AML Risk Assessment

Risikovurdering — Hvitvasking og terrorfinansiering

Dokument: Virksomhetsinnrettet risikovurdering, jf. hvitvaskingsloven §6 **Virksomhet:** ALAI Holding AS, org.nr 932 516 136 **Produkt:** Drop — betalingsformidling og pengeoverføringer **Versjon:** 1.0 **Dato:** 2026-02-12 **Utarbeidet av:** Compliance **Godkjent av:** Styre **Neste revisjon:** 2027-02-12

---

1. Innledning

1.1 Formål

Denne risikovurderingen er utarbeidet i henhold til hvitvaskingsloven §6, som pålegger rapporteringspliktige å identifisere og vurdere risikoen for at virksomheten kan bli brukt til hvitvasking eller terrorfinansiering. Vurderingen danner grunnlaget for Selskapets risikobaserte tilnærming til kundetiltak og transaksjonsovervåking.

1.2 Metode

Risikovurderingen er basert på:

- Nasjonal risikovurdering (NRA) utgitt av Justis- og beredskapsdepartementet
- Finanstilsynets veiledning til hvitvaskingsregelverket
- FATFs risikovurderingsmetodikk
- EUs overnasjonale risikovurdering (SNRA)
- Egne erfaringer og bransjeanalyse

1.3 Risikomatrise — vurderingsmetodikk

Sannsynlighet:

Nivå	Beskrivelse
1 — Lav	Lite sannsynlig at risikoen materialiserer seg
2 — Middels	Kan forekomme i enkelte tilfeller
3 — Høy	Sannsynlig at risikoen materialiserer seg jevnlig
4 — Svært høy	Nærmest sikkert / har allerede forekommet

Konsekvens:

Nivå	Beskrivelse
1 — Lav	Begrenset økonomisk tap, ingen regulatorisk konsekvens
2 — Middels	Moderat tap, mulig tilsynsreaksjon
3 — Høy	Vesentlig tap, tilsynssanksjon, omdømmeskade
4 — Svært høy	Konsesjonsinndragelse, straffeansvar

Iboende risiko = Sannsynlighet x Konsekvens (uten tiltak) **Restrisiko** = Risiko etter implementerte tiltak

---

2. Virksomhetsbeskrivelse

2.1 Om Selskapet

ALAI Holding AS utvikler og drifter betalingsapplikasjonen Drop, som tilbyr:

1. **Pengeoverføringer (remittance):** Grensekryssende overføringer fra Norge til 30+ land
2. **QR-betalinger:** Betalinger i butikk via QR-kode, tilgjengelig for alle merchanter

2.2 Forretningsmodell

- **Pass-through-modell:** Drop holder aldri kundemidler. Transaksjoner initieres via PSD2-grensesnitt (PISP/AISP) mot kundens egen norske bankkonto.
- **Målgruppe:** Alle innbyggere i Norge og Skandinavia som er 18+ med norsk BankID
- **Autentisering:** Norsk BankID (høyt sikkerhetsnivå)

2.3 Produkter og tjenester

Tjeneste	Beskrivelse	Volum (forventet år 1)

Remittance	Overføring fra norsk bank til mottaker i utlandet	~36 000 transaksjoner
QR-betaling	Betaling i butikk via QR-kode	~120 000 transaksjoner
Merchant onboarding	Registrering av butikker for QR-mottak	~200 merchanter

---

3. Kundebasert risiko

3.1 Kundeprofil

Drops kundebase består av alle innbyggere i Norge som ønsker å sende penger til utlandet eller betale i butikk. Kundene identifiseres og verifiseres gjennom norsk BankID.

3.2 Kunderisikofaktorer

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
Stråmenn (muldyr) — kunder som utfører transaksjoner på vegne av andre	3 x 3 = 9 (Høy)	BankID-verifisering, transaksjonsovervåking, adferdsmønster-analyse	2 x 3 = 6 (Middels)
Kunder med høyt transaksjonsvolum — volumet overstiger oppgitt formål	2 x 3 = 6 (Middels)	Automatisk flagging ved avvik fra profil, EDD ved >200%	1 x 3 = 3 (Lav)
PEP-kunder — politisk eksponerte personer	1 x 4 = 4 (Middels)	Automatisk PEP-screening ved onboarding og løpende, EDD	1 x 3 = 3 (Lav)
Kunder som sender til mange ulike mottakere — indikasjon på pengeformidling	2 x 3 = 6 (Middels)	Maks antall mottakere per periode, manuell review	1 x 3 = 3 (Lav)
Kunder som sender til høyrisikoland — korridorbasert risiko	3 x 3 = 9 (Høy)	EDD for høyrisikokorridorer, lavere terskler, dokumentasjon av formål	2 x 2 = 4 (Middels)
Nye kunder med umiddelbart høyt volum — avvikende fra normalt mønster	2 x 3 = 6 (Middels)	Gradvis volumøkning, automatisk flagging, EDD	1 x 3 = 3 (Lav)

3.3 Merchant-risikofaktorer

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
Kontantintensive virksomheter — restauranter, kiosker, frisører	3 x 3 = 9 (Høy)	Verifisering av org.nr mot Brønnøysundregistrene, transaksjonsovervåking, EDD	2 x 2 = 4 (Middels)
Nyetablerte foretak — kort driftshistorikk	2 x 2 = 4 (Middels)	Utvidet KYC ved registrering, hyppigere oppfølging	1 x 2 = 2 (Lav)
Uvanlig transaksjonsmønster — refusjoner, splitting	2 x 3 = 6 (Middels)	Automatisk overvåking av refusjonsandel og transaksjonsmønster	1 x 3 = 3 (Lav)

---

4. Geografisk risiko

4.1 Metodikk

Geografisk risiko vurderes basert på:

- FATFs vurderinger (gråliste/svarteliste)
- EUs liste over høyrisikoland (delegert forordning)
- Transparency Internationals Corruption Perceptions Index (CPI)
- Nasjonal risikovurdering (NRA)
- Basel AML Index

4.2 Korridorklassifisering

Korridor	Land	FATF-status	CPI (2024)	EU høyrisiko	Risikonivå	Tiltak
NOK → EUR	EU/EØS	Compliant	Varierer, generelt høy	Nei	**Lav**	Standard CDD
NOK → PLN	Polen	Compliant	54	Nei	**Lav**	Standard CDD
NOK → GBP	Storbritannia	Compliant	71	Nei	**Lav**	Standard CDD
NOK → RSD	Serbia	Under evaluering (MONEYVAL)	36	Nei	**Middels**	Standard CDD + formålsdokumentasjon
NOK → BAM	Bosnia-Hercegovina	Under evaluering (MONEYVAL)	35	Nei	**Middels**	Standard CDD + formålsdokumentasjon

Korridor	Land	FATF-status	CPI (2024)	EU høyrisiko	Risikonivå	Tiltak
NOK → TRY	Tyrkia	Under evaluering (FATF)	34	Nei (per 2025)	**Middels**	Standard CDD + formålsdokumentasjon
NOK → PKR	Pakistan	Gråliste-historikk	24	Varierer	**Høy**	EDD obligatorisk
NOK → sanksjonerte land	Iran, Nord-Korea, etc.	Svarteliste	N/A	Ja	**Sperret**	Blokkert i systemet

4.3 Geografisk risikovurdering — oppsummering

Risikonivå	Andel av forventet volum	Tiltak
Lav	~30%	Standard CDD, standard overvåking
Middels	~50%	CDD + ekstra formålskontroll, lavere terskler
Høy	~15%	EDD, dokumentasjon av midlers opprinnelse, manuell review
Sperret	0%	Korridoren er blokkert

---

5. Produkt- og tjenestebasert risiko

5.1 Remittance (grensekryssende overføringer)

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
Grensekryssende karakter — midler forlater norsk jurisdiksjon	3 x 3 = 9 (Høy)	Korridorbasert risikotilnærming, BaaS-partner med egne kontroller	2 x 2 = 4 (Middels)
Hastighet — rask gjennomføring vanskeliggjør intervensjon	2 x 3 = 6 (Middels)	Pre-transaksjon sankssjonsscreening, automatisk hold ved flagging	1 x 3 = 3 (Lav)
Tredjeparts mottaker — mottaker er ofte annen person	2 x 2 = 4 (Middels)	Registrering av mottaker, begrensning av antall unike mottakere	1 x 2 = 2 (Lav)

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
Smurfing/splitting — flere små transaksjoner for å unngå terskler	3 x 3 = 9 (Høy)	Kumulativ overvåking (daglig, ukentlig, månedlig), mønstergjenkjenning	2 x 2 = 4 (Middels)

5.2 QR-betalinger (innenlandske)

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
Lavere iboende risiko — innenlandsk, begge parter identifisert	1 x 2 = 2 (Lav)	Standard CDD, transaksjonsovervåking	1 x 1 = 1 (Lav)
Fiktive transaksjoner — oppkonstruerte transaksjoner mellom nærstående	2 x 2 = 4 (Middels)	Overvåking av transaksjonsmønster, kontroll av merchant-legitimitet	1 x 2 = 2 (Lav)
Refusjonssvindel — systematisk misbruk av refusjoner	1 x 2 = 2 (Lav)	Automatisk overvåking av refusjonsandel per merchant	1 x 1 = 1 (Lav)

5.3 Samlet produktrisiko

Produkt	Iboende risikonivå	Etter tiltak
Remittance	**Høy**	**Middels**
QR-betaling	**Lav**	**Lav**

---

6. Kanal- og leveringsrisiko

6.1 Digital onboarding

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
Ikke-fysisk kontakt — kunden er aldri fysisk til stede	2 x 2 = 4 (Middels)	BankID gir høyt identitetssikkerhetsnivå (eIDAS «høyt»), kompenserer for manglende fysisk oppmøte	1 x 2 = 2 (Lav)
Identitetstyveri — noen bruker andres BankID	1 x 4 = 4 (Middels)	BankID krever personlig kodebrikke/mobil, svært vanskelig å misbruke	1 x 3 = 3 (Lav)

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
Mobilapp — enhet kan kompromitteres	1 x 2 = 2 (Lav)	Enhetsautentisering, sesjonstokens, anomalideteksjon	1 x 1 = 1 (Lav)

6.2 Samlet kanalrisiko

Digital kanal med BankID vurderes som **lav restrisiko** grunnet høyt identitetssikkerhetsnivå.

---

7. Terrorfinansieringsrisiko

7.1 Vurdering

Nasjonal risikovurdering (NRA) identifiserer grensekryssende overføringer som en potensiell kanal for terrorfinansiering, særlig:

- Små beløp til høyrisikoområder (under rapporteringsterskler)
- Bruk av stråmenn/muldyr

7.2 Spesifikke risikofaktorer

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
Overføringer til konfliktområder	3 x 4 = 12 (Svært høy)	Blokkering av sanksjonerte land, EDD for naboland til konfliktområder, lavere overvåkingsterskler	2 x 3 = 6 (Middels)
Mange små overføringer til samme region	2 x 3 = 6 (Middels)	Kumulativ overvåking, mønstergjenkjenning	1 x 3 = 3 (Lav)
Innsamlingsaksjoner via plattformen	1 x 4 = 4 (Middels)	Drop tillater kun P2P-overføringer, ingen innsamlingsfunksjon	1 x 3 = 3 (Lav)

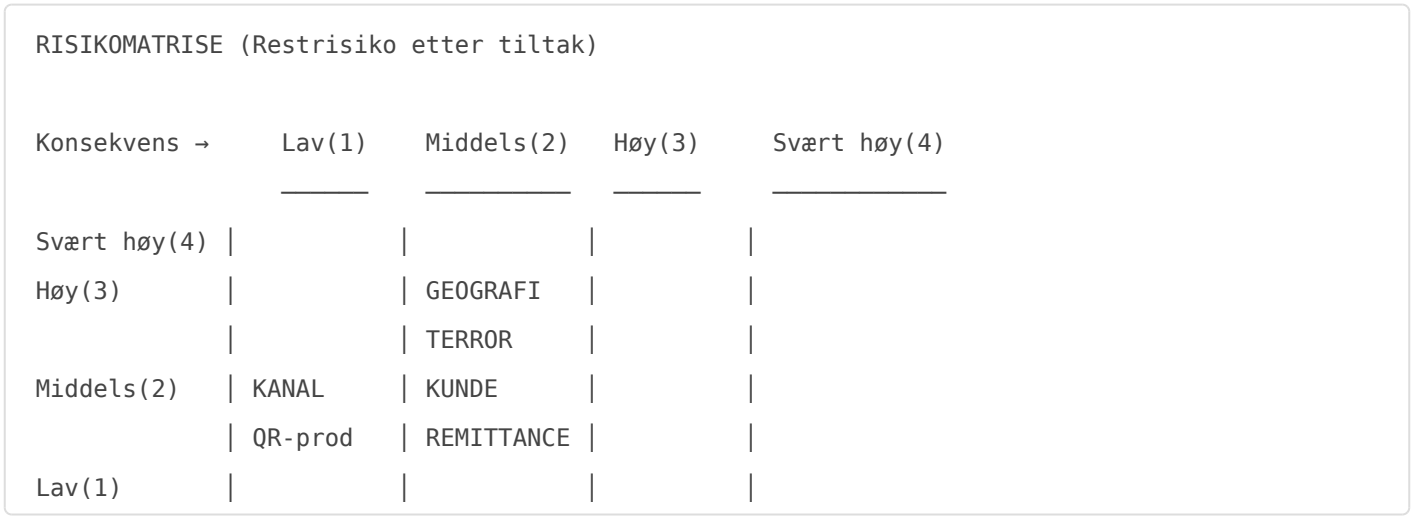
---

8. Samlet risikovurdering — risikomatrise

8.1 Overordnet risikobilde

Risikokategori	Iboende risiko	Restrisiko (etter tiltak)
Kundebasert risiko	Middels-Høy	Lav-Middels
Geografisk risiko	Høy	Middels
Produktrisiko (remittance)	Høy	Middels
Produktrisiko (QR)	Lav	Lav
Kanalrisiko	Middels	Lav
Terrorfinansieringsrisiko	Høy	Middels
Samlet virksomhetsrisiko	**Høy**	**Middels**

8.2 Visualisering



8.3 Konklusjon

Virksomhetens samlede restrisiko vurderes som **middels** etter implementering av tiltak beskrevet i dette dokumentet og i hvitvaskingsrutinene. De viktigste risikoreduserende faktorene er:

1. **BankID-verifisering** — sikrer høyt identitetsnivå for alle kunder
2. **Pass-through-modell** — Drop holder aldri kundemidler, noe som begrenser misbruksmuligheter
3. **Korridorbasert risikovurdering** — differensierte tiltak etter mottakerland
4. **Automatisert transaksjonsovervåking** — regelbasert overvåking med konfigurbare terskler

---

9. Handlingsplan

9.1 Tiltak som skal implementeres før lansering

Nr	Tiltak	Ansvarlig	Frist	Status
1	Implementere PEP- og sanksjonsscreening (API-integrasjon)	Tech Lead	Før lansering	Planlagt
2	Implementere automatisert transaksjonsovervåking	Tech Lead	Før lansering	Planlagt
3	Etablere compliance-dashboard	Tech Lead	Før lansering	Planlagt
4	Inngå avtale med PEP/sanksjons-dataleverandør	Daglig leder	Før lansering	Planlagt
5	Gjennomføre opplæring av alle ansatte	Hvitvaskingsansvarlig	Før lansering	Planlagt
6	Registrere rapporteringskanal hos Altinn/EFE	Hvitvaskingsansvarlig	Før lansering	Planlagt
7	Etablere rutine for korridorblokkering	Tech Lead	Før lansering	Planlagt

9.2 Løpende tiltak

Tiltak	Frekvens	Ansvarlig
Oppdatering av risikovurdering	Årlig + ved vesentlige endringer	Hvitvaskingsansvarlig
Oppdatering av korridorklassifisering	Kvartalsvis	Hvitvaskingsansvarlig
Re-screening mot PEP/sanksjonslister	Løpende (automatisk)	System
Gjennomgang av transaksjonsovervåkingsregler	Halvårlig	Hvitvaskingsansvarlig
Rapport til styret	Kvartalsvis	Hvitvaskingsansvarlig
Ekstern revisjon av AML-program	Årlig	Ekstern revisor

10. Endringslogg

Versjon	Dato	Endring	Godkjent av
1.0	2026-02-12	Førstegangs utarbeidelse	Styre

Dokumentet er utarbeidet i henhold til hvitvaskingsloven §6 og Finanstilsynets veiledning om virksomhetsinnrettet risikovurdering. Risikovurderingen skal gjennomgås og oppdateres minst årlig.

Revision #5
Created 2026-02-18 08:44:37 UTC by John
Updated 2026-05-25 07:24:19 UTC by John