende uten fysisk etablering i vertslandet, og rapporterer dermed heller ikke til valutaregisteret. I tillegg er det mulig at transaksjoner i større grad går via uformelle og ulovlige systemer, men en betydelig andel kan også ha funnet veien til andre, lovlige tjenester som ikke rapporterer til valutaregisteret.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** som BETYDELIG for agenter for utenlandske betalingsforetak. Dette er en nedjustering fra høy i forrige NRA. Den samlede risikoen trekkes ned av omfanget på pengestrømmer og nedgangen i antall agenter. Samtidig påvirkes risikonivået spesielt av stor sårbarhet blant annet som følge av begrenset kontroll med sektoren, manglende kompetanse og varierende kundekontroll.

Trusselen vurderes som BETYDELIG. Finanstilsynet anslår at det i 2024 ble gjennomført transaksjoner for om lag 2,4 milliarder kroner gjennom slike agenter. Trusselen knyttes særlig til kontantgenererende kriminalitet og at midlenes opprinnelse er vanskelig å kontrollere. Videre er det observert tette knytninger mellom kriminelle og enkelte agenter i sektoren. Slike koblinger kan

innebære at agenter bevisst tilrettelegger for hvitvasking[117], eller at kriminelle utnytter agenter med svakere kontrollrutiner og lavere kompetanse i regelverksetterlevelse. I tillegg kan kriminelle aktører selv søke å etablere seg som agenter, for dermed å få direkte tilgang til betalingsinfrastruktur.

Sektoren er også eksponert for utenlandske pengestrømmer, noe som kan øke kompleksiteten i kundekontroll og oppfølging. Grensekryssende transaksjoner kan involvere flere ledd og jurisdiksjoner, og på den måten redusere sporbarhet. Dette er særlig relevant der transaksjonene berører land eller miljøer med svakere kontrollregimer, eller der det forekommer bruk av mellommenn og stråpersoner.

Sårbarheten vurderes som HØY. Nivået påvirkes spesielt av begrenset tilsynsvirksomhet de siste årene. I tillegg til agentenes organisatoriske struktur med mange små virksomheter, ofte organisert som enkeltpersonforetak eller små foretak, med begrensede ressurser til internkontroll, opplæring og systematisk etterlevelse. Sårbarheten trekkes også opp av at agenter kan tilby en grad av anonymitet, særlig gjennom håndtering av kontanter. Kontantbaserte eller kontantnære transaksjoner innebærer ofte begrenset kontroll med midlenes opprinnelse, og i enkelte tilfeller svakere verifisering av kundens identitet. Videre forsterkes sårbarheten gjennom at slike agenter er svært tilgjengelig for mange ulike grupper og miljøer, herunder personer med begrenset tilgang til ordinære banktjenester. Det brede nedslagsfeltet kan gjøre det vanskelig å skille lovlige behov fra utnyttelse til hvitvasking, og kan bidra til et høyt transaksjonsvolum med varierende kvalitet på kundekontroll.

Sårbarheten øker også grunnet begrenset tilgang til banktjenester for både agenter og utenlandske betalingsforetaks egne enheter i Norge. I praksis har det blitt stadig vanskeligere å etablere og opprettholde kundeforhold i bank. Dette kan i ytterste konsekvens føre til at regulerte aktører får problemer med å drive lovlig pengeoverføringsvirksomhet. En mulig følge av dette er økt bruk av ulovlig betalingstjenestevirksomhet, herunder hawala-lignende tjenester eller andre uformelle mekanismer for irregulær verdioverføring over landegrenser. Slike systemer opererer i stor grad utenfor regulering og tilsyn, og innebærer vesentlig høyere hvitvaskingsrisiko.

Konsekvensnivået vurderes som BETYDELIG. Utnyttelse av sektoren til hvitvasking vil kunne undergrave samfunnets tillit til slik betalingsformidling og tilsynsregimet, særlig dersom det avdekkes gjentatte ulovligheter eller det blir kjent at enkelte agenter har kriminelle koblinger. Tillitstap kan også svekke sektorens legitime rolle i grensekryssende betalinger, blant annet for arbeidstakere, studenter og virksomheter med internasjonale behov.

117 På engelsk: crime-as-a-service (CaaS).

Foto: Pexels

Risiko for hvitvasking i rapporteringspliktig sektor

NORSKE TILBYDERE AV KRYPTOEIENDELSTJENESTER (VIRTUELLE TJENESTER)

Statistikk og faktaboks *Norske tilbydere av kryptoeiendelstjenester*

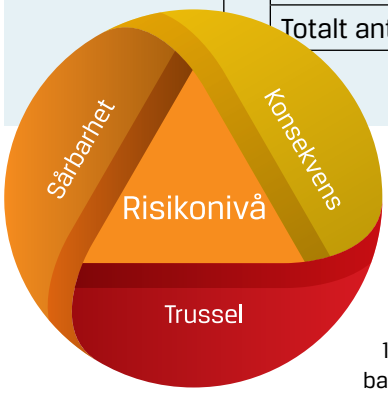
Kryptoeiendelstjenestesektoren omfattes av hvitvaskingsloven §4 (1) bokstav p.

Antall foretak

Ved utgangen av 2025 hadde ingen foretak fått tillatelse til å yte kryptoeiendelstjenester etter ny forordning, (EU) 2023/1114 om markeder for kryptoeiendeler (MiCA) artikkel 60 nr. 3, jf. kryptoeiendelsloven § 1, men det var flere søknader til behandling.[118]

Antall MF-rapporter 2023–2025[119]

Antall MFR	2023	2024	2025
Kryptotilbyder	635	424	401
Totalt antall	23 703	30 658	33 313



118 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

119 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

Sektoren omfatter foretak som yter kryptoeiendelstjenester herunder veksling av kryptoeiendeler mot *fiatvaluta* eller andre kryptoeiendeler, oppbevaring og administrasjon av kryptoeiendeler på vegne av kunder, overføring av kryptoeiendeler samt drift av handelsplattformer. Tjenestene er i stor grad digitalt tilgjengelige, krever begrenset teknisk kompetanse for sluttbruker og kan benyttes på tvers av landegrenser uten bruk av tradisjonelle finansielle mellomledd. Handel og oppbevaring av kryptovaluta er tilgjengelig for de fleste og krever lite eller ingen spesiell kompetanse.

Kryptoeiendeler kan overføres raskt og grensekryssende. Bruk av pseudonyme adresser, egenforvaltede lommebøker og komplekse transaksjonskjeder innebærer fortsatt særskilte utfordringer knyttet til blant annet sporbarhet og identifisering av reelle rettighetshavere.

Sektoren er attraktiv for hvitvasking i alle tre fasene, tilsløring, integrering og plassering.

Mange nordmenn bruker utenlandske kryptoaktører som ikke er rapporteringspliktige i Norge, siden norske aktører har en liten andel av det globale markedet for veksling til virtuell valuta. Vurderingene av sektoren i denne delen av rapporten må sees i sammenheng med relevante kapitler i del tre, fire og fem.

Risikoen for hvitvasking gjennom norske tilbydere av kryptoeiendelstjenester vurderes som BETYDELIG. Det er en oppjustering fra moderat i forrige NRA.

Spesifikke endringer

Siden NRA 2022 har det skjedd vesentlige regelverksendringer som også omfatter kryptoeiendelsektoren, herunder innføringen av et mer harmonisert EU-regelverk for kryptoeiendeler, MiCA.[120] Regelverket er inntatt i norsk rett ved lov om kryptoeiendeler[121] Foretak med tillatelse etter gammelt regelverk er omfattet av en overgangsordning frem til juni 2026. Ved utgangen av 2025 var det ikke gitt noen tillatelser etter MiCA.

Siden forrige NRA i 2022 har kryptovaluta blitt en tilgjengelig investeringsform som mange benytter seg av. Flere stater vurderer å opprette beholdninger av kryptovaluta.

1. januar 2026 ble det innført opplysningsplikt for tilbydere av vekslings- og oppbevaringstjenester for kryptoeiendeler (CARF).[122]

120 Forordning (EU) 2023/1114 om markeder i kryptoeiendeler.
121 Lov om kryptoeiendeler (Kryptoeiendelsloven).
122 Skatteetaten. Frigitt 04.05.2026: https://www.skatteetaten.no/bedrift-og-organisasjon/rapportering-og-bransjer/tredjepartsopplysninger/bank-finans-og-forsikring/kryptoeiendeler-carf/

> Siden NRA 2022 har kryptovaluta blitt en tilgjengelig investeringsform mange benytter seg av

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** via norske tilbydere av kryptoeiendelstjenester som BETYDELIG. Risikonivået påvirkes spesielt av stadig endringer og rask utvikling, blant annet innen teknologi. Egenskapene ved tjenestene som tilbys, tjenestetilbydernes eksponering mot blant annet kunder, kundegrupper, geografi og hvilke valutaer foretakene er i befatning med, påvirker risikoen løpende. Tilsynserfaring underbygger at foretakene i stor grad risikerer å bli utnyttet til hvitvasking.

Varierende regeletterlevelse og lav modenhet i AHV-arbeidet hos deler av sektoren, kombinert med forekomst av ulovlige og uregistrerte aktører, forsterker risikoen. Innføringen av MiCA-regelverket vurderes å ha en risikodempende effekt for den regulerte delen av markedet, og sentrale norske aktørers etterlevelse bidrar positivt. Den er imidlertid ikke tilstrekkelig til å redusere den samlede risikoen på kort sikt, blant annet som følge av fortsatt høy aktivitet i uregulerte og grensekryssende deler av markedet. Risikoen for hvitvasking i kryptoeiendelssektoren vurderes i stor grad å avhenge av graden av regulering, kvaliteten på aktørenes risikostyring og effektiv samhandling mellom kryptotilbydere, finanssektoren og myndighetene.

Trusselen vurderes som HØY. Det flyter store summer gjennom sektoren og verdiene forflyttes gjennom en variasjon av ulike produkter og tjenester. I flere straffesaker er det foretatt beslag og inndragning av kryptoeiendeler. Det er vanskelig å anslå det samlede omfanget, blant annet som følge av grensekryssende virksomhet og bruk av utenlandske aktører. Selv om det er få norske aktører i markedet, kan utenlandske aktører benyttes i kombinasjon med norske tilbydere. Det kan for eksempel skje ved at kryptoeiendeler opptjenes, veksles eller flyttes over utenlandske plattformer før midler tas ut via norske aktører. Dette medfører at norske tilbydere av kryptoeiendelstjenester kan bli eksponert for kapital med opprinnelse fra utlandet.

Videre er det mistanke om omfattende ulovlig virksomhet i det norske markedet, herunder at mange aktører tilbyr kryptoeiendelstjenester uten nødvendig tillatelse. Finanstilsynet mottar jevnlig varsler om slike foretak. Blant annet brukes desentraliserte løsninger, stråpersoner og selskapsstrukturer.

Kriminelle ønsker også å tilby krypto-tjenester selv.

Sårbarheten vurderes som BETYDELIG. Det er spesielt lite gjennomsiktige, komplekse tjenester og anonymitet som øker sårbarheten og gjør sektoren attraktiv for hvitvasking. Sektoren utvikler seg raskt, har lav forståelse for kravene i hvitvaskingsregelverket, preges av manglende etterlevelse og risikoforståelse ved egen virksomhet. Dette forsterker sårbarheten. I tillegg er det høy eksponering fra midler i utlandet som i mange tilfeller er utfordrende å spore.

Kryptoeiendelsektoren samhandler i økende grad med banker, betalingstjenesteytere og andre finansforetak, blant annet gjennom inn- og utbetalingstjenester, oppbevaring og formidling. Disse grenseflatene kan representere både et kontrollpunkt og en sårbarhet. Mangelfull informasjonsdeling, ulik vurdering av risiko og etterlevelse av regelverk gir kriminelle aktører handlingsrom til å flytte midler mellom regulerte og mindre regulerte deler av systemet. Videre har MiCA strammet opp regelverket knyttet til hvitvasking, særlig for attraktive produkter som *stablecoins*. Med nytt regelverk er det også innført flere tilsynsverktøy som reduserer sårbarheten. Viktige norske aktører følger opp regelverket og det reduserer sektorens sårbarhet i Norge.

Konsekvensnivået vurderes som MODERAT. Kryptovaluta er ikke sentralt for det finansielle systemet i Norge, men bruken og omfanget er økende. At sektoren benyttes i hvitvasking, kan påføre samfunnet tap hvis midlene også holdes skjult for skattemyndighetene. Det kan forøvrig påvirke sektorens rykte negativt.

Foto: iStock

Risiko for hvitvasking i rapporteringspliktig sektor

FORSIKRINGS- OG FORSIKRINGSFORMIDLINGS-FORETAK

Statistikk og faktaboks *Forsikrings- og forsikringsformidlingsforetak*

Forsikrings- og forsikringsformidlingsforetak omfattes av hvitvaskingsloven § 4 (1) bokstav j og k.

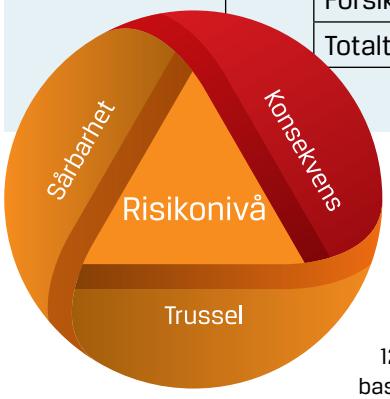
Antall foretak

Ved utgangen av 2025 hadde 57 norske foretak konsesjon som forsikringsforetak, og 31 utenlandske foretak drev grensekryssende virksomhet gjennom filial i Norge. I tillegg rapporterer 411 foretak om grensekryssende virksomhet inn til Norge, uten etablering av filial.

Ved utgangen av 2025 hadde 2 566 norske foretak tillatelse til å drive forsikrings-formidling, og 14 utenlandske foretak drev grensekryssende virksomhet gjennom filial i Norge.[123]

Antall MF-rapporter 2023–2025[124]

Antall MFR	2023	2024	2025
Forsikringsforetak	386	470	468
Forsikringsformidling	3	7	7
Totalt antall	23 703	30 658	33 313



123 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

124 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

Hvitvasking kan forekomme når illegale midler benyttes til betaling av forsikringspremier, sparing eller investering, og senere utbetales som forsikringsytelser til kunde eller tredjepart. Dette gjelder særlig produkter med sparings- og investeringskomponenter, som kapital- og livsforsikring. Det utbetales årlig betydelige beløp gjennom forsikringssektoren, hvorav hoveddelen er legitime erstatnings- og forsikringsutbetalinger. I 2024 ble det alene utbetalt over 65 milliarder kroner i skadeforsikring, i tillegg til betydelige beløp innen person- og livsforsikring.

Sektoren omfatter forsikringsforetak samt forsikringsmeglere, gjenforsikringsmeglere og forsikringsagenter, herunder aksessoriske forsikringsagenter. Hoveddelen av markedet domineres av noen få store foretak.[125] Livsforsikring utgjør størstedelen av forsikringsmarkedet målt i premieinntekter. Skadeforsikring kjennetegnes av et større antall foretak og et bredt produktspekter.

Hvitvasking kan også finne sted før utbetaling, ved at illegale midler plasseres i forsikringsprodukter, eksempelvis gjennom engangsinnskudd i kapitalforsikring eller andre spareprodukter, for deretter å fremstå som legitime midler ved senere uttak eller overføring. Forsikringssektoren fremheves derfor som særlig relevant i plasserings- og integreringsfasen av hvitvasking.

Risikoen for hvitvasking gjennom tilbydere av forsikrings- og forsikringsformidlingsforetak vurderes som BETYDELIG. Dette er en oppjustering fra moderat i forrige NRA.

Spesifikke endringer

Sjøforsikring, som i stor grad er preget av grensekryssende virksomhet, komplekse kontraktsforhold og bruk av internasjonale aktører, er særlig utsatt for mulig brudd på sanksjonsregelverk, hvitvaskingsregelverk og dokumentforfalskning. Forsikring av fartøy, last og transport kan innebære involvering av høyrisikojurisdiksjoner, komplekse eierstrukturer og begrenset transparens om reelle rettighetshavere. Dette kan gjøre det krevende å vurdere risiko knyttet til både kunder, forsikrede objekter og underliggende transaksjoner.

125 Livsforsikring: KLP, Storebrand Livsforsikring og Nordea Liv. Skadeforsikring: Gjensidige, If Skadeforsikring, Fremtind Forsikring og Tryg, ifølge Norges Bank, *Det norske finansielle systemet,* (Norges Bank, 2025).

Vurderinger

Samlet sett vurderes **hvitvaskings-risikoen** for forsikringssektoren som BETYDELIG. Dette er en oppjustering fra moderat i forrige NRA. Risikonivået og oppjusteringen begrunnes spesielt av stort omfang og økt profesjonalisering og organisering hos trusselaktører. Til tross for økt bevissthet knyttet til hvitvaskingsrisiko i bransjen, trekkes risikoen opp av komplisert regelverk som gir rom for ulik tolkning, begrenset tilsynsvirksomhet og kontroll i bransjen. Livsforsikringsområdet antas å ha høyere hvitvaskingsrisiko enn skadeforsikringsområdet. På dette punktet skiller Norge seg fra resten av Europa, ved at skadeforsikring er omfattet av hvitvaskingsregelverket.

Trusselen vurderes som BETYDELIG. I 2025 ble det avdekket forsikringssvindel for over en halv milliard kroner. Dette er det høyeste nivået registrert noen gang i Norge.[126] Tabell 1 viser avslått beløp for de tre siste årene. Forsikringsbransjen avgjør mange saker, uten at dette blir registrert som svik, derfor gir oversikten kun en indikasjon på omfanget av svindel per år. Det antas også at det er betydelige mørketall, og det er derfor knyttet moderat usikkerhet til vurderingen.

Produkter innen individuelle livsforsikringsavtaler med stort innslag av spare- og investeringselement vurderes å være mer utsatt for hvitvasking enn alminnelige skade- og livsforsikrings-

Foto: iStock

126 FinansNorge, *Forsikringssvindel i Norge – Svik statistikk for avdekkede saker i 2025,* (FinansNorge, 2026).

> Gransking av næringskunder og mer komplekse eier- og kontrollstrukturer er ofte mer ressurskrevende enn gransking av privatpersoner

År	2023	2024	2025
Avslått beløp	491 mill. kr	496 mill. kr	526 mill. kr

Tabell 1: Avslåtte beløp i millioner kroner per år. Kilde: Forsikringsdrift.[127]

produkter, særlig der produktene kombinerer mulighet for store innbetalinger med fleksibilitet ved uttak og endringer i avtalen.[127] Disse forsikringene har til sammen befatning med store verdier. Ved utgangen av 2025 utgjorde innskutt beløp rundt 150 milliarder kroner. Livsforsikringsforetakenes øvrige forsikringsforpliktelser utgjorde på samme tid rundt 2 000 milliarder kroner. Selv om produktene omfatter betydelige beløp, utgjør de likevel en begrenset andel av livsforsikringsforetakenes samlede forpliktelser.

Hvitvasking i skadeforsikring skjer ofte i kombinasjon med forsikringssvindel. Typiske fremgangsmåter er blant annet (i) betaling av egne eller andres forsikringspremier med utbytte fra kriminalitet, (ii) innbetaling av for høy forsikringspremie etterfulgt av tilbakebetaling til forsikringstaker eller tredjepart, og (iii) forsikring av relativt kostbare objekter der midlenes opprinnelse ikke kan dokumenteres. Videre observeres ofte svart arbeid, uregistrert eller skjult næringsvirksomhet og anskaffelse av verdigjenstander uten dokumenterbar finansiering i slike saker. Det kan være saker der privatpersoner driver skjult næringsvirksomhet for eksempel omfattende kjøp og salg av kjøretøy, eller saker der det er et klart misforhold mellom forsikringstakers kjente inntekt eller formue og verdien av objektene som ønskes forsikret, eller premiens størrelse.

127 Finanstilsynet, *Risikovurdering 2023*, (Finanstilsynet, 2023).
128 Nettlenke, 11.03.2026: https://www.forsikringsdrift.no/artikler/2026/forsikringssvindel-for-over-en-halv-milliard-avsl%C3%B8rt

Trusselaktørene som utnytter sektoren spenner fra opportunistiske enkeltpersoner til profesjonelle og organiserte kriminelle nettverk. Forsikringsbransjen vurderer at kriminelle aktører over tid har utviklet økt kapasitet og bedre organisering nasjonalt og på tvers av landegrenser, samt tilegnet seg høyere kompetanse og blitt mer profesjonelle. Det er tegn til organisering i enkelte saker knyttet til små og mellomstore bedrifter (SME), hvor håndverks- og tjenesteytende virksomheter fremstår som særlig utsatte. Samtidig er det kun en lav andel MFR som gjelder foretak. Når det gjelder utsatthet for hvitvasking av midler fra kriminalitet i utlandet, vurderes enkeltpersonforetak (ENK) som sårbare, blant annet fordi disse ofte har utenlandske innehavere, og bransjestatistikk viser at denne registreringsformen er overrepresentert i hvitvaskingssaker.

Trusselbildet forsterkes av utviklingstrekk som økt digitalisering og fjernkundeløsninger, mer komplekse produkter og betalingsstrømmer samt at kriminelle aktører i større grad kjenner til rapporteringsgrenser og kontrollrutiner. Dette kan gi trusselaktørene økt handlingsrom og gjøre avdekking mer ressurskrevende.

Sårbarheten vurderes som BETYDELIG. Nivået påvirkes spesielt av begrenset tilsynsvirksomhet, mangler i etterlevelsen av hvitvaskingsregelverket samt risikovurderinger og rutiner hos deler av foretakene. I tillegg kommer ujevn opplæring og utfordringer knyttet til komplekst regelverk og informasjonsdeling. Til tross for at det er rapportert om styrket kompetanse og bevissthet i bransjen de senere årene, vurderes disse tiltakene foreløpig ikke som tilstrekkelige til å redusere den samlede sårbarheten i sektoren.

I tillegg kan kompleksiteten i produkt og prosess, herunder lange kundeforhold, ulike betalingsstrømmer og bruk av digitale løsninger, gjøre det mer krevende å oppnå tilstrekkelig kundekunnskap og oppdage avvik over tid. Gransking av næringskunder og mer komplekse eier- og kontrollstrukturer er ofte mer ressurskrevende enn gransking av privatpersoner. Dette kan bidra til at sviksaker ikke fanges opp tidlig eller tilstrekkelig, særlig der virksomheter benyttes som skalkeskjul for hvitvasking.

Konsekvensnivået vurderes som HØYT. Forsikringssektoren er en viktig brikke i det norske samfunnet og konsekvensene av hvitvasking vurderes som alvorlige, både for foretak, kunder og samfunnet. Misbruk av sektoren kan svekke tilliten til finanssystemet, undergrave samfunnsstrukturen og skade omdømmet til bransjen. I tillegg kan det bidra til å legitimere kriminelt utbytte og understøtte videre kriminalitet. Selv om enkeltstående saker kan fremstå som begrenset i omfang, kan den samlede effekten over tid være vesentlig.

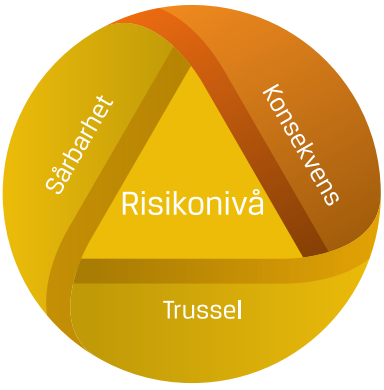
Risiko for hvitvasking i rapporteringspliktig sektor

VERDIPAPIRSEKTOREN

Verdipapirsektoren i Norge omfatter et bredt spekter av virksomheter, produkter, markedsplasser og regelverk knyttet til tilrettelegging av, handel med og forvaltning av, finansielle instrumenter. Sektoren dekker hele verdikjeden fra utstedelse, registrering og notering av finansielle instrumenter, via rådgivning, forvaltning, megling og handel, oppgjør herunder *clearing* og offentlig tilsyn. Verdipapirsektoren avgrenses her til verdipapirforetak og andre foretak regulert i verdipapirhandelloven samt verdipapirsentraler.

Aktørene er verdipapirforetak, herunder meglerhus og investeringsbanker, forvaltere av verdipapirfond med flere.

Sektoren omfatter også kredittinstitusjoner som har tillatelse til å yte investeringstjenester, regulerte markeder, verdipapir- og oppgjørssentraler og tilsynsmyndigheten. Eksempler på produkter er aksjer, obligasjoner, sertifikater, derivater, verdipapirfond og strukturerte produkter med mer. Tjenestene spenner fra handel og megling, investeringsrådgivning, kapitalinnhenting og børsnotering til forvaltning av kundemidler, oppgjør og depot med mer. Reguleringen skjer hovedsakelig ved inkorporasjon eller transformasjon av EØS-relevant regelverk inntatt i norsk rett, blant annet gjennom verdipapirhandelloven.[129]



129 Verdipapirhandelloven inkorporerer blant annet markedsmisbruksforordningen (MiFIR/MiFID II og prospektforordningen), finansmarkedsforordningen og prospektforordningen. I tillegg inneholder finansforetaksloven og AIF-loven, verdipapirfondloven, verdipapirsentralloven, tilhørende verdipapirregisterforordningen (CSDR), finansforetaksloven og finanstilsynsloven viktige bestemmelser.

Statistikk og faktaboks *Verdipapirsektoren*

Verdipapirsektoren omfattes av hvitvaskingsloven § 4 (1) bokstav h og l.

Antall foretak

Ved utgangen av 2025 hadde 99 verdipapirforetak tillatelse til å yte investeringstjenester i Norge, og 20 utenlandske foretak drev grensekryssende virksomhet gjennom filial i Norge. I tillegg meldte 670 utenlandske foretak om grensekryssende virksomhet inn til Norge, uten etablering av filial. Ett norsk foretak hadde tillatelse til å drive som verdipapirsentral, og tre norske foretak hadde tillatelse til å drive som markedsoperatør.[130]

Antall MF-rapporter 2023–2025[131]

Antall MFR	2023	2024	2025
Verdipapirsektoren	15	8	28
Totalt antall	23 703	30 658	33 313

Handelsaktiviteten i annenhåndsmarkedet på Oslo børs har i perioden 2020–2025 stabilisert seg på et relativt høyt nivå, med en gjennomsnittlig omsetning mellom 5,2 og 6,6 milliarder kroner daglig. Aktiviteten i førstehåndsmarkedet har imidlertid falt betydelig fra toppårene. I 2025 hentet selskapene på Oslo børs inn nær 25 milliarder kroner gjennom aksjeemisjoner, mens tilsvarende emisjonsbeløp oversteg 160 milliarder kroner i toppåret 2021. I samme periode har det vært jevn vekst i utestående verdi av foretaksobligasjoner notert på Oslo børs, og ved utgangen av 2025 hadde samlet verdi for alle obligasjonene og sertifikater notert på Børsen passert 3 000 milliarder kroner.

Flere internasjonale risikovurderinger, herunder fra EU, peker på at strukturelle endringer i markedene kan påvirke risikobildet. Lavere aktivitet i primærmarkedet kan føre til konsentrasjon av kapital og økt bruk av alternative instrumenter og markedsplasser, mens økt obligasjonsfinansiering kan innebære mer komplekse eier og finansieringsstrukturer.[132] Verdipapirmarkedet anses å være attraktivt i tilslørings- og integreringsfasen av hvitvaskingen av ulovlig opptjente penger. Ulovlig deling av innsideinformasjon kan også fungere som

130 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

131 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

132 EU COM, *Supranational Risk Assessment 2022 (SNRA)*, (EU COM 2022).

skjult vederlag for straffbare handlinger. Ifølge FATF kan illegale midler for øvrig oppstå i verdipapirmarkedet gjennom innsidehandel, markedsmanipulasjon og verdipapirsvindel.[133]

Risikoen for hvitvasking gjennom verdipapirsektoren vurderes som MODERAT. Dette er uendret fra forrige NRA.

Spesifikke endringer

MiCA, som er innført i norsk rett ved kryptoeiendelsforordningen har ført til at verdipapirforetak også kan yte kryptoeiendelstjenester.

Fra 1. april 2026 ble større tilsynsoppgaver som tilbuds- og informasjonsplikten, overført fra Oslo Børs til Finanstilsynet.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for verdipapirsektoren som MODERAT. Sektoren håndterer store verdier og det knytter seg høyere risiko til enkeltsaker, bestemte produkter, strukturer og aktørtyper som kan gi muligheter for verdioverføring og tilsløring. Den samlede risikoen reduseres imidlertid av at store deler av markedet er regulert, preget av etablerte kontrollmekanismer og høyere grad av sporbarhet og transparens enn i flere andre finansielle delsektorer.

Trusselen vurderes som MODERAT. Sektoren håndterer store verdier. Eksempelvis var den totale markedsverdien av verdipapir registrert i Verdipapirsentralen (VPS) per fjerde kvartal 2025 på i underkant av 7 700 mrd. NOK.[134] I tillegg tilbyr sektoren produkter og tjenester som kan benyttes til å plassere, overføre og integrere kriminelt utbytte. En sentral trussel knytter seg til geografisk eksponering og bruk av komplekse eier- og kontrollstrukturer, særlig der eierskap er organisert på tvers av jurisdiksjoner. I slike tilfeller kan det være krevende å identifisere reelle rettighetshavere og bakenforliggende kontroll, noe som gjør sektoren attraktiv for aktører som ønsker å skjule opprinnelsen til midler eller den faktiske eierskapssituasjonen. Profesjonelle tilretteleggere, herunder selskapsstrukturer og stråpersoner, vurderes som aktuelle trusselaktører i denne sammenheng.

Videre er unoterte produkter attraktive på grunn av fravær av regulering og transparens knyttet til transaksjonskurser, som skaper sikkerhet knyttet til verdi. Dette kan muliggjøre overføring av verdier ved kjøp eller salg til over- eller underpris, og dermed fungere som en mekanisme for tilslørt verdioverføring. Slike forhold er kjent fra både nasjonale og internasjonale risikovurderinger. I tillegg kan innsideinformasjon ha stor verdi og potensielt utnyttes av kriminelle.[135]

---

133 FATF, *Guidance for a risk based approach for the securities sector,* (FATF, 2018).

134 SSB, 2026, publisert 23.02.26. Nettlenke: https://www.ssb.no/bank-og-finansmarked/verdipapirmarkeder/statistikk/verdipapirer/artikler/mindre-utbytte-fra-aksjer

135 FATF, *Money Laundering and Terrorist Financing in the Securities Sector 2009,* (FATF, 2009), FATF, *Risk-Based Approach Guidance for the Securities Sector,* (FATF, 2018). EU COM, Supranational Risk Assessment 2022 (SNRA), (EU COM 2022).

Foto: Pexels

Det fremstår videre å være økt omfang av aktører som yter investeringstjenester uten nødvendig tillatelse, både i Norge og internasjonalt. Finanstilsynet jobber aktivt med å avdekke, hindre og stanse slik virksomhet. Økt forekomst av virksomhet uten konsesjon kan gjøre slike aktører særlig attraktive for kriminelle, ettersom de ofte opererer utenfor etablerte kontroll- og rapporteringsmekanismer. Det foreligger per i dag begrenset statistikk som entydig bekrefter omfanget av dette.

Sårbarheten vurderes som MODERAT. Verdipapirmarkedet er godt regulert, og sammen med transparens og struktur i markedet bidrar dette samlet sett til å begrense handlingsrommet for kriminelle aktører sammenlignet med eksempelvis bank- og kryptosektoren. I tillegg er det høy grad av kontroll etter sektorregelverket, dette reduserer også sårbarheten. Imidlertid varierer kompetansen og bevisstheten knyttet til hvitvaskingsrisiko, noe som øker sårbarheten. Sektoren er også preget av økt digitalisering, algoritmebasert handel og bruk av avanserte handels- og forvaltningssystemer som har økt markedets effektivitet, men også kompleksiteten. Høy transaksjonshastighet, komplekse produkter og grensekryssende investeringer kan gjøre det vanskeligere å identifisere reelle rettighetshavere og mistenkelige mønstre, særlig når flere jurisdiksjoner og aktører er involvert. Bruk av nomineestrukturer, fondkonstruksjoner og tredjepartsforvaltere kan ytterligere redusere transparensen.

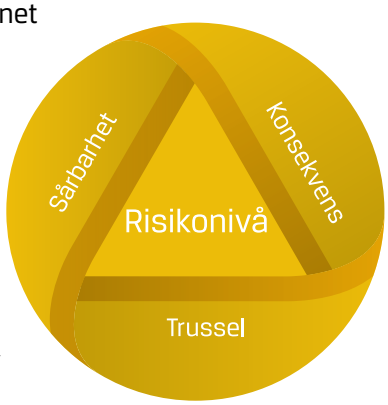
Konsekvensnivået vurderes som BETYDELIG. Vurderingen reflekterer sektorens sentrale rolle i det finansielle systemet og det store omfanget av verdier som forvaltes og omsettes. I tillegg vil tillitstap i kapitalmarkeder være særlig alvorlig, ettersom det er - en grunnleggende forutsetning for velfungerende kapitalmarkeder. Misbruk av verdipapirsektoren kan medføre betydelige økonomiske tap og undergrave tilliten til markedsaktørene og markedene, både nasjonalt og internasjonalt.

Risiko for hvitvasking i rapporteringspliktig sektor

FONDSEKTOREN

Fondsektoren i Norge omfatter forvaltningsselskaper for verdipapirfond og forvaltere av alternative investeringsfond (AIF-forvaltere). Fondene er kollektive investeringsstrukturer som forvalter betydelige verdier på vegne av investorer, og inngår som en sentral del av kapitalmarkedet. Sektoren er underlagt omfattende regulering og tilsyn, herunder krav til organisering, forvaltning, investorbeskyttelse og risikostyring. Fondsektoren anses gjennomgående som lite egnet for plassering av utbytte fra kriminalitet, blant annet som følge av krav til kundetiltak og manglende direkte kontroll for investorene over fondets daglige disposisjoner. Samtidig forvaltes det store verdier og er høy grad av hemmelighold i sektoren, noe som gjør fond attraktive som ledd i tilslørings- og integreringsfasen av hvitvasking, ved at midler kan reinvesteres i tilsynelatende legitime finansielle strukturer.

AIF-fond skiller seg fra verdipapirfond ved at fondene ofte har et begrenset antall investorer med større eierandeler og dermed større mulighet til å påvirke fondets investeringer. Transparency International fremhever blant annet hvitvaskingsrisiko knyttet til AIF-fond på bakgrunn av tøff konkurranse i bransjen og en insentivstruktur som gjør dem tilbøyelige til å lempe på AHV-krav for å få inn investorer.[136] Dette innebærer isolert sett en høyere hvitvaskingsrisiko enn for verdipapirfond, særlig der fondene benyttes til investeringer i mindre likvide aktiva eller komplekse strukturer. Samtidig er AIF-fond i Norge i betydelig grad lukkede fond, uten løpende tegning og innløsning. Dette reduserer fleksibiliteten for misbruk sammenlignet med mer åpne investeringsløsninger.



136 Matthew Jenkins, *Alternative Investment Funds in Europe: money laundering and corruption risks.* Frigitt, 30.09.2024: https://knowledgehub.transparencycdn.org/helpdesk/AIFs-in-Europe_ML-and-corruption-risks_Final_10.10.24.pdf (Transparency International 2024).

Statistikk og faktaboks *Fondsektoren*

Fondsektoren omfattes av hvitvaskingsloven § 4 (1) bokstav i og n.

Antall foretak
Ved utgangen av 2025 hadde 248 norske foretak tillatelse eller var registrert som forvaltere. Dette inkluderer både tillatelse som forvaltningsselskap for verdipapirfond og forvalter av AIF og registrerte forvaltere. Seks utenlandske foretak drev grensekryssende virksomhet gjennom filial i Norge. I tillegg meldte 123 utenlandske foretak om grensekryssende virksomhet inn til Norge, uten etablering av filial. Noen av disse er AIF-forvaltere som har doble konsesjoner.[137]

Antall MF-rapporter
Fondsektoren har ikke egen kategori under virksomhetsområde i hvitvaskingsregisteret.[138]

Norske verdipapirfond og AIF-forvaltere kan markedsføres til investorer i andre EØS-land i henhold til passrettighetene i UCITS- og AIFM-direktivene. Tilsvarende kan utenlandske fond markedsføres i Norge. Norske forvaltere kan også markedsføre fond utenfor EØS i samsvar med reglene i hvert enkelt land utenfor EØS. AIF-forvaltere etablert utenfor EØS markedsføres til profesjonelle investorer i Norge etter særskilt tillatelse. Dette gir fondene en grensekryssende investorbase og innebærer at hvitvaskingsrisikoen også må vurderes i et internasjonalt perspektiv.

Risikoen for hvitvasking gjennom fondsektoren vurderes som MODERAT. Dette er uendret fra forrige NRA.

Spesifikke endringer

Sektoren har de senere årene vært preget av økt kapitaltilførsel, mer komplekse fondskonstruksjoner og sterkere internasjonal integrasjon. Fondstrukturer er i økende grad grensekryssende, både når det gjelder investorer, investeringer og forvaltningsoppsett. Bruk av master-feeder-strukturer, holdingselskaper og fond registrert i ulike jurisdiksjoner kan redusere transparensen rundt reelle rettighetshavere og kapitalens opprinnelse.

137 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

138 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste. Avvik kan forekomme fordi hvitvaskingsregisterets virksomhetskategorier ikke fullt ut samsvarer med sektorinndelingen i NRA.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for fondsektoren som MODERAT. Nivået påvirkes spesielt av at sektoren er regulert og preget av etablerte kontrollmekanismer, samtidig som den håndterer betydelige verdier og har høy internasjonal eksponering. Risikoen forsterkes imidlertid ved at det er komplekse strukturer, begrenset kontroll med enkelte deler av sektoren, og interne variasjoner i AHV-etterlevelsen.

Trusselen vurderes som MODERAT. Nivået påvirkes spesielt av internasjonal eksponering og komplekse strukturer. Ulike deler av sektoren har ulik risikoprofil og kan være mer attraktive for hvitvasking enn andre. Det stilles derfor ulike krav til hvordan de ulike delene av sektoren kan gjennomføre investeringer. Trusselen begrenses av regulering, markedsovervåking og etablerte kontrollmekanismer. Hvitvasking i denne sektoren krever for øvrig en viss ekspertise.

Både i fondsektoren og verdipapirsektoren er uregulerte eller svakt regulerte markedsplasser, særlig etablert i jurisdiksjoner med svak tilsyns- og kontrollstruktur, vurderes som mer eksponert for hvitvasking enn regulerte markeder. Slike plattformer kan tilby lavere grad av transparens, svakere kundetiltak og begrenset myndighetsoppfølging, og kan derfor inngå som ledd i grensekryssende hvitvasking. Manglende sentral registrering og begrenset innsyn kan gjøre det vanskeligere å identifisere reelle eiere og kontrollere transaksjoner.

Sårbarheten vurderes som MODERAT. Sektoren er i hovedsak underlagt omfattende regulering og kontroll, men har samtidig strukturelle trekk som kan utnyttes av profesjonelle aktører i mer kompleks hvitvasking. Norske verdipapirfond er underlagt detaljert regulering, herunder krav til plasseringer, tegning og innløsning av fondsandeler. Disse rammene begrenser fleksibiliteten i fondenes disposisjoner og bidrar til økt

Foto: iStock

Foto: iStock

transparens og sporbarhet, noe som samlet sett reduserer sårbarheten. Det gjør også kravet om at hvert verdipapirfond skal ha en depotmottaker med ansvar for oppbevaring av fondets eiendeler og kontrolloppgaver, herunder kontroll med etterlevelse av hvitvaskingsregelverket. I det norske markedet har bankene rollen som depotmottakere, noe som kan bidra til ytterligere styrking av kontrollnivået, forutsatt at bankene også etterlever pliktene i regelverket. Sårbarheten av at registrerte AIF-forvaltere er utenfor de tradisjonelle verdipapirfondene. Selv om disse er underlagt hvitvaskingsregelverket, er de gjenstand for mer begrenset regulering og tilsyn enn forvaltere av verdipapirfond. Dette kan gi svakere rammer for internkontroll, risikovurdering og løpende oppfølging. For AIF-strukturer kan sårbarheten forhøyes der tegning i fond skjer via kontoer, mellommenn eller tredjeparter i flere jurisdiksjoner. Slike strukturer kan gjøre det krevende å få tilstrekkelig innsikt i midlenes opprinnelse og i hvem som er reell investor eller rettighetshaver. Bruk av fond-i-fond-strukturer, holdingselskaper eller utenlandske enheter kan ytterligere redusere transparensen.

Konsekvensnivået vurderes som MODERAT. Misbruk av fondsektoren kan bidra til å undergrave tilliten til fond som investeringsform og til forvaltningsmiljøene, særlig dersom fond benyttes til å skjule eierskap eller legitimere utbytte fra kriminalitet. Tillit er en sentral forutsetning for velfungerende kapitalmarkeder, og svekket tillit kan på sikt påvirke investeringsvilje og kapitaltilgang for legitime formål. I tillegg er det et potensial for betydelige økonomiske tap og tillitsskade i enkeltsaker, imidlertid uten samme systemiske rekkevidde som ved tilsvarende misbruk av bank- eller betalingssektoren.

Risiko for hvitvasking i rapporteringspliktig sektor

REVISORER

Statistikk og faktaboks *Revisorer*

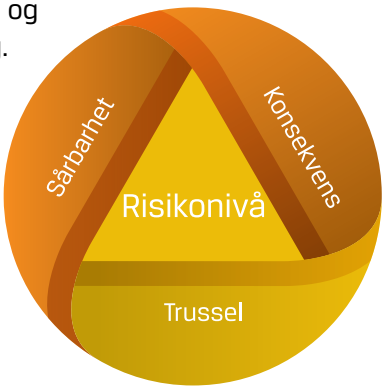
Revisorbransjen omfattes av hvitvaskingsloven § 4 (2) bokstav a.

Antall foretak
Ved utgangen av 2025 var det 4 903 autoriserte revisorer, og 444 norske revisorforetak. I tillegg var det registrert 17 tredjelandsrevisorer i Norge.[139]

Antall MF-rapporter 2023–2025[140]

Antall MFR	2023	2024	2025
Revisor	71	88	82
Totalt antall	23 703	30 658	33 313

Revisjonssektoren i Norge omfatter revisjonsforetak og statsautoriserte revisorer som yter lovpålagt og frivillig revisjon, samt tilknyttede tjenester innen attestasjon, kontroll og rådgivning. Sektoren spiller en sentral rolle i det finansielle og økonomiske systemet ved å bidra til tillit, transparens og kvalitet i finansiell rapportering. Samtidig fungerer den som en portvokter mot økonomisk kriminalitet. Sektoren



139 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

140 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

Revisorsektoren fungerer som en portvokter mot økonomisk kriminalitet

har tradisjonelt vært dominert av de største revisjonsforetakene. I 2024 hadde de fem største aktørene samlet en markedsandel på om lag 63 prosent målt i revisjonshonorar, ned fra om lag 70 prosent i 2022. Utviklingen i 2025 indikerer at markedet beveger seg fra en to-delt struktur mot en tredeling. Strukturendringene har skutt fart og drives særlig av teknologisk utvikling, økt spesialisering og internasjonalisering.

Tjenestene revisorer yter er i utgangspunktet ikke egnet til direkte plassering av utbytte fra kriminalitet, men revisjonsforetak kan misbrukes ved at deres tjenester benyttes til å legitimere eller tilsløre ulovlig aktivitet gjennom tilpasning av regnskapsinformasjon, selskapsstrukturer eller transaksjoner. Sektoren er derfor attraktiv for hvitvasking i tilslørings- og integreringsfasen.

Risikoen for hvitvasking gjennom revisorer vurderes som MODERAT. Dette er uendret fra forrige NRA.

Spesifikke endringer

Teknologisk utvikling, herunder økt bruk av KI i revisjonsarbeidet, har gitt mer effektive løsninger for innhenting, analyse og dokumentasjon av regnskapsposter og revisjonsbevis. Samtidig stiller slik teknologi nye krav til kompetanse, modellforståelse og etterfølgende kontroll. Manglende forståelse av KI-verktøy, utilstrekkelig kvalitetssikring eller overdreven tillit til automatiserte analyser kan svekke revisors evne til å identifisere uvanlige eller mistenkelige forhold, herunder indikasjoner på hvitvasking, terrorfinansiering eller tilknyttede økonomiske lovbrudd.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for revisorer som MODERAT, til tross for at både sårbarheten og konsekvensen av utnyttelse til hvitvasking vurderes som betydelig. Sektorens rolle som forebygger og kontrollør ivaretas i all hovedsak av seriøse aktører. I kombinasjon med at det er få saker eller hendelser og at trusselen vurderes som moderat, reduserer dette risikonivået. Hvitvaskingsrisikoen relaterer seg særlig til kundeforhold med komplekse eier- og kontrollstrukturer, nær tilknytning mellom eier og ledelse, grensekryssende virksomhet eller tilknytning til utbyttegenererende kriminalitet. Samtidig viser tilsynserfaringer at enkelte revisjonsforetak har hatt utfordringer med etterlevelse av hvitvaskingsregelverket, særlig knyttet til risikovurderinger, kundetiltak og dokumentasjon.

Trusselen vurderes som MODERAT. Nivået påvirkes spesielt av at større og mer profesjonelle kriminelle aktører, ofte med stort økonomisk utbytte, benytter selskaper og virksomheter som ledd i hvitvasking. Dette foregår i stor grad via regnskapsmanipulasjon, tilsløring, fiktiv omsetning og misbruk av selskapsstrukturer. Det er imidlertid få tilfeller hvor en revisor selv har hatt stort økonomisk utbytte av hvitvasking. De spiller i større grad rollen som profesjonelle tilretteleggere, utilsiktet eller bevisst. Trusselnivået forsterkes også ved at sektoren utnyttes av aktører som søker å legitimere kriminelt utbytte, uavhengig av om utbyttet er generert nasjonalt eller internasjonalt. Dette kan skje gjennom revisjon, attestasjon av fiktive eller manipulerte regnskaper og skattemeldinger eller rådgivning. Slike tjenester er attraktive for kriminelle aktører, da de kan brukes til å skjule ulovlige transaksjoner, svart arbeid og skatteunndragelser, samt til å muliggjøre bedrageri mot banker og offentlige etater som Nav og Skatteetaten.

Sårbarheten vurderes som BETYDELIG. Det påvirker sårbarheten negativt at aktørenes kapabilitet til å utnytte sårbarheter har økt. Dette ses i sammenheng med at det er registrert mer misbruk av offentlige registre og offentlige støtteordninger enn tidligere. I tillegg trekkes sårbarheten opp av at det er stor variasjon i etterlevelse av hvitvaskingsregelverket innad i sektoren. Dette gjelder særlig forskjeller i kunnskap, kompetanse, opplæring og bevissthet knyttet til regelverket og revisors rolle som rapporteringspliktig. Slike variasjoner kan gjøre enkelte revisjonsmiljøer mer attraktive for kriminelle aktører som bevisst søker miljøer med svakere kontrollfunksjoner.

Konsekvensnivået vurderes som BETYDELIG. Det begrunnes særlig i revisors sentrale tillitsrolle i økonomien og betydning for offentlige og private beslutningsprosesser. Konsekvensene ved utnyttelse kan i vesentlig grad undergrave systemet, skade tilliten til sektoren og dens rolle i det finansielle systemet. Det kan også medføre betydelige økonomiske tap, både gjennom direkte utbetalinger basert på feilaktige grunnlag og tap knyttet til mislighold, konkurs og etterfølgende inndrivelse eventuelt etterforskning. I tillegg kan misbruk av revisjonsfunksjonen undergrave markedsintegritet og like konkurransevilkår. Dette kan skade seriøse aktører og bidra til konkurransevridning.

Foto: Pexels

Risiko for hvitvasking i rapporteringspliktig sektor

REGNSKAPSFØRERE

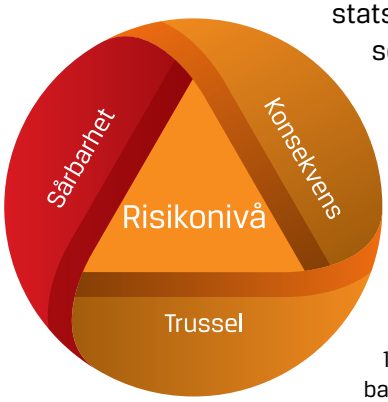
Statistikk og faktaboks *Regnskapsførere*

Regnskapsførersektoren omfattes av hvitvaskingsloven § 4 (2) bokstav b.

Antall foretak
Ved utgangen av 2025 var det 12 627 autoriserte regnskapsførere, og 2 390 norske regnskapsførerforetak. I tillegg var seks utenlandske regnskapsforetak registrert med filial i Norge.[141]

Antall MF-rapporter 2023–2025[142]

Antall MFR	2023	2024	2025
Regnskapsførere	138	192	278
Totalt antall	23 703	30 658	33 313



Regnskapsførersektoren i Norge omfatter autoriserte regnskapsforetak og statsautoriserte regnskapsførere som yter tjenester innen regnskapsføring, lønn, bokføring, rapportering, årsoppgjør og tilknyttede rådgivningstjenester. Den betjener i hovedsak små og mellomstore virksomheter både private og offentlige.

Sektoren er preget av en todelt struktur, med et begrenset antall større selskaper

141 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

142 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

og konsern som dominerer deler av markedet, og et stort antall mindre virksomheter i den andre delen. Det har over tid vært en nedgang i antall statsautoriserte regnskapsførere som driver virksomhet i enkeltpersonforetak, parallelt med økt konsolidering og profesjonalisering i bransjen. Regnskapsforetak eid av banker øker og utvider sitt tjenestetilbud, samtidig som flere større aktører ekspanderer gjennom oppkjøp og organisk vekst.

Regnskapsførere har en sentral rolle i å sikre korrekt og transparent regnskapsrapportering. Samtidig fremheves sektoren som særlig utsatt for misbruk til hvitvasking. Tjenestene regnskapsførere yter, er egnet til utnyttelse for å legitimere, tilsløre og videreføre utbytte fra kriminalitet, som blant annet skjer gjennom fiktiv fakturering, skatte- og avgiftsunndragelser, arbeidslivskriminalitet og bruk av komplekse selskapsstrukturer. Sektoren er derfor attraktiv for hvitvasking i tilslørings- og integreringsfasen.

Risikoen for hvitvasking gjennom regnskapsførere vurderes som BETYDELIG. Dette er uendret fra NRA 2022.

Spesifikke endringer

I 2025 har enkelte regnskapsforetak etablert tettere samarbeid eller felles virksomhet med advokatkontorer. Slike tverrfaglige konstellasjoner kan gi effektiv tjenesteyting, men det kan også skape uklare grenser når det gjelder roller, ansvar og rapporteringsplikt. Økt bredde i tjenestetilbudet kan gjøre det mer krevende å opprettholde tilstrekkelig risikoforståelse og kontroll på tvers av fagområder.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for regnskapsførere som BETYDELIG. Risikonivået reflekterer sektorens brede kundekontakt, nære involvering i kundenes økonomiske disposisjoner, erfaringer fra tilsyn og etterforskning som viser at regnskapsførere i enkelte tilfeller utnyttes som ledd i organisert og økonomisk kriminalitet. Stor variasjon i etterlevelse, kunnskap, opplæring og kompetanse innad i bransjen forsterker også risikoen. Forhold som tilsyn, reaksjonsmuligheter og at revisjonspliktige kunder også kontrolleres av uavhengig revisor, reduserer imidlertid risikoen i deler av markedet.

Trusselen vurderes som BETYDELIG. Omfanget av saker påvirker trusselen negativt og underbygger nivået. I tillegg til at regnskapsførere i praksis ofte sitter tett på virksomheters økonomi, transaksjoner og dokumentasjon. Bruk av selskaper og selskapsstrukturer er en sentral fremgangsmåte for hvitvasking. På linje med revisorer kan regnskapsførere bli en kritisk brikke som tilrettelegger dersom regeletterlevelsen svikter, eller ved bevisst medvirkning. Det er også få kjente tilfeller hvor en regnskapsfører selv har hatt stort økonomisk utbytte. De kan likevel ha en viktig tilretteleggerrolle eller ha dobbeltroller som er underkommunisert.

Regnskapsførere kan også utnyttes som rådgivere i strukturer som har til hensikt å tilsløre reell formue, eierskap eller kontroll, for eksempel gjennom omorganiseringer, flytting av fordringer, endringer i eierregistreringer eller bruk av stråpersoner og mellomledd. Regnskapsfører kan på linje med revisor også benyttes

til å skjule eller tåkelegge formue. Videre kan en uredelig regnskapsfører tilby regnskapstjenester som en kriminell tjeneste[143] for eksempel etablering av skallselskaper med og uten virksomhetshistorikk, produksjon av falsk regnskapsdokumentasjon, fiktiv fakturering eller tilrettelegging av svart økonomi.

I tillegg utgjør ulovlig regnskapsførervirksomhet en del av trusselbildet, ettersom aktører uten tilsyn og autorisasjon ikke oppfyller de krav regnskapsførerloven stiller for å kunne utføre regnskapsføring for andre. Disse kan bidra til feilrapportering, tilsløring av reelle økonomiske forhold og bevisst tilrettelegging for hvitvasking.

Sårbarheten vurderes som HØY. Regnskapsfører har en sentral rolle i virksomheters løpende økonomiforvaltning, og har et nært og ofte tillitsbasert forhold til oppdragsgiver. De har også nær kundekontakt og er avhengig av kundelevert informasjon. Selv om tilsyn, reaksjonsmuligheter og samspill med revisor bidrar til å redusere sårbarheten i deler av markedet, gir sektorens struktur og rolle fortsatt et potensial for utnyttelse i hvitvasking.

Sårbarheten forsterkes av at det er stor variasjon i etterlevelse av hvitvaskingsregelverket innad i bransjen. Det foreligger betydelige forskjeller når det gjelder kunnskap, opplæring, kompetanse og bevissthet knyttet til regelverket og regnskapsførerens rolle som rapporteringspliktig. Mangler i risikovurderinger, kundetiltak og løpende oppfølging kan gjøre enkelte regnskapsforetak mer attraktive for kriminelle aktører som aktivt søker miljøer med svakere kontrollfunksjoner.

Samtidig finnes det forhold som reduserer sårbarheten. Regnskapsførere er underlagt flere tilsyn- og kontrollmekanismer, med tilhørende reaksjonsmuligheter. Videre vil kunder som er revisjonspliktige, også være underlagt kontroll fra en uavhengig revisor. I tilfeller der virksomheter har både regnskapsfører og revisor, er det dermed to separate rapporteringspliktige aktører involvert i utarbeidelse og kontroll av årsregnskapet.

Konsekvensnivået vurderes som BETYDELIG. Misbruk av regnskapsførertjenester kan medføre betydelige økonomiske tap, gjennom utbetaling av offentlige ytelser og støtteordninger basert på feilaktige regnskaps- og skattegrunnlag. I tillegg gjennom kredittgivning fra banker og finansforetak som baserer beslutninger på regnskapsinformasjon utarbeidet eller kvalitetssikret av regnskapsfører. Regnskapsførere bidrar til å sikre kvalitet og pålitelighet i økonomisk rapportering. Misbruk kan føre til vesentlig skade på tilliten til bransjen generelt og kan også få brede ringvirkninger i samfunnet.

143 På engelsk: crime-as-a-service (CaaS).

Risiko for hvitvasking i rapporteringspliktig sektor

ADVOKATER

Statistikk og faktaboks *Advokater*

Advokatsektoren omfattes av hvitvaskingsloven § 4 (2) bokstav c.

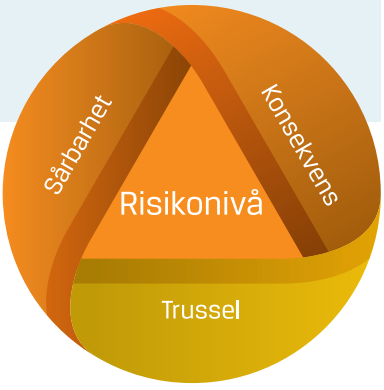
Antall foretak
Per 30.4.2026 hadde 1 589 advokatforetak sendt inn egenerklæring for regnskapsåret 2025 til Advokattilsynet. 573 foretak opplyste at de hadde hatt oppdrag som var omfattet av hvitvaskingsloven i 2025.

Det ble rapportert om totalt 29 308 transaksjoner via foretakenes klientbankkonto. Av disse var 1 033 registrert som internasjonale transaksjoner, hvorav 371 var utenfor EU/EØS.

Ved utgangen av 2025 var det registrert 9 980 advokater i Norge.

Antall MF-rapporter 2023–2025[144]

Antall MFR	2023	2024	2025
Advokater	23	27	24
Totalt antall	23 703	30 658	33 313



144 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

Foto: iStock

Hvitvaskingsloven gjelder for advokater og advokatforetak når de utfører finansielle transaksjoner eller transaksjoner som gjelder fast eiendom på vegne av klient. Den gjelder også når de bistår ved planlegging eller utfører transaksjoner for klient i forbindelse med kjøp og salg av fast eiendom eller virksomhet, forvalter en klients penger, verdipapir eller andre aktiva. Videre gjelder den også når advokaten bistår i forbindelse med åpning eller forvaltning av bank- eller verdipapirkonto, fremskaffelse av kapital til opprettelse, drift eller ledelse av selskap, fond eller lignende juridisk person eller formuesmasse, herunder utenlandsk trust eller tilsvarende juridisk arrangement.

Hvert år er advokatenes bistand knyttet til transaksjonsvirksomhet betydelig. De ti mest aktive advokatforetakene rapporterte selv å ha bistått med transaksjoner til en samlet verdi av 1 372 milliarder kroner i 2023.[145] Sektoren er attraktiv for hvitvasking i plasserings- og integreringsfasene.

Risikoen for hvitvasking gjennom advokater vurderes som BETYDELIG. Dette er uendret fra NRA 2022.

Spesifikke endringer

Med virkning fra 1. januar 2025 trådte den nye advokatloven i kraft. I den forbindelse ble Advokattilsynet opprettet. Tilsynet kan blant annet tilbakekalle advokatbevillinger, nedlegge forbud mot å yte rettslig bistand, ilegge pålegg og overtredelsesgebyr etter hvitvaskingsloven og kreve refusjon av tilsynskostnader.

Med virkning fra juli 2025 ble hvitvaskingsloven § 4 andre ledd bokstav c endret, med det formål å presisere at advokatforetak etter gjeldende rett er underlagt hvitvaskingsloven i de situasjonene som er angitt i § 4 bokstav c. Advokattilsynet ble dermed sikret et tydeligere hjemmelsgrunnlag for å ilegge advokatforetak overtredelsesgebyr etter hvitvaskingsloven § 49.

145 Advokatforeningen, «Advokatforeningens årstale 2024: om tillit og krav til advokater». Nettlenke 30.11.2024: https://www.advokatforeningen.no/aktuelt/nyheter/2024/november/advokatforeningens-arstale-2024-om-tillit-og-krav-til-advokatene/

Sakseksempel
Svindelsak

Sakseksempel

I 2024 ble en av norgeshistoriens største svindelsaker avdekket, der en ansett advokat benyttet sitt eget advokatselskaps felles klientbankkonto til å formidle lån til fiktive låntakere i et såkalt Ponzi-opplegg. Det er grunn til å tro at advokatforetaket også ble misbrukt til å hvitvaske deler av utbyttet, ved at advokaten solgte juridiske tjenester til et annet selskap advokaten eide, og som mottok betydelige midler fra svindelen. Bistanden ble fakturert fra advokatselskapet.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for advokater som BETYDELIG. Antallet MF-rapporter har vært stabilt lavt over flere år til tross for økt oppmerksomhet om hvitvaskingsrisiko, økning i antall transaksjoner og økt MF-rapportering generelt. Det er for øvrig mistanke om mørketall. Antakelsen om underrapportering underbygges av informasjon i MF-rapporter av andre rapporteringspliktige og av funn gjort gjennom tilsyn, hvor det årlig avdekkes flere transaksjoner som etter tilsynets vurdering skulle vært innrapportert som mistenkelige. Misbruk av klientbankkonto forsterker risikoen, ettersom opplysninger om transaksjoner via denne kontoen er beskyttet av advokatens lovbestemte taushetsplikt. Behovet for tjenesten er ofte begrunnet ut fra praktiske hensyn, noe som gjør det utfordrende for advokaten å skille klientens legitime behov fra illegitime.

Trusselen vurderes som MODERAT blant annet som følge av få saker. Det knyttes imidlertid usikkerhet til vurderingen fordi det antas at det er store mørketall. Trusselen reflekterer både misbruk av advokater uten at de er klar over hvitvaskingen og tilfeller der advokaten selv har en grad av medvirkning. Det er informasjon om at advokater skal ha gått god for kundens AHV-dokumentasjon til tross for åpenbare mangler, med det formål at klienten får gjennomført sin transaksjon eller sitt kundeforhold mot den rapporteringspliktige.

Advokattilsynet har de siste årene avdekket 1-2 saker per år der det er mistanke om at advokaten bevisst har tilrettelagt for grov økonomisk kriminalitet. Videre er det eksempler på at kontrollen med advokatforetak i realiteten utøves av andre enn de personene som formelt står oppført som daglig leder eller eier av advokatforetak. Det kan for eksempel skje gjennom familierelasjoner eller andre former for avhengighetsforhold. Det er også eksempler på bakmenn som har vært tidligere dømt, mistenkt for alvorlig kriminalitet eller for medvirkning til dette.

I tillegg avdekkes det flere tilfeller hvert år der det foreligger mistanke om at advokatens tjenester kan ha blitt misbrukt i hvitvaskingsøyemed. Advokattilsynet har også de senere årene sett eksempler der advokater direkte eller indirekte går god for verdivurderinger av aksjer eller selskaper foretatt av andre, men som det etter nærmere vurdering er grunn til å anta at ikke samsvarer med markedsverdien.

Sårbarheten vurderes som BETYDELIG. Uklart regelverk i grensedragningen mot konsesjonspliktig betalingsformidling trekker sårbarheten opp. I tillegg er ikke bruk av advokatforetaks felles klientkonto nærmere regulert. Det forsterker også sårbarheten at antallet innsendte MF-rapporter fra advokater har vært stabilt lavt de siste årene sammenliknet med andre rapporteringspliktige det er naturlig å sammenlikne med, for eksempel eiendomsmeglere, regnskapsførere og revisorer. Få rapporteringer av mistenkelige forhold når sektoren er vurdert med betydelig risiko gir indikasjon på lav kunnskap og mangel på kompetanse når det gjelder AHV-arbeid. Videre er det gjennom tilsyn avdekket manglende eller mangelfull internkontroll. Dette øker sårbarheten.

Konsekvensnivået vurderes som BETYDELIG. Advokater nyter generelt stor tillit i samfunnet, og den kan også misbrukes. Mislighold og brudd på etterlevelsen av sentralt hvitvaskingsregelverk bidrar til å undergrave tillit til advokatbransjen og rettsstaten. Det utgjør et stort skadepotensial med vesentlige konsekvenser dersom advokater bevisst eller ubevisst lar sin virksomhet bli utnyttet.[146] Et viktig prinsipp er også advokaters taushetsplikt som innebærer at klienter skal kunne snakke fortrolig med en advokat for å få gode råd. Dersom taushetsplikten misbrukes og man mister tilliten til advokatbransjen, kan det igjen gå ut over klientene.

Foto: iStock

146 Ibid.

Risiko for hvitvasking i rapporteringspliktig sektor

EIENDOMSMEGLING

Statistikk og faktaboks *Eiendomsmegling*

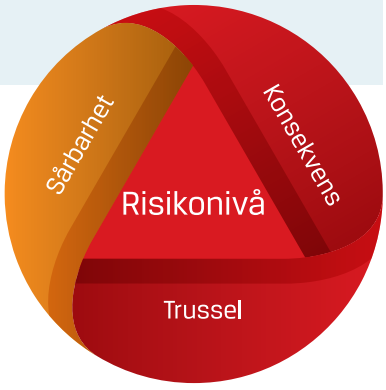
Eiendomsmeglerbransjen omfattes av hvitvaskingsloven § 4 (2) bokstav d.

Antall foretak

Ved utgangen av 2025 hadde 497 foretak tillatelse til å drive eiendomsmeglingsvirksomhet. I tillegg var 6 403 personer registrert som eiendomsmegler.[147] Dette inkluderer advokater som har stilt sikkerhet for å drive eiendomsmeglingsvirksomhet, jurist med tillatelse til å være ansvarlig megler i et foretak som innehar tillatelse til å drive eiendomsmeglingsvirksomhet eller rettshjelper som oppfyller vilkår for eiendomsmegling.[148]

Antall MF-rapporter 2023–2025[149]

Antall MFR	2023	2024	2025
Eiendomsmegling	2 359	2 940	3 301
Totalt antall	23 703	30 658	33 313



147 Dette omfatter personer med tillatelse til å være ansvarlig megler etter Forskrift om overgangsregler til lov 29. juni 2007 nr. 73 om eiendomsmegling § 5.

148 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

149 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.

2024*	Antall	Verdi
Formidlinger eiendomsmeglingsforetak	145 000 (157 000)	670 milliarder (680)
Formidlinger advokater	5 740 (5 800)	40 milliarder (40,3)
Sum	**150 740 (162 800)**	**710 milliarder (720,3)**

Tabell 2: Antall eiendomsformidlinger og verdi for 2024 – tallene er avrundet.
** inkludert utleieoppdrag i parentes*

Eiendomsmeglersektoren i Norge omfatter tjenester knyttet til omsetning og forvaltning av fast eiendom, herunder salgsmegling, utleiemegling og rene oppgjørsoppdrag. Tjenestene ytes i hovedsak av eiendomsmeglere og eiendomsmeglingsforetak, men også advokater kan ha tillatelse til å utføre eiendomsmeglingsvirksomhet når vilkårene i regelverket er oppfylt.

Eiendomssektoren i Norge kjennetegnes av høyt transaksjonsvolum og håndtering av betydelige verdier. Som tabell 2 viser foregår det største volumet av formidlinger gjennom eiendomsmeglingsforetakene. Utleieoppdrag utgjør en liten andel av totalen.[150] Et særnorsk trekk er at en stor andel av befolkningen eier sin egen bolig, og eiendomsmeglere er blant de aktørene som rapporterer relativt mange mistenkelige transaksjoner.

Eiendomsmeglersektoren anses som attraktiv for hvitvasking fordi fast eiendom er kapitalintensiv og muliggjør hvitvasking av store beløp gjennom enkelttransaksjoner. Videre kan eiendom gi mulighet for å skjule eierskap og midlenes opprinnelse gjennom bruk av komplekse selskaps- og eierstrukturer, stråpersoner og skallselskaper.

Foto: iStock

150 Tall fra Finanstilsynet.

Misbruk av eiendomsmarkedet kan skape betydelige økonomiske konsekvenser

Hvitvasking i eiendomssektoren kan blant annet skje ved kjøp og salg av eiendom, videresalg etter kort eiertid, bruk av nybygg og kontraktsposisjoner eller leiligheter med høy fellesgjeld. Slike strukturer kan benyttes for å tilsløre midlenes opprinnelse og reelle rettighetshavere.

Som følge av blant annet større transaksjonsbeløp og mer komplekse oppgjørsstrukturer innebærer fast eiendom høyere hvitvaskingsrisiko enn utleiemegling. Eiendomssektoren anses som relevant for hvitvasking i alle fasene plassering, tilsløring og integrering, med særlig risiko knyttet til transaksjoner som involverer store verdier og komplekse strukturer.

Risikoen for hvitvasking gjennom eiendomsmeglere vurderes som HØY. Dette er en oppjustering fra betydelig i forrige NRA.

Spesifikke endringer

Eiendomsmarkedets utvikling de fire siste årene har vært gunstig for hvitvasking, med stadig økende priser, høy turnover, utbygging og oppussing. I tillegg er økende leiepriser og markedet for korttidsutleie gunstig for de som bruker eiendom til hvitvasking av profitt fra kriminalitet.

Med virkning fra 1. juli 2025 ble det innført krav til egnethet og fremleggelse av politiattest for oppgjørsmedhjelpere og eiendomsmeglerfullmektiger.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for eiendomsmegling som HØY. Dette er en oppjustering fra betydelig i forrige NRA. Risikoen påvirkes spesielt av at sektoren håndterer store verdier, dokumentert bruk i hvitvaskingssaker, bruk av profesjonelle tilretteleggere og innsidere. I tillegg gjør strukturelle forhold eiendom egnet for lagring og integrering fra kriminelt utbytte, skjult eierskap og komplekse transaksjoner. Varierende AHV-kompetanse og begrenset tilsyn forsterker sårbarheten. Dette bidrar til å gi kriminelle aktører et reelt handlingsrom.

Risikoen vurderes som størst i segmenter og oppdrag med lavere transparens og høyere kompleksitet, særlig innen næringsmegling og transaksjoner med komplekse selskapsstrukturer, utenlandske eiere og utfordringer knyttet til verdsettelse. Risikoen for hvitvasking knyttet til ordinære salgsmeglingsoppdrag for bolig- og fritidseiendom vurderes som lavere enn for de mest komplekse segmentene, særlig når kundene er privatpersoner og formålet fremstår som egen bruk.

Faktaboks *Register over reelle rettighetshavere*

Register over reelle rettighetshavere
Registeret åpnet for registrering 1. oktober 2024. Registreringsplikten har vært løpende siden 31. juli 2025. Ved utgangen av 2025 var det ikke tilstrekkelig grunnlag for å vurdere den faktiske effekten av registeret for hvor attraktiv fast eiendom er for hvitvasking. Finanstilsynet hadde heller ikke tilsynserfaring for hvordan registeret påvirker eiendomsmeglersektorens arbeid med kundekontroll og identifisering av eiendommens eiere og reelle rettighetshavere.

Trusselen vurderes som HØY og er en oppjustering fra forrige NRA. Nivået påvirkes spesielt av stort økonomisk omfang og informasjon om aktuelle aktører knyttet til kriminelle nettverk som utnytter eiendomsmarkedet til hvitvasking. Eiendomskjøp inngår i flere straffesaker som omfatter hvitvasking. Bedragerier og korrupsjon knyttet til lånesøknader og boliglån underbygger hvor viktig eiendom er for hvitvasking og finansiering av kriminalitet. Trusselen forsterkes også av at det de siste årene har vært flere saker med innsidere og profesjonelle tilretteleggere relatert til eiendom, blant annet bankansatte, eiendomsmeglere og utbyggere. Disse har i kraft av sin posisjon bidratt til å omgå kontrolltiltak eller aktivt lagt til rette for hvitvasking. Omfanget av kapital som kanaliseres gjennom eiendomsmarkedet, og utfordringer knyttet til kompliserte eier-strukturer, er tidligere belyst gjennom analyser som Transparency Internationals kartlegging av eierskap i Oslo. Til tross for at utvalget er fra et begrenset geografisk område i Oslo fem år tilbake i tid, illustrerer slike funn hvordan eiendomsmarkedet kan utnyttes til å skjule verdier og eierskap over tid.[151]

Videre er trusselen knyttet til grensekryssende transaksjoner og eierskap samt bruk av skjulte eller komplekse eierskapsstrukturer. Bruk av utenlandske selskaper, stråpersoner og løsninger som blanko-skjøter kan bidra til å skjule reell kontroll og midlenes opprinnelse. Fast eiendom har flere egenskaper som kan muliggjøre anonymitet, høy verdilagring og langsiktig integrering av midler, noe som gjør sektoren attraktiv for hvitvasking.

Sårbarheten vurderes som BETYDELIG. Det påvirker nivået spesielt at AHV-håndtering er svak i deler av bransjen. I tillegg er det manglende eller lav kompetanse, utilstrekkelig opplæring, svake risikovurderinger og mangelfulle rutiner samt svak etterlevelse av

151 Transparency International Norge, «*Hvem eier Oslo? Hvitvaskingsrisiko i eiendomsmarkedet?*». Frigitt 27.01.2021: https://www.transparency.no/publikasjonerverkty/2021/01/27/hvem-eier-oslo-hvitvaskingsrisiko-i-eiendomsmarkedet

hvitvaskingsregelverket. Mange meglere mangler også egnede muligheter for å kontrollere egenkapital, og flere aktører har for få eller ingen systemer for effektiv avdekking av hvitvasking. Det ble imidlertid sendt flere MF-rapporter i 2025 enn året før. Dette kan indikere økt bevissthet knyttet til AHV-arbeidet hos enkelte større aktører og reduserer sårbarheten.

Muligheten til å skjule eierskap, verdier og transaksjoner over tid, forsterker også sårbarheten. Imidlertid kan innføringen av registeret over reelle rettighetshavere bidra til å redusere sårbarheten knyttet til skjult eierskap og komplekse selskapsstrukturer.

Sårbarheten vurderes som høyere innen næringseiendom og næringsmegling. Her er det ofte mulig å benytte komplekse selskapsstrukturer eller utenlandske eiere som megleren kan ha begrenset mulighet til å identifisere fullt ut. Videre er det generelt vanskeligere å vurdere om næringseiendommen er riktig priset i markedet, noe som øker risikoen for verdimanipulering. Bruk av eksempelvis falske eller kunstig oppblåste leiekontrakter kan bidra til å påvirke verdsettelsen og gi rom for hvitvasking gjennom over- eller underprising.

Der megleroppdraget omfatter rene oppgjør, foreligger det en særskilt sårbarhet knyttet til selve gjennomføringen av transaksjonen fordi megler ofte har lavere kjennskap til både partene i handelen og eiendommen enn ved fullverdige salgsoppdrag. Dette kan redusere muligheten for å identifisere mistenkelige forhold. Det vurderes videre at advokater som driver eiendomsmegling i mindre foretak, særlig der virksomheten er begrenset og uten et tydelig rammeverk for risikostyring og internkontroll, kan ha noe høyere sårbarhet enn bransjen for øvrig. Dette gjelder spesielt der oppdragene i stor grad omfatter rene oppgjørsoppdrag som nevnt over. I denne sammenheng knyttes det også særskilt risiko til virksomheters klientkonto, som kan misbrukes som mellomstasjon i transaksjoner og tilsløring dersom kontrolltiltak og oppfølging ikke er tilstrekkelig risikobasert.

Konsekvensnivået vurderes som HØYT. Eiendomsmarkedet er en viktig del av norsk økonomi og samfunn. Mislighold eller kriminalitet i sektoren vil kunne bidra til svekket tillit, men også konkurransevridning av markedet og undergraving av den legale økonomien. Misbruk av eiendomsmarkedet kan også skape betydelige økonomiske konsekvenser, både direkte og indirekte. Indirekte kan hvitvasking bidra til prispress og markedsskjevheter, særlig dersom kriminelle aktører kan by over markedspris eller operere med lavere avkastningskrav fordi formålet primært er å integrere midler. Dette kan påvirke bolig- og næringseiendomsmarkedet negativt og svekke like konkurransevilkår for seriøse aktører.

Risiko for hvitvasking i rapporteringspliktig sektor

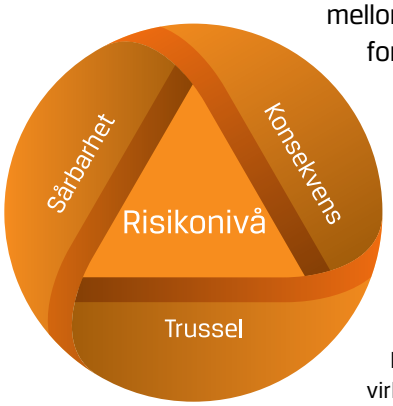
LÅNEFORMIDLING

Statistikk og faktaboks *Låneformidling*

Låneformidlerbransjen omfattes av hvitvaskingsloven § 4 (1) bokstav o (finansmeglerforetak)

Antall foretak
Ved utgangen av 2025 var det registrert 2 315 norske låneformidlere, og ett norsk foretak som hadde konsesjon som finansmegler. I tillegg var det fem finansmeglerforetak som drev grensekryssende virksomhet inn til Norge, uten etablering av filial.[152]

Antall MF-rapporter
Låneformidlingsforetak har ikke egen kategori under virksomhetsområde i hvitvaskingsregisteret.[153]



Låneformidlingssektoren i Norge omfatter foretak som opptrer som mellomledd mellom långivere og låntakere ved formidling av lån, uten selv å yte kreditt. Sektoren inkluderer blant annet låneformidlere, finansmeglerforetak og finansagenter som formidler lån, kreditt og finansieringsløsninger på vegne av banker, finansieringsforetak eller andre långivere. I tillegg inngår digitale plattformer for folkefinansiering, som har hatt betydelig vekst de senere årene. Flere låneformidlere tilbyr også tilleggstjenester

152 Finanstilsynets virksomhetsregister. Nettlenke, 27.03.2026: https://www.finanstilsynet.no/virksomhetsregisteret/?p=1

153 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste. Avvik kan forekomme fordi hvitvaskingsregisterets virksomhetskategorier ikke fullt ut samsvarer med sektorinndelingen i NRA.

knyttet til betaling og oppgjør. Enkelte har derfor konsesjon som betalingsforetak eller benytter betalingsforetak til å håndtere midler mellom långivere og låntakere.

Finansagenter og finansmeglerforetak har ofte tett kundekontakt og kan være involvert i hele prosessen, fra markedsføring og kundekontakt til innhenting av dokumentasjon og gjennomføring av låneopptak. Enkelte foretak har også oppgjørs-, eller betalingsfunksjon, enten gjennom egen konsesjon som betalingsforetak eller ved bruk av agenter og underleverandører. Foretak som håndterer kundemidler eller gjennomfører betalinger på vegne av långivere og låntakere, anses å ha forhøyet hvitvaskingsrisiko. Låneformidlingssektoren fremheves som særlig relevant i tilsløringsfasen av hvitvasking.

Folkefinansiering utgjør en særskilt del av låneformidlingssektoren og omfatter digitale plattformer som formidler lån eller investeringer mellom et større antall långivere og låntakere. Slike plattformer[154] fungerer som mellomledd og kan formidle både forbrukslån, næringslån og prosjektfinansiering, ofte med mange involverte parter og høy transaksjonsfrekvens. Enkelte folkefinansieringsplattformer har eller benytter konsesjon som betalingsforetak, og håndterer inn- og utbetalinger mellom långivere og låntakere. Dette innebærer at midler kan samles inn, fordeles og tilbakebetales gjennom plattformen, noe som øker risikoen for at tjenestene kan misbrukes til hvitvasking.

Risikoen for hvitvasking gjennom låneformidlere vurderes som BETYDELIG.

Spesifikke endringer

Låneformidlingssektoren risikovurderes som egen rapporteringspliktig sektor for første gang i denne NRA-en, etter ikrafttredelsen av låneformidlingsloven med forskrift 1. juli 2023.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for låneformidling som BETYDELIG. Risikonivået påvirkes spesielt av forekomstene av uregistrert og ulovlig låneformidlingsvirksomhet, kombinert med lave etableringsbarrierer for deler av markedet, spesielt ved formidling av lån til næringsdrivende. Manglende egnethetsvurderinger og begrenset forhåndskontroll ved registrering gir kriminelle aktører et handlingsrom til å operere i eller rundt sektoren. Bruk av uformelle, digitale kanaler og sosiale medier for låneformidling bidrar ytterligere til å øke risikoen. Videre forsterkes risikoen av at det er begrenset tilsynserfaring og fragmentert oversikt over aktører og pengestrømmer, særlig der virksomheten skjer utenfor etablerte og kontrollerte strukturer.

Trusselen vurderes som BETYDELIG. Ifølge Finanstilsynet er det flere foretak som tilsynelatende formidler lån uten nødvendig tillatelse eller registrering. Forekomsten vurderes som størst innen formidling av lån til næringsdrivende, hvor kravene til registrering og tilsyn

154 Ifølge FT er det kun få registrerte foretak som har fått innvilget konsesjon.

i praksis kan være mindre synlige for kundene. Samtidig forekommer det også ulovlig låneformidling hvor midlene stammer fra kriminelt utbytte. Lånetilbud fra disse rettes mot uvitende forbrukere. Forbrukernes tilbakebetaling gir midlene et skinn av legitimitet. Dette trekker trusselen opp. Sektorens karakter, lav inngangsbarriere og økende digitalisering gjør at det er mistanke om mørketall. Faktisk omfang kan derfor være større enn det som er kjent gjennom tilsyn og registrerte saker hos politiet.

En fremtredende utvikling er økt bruk av uformelle digitale plattformer og sosiale medier, herunder grupper på Facebook, hvor privatpersoner formidler eller yter lån til andre privatpersoner. Slike arenaer opererer ofte utenfor etablerte kontroll- og rapporteringsmekanismer, og kan benyttes til å flytte, plassere eller legitimere midler med uklar opprinnelse. Denne typen virksomhet vurderes som attraktiv for kriminelle aktører nettopp fordi den preges av lav terskel for deltakelse, begrenset innsyn og svak sporbarhet.

Trusselaktørene omfatter ikke bare økonomiske kriminelle og organiserte nettverk, men også enkeltpersoner som utnytter manglende regulering eller tilsyn for å tilby låneformidling som ledd i hvitvasking, bedrageri eller annen økonomisk kriminalitet. Det kan også skje gjennom bruk av stråpersoner som låntakere eller långivere, samt komplekse transaksjonsstrukturer der formidling, betaling og tilbakebetaling skjer gjennom flere ledd. Trusselen forsterkes der virksomheten kombinerer formidling av lån med betalingstjenester eller grensekryssende aktivitet.

Sårbarheten vurderes som BETYDELIG. Nivået påvirkes spesielt av lave etableringsbarrierer, begrenset tilsynserfaring og potensial for uregistrert virksomhet. Samtidig bidrar formelle avtalestrukturer og sporbarhet i betalingsstrømmene til å redusere sårbarheten sammenlignet med tjenester som i større grad håndterer kontanter med tilhørende anonymitet. Sårbarheten øker imidlertid av at formidling av lån til næringsdrivende i hovedsak kun krever registrering, og er underlagt begrenset saksbehandling, herunder uten egnethetsvurderinger av ledelse og eiere. Sårbarheten forsterkes av at det er få tilsyn og begrenset praksisutvikling ettersom relevant regelverk er relativt nytt.

Videre kan fragmentert informasjonsgrunnlag og bruk av uformelle kanaler, særlig i grenseflaten mot uregistrert virksomhet og privat utlånsformidling, gjøre det krevende å få tilstrekkelig oversikt over aktører, pengestrømmer og reelle parter i transaksjonene. Det reduserer imidlertid sårbarheten at låneformidling innebærer lavere grad av anonymitet enn enkelte andre finansielle tjenester, ettersom transaksjonene normalt er knyttet til identifiserbare parter, formelle låneavtaler og sporbare betalingsstrømmer.

Konsekvensnivået vurderes som BETYDELIG. Misbruk av låneformidlingssektoren kan medføre store økonomiske tap for långivere, investorer og andre berørte parter, og kan undergrave tilliten til låneformidling som finansieringskanal. Dersom sektoren i økende grad assosieres med hvitvasking eller tilgrensende ulovlig virksomhet, kan dette få ringvirkninger for kredittmarkedene og for tilgrensende deler av finanssystemet.

Risiko for hvitvasking i rapporteringspliktig sektor

INNENLANDSKE SELSKAPER SOM TILBYR SPILLTJENESTER

Statistikk og faktaboks *Innenlandske selskaper som tilbyr spilltjenester*

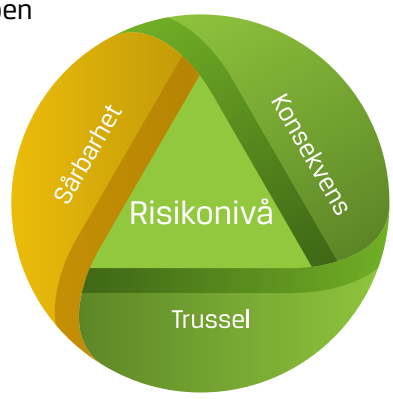
Innenlandske spilltilbydere omfattes av hvitvaskingsloven § 4 (2) bokstav g.

Antall foretak
Ved utgangen av 2025 var 45 spilltilbydere underlagt hvitvaskingsloven. Ingen har grensekryssende virksomhet.

Antall MF-rapporter 2023–2025[155]

Antall MFR	2023	2024	2025
Innenlandske spilltilbydere	59	17	39
Totalt antall	23 703	30 658	33 313

Det norske regulerte pengespillmarkedet hadde netto omsetning på 12,7 milliarder kroner i 2025.[156] En stor andel av omsetningen fra regulerte pengespill går til ideelle formål, hvor idretten mottar mest. Med noen få unntak,



155 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste.
156 Lotteritilsynet, *Ansvarligheit og kanalisering hos Norsk Tipping og Norsk Rikstotto, mars 2026*, (Lotteritilsynet, 2026).

er alle som arrangerer spill som krever tillatelse i henhold til pengespilloven omfattet av hvitvaskingsregelverket. Dette kapittelet tar kun for seg norske selskaper som tilbyr spilltjenester.[157] Det er imidlertid et stort marked av utenlandske pengespill som ikke har lov til å tilby pengespill i Norge, men som er tilgjengelige og rettet mot Norge. Disse omtales i del fire. Det regulerte markedet viser at pengespill i Norge til en viss utstrekning er eksponert for hvitvasking, i tilslørings- og plasseringsfasen.

Risikoen for hvitvasking gjennom innenlandske selskaper som tilbyr spilltjenester vurderes som LAV. Dette er uendret fra NRA 2022.

Spesifikke endringer

I 2025 ble det innført registrert spill- og maksimale tapsgrenser per dag og måned for bingo ved elektronisk hovedspill og databingo. Dette reduserer muligheten for anonymitet i disse spillene, og begrenser hvor store beløp som kan hvitvaskes gjennom dem.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for innenlandske spilltilbydere som LAV. Det knytter seg stor usikkerhet til vurderingen fordi det er informasjonshull når det gjelder omfang av hvitvasking gjennom sektoren. Hvitvaskingsrisikoen relaterer seg imidlertid primært til

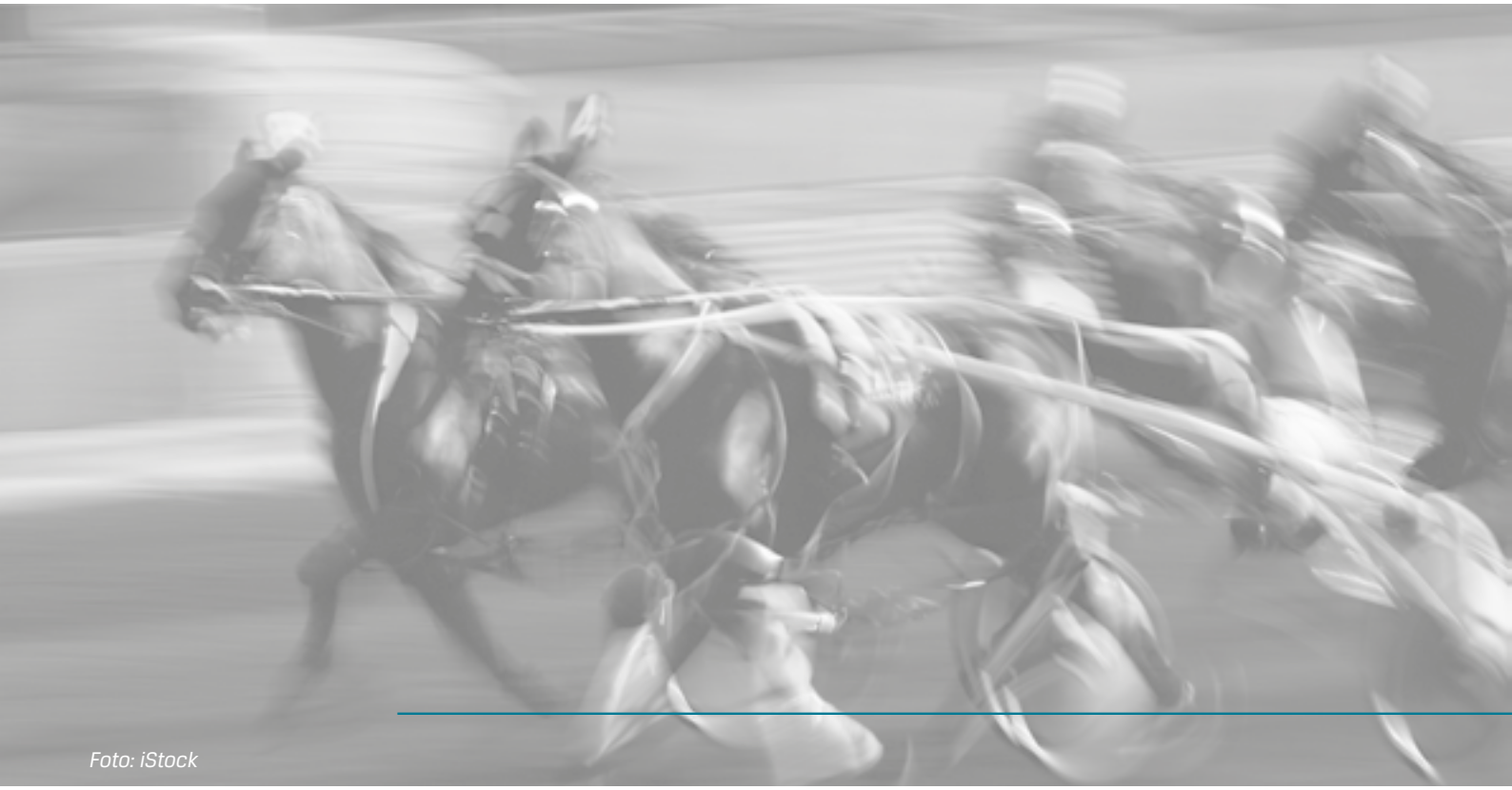


Foto: iStock

157 Det omfatter Norsk Tipping, Norsk Rikstoto og landsdekkende lotteri, bingomedhjelpere og en spilltilbyder av spill på skip.

> At regelverket oppleves som lite relevant kan føre til manglende etterlevelse

sportsspill med høy gevinstandel eller som er sårbare for resultatmanipulering, spillterminaler med høy gevinstandel og bruk av kontanter. Videre trekkes risikoen opp av at spilltilbyderne har begrenset opplæring, kontroll og mangler ved etterlevelse av regelverket.

Trusselen vurderes som LAV. Det knytter seg imidlertid stor usikkerhet til vurderingen som følge av mangelfull informasjon om hvitvaskingshendelser. Det flyter store summer gjennom sektoren årlig. I 2025 ble det omsatt for over 66 milliarder kroner i Norge, hvorav i underkant av 54 milliarder ble utbetalt som gevinster. Informasjon gjennom blant annet MF-rapporter og tilsyn viser at det er flere mulige metoder for hvitvasking gjennom pengespill, for eksempel utlån av kundeforhold, misbruk av spillekonto, spillere med problematisk spilleadferd, som utnyttes og forbruk av kriminelle midler. Bruk av muldyr og stråpersoner vil også være aktuelt, i tillegg til ID-misbruk. Sistnevnte gjelder primært utlån av kundeforhold eller spillekort. De fleste spilltilbydere har et krav om å registrere spillerne på en sikker måte. De fleste bruker registrering med BankID. Utlån av kundeforhold kan foregå ved å tillate en annen person å spille fra sin spillekonto eller ved endring av kontonummer eller mobilnummer som for eksempel brukes til Vipps-betalinger.

Sårbarheten vurderes som MODERAT. Det er gjennomgående mangler i regeletterlevelse, rutiner, kunnskap og kompetanse i AHV-arbeidet hos spilltilbydere. I tillegg opplever bransjen at regelverket er omfattende og ikke tilpasset spillsektoren. At regelverket oppleves som lite relevant, kan føre til manglende etterlevelse, noe gjennomførte tilsyn har avdekket. I tillegg mangler spilltilbyderne gode verktøy for å kunne identifisere midlenes opprinnelse. Dette forsterker sårbarheten. Innføringen av og registrert spill og tapsgrenser på bingo reduserer imidlertid sårbarhetene i integreringsfasen spesielt. Samtidig forutsetter tapsgrensen aktivt spill for å nå grensen. Derfor er det fortsatt handlingsrom for overføring av summer via spillkonto uten å spille, dette trekker sårbarheten opp.

Konsekvensnivået vurderes som LAVT med tanke på undergraving av samfunnsstrukturer og tillit. Det er særlig et mindre tapsomfang sammenlignet med andre sektorer med større volum som påvirker vurderingen. Imidlertid kan misbruk påvirke tilliten til sektoren negativt og undergrave dagens modell og enerettstilbyderne.

Risiko for hvitvasking i rapporteringspliktig sektor

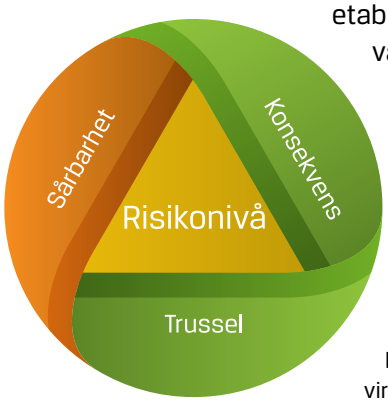
TILBYDERE AV VIRKSOMHETSTJENESTER

Statistikk og faktaboks *Tilbydere av virksomhetstjenester*

Tilbydere av virksomhetstjenester omfattes av hvitvaskingsloven § 4 (1) bokstav p.

Antall foretak
Ved utgangen av 2025 var 10 norske foretak registrert som tilbydere av virksomhetstjenester.

Antall MF-rapporter 2023–2025
Tilbydere av virksomhetstjenester[158] har ikke egen kategori under virksomhetsområde i hvitvaskingsregisteret.



Sektoren omfatter fysiske og juridiske personer som tilbyr tjenester knyttet til etablering, organisering og forvaltning av selskaper og andre juridiske enheter, eller som opptrer på vegne av tredjeperson i slike forhold.

Virksomhetstjenestetilbydere utgjør en liten og begrenset sektor i Norge. Regnskapsdata fra senere år underbygger at virksomhetene gjennomgående har et lavere omfang sammenlignet med flere andre rapporteringspliktige sektorer.

158 Tallene bygger på rapporteringspliktiges egenregistrering i hvitvaskingsregisteret basert på en forhåndsdefinert liste. Avvik kan forekomme fordi hvitvaskingsregisterets virksomhetskategorier ikke fullt ut samsvarer med sektorinndelingen i NRA.

Bistand til opprettelse av selskap omfatter også bistand i form av salg av *hylleselskaper*. Slike tjenester kan også tilbys som en del av tjenestetilbudet til andre rapporteringspliktige, herunder advokater, revisorer og regnskapsførere. Det samme gjelder for tjenesten som stiller forretningsadresse eller postadresse til rådighet. En annen relevant tjeneste er knyttet til det å opptre i særlige roller i selskapet, som styremedlem eller daglig leder. I tillegg omfatter virksomhetstjenester det å stå som såkalt nominee for aksjeeiere. Dette innebærer å «opptre» som aksjeeier. I norske selskaper er dette forbeholdt banker eller andre finansforetak som har konsesjon som forvalter. Slike forvaltere vil ikke være virksomhetstjenestetilbydere, men rapporteringspliktige på annet grunnlag.

Til sist nevnes det å forvalte en *trust* eller liknende juridisk arrangement. Det innebærer at en tredjeperson forvalter formuesmasse på vegne av en rettighetshaver. Rettighetshaveren har bare rett til å motta utdelinger fra trusten. Det kan ikke utelukkes at norske enkeltpersoner eller foretak kan forvalte utenlandske truster eller liknende juridiske arrangementer. Ingen slike har så langt søkt om å registrere seg hos Finanstilsynet.

Risikoen for hvitvasking er knyttet til muligheten for å etablere og vedlikeholde komplekse og lite transparente selskapsstrukturer for eierskap eller forflytning av midler, samt bidra til å skape et skinn av legitimitet rundt utbytte fra kriminalitet og muliggjøre videre integrering i den lovlige økonomien. Slik tjenestene tilbys i Norge, er de først og fremst relevante som ledd i oppsett av selskapsstrukturer hvor hvitvasking kan gjennomføres. Virksomhetstjenestetilbydere fremheves som særlig relevante i tilretteleggings- og tilsløringsfasen av hvitvasking.

Risikoen for hvitvasking gjennom tilbydere av virksomhetstjenester vurderes som MODERAT.

Spesifikke endringer

Tilbydere av virksomhetstjenester var ikke omtalt i NRA 2022. Seks av de ti selskapene som er registrert som virksomhetstilbydere ble registrert etter 2022.

Vurderinger

Samlet sett vurderes **hvitvaskingsrisikoen** for tilbydere av virksomhetstjenester som MODERAT. Sektoren fremstår ikke som en primær kanal for hvitvasking, men som et støttende og muliggjørende element i mer komplekse kriminalitetsstrukturer. Risikoen trekkes imidlertid opp som følge av betydelige sårbarheter i sektoren. Det gjelder blant annet små foretak med begrensede kontrollressurser, varierende forståelse og etterlevelse av hvitvaskingsregelverket, begrenset tilsynserfaring og svakheter i det regulatoriske autorisasjons- og egnethetsregimet.

Trusselen vurderes som LAV. Det er få aktører som tilbyr slike tjenester i Norge, og foretakene kjennetegnes i hovedsak av få ansatte og begrenset omsetning. Tjenestene omfatter begrensede verdier sammenliknet med øvrige sektorer. Misbruk av virksomhetstjenestetilbydere kan bidra til å etablere og opprettholde selskapsstrukturer som gir kriminelle aktører et skinn av legitimitet. Dette

Foto: Unsplash

knytter seg særlig til tilfeller der virksomhetstjenestetilbydere i tillegg tilbyr ulovlige stråpersontjenester.

Sårbarheten vurderes som BETYDELIG. Vurderingen reflekterer at sektoren i stor grad består av små foretak med få ansatte, noe som ofte innebærer begrensede ressurser til internkontroll, kompetansebygging og systematisk etterlevelse. Det er varierende og til dels mangelfull etterlevelse av hvitvaskingsregelverket. Dette kan gi kriminelle aktører et reelt handlingsrom til å utnytte svakheter i kundetiltak, risikovurderinger og løpende oppfølging. I tillegg trekkes sårbarheten opp av at det ikke foreligger en fullstendig oversikt over hvorvidt alle relevante aktører faktisk er registrert. Sårbarheten forsterkes også av at det er begrenset tilsynserfaring med sektoren og svakheter i autorisasjons- og egnethetsmekanismene. Regelverket gir begrensede muligheter til å avslå søknader om autorisasjon.

Konsekvensnivået vurderes som LAVT. Nivået påvirkes spesielt av at sektoren har en begrenset plass i det finansielle systemet med begrenset omfang. Sektoren håndterer eller flytter i begrenset grad betydelige verdier. Tjenestene som tilbys berører i hovedsak ikke finansielle aktiva som er direkte attraktive for hvitvaskingsformål.

Temaboks
Klimakvoter

Risiko for hvitvasking i rapporteringspliktig sektor

KLIMAKVOTER

Erfaringer fra flere europeiske land viser at klimakvoteregistre kan være utsatt for økonomisk kriminalitet. Klimakvoter er lett omsettelige og kan misbrukes som ledd i hvitvasking, blant annet ved å bidra til å tilsløre utbytte av straffbare handlinger gjennom kjøp og salg av kvoter.

Rapportering av mistenkelige forhold fra Miljødirektoratet til FIU i Økokrim gir myndighetene viktig informasjon som ellers ikke ville vært tilgjengelig. Slik informasjon kan bidra til å avdekke mønstre og metoder knyttet til hvitvasking og terrorfinansiering i forbindelse med omsetning av klimakvoter. Dette styrker samtidig muligheten til å redusere risikoen for at klimakvotemarkedet utnyttes av kriminelle aktører som et middel til å integrere eller flytte utbytte fra straffbare handlinger inn i den legale økonomien.

I Norge er Miljødirektoratet registermyndighet for klimakvoteregisteret. Selv om direktoratet ikke er rapporteringspliktig etter hvitvaskingsloven, er klimakvoteregisteret underlagt rapporteringsplikt etter EUs registerforordning. Dette innebærer blant annet en plikt til å iverksette tiltak for å forebygge og avdekke hvitvasking og terrorfinansiering, herunder å rapportere mistenkelige forhold til FIU i Økokrim.

> EUs nye hvitvaskingspakke vil få stor betydning for det norske antihvitvaskingsregimet

DEL 7

VEDLEGG

Foto: iStock

Oppsummering risikovurdering fremgangsmåter for hvitvasking – NRA 2026

Fremgangsmåter	Risikonivå	Trussel	Sårbarhet	Konsekvens
Grensekryssende pengestrømmer og betalings-infrastruktur	HØY	HØY	BETYDELIG	HØY
Kontanter	BETYDELIG	HØY	BETYDELIG	BETYDELIG
Kryptovaluta	HØY	HØY	HØY	MODERAT
Verdier utover penger: Fysiske og digitale verdigoder	HØY	HØY	HØY	BETYDELIG
Uformelle pengestrømmer, fra delingsøkonomi til illegal bankvirksomhet	HØY	HØY	HØY	BETYDELIG
Handelsbasert hvitvasking	HØY	HØY	HØY	HØY
Utnyttelse av virksomhetsstrukturer	HØY	HØY	HØY	HØY
Skjult eierskap	HØY	HØY	HØY	HØY
Profesjonelle tilretteleggere og innsidere	HØY	BETYDELIG	HØY	HØY
Sosiale medier, digitale plattformer og gavekort	BETYDELIG	MODERAT	HØY	BETYDELIG
Pengespill	MODERAT	MODERAT	BETYDELIG	LAV
Eiendom	HØY	HØY	BETYDELIG	HØY
Handel med gull	BETYDELIG	BETYDELIG	HØY	MODERAT
Kriminelle nettverk	HØY	HØY	BETYDELIG	HØY
Utbytte fra kriminalitet i utlandet				
Muldyr og identitetsmisbruk				

Oppsummering risikovurdering kriminalitetsområder – NRA 2026

Kriminalitetsområder	Risikonivå	Trussel	Sårbarhet	Konsekvens
Bedrageri	HØY	HØY	HØY	HØY
Utnyttelse av offentlige ordninger	HØY	BETYDELIG	HØY	HØY
Skatte- og avgiftskriminalitet	HØY	HØY	BETYDELIG	HØY
Korrupsjon	MODERAT	MODERAT	MODERAT	HØY
Narkotika og vinningsforbrytelser	HØY	HØY	MODERAT	HØY
Mennesker som varer: seksuallovbrudd, menneskehandel og menneskesmugling	HØY	HØY	BETYDELIG	HØY
Cyberkriminalitet	BETYDELIG	BETYDELIG	BETYDELIG	HØY
Miljøkriminalitet	BETYDELIG	BETYDELIG	HØY	HØY
Arbeidslivskriminalitet	BETYDELIG	BETYDELIG	BETYDELIG	BETYDELIG
Fiskeri- og havbruksnæringen	HØY	HØY	BETYDELIG	HØY
Hvitvasking i utvalgte bransjer				
Energibransjen				
Datasentre				
Utpressing				

Oppsummering risikovurdering sektor – NRA 2026

Sektor	Risikonivå	Trussel	Sårbarhet	Konsekvens
Bank	HØY	HØY	BETYDELIG	HØY
Kredittforetak	MODERAT	MODERAT	MODERAT	MODERAT
Finansieringsforetak	BETYDELIG	BETYDELIG	BETYDELIG	BETYDELIG
Betalingsforetak og e-pengeforetak	HØY	HØY	HØY	BETYDELIG
Agenter for utenlandske betalingsforetak	BETYDELIG	BETYDELIG	HØY	BETYDELIG
Norske tilbydere av kryptoeiendelstjenester	BETYDELIG	HØY	BETYDELIG	MODERAT
Forsikrings- og forsikringsformidlingsforetak	BETYDELIG	BETYDELIG	BETYDELIG	HØY
Verdipapirsektoren	MODERAT	MODERAT	MODERAT	BETYDELIG
Fondsektoren	MODERAT	MODERAT	MODERAT	MODERAT
Revisor	MODERAT	MODERAT	BETYDELIG	BETYDELIG
Regnskapsfører	BETYDELIG	BETYDELIG	HØY	BETYDELIG
Advokatbransjen	BETYDELIG	MODERAT	BETYDELIG	BETYDELIG
Eiendomsmegling	HØY	HØY	BETYDELIG	HØY
Låneformidling	BETYDELIG	BETYDELIG	BETYDELIG	BETYDELIG
Innenlandske selskaper som tilbyr spilltjenester	LAV	LAV	MODERAT	LAV
Tilbydere av virksomhetstjenester	MODERAT	LAV	BETYDELIG	LAV

Oppsummering risikovurdering sektor

Sektor	Risikonivå NRA 2022	Risikonivå NRA 2026
Bank	HØY	HØY
Kredittforetak	MODERAT	MODERAT
Finansieringsforetak	MODERAT	BETYDELIG
Betalingsforetak og e-pengeforetak	HØY BETYDELIG	HØY
Agenter for utenlandske betalingsforetak	HØY	BETYDELIG
Norske tilbydere av kryptoeiendelstjenester	MODERAT	BETYDELIG
Forsikrings- og forsikringsformidlingsforetak	MODERAT	BETYDELIG
Verdipapirsektoren	MODERAT	MODERAT
Fondsektoren	MODERAT	MODERAT
Revisor	MODERAT	MODERAT
Regnskapsfører	BETYDELIG	BETYDELIG
Advokatbransjen	BETYDELIG	BETYDELIG
Eiendomsmegling	BETYDELIG	HØY
Låneformidling		BETYDELIG
Innenlandske selskaper som tilbyr spilltjenester	LAV	LAV
Tilbydere av virksomhetstjenester		MODERAT

Begrepsavklaringer[159]

Blokkjede – (engelsk: blockchain) en distribuert hovedbok som lagrer transaksjoner eller annen data (blant annet kryptovaluta) i sammenkoblede blokker, der informasjonen er sikret med kryptografi og vanskelig å endre i ettertid.

Broer – (engelsk: bridges) en protokoll eller teknologi som gjør det mulig å flytte digitale eiendeler (som tokens eller NFT-er) og data mellom ulike blokkjedenettverk.

Brotransaksjoner – (engelsk: blockchain bridge) en protokoll som gjør det mulig å overføre data eller digitale aktiva (som kryptovaluta) fra en blokkjede til en annen.

Clearing – avregning eller oppgjør av økonomiske transaksjoner.

Fiatvaluta – nasjonal valuta, for eksempel NOK.

Fintech – finansteknologi. En samlebetegnelse for teknologi som brukes i finansielle produkter og tjenester.

Flipping – kjøp av eiendom for raskt å selge videre for fortjeneste, eksempelvis etter oppussing.

Hacks – ulovlig aktivitet der hackere skaffer seg uautorisert tilgang til blokkjedesystemer, kryptobørser, digitale lommebøker eller smarte kontrakter for å stjele digitale eiendeler.

Hylleselskaper – selskaper som er ferdig stiftet og registrert, men som ikke har verdier eller virksomhet ut over det pålagte kravet til aksjekapital.

Kjedehopping – (engelsk: chain hopping) er prosessen hvor en bruker flytter kryptovaluta raskt fra en blokkjede til en annen.

Kriminalitet som tjeneste – (engelsk: crime-as-a-service) tjenester som tilbys i et kriminelt marked, slik lovlige tjenester tilbys i det lovlige markedet.

Løsepengevirus – skadevare som krypterer filer og mapper på en datamaskin eller et datanettverk, og der angriperen krever betaling for å gjenopprette tilgangen.

Miksere/miksetjeneste – tjenester eller protokoller som blander kryptoeiendeler fra flere brukere for å skjule forbindelsen mellom avsender og mottaker.

NFT-er – non-fungible tokens er unike digitale tokens på en blokkjede som kan representere et digitalt eller fysisk objekt, en rettighet eller annen verdi. En NFT dokumenterer tokenens registrering og transaksjonshistorikk.

OTC-ledd – over the counter, fagbegrep for handel utenom regulert marked eller handelsplass.

159 Begreper slik de er forstått i denne rapporten.

P2P-kanaler – peer-to-peer-kanaler der brukere kan overføre eller handle verdier direkte med hverandre, for eksempel kjøp og salg av kryptoeiendeler uten at en tradisjonell finansinstitusjon er part i handelen.

Pengemuldyr – personer som stiller sin konto til disposisjon for kriminelle.

Privacy coins – kryptovaluta designet for å sikre anonymitet ved å skjule eksempelvis avsender, mottaker og transaksjonsbeløp.

RegTech – reguleringsteknologi. Bruk av ny teknologi for å hjelpe bedrifter med å oppfylle lover og regulatoriske krav mer effektivt.

Returprovisjon (engelsk: kick-back) – en godtgjørelse eller del av et forvaltningshonorar som en tjenesteyter (som bank eller fondsplattform) mottar fra en tredjepart (som fondselskap) for å formidle et produkt.

Skins – er blant annet utstyr til våpen og klær til figurer i dataspill.

Smurfing – dele opp penger i mindre beløp og spre dem til flere personer, kontoer eller steder.

Stablecoins – kryptoeiendeler som er ment å holde stabil verdi ved å være knyttet til én offisiell valuta, flere valutaer, råvarer eller andre eiendeler/rettigheter. Etter MiCA skilles det blant annet mellom e-pengetokener og eiendelsrefererte tokener.

Syntetisk overgrepsmateriale – samlebetegnelse for alt materiale (bilder, video, tekst m.v.) som viser seksuelle overgrep mot barn eller på annen måte seksualiserer barn, som er generert med bruk av generativ kunstig intelligens.

Token-swaps – en direkte utveksling av en kryptovaluta (token) til en annen.

Tokenisering – det å representere eiendeler som digitale objekter, såkalte «tokens», på en blokkjede.

Trust – truster er en rettslig konstruksjon som ikke har en direkte parallell i norsk rett.

Wallet – lommebok (på norsk) er en app, et program, elektronisk enhet eller papirlapp som inneholder nødvendig informasjon for å kunne oppbevare og sende kryptovaluta.

ØKOKRIM

Økokrim
Postboks 2096 Vika, 0125 Oslo
Telefon: 23 29 10 00
E-post: post.okokrim@politiet.no