

# AML & Risk

- [AML Procedures](#)
- [AML Risk Assessment](#)
- [Suitability Assessment](#)

# AML Procedures

## Hvitvaskingsrutiner — Drop (ALAI Holding AS)

**Dokument:** Internrutiner for tiltak mot hvitvasking og terrorfinansiering **Hjemmel:** Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven, LOV-2018-06-01-23) **Virksomhet:** ALAI Holding AS, org.nr 932 516 136 **Produkt:** Drop — betalingsformidling og pengeoverføringer **Versjon:** 1.0 **Dato:** 2026-02-12 **Godkjent av:** Daglig leder / Styre **Neste revisjon:** 2027-02-12

---

## 1. Formål og virkeområde

### 1.1 Formål

Disse rutinene skal sikre at ALAI Holding AS («Selskapet») gjennom produktet Drop etterlever kravene i hvitvaskingsloven med forskrifter, og bidrar til å forebygge og avdekke hvitvasking og terrorfinansiering.

### 1.2 Virkeområde

Rutinene gjelder for all virksomhet knyttet til Drop, herunder:

- Pengeoverføringer til utlandet (remittance) til 30+ land
- QR-baserte betalinger i butikk
- Kunderegistrering og -oppfølging
- Alle ansatte, styremedlemmer og tredjeparter som utfører oppgaver på vegne av Selskapet

### 1.3 Forretningsmodell — pass-through

Drop opererer en pass-through-modell under PSD2 (PISP/AISP). Drop holder aldri kundemidler. Alle transaksjoner initieres via Open Banking-grensesnitt mot kundens egen bankkonto. Denne modellen reduserer enkelte risikoer, men endrer ikke de grunnleggende pliktene etter hvitvaskingsloven.

# 1.4 Regulatorisk klassifisering

Selskapet søker konsesjon som betalingsforetak etter finansforetaksloven, jf. også hvitvaskingsloven §4 første ledd bokstav c (betalingsforetak).

## 2. Lovgrunnlag og sentrale bestemmelser

Bestemmelse	Innhold
Hvv. §4	Rapporteringspliktige — betalingsforetak er omfattet
Hvv. §6	Virksomhetsinnrettet risikovurdering
Hvv. §§7-8	Rutiner og internkontroll
Hvv. §§9-18	Kundetiltak (CDD)
Hvv. §§17-18	Forsterkede kundetiltak (EDD)
Hvv. §§24-25	Løpende oppfølging
Hvv. §26	Undersøkelsesplikt
Hvv. §26 tredje ledd	Rapporteringsplikt til Økokrim/EFE
Hvv. §30	Oppbevaringsplikt (5 år)
Hvv. §§36-38	Internkontroll og opplæring
Sanksjonslovgivningen	FN, EU, norske sanksjonslister
PEP-forskriften	Politisk eksponerte personer

## 3. Virksomhetsinnrettet risikovurdering (§6)

### 3.1 Krav

Selskapet skal gjennomføre og dokumentere en helhetlig risikovurdering av virksomheten, som identifiserer og vurderer risikoen for hvitvasking og terrorfinansiering. Risikovurderingen oppdateres minst årlig og ved vesentlige endringer.

## 3.2 Risikokategorier

Risikovurderingen dekker følgende kategorier:

- **Kundebasert risiko** — risikobasert tilnærming basert på kundens adferd, transaksjonsvolum og korridorer
- **Geografisk risiko** — land og korridorer med høyere HV/TF-risiko
- **Produkt- og tjenestebasert risiko** — grensekryssende overføringer, QR-betalinger
- **Kanal- og leveringsrisiko** — digital onboarding, mobilapp

Se eget dokument: [risikovurdering-hvitvasking.md](#)

## 3.3 Risikonivåer

Nivå	Beskrivelse	Tiltak
Lav	Norsk bosatt, norsk BankID, lavrisiko-korridor	Standard kundetiltak (CDD)
Middels	Høyere transaksjonsvolum, middels risiko-korridor	Utvidet overvåking, mulig EDD
Høy	Høyrisiko-korridor, PEP, uvanlig transaksjonsmønster	Forsterkede kundetiltak (EDD)
Uakseptabel	Sanksjonert person/land, bekreftet mistanke	Avvisning eller avvikling av kundeforhold

## 4. Kundetiltak (KYC/CDD) — §§9-16

### 4.1 Når kundetiltak skal gjennomføres

Kundetiltak skal gjennomføres ved:

- Etablering av kundeforhold (registrering i Drop), jf. §10
- Enkeltstående transaksjoner over NOK 10 000 utenfor etablert kundeforhold, jf. §10
- Mistanke om hvitvasking eller terrorfinansiering, uavhengig av beløp, jf. §10
- Tvil om tidligere innhentede opplysninger, jf. §24

### 4.2 Standard kundetiltak (CDD)

#### 4.2.1 Fysiske personer (alle kunder)

Følgende opplysninger skal innhentes og verifiseres, jf. §12:

Opplysning	Kilde	Verifisering
Fullt navn	BankID	Automatisk via BankID-integrasjon
Fødselsnummer (11 siffer)	BankID	Automatisk — brukes til alderskontroll (18+) og identifisering
Adresse	Kunde oppgir, sjekkes mot Folkeregisteret	Folkeregisteroppslag
Statsborgerskap	Kunde oppgir	Krysssjekk mot BankID-data
Formål med kundeforholdet	Kunde velger ved registrering	Dokumenteres i kundeprofil

## 4.2.2 Juridiske personer (merchants)

For merchanter som registrerer seg for QR-betalinger:

Opplysning	Kilde	Verifisering
Foretaksnavn og org.nr	Kunde oppgir	Brønnøysundregistrene
Forretningsadresse	Kunde oppgir	Brønnøysundregistrene
Reelle rettighetshavere	Kunde oppgir	Aksjonærregisteret, egenopp-gave
Daglig leder/kontaktperson	Kunde oppgir	BankID-verifisering av kontaktperson
Formål med kundeforholdet	Kunde velger	Dokumenteres

## 4.2.3 Identitetsbekreftelse

- **Primær metode:** Norsk BankID (nivå «høyt» etter eIDAS)
- BankID gir verifisert navn, fødselsnummer og sikrer at kunden er den de utgir seg for
- Kunder uten gyldig norsk BankID kan ikke registrere seg i Drop
- Minstealder 18 år kontrolleres automatisk basert på fødselsnummer

# 4.3 Forsterkede kundetiltak (EDD) — §§17-18

Forsterkede tiltak skal gjennomføres når risikoen er vurdert som høy, herunder:

## 4.3.1 Situasjoner som utløser EDD

- Kunder som sender penger til høyrisikoland (jf. EUs liste over høyrisikoland og FATFs gråliste/svarteliste)
- Politisk eksponerte personer (PEP), jf. §18
- Uvanlige eller mistenkelige transaksjonsmønstre
- Kunder med vesentlig høyere transaksjonsvolum enn oppgitt formål tilsier
- Kundeforhold der det er vanskelig å verifisere reelle rettighetshavere

## 4.3.2 EDD-tiltak

- Innhenting av tilleggsinformasjon om midlenes opprinnelse
- Innhenting av dokumentasjon for formålet med transaksjonen
- Hyppigere oppdatering av kundeinformasjon
- Økt transaksjonsovervåking (lavere terskelverdier)
- Godkjenning av kundeforholdet av hvitvaskingsansvarlig
- Risikovurdering dokumenteres i kundeprofilen

## 4.4 PEP-screening — §18

### 4.4.1 Hvem er PEP

Politisk eksponerte personer inkluderer:

- Statsoverhoder, regjeringsmedlemmer, parlamentsmedlemmer
- Høyesterettsdommere, riksrevisorer, sentralbankstyremedlemmer
- Ambassadører, militære offiserer av høy rang
- Ledere av statsforetak
- Nære familiemedlemmer og kjente medarbeidere til ovennevnte

### 4.4.2 PEP-prosedyre

1. **Screening ved onboarding:** Automatisk PEP-sjekk mot anerkjent database (f.eks. Refinitiv World-Check, Dow Jones)
2. **Løpende screening:** Automatisk re-screening ved endringer i PEP-lister
3. **Positive treff:** Manuell vurdering av hvitvaskingsansvarlig
4. **EDD ved bekreftet PEP:** Tilleggsdokumentasjon, godkjenning av daglig leder, hyppigere overvåking

## 4.5 Sanksjonsscreening

### 4.5.1 Lister som sjekkes

- FNs konsoliderte sanksjonsliste
- EUs konsoliderte sanksjonsliste
- Norske forskrifter om sanksjoner (UD)
- OFAC SDN-listen (for USD-transaksjoner)

### 4.5.2 Prosedyre

1. **Ved onboarding:** Automatisk screening av kundens navn og fødselsdato mot alle sanksjonslister
2. **Ved hver transaksjon:** Automatisk screening av mottaker mot sanksjonslister
3. **Positive treff:** Transaksjon fryses automatisk. Hvitvaskingsansvarlig varsles.

4. **Bekreftet treff:** Transaksjon avvises. Rapportering til Utenriksdepartementet og EFE.
5. **Falske positive:** Dokumenteres og godkjennes av hvitvaskingsansvarlig.

## 5. Løpende oppfølging — §§24-25

### 5.1 Transaksjonsinformasjon

Alle transaksjoner skal inneholde følgende informasjon, jf. betalingssystemloven og EU-forordning 2015/847:

- Avsenders fulle navn, adresse, kontonummer
- Mottakers fulle navn, kontonummer/referanse
- Beløp og valuta
- Tidspunkt
- Formål (for beløp over NOK 10 000)

### 5.2 Transaksjonsovervåking

#### 5.2.1 Automatisk overvåking

Selskapet implementerer et automatisert transaksjonsovervåkingssystem som flagger:

Regel	Terskel	Handling
Enkelt-transaksjon over terskel	> NOK 50 000	Manuell gjennomgang
Kumulativt daglig volum	> NOK 100 000	Manuell gjennomgang
Kumulativt månedlig volum	> NOK 500 000	EDD-vurdering
Hyppe transaksjoner til høyrisikoland	> 5/uke til samme korridor	Manuell gjennomgang
Splitting av transaksjoner	Flere transaksjoner like under terskel	Automatisk flagging
Avvik fra kundeprofil	> 200% av oppgitt bruksformål	Manuell gjennomgang
Round-trip-transaksjoner	Penger sendt og mottatt fra samme korridor	Automatisk flagging
Uvanlig adferd	Hurtig endring av mottakerland	Manuell gjennomgang

#### 5.2.2 Manuell gjennomgang

- Flaggede transaksjoner gjennomgås av compliance-teamet innen 24 timer
- Vurderingen dokumenteres med konklusjon og eventuell oppfølgingshandling

- Ved fortsatt mistanke: undersøkelsesplikt, jf. §26

## 5.3 Oppdatering av kundeinformasjon

- **Lav risiko:** Kundeinformasjon oppdateres hvert 3. år
  - **Middels risiko:** Kundeinformasjon oppdateres årlig
  - **Høy risiko:** Kundeinformasjon oppdateres hvert halvår
  - **Ved enhver transaksjon:** Kontroll av at kundeinformasjon er oppdatert
- 

# 6. Undersøkelsesplikt og rapportering — §26

## 6.1 Undersøkelsesplikt

Når det foreligger forhold som gir grunnlag for mistanke om at en transaksjon har tilknytning til hvitvasking eller terrorfinansiering, skal Selskapet:

1. **Gjennomføre nærmere undersøkelser** — innhente tilleggsinformasjon om kundens identitet, midlenes opprinnelse, transaksjonens formål
2. **Dokumentere undersøkelsen** — alle funn, vurderinger og konklusjoner nedtegnes
3. **Konkludere** — enten avkreftes mistanken (dokumenteres) eller bekreftes (rapportering)

## 6.2 Rapportering til Økokrim/EFE

Dersom undersøkelsen ikke avkrefter mistanken:

1. **Rapport sendes til EFE (Enheten for finansiell etterretning)** via Altinn-portalen
2. **Rapporten skal inneholde:**
  - Identifikasjon av kunden (navn, fødselsnummer, adresse)
  - Beskrivelse av transaksjonen(e)
  - Grunnlag for mistanken
  - Resultater av undersøkelsen
  - Relevant dokumentasjon
3. **Tidsfrist:** Uten ugrunnet opphold etter at undersøkelsen er fullført
4. **Konfidensialitet:** Kunden skal ikke underrettes om at rapport er sendt (tipping off-forbud, §28)
5. **Transaksjoner kan holdes tilbake** i inntil 2 virkedager etter rapportering, jf. betalingsystemloven

## 6.3 Statistikk og oppfølging

- Antall flaggede transaksjoner per måned
  - Antall undersøkelser gjennomført
  - Antall rapporter sendt til EFE
  - Rapporterer kvartalsvis til styret
- 

# 7. Oppbevaringsplikt — §30

## 7.1 Lagringstid

Alle opplysninger innhentet i forbindelse med kundetiltak og transaksjonsovervåking skal oppbevares i **minst 5 år** etter at kundeforholdet er avsluttet eller transaksjonen er gjennomført.

## 7.2 Hva oppbevares

Datatype	Lagringstid	Format
Kundidentifikasjon (KYC-data)	5 år etter avsluttet kundeforhold	Kryptert database
Kopi av legitimasjon/BankID-bekreftelse	5 år etter avsluttet kundeforhold	Kryptert lagring
Transaksjonsdata	5 år etter transaksjonsdato	Database med revisjonsspor
Korrespondanse med kunden	5 år etter avsluttet kundeforhold	Kryptert lagring
Risikovurderinger og EDD-dokumentasjon	5 år etter avsluttet kundeforhold	Kryptert lagring
Undersøkelser og rapporter til EFE	5 år etter avsluttet kundeforhold	Kryptert lagring
Opplæringslogg	5 år etter gjennomføring	Intern database

## 7.3 Datasikkerhet

- All KYC- og transaksjonsdata krypteres ved lagring (AES-256)
  - Tilgang logges og begrenses til autorisert personell
  - GDPR/personopplysningsloven overholdes — personopplysninger slettes etter utløp av lovpålagt oppbevaringstid
-

# 8. Korridorbasert risikovurdering

## 8.1 Tilnærming

Drop tilbyr pengeoverføringer til 30+ land. Risikoen varierer etter mottakerland/korridor. Selskapet benytter en risikobasert tilnærming der **alle kunder** vurderes etter samme rammeverk, uavhengig av etnisk bakgrunn eller statsborgerskap. Risikofaktoren er knyttet til **transaksjonskorridoren** (mottakerlandet), ikke kundens opprinnelse.

## 8.2 Korridor klassifisering

Risikonivå	Land/korridorer	Grunnlag
Lav	EU/EØS-land (PLN, EUR), Storbritannia	FATF-compliant, EU-regulerte
Middels	Serbia (RSD), Bosnia-Hercegovina (BAM), Tyrkia (TRY)	Ikke EU, men MONEYVAL/FATF-prosesser pågår
Høy	Pakistan (PKR)	FATF gråliste-historikk, høy korrupsjonsrisiko
Svært høy / sperret	Land på EUs høyrisikoliste eller FNs/EUs sanksjonslister	EU-forordning, FN-resolusjon

## 8.3 Tiltak per korridorrisiko

Korridorrisiko	CDD	Transaksjonsovervåking	Tilleggstiltak
Lav	Standard	Standard terskler	Ingen
Middels	Standard + ekstra spørsmål om formål	Lavere terskler (50% av standard)	Kvartalsvis profiloppdatering
Høy	EDD obligatorisk	Halverte terskler, manuell review >NOK 25 000	Dokumentasjon av midlers opprinnelse, månedlig oppdatering
Svært høy / sperret	Avvises	N/A	Korridor blokkert i systemet

# 9. Roller og ansvar

## 9.1 Hvitvaskingsansvarlig

Selskapet utpeker en hvitvaskingsansvarlig (AML Compliance Officer), jf. §8 fjerde ledd.

## Ansvar:

- Daglig oppfølging av hvitvaskingsrutinene
- Behandling av flaggede transaksjoner og EDD-saker
- Rapportering til EFE
- Årlig revisjon av risikovurdering og rutiner
- Opplæring av ansatte
- Rapportering til styret

## 9.2 Daglig leder

- Overordnet ansvar for etterlevelse av hvitvaskingsloven
- Godkjenner høyrisiko-kundeforhold
- Sikrer tilstrekkelige ressurser til compliance

## 9.3 Styret

- Godkjenner hvitvaskingsrutiner og risikovurdering
- Mottar kvartalsvis rapport fra hvitvaskingsansvarlig
- Beslutter risikoappetitt

## 9.4 Alle ansatte

- Plikter å følge disse rutinene
- Plikter å rapportere mistenkelige forhold til hvitvaskingsansvarlig
- Plikter å gjennomføre obligatorisk opplæring

---

# 10. Opplæring — §36

## 10.1 Obligatorisk opplæring

Alle ansatte med kundetilgangs- eller transaksjonsrelaterte oppgaver skal gjennomføre opplæring i:

- Hvitvaskingsloven og forskrifter — grunnleggende forståelse
- Selskapets hvitvaskingsrutiner
- Gjenkjenning av mistenkelige transaksjoner
- Rapporteringsprosedyrer
- PEP- og sanksjonsregler
- Roller og ansvar

## 10.2 Frekvens

- **Ved ansettelse:** Grunnkurs (innen 30 dager)
- **Årlig:** Oppdateringskurs med gjennomgang av endringer i lovverk og rutiner
- **Ved vesentlige endringer:** Ekstra opplæring ved nye produkter, korridorer eller regelverk

## 10.3 Dokumentasjon

- Opplæring registreres med dato, deltaker, innhold og beståttresultat
  - Opplæringslogg oppbevares i 5 år
- 

# 11. Internkontroll og revisjon — §37

## 11.1 Internkontroll

- Hvitvaskingsansvarlig utfører stikkprøvekontroller månedlig
- Minimum 10% av flaggede transaksjoner re-vurderes
- Kvaliteten på KYC-dokumentasjon kontrolleres kvartalsvis

## 11.2 Uavhengig gjennomgang

- Årlig uavhengig gjennomgang av hvitvaskingsrutinene
- Utføres av ekstern revisor eller compliance-rådgiver
- Funn rapporteres til styret med handlingsplan

## 11.3 Avviksbehandling

- Avvik fra rutinene dokumenteres umiddelbart
  - Korrigerende tiltak iverksettes innen 30 dager
  - Alvorlige avvik rapporteres til styret og eventuelt Finanstilsynet
- 

# 12. Behandling av avviste eller avsluttede kundeforhold

## 12.1 Avvisning

Dersom kundetiltak ikke kan gjennomføres tilfredsstillende, jf. §21:

- Kundeforholdet **skal ikke etableres**
- Eksisterende kundeforhold **skal avsluttes**
- Vurdering av om forholdet skal rapporteres til EFE

## 12.2 Avslutning av kundeforhold

- Kunden informeres om at kundeforholdet avsluttes (uten å oppgi HV/TF som grunn dersom rapport sendes)
  - Eventuelle midler tilbakeføres til kundens opprinnelige bankkonto
  - KYC-dokumentasjon oppbevares i 5 år etter avslutning
- 

# 13. Tekniske tiltak

## 13.1 Automatiserte kontroller i Drop-appen

- BankID-verifisering ved registrering (alderskontroll, identifikasjon)
- Automatisk PEP- og sanksjonsscreening ved onboarding og ved transaksjoner
- Regelbasert transaksjonsovervåking med konfigurbare terskler
- Automatisk blokkering av transaksjoner til sanksjonerte land/personer
- Logging av alle transaksjoner med fullstendig revisjonsspor

## 13.2 Manuelt dashboard

- Compliance-dashboard for hvitvaskingsansvarlig
  - Oversikt over flaggede transaksjoner, ventende EDD-saker, rapporterte saker
  - Søkefunksjon i transaksjonshistorikk
- 

# 14. Forholdet til personopplysningsloven (GDPR)

## 14.1 Behandlingsgrunnlag

- KYC-data behandles med hjemmel i **rettslig forpliktelse** (GDPR art. 6(1)(c)), jf. hvitvaskingsloven
- Oppbevaringstiden på 5 år har hjemmel i hvitvaskingsloven §30
- Etter utløp av oppbevaringstiden slettes personopplysningene

## 14.2 Personvernserklæring

- Kundene informeres om behandling av personopplysninger i forbindelse med hvitvaskingslovens krav
- Informasjon gis i personvernserklæring og ved registrering

## 15. Endringslogg

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

## 16. Vedlegg

- **Vedlegg A:** Risikovurdering — `risikovurdering-hvitvasking.md`
- **Vedlegg B:** Internkontrollrutiner — `internkontroll.md`
- **Vedlegg C:** EFE-rapporteringsskjema (Altinn-mal)
- **Vedlegg D:** Sjekkliste for kundetiltak
- **Vedlegg E:** Opplæringsplan

Dokumentet er utarbeidet i henhold til hvitvaskingsloven (LOV-2018-06-01-23) med tilhørende forskrift, Finanstilsynets veiledning om tiltak mot hvitvasking og terrorfinansiering, og FATFs anbefalinger.

# 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:

- Pengeoverføringer (remittance):** Grensekryssende overføringer fra Norge til 30+ land
- 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

Tjeneste	Beskrivelse	Volum (forventet år 1)
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
<b>Stråmenn (muldyr)</b> — kunder som utfører transaksjoner på vegne av andre	3 x 3 = 9 (Høy)	BankID-verifisering, transaksjonsovervåking, adferdsmønster-analyse	2 x 3 = 6 (Middels)
<b>Kunder med høyt transaksjonsvolum</b> — volumet overstiger oppgitt formål	2 x 3 = 6 (Middels)	Automatisk flagging ved avvik fra profil, EDD ved >200%	1 x 3 = 3 (Lav)
<b>PEP-kunder</b> — politisk eksponerte personer	1 x 4 = 4 (Middels)	Automatisk PEP-screening ved onboarding og løpende, EDD	1 x 3 = 3 (Lav)
<b>Kunder som sender til mange ulike mottakere</b> — indikasjon på pengeformidling	2 x 3 = 6 (Middels)	Maks antall mottakere per periode, manuell review	1 x 3 = 3 (Lav)
<b>Kunder som sender til høyrisikoland</b> — korridorbasert risiko	3 x 3 = 9 (Høy)	EDD for høyrisikokorridorer, lavere terskler, dokumentasjon av formål	2 x 2 = 4 (Middels)
<b>Nye kunder med umiddelbart høyt volum</b> — 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
<b>Kontantintensive virksomheter</b> — restauranter, kiosker, frisører	3 x 3 = 9 (Høy)	Verifisering av org.nr mot Brønnøysundregistrene, transaksjonsovervåking, EDD	2 x 2 = 4 (Middels)
<b>Nyetablerte foretak</b> — kort driftshistorikk	2 x 2 = 4 (Middels)	Utvidet KYC ved registrering, hyppigere oppfølging	1 x 2 = 2 (Lav)
<b>Uvanlig transaksjonsmønster</b> — 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	Varies, generelt høy	Nei	<b>Lav</b>	Standard CDD
NOK → PLN	Polen	Compliant	54	Nei	<b>Lav</b>	Standard CDD
NOK → GBP	Storbritannia	Compliant	71	Nei	<b>Lav</b>	Standard CDD
NOK → RSD	Serbia	Under evaluering (MONEYVAL)	36	Nei	<b>Middels</b>	Standard CDD + formålsdokumentasjon
NOK → BAM	Bosnia-Hercegovina	Under evaluering (MONEYVAL)	35	Nei	<b>Middels</b>	Standard CDD + formålsdokumentasjon

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

## 4.3 Geografisk risikovurdering — oppsummering

Risikonivå	Andel av forventet volum	Tiltak
Lav	~30%	Standard CDD, standard overvåking
Middels	~50%	CDD + ekstra formålsskontroll, 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
<b>Grensekryssende karakter</b> — midler forlater norsk jurisdiksjon	3 x 3 = 9 (Høy)	Korridorbasert risikotilnærming, BaaS-partner med egne kontroller	2 x 2 = 4 (Middels)
<b>Hastighet</b> — rask gjennomføring vanskeliggjør intervensjon	2 x 3 = 6 (Middels)	Pre-transaksjon sanksjonsscreening, automatisk hold ved flagging	1 x 3 = 3 (Lav)
<b>Tredjeparts mottaker</b> — 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
<b>Smurfing/splitting</b> — flere små transaksjoner for å unngå terskler	$3 \times 3 = 9$ (Høy)	Kumulativ overvåking (daglig, ukentlig, månedlig), mønstergjenkjenning	$2 \times 2 = 4$ (Middels)

## 5.2 QR-betalinger (innenlandske)

Risikofaktor	Iboende risiko	Mitigerende tiltak	Restrisiko
<b>Lavere iboende risiko</b> — innenlandsk, begge parter identifisert	$1 \times 2 = 2$ (Lav)	Standard CDD, transaksjonsovervåking	$1 \times 1 = 1$ (Lav)
<b>Fiktive transaksjoner</b> — oppkonstruerte transaksjoner mellom nærstående	$2 \times 2 = 4$ (Middels)	Overvåking av transaksjonsmønstre, kontroll av merchant-legitimitet	$1 \times 2 = 2$ (Lav)
<b>Refusjonssvindler</b> — systematisk misbruk av refusjoner	$1 \times 2 = 2$ (Lav)	Automatisk overvåking av refusjonsandel per merchant	$1 \times 1 = 1$ (Lav)

## 5.3 Samlet produktrisiko

Produkt	Iboende risikonivå	Etter tiltak
Remittance	<b>Høy</b>	<b>Middels</b>
QR-betaling	<b>Lav</b>	<b>Lav</b>

# 6. Kanal- og leveringsrisiko

## 6.1 Digital onboarding

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

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

# 8. Samlet risikovurdering — risikomatrixe

## 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
<b>Samlet virksomhetsrisiko</b>	<b>Høy</b>	<b>Middels</b>

## 8.2 Visualisering

RISIKOMATRISJE (Restrisiko etter tiltak)				
Konsekvens →	Lav(1)	Middels(2)	Høy(3)	Svært høy(4)
Svært høy(4)				
Høy(3)		GEOGRAFI		
		TERROR		
Middels(2)	KANAL	KUNDE		
	QR-prod	REMITTANCE		
Lav(1)				

## 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:

- BankID-verifisering** — sikrer høyt identitetsnivå for alle kunder
- Pass-through-modell** — Drop holder aldri kundemidler, noe som begrenser misbruksmuligheter
- Korridorbasert risikovurdering** — differensierte tiltak etter mottakerland
- 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.*

# Suitability Assessment

## Egnethetsvurdering — Fit & Proper

**Dokument:** Rutiner for egnethetsvurdering av styre, ledelse og nøkkelpersoner **Hjemmel:** Finansforetaksloven §§3-5 til 3-7 (LOV-2015-04-10-17) **Virksomhet:** ALAI Holding AS, org.nr 932 516 136 **Produkt:** Drop — betalingsformidling og pengeoverføringer **Versjon:** 1.0 **Dato:** 2026-02-12 **Godkjent av:** Styre **Neste revisjon:** 2027-02-12

### 1. Formål

Denne rutinen beskriver Selskapets prosess for vurdering av egnethet («fit & proper») for personer som innehar eller skal inntre i ledende stillinger, styreverv eller andre nøkkelroller i virksomheten. Egnethetsvurderingen sikrer at Selskapet oppfyller kravene i finansforetaksloven og Finanstilsynets retningslinjer.

### 2. Lovgrunnlag

#### 2.1 Relevante bestemmelser

Bestemmelse	Innhold
Finansforetaksloven §3-5	Krav til egnethet for styre og ledelse
Finansforetaksloven §3-6	Plikt til å melde fra om endringer
Finansforetaksloven §3-7	Finanstilsynets myndighet til å kreve fratredelse
Hvitvaskingsloven §8 fjerde ledd	Krav til hvitvaskingsansvarlig
EBA/ESMA Guidelines on suitability	Europeiske retningslinjer for egnethetsvurdering
Finanstilsynets rundskriv	Veiledning om egnethetsvurdering

#### 2.2 Hvem vurderes

Egnethetsvurdering skal gjennomføres for:

- Styremedlemmer (inkludert styreleder og varamedlemmer)
- Daglig leder
- Faktisk leder (dersom annen enn daglig leder)
- Hvitvaskingsansvarlig
- Leder for compliance-funksjon
- Leder for IT/teknologi
- Andre personer med vesentlig innflytelse på virksomheten
- Eiere med kvalifisert eierandel (10% eller mer)

## 3. Egnethetskrav

### 3.1 Hederlig vandel og god forretningsførsel

Krav	Dokumentasjon	Vurdering
Ingen straffedommer for relevante lovbrudd	Politiattest	Absolutt krav — brudd diskvalifiserer
Ingen konkurshistorikk (personlig)	Konkursregisteret	Vurderes individuelt
Ingen tilsynssanksjoner	Egenoppgave + bakgrunnsjekk	Vurderes individuelt
Ingen pågående etterforskning for økonomisk kriminalitet	Egenoppgave	Absolutt krav under etterforskning
God forretningsførsel i tidligere roller	Referanser	Vurderes helhetlig

### 3.2 Kompetanse og erfaring

#### 3.2.1 Styret samlet

Styret skal samlet besitte kompetanse innen:

- Finansiell virksomhet og betalingstjenester
- Risikostyring og internkontroll
- Regulatorisk kunnskap (finansregulering, AML)
- IT og cybersikkerhet
- Forretningsutvikling og strategi
- Regnskaps- og revisjonsforståelse

#### 3.2.2 Daglig leder

Kompetanseområde	Minimumskrav
------------------	--------------

Ledererfaring	Dokumentert ledererfaring fra relevant bransje
Finansiell forståelse	Kjennskap til regelverk for betalingsforetak
Operasjonell kompetanse	Erfaring med drift av digitale tjenester
Regulatorisk kunnskap	Grunnleggende forståelse av tilsynskrav

### 3.2.3 Hvitvaskingsansvarlig

Kompetanseområde	Minimumskrav
AML-kompetanse	Min. 3 års erfaring med AML/compliance
Sertifisering	CAMS eller tilsvarende (sterkt anbefalt)
Regelverkskunnskap	Inngående kjennskap til hvitvaskingsloven
Rapporteringskompetanse	Erfaring med EFE-rapportering

## 3.3 Kapasitet og tilgjengelighet

Krav	Beskrivelse
Tilstrekkelig tid	Personen må ha tilstrekkelig tid til å utføre vervet forsvarlig
Antall verv	Vurderes om antall øvrige verv/stillinger tillater tilstrekkelig engasjement
Tilgjengelighet	Må kunne delta på styremøter og være tilgjengelig ved behov

## 3.4 Uavhengighet og interessekonflikter

Krav	Vurdering
Ingen vesentlige interessekonflikter	Egenoppgave av alle verv, eierinteresser, nærståendes interesser
Uavhengighet fra kontrollerte enheter	Styremedlemmer bør ha tilstrekkelig uavhengighet
Konkurrerende virksomhet	Verv/interesser i konkurrerende foretak vurderes
Nærstående	Familiære og forretningsmessige forbindelser vurderes

## 4. Prosess for egnethetsvurdering

### 4.1 Ved nyansettelse / nytt verv

**STEG 1: KANDIDAT**

Identifisert av  
styre/valgkomité

**STEG 2: DOKUMENTASJON**

Kandidaten fremlegger:

- CV
- Egenoppgave (vedlegg A)
- Politiattest
- Referanser

**STEG 3: VURDERING**

Compliance gjennomfører:

- Bakgrunnsjekk
- PEP/sanksjonsscreening
- Referansesjekk
- Kompetansevurdering
- Interessekonfliktvurdering

**STEG 4: BESLUTNING**

Styret beslutter:

- Godkjent
- Betinget godkjent
- Avvist

**STEG 5: MELDING**

Melding til Finanstilsynet  
innen 1 mnd (nye nøkkelpersoner)

**STEG 6: OPPFØLGING**

Årlig fornyet vurdering

## 4.2 Ved tiltredelse — sjekkliste

Nr	Kontrollpunkt	Dokumentasjon	Bekreftet
1	Fullstendig CV mottatt	CV på fil	<input type="checkbox"/>
2	Egenoppgave utfylt (vedlegg A)	Signert skjema	<input type="checkbox"/>
3	Politiattest innhentet (ikke eldre enn 3 mnd)	Attest	<input type="checkbox"/>
4	Konkursregistersjekk gjennomført	Utskrift	<input type="checkbox"/>
5	PEP/sanksjonsscreening gjennomført	Screeningresultat	<input type="checkbox"/>
6	Referansesjekk gjennomført (min. 2 referanser)	Notat	<input type="checkbox"/>
7	Interessekonfliktanalyse gjennomført	Notat	<input type="checkbox"/>
8	Kompetansevurdering mot krav	Notat	<input type="checkbox"/>
9	Samlet egnethetsvurdering dokumentert	Rapport	<input type="checkbox"/>

Nr	Kontrollpunkt	Dokumentasjon	Bekreftet
10	Styrevedtak om godkjenning	Protokoll	<input type="checkbox"/>
11	Melding til Finanstilsynet sendt	Kvittering	<input type="checkbox"/>

## 4.3 Løpende egnethetsvurdering

Aktivitet	Frekvens	Ansvarlig
Fornytt PEP/sanksjonsscreening	Årlig	Compliance
Oppdatering av interessekonfliktvurdering	Årlig	Compliance
Gjennomgang av vervliste og kapasitet	Årlig	Styreleder
Sjekk mot konkursregister	Årlig	Compliance
Samlet fornytt egnethetsvurdering	Årlig	Compliance → Styre

## 4.4 Ved endrede forhold

Nøkkelpersoner plikter å melde fra om endringer som kan påvirke egnethetsvurderingen, herunder:

- Nye straffedommer eller igangsatt etterforskning
- Konkurs eller gjeldsforhandlinger
- Nye verv eller eierinteresser som kan medføre interessekonflikt
- Endringer i tilgjengelighet/kapasitet
- Tilsynssanksjoner i andre foretak

# 5. Styrets samlede kompetanse

## 5.1 Kompetansematrise

Kompetanseområde	Styreled.	Medlem 1	Medlem 2	Samlet
Finansiell virksomhet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Minimum 1
Betalingstjenester / fintech	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Minimum 1

Kompetanseområde	Styreled.	Medlem 1	Medlem 2	Samlet
Risikostyring / compliance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Minimum 1
IT / cybersikkerhet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Minimum 1
Regnskap / revisjon	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Minimum 1
Forretningsutvikling	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Minimum 1
Juridisk kompetanse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Ønskelig

## 5.2 Mangfold

Styret skal tilstrebe mangfold med hensyn til:

- Kjønn
- Alder
- Faglig bakgrunn
- Yrkeserfaring
- Geografisk tilknytning

## 6. Eiere med kvalifisert eierandel

### 6.1 Krav

Eiere med kvalifisert eierandel (10% eller mer) skal egnethetsvurderes, jf. finansforetaksloven §6-3.

### 6.2 Vurderingskriterier for eiere

Krav	Dokumentasjon
Hederligandel	Politiattest
Finansiell soliditet	Revisorbekreftet kapital / årsregnskap
Ingen tilknytning til kriminell virksomhet	Egenoppgave + bakgrunnssjekk
Midlenes opprinnelse	Dokumentasjon av investeringsmidler
Ikke sanksjonert	Sanksjonsscreening

### 6.3 Meldeplikt

Erverv av kvalifisert eierandel skal meldes til Finanstilsynet **før** gjennomføring, jf. finansforetaksloven §6-1.

---

## 7. Dokumentasjon og oppbevaring

### 7.1 Dokumentasjonskrav

For hver person som underlegges egnethetsvurdering skal følgende oppbevares:

- Utfylt egenoppgave (vedlegg A)
- CV
- Politiattest
- Resultat av PEP/sanksjonsscreening
- Referansenotater
- Kompetansevurdering
- Interessekonfliktvurdering
- Samlet egnethetsvurdering med konklusjon
- Styrevedtak

### 7.2 Oppbevaringstid

- Dokumentasjon oppbevares i hele perioden personen innehar vervet/stillingen
  - Etter fratreden: oppbevares i 5 år
  - Avviste kandidater: dokumentasjon oppbevares i 3 år
- 

## 8. Vedlegg A — Egenoppgave for egnethetsvurdering

### Skjema: Egenoppgave

#### Del 1 — Personopplysninger

Felt	Verdi
Fullt navn	
Fødselsdato	

Felt	Verdi
Fødselsnummer	
Adresse	
Telefon	
E-post	
Stilling/verv det søkes om	

## Del 2 – Utdanning og yrkeserfaring

Periode	Institusjon/Arbeidsgiver	Utdanning/Stilling	Beskrivelse

## Del 3 – Øvrige verv og engasjementer

Virksomhet	Org.nr	Verv/Rolle	Eierandel	Siden

## Del 4 – Erklæringer

Undertegnede bekrefter at:

Nr	Erklæring	Ja	Nei
1	Jeg har ikke vært straffet for forbrytelse eller forseelse	<input type="checkbox"/>	<input type="checkbox"/>
2	Jeg er ikke under etterforskning for økonomisk kriminalitet	<input type="checkbox"/>	<input type="checkbox"/>
3	Jeg har ikke vært gjenstand for konkurs eller gjeldsforhandling	<input type="checkbox"/>	<input type="checkbox"/>
4	Jeg har ikke vært gjenstand for tilsynssanksjoner	<input type="checkbox"/>	<input type="checkbox"/>
5	Jeg har ikke blitt nektet konsesjon/registrering hos finanstilsyn	<input type="checkbox"/>	<input type="checkbox"/>
6	Jeg har ikke blitt fjernet fra styre/ledelse av tilsynsmyndighet	<input type="checkbox"/>	<input type="checkbox"/>
7	Jeg har ingen interessekonflikter knyttet til stillingen/vervet	<input type="checkbox"/>	<input type="checkbox"/>

Nr	Erklæring	Ja	Nei
8	Jeg har tilstrekkelig tid og kapasitet til å utføre vervet	<input type="checkbox"/>	<input type="checkbox"/>

Dersom «Nei» er avkrysset på noen av punktene, gi utfyllende forklaring:

---



---



---

## Del 5 — Samtykke

Undertegnede samtykker til at ALAI Holding AS kan:

- Innhente politiattest
- Gjennomføre PEP- og sanksjonsscreening
- Kontakte oppgitte referanser
- Foreta bakgrunnssjekk i relevante registre

### Underskrift:

Sted: \_\_\_\_\_ Dato: \_\_\_\_\_

Signatur: \_\_\_\_\_

Navn i blokkbokstaver: \_\_\_\_\_

# 9. Vedlegg B — Mal for samlet egnethetsvurdering

Kandidat: [Navn]

Stilling/verv: [Rolle]

Dato for vurdering: [Dato]

Vurderingskriterie	Vurdering	Kommentar
Hederligandel	Godkjent / Ikke godkjent	
Relevant kompetanse	Tilstrekkelig / Utilstrekkelig	

Vurderingskriterie	Vurdering	Kommentar
Yrkeserfaring	Tilstrekkelig / Utilstrekkelig	
Kapasitet og tilgjengelighet	Tilstrekkelig / Utilstrekkelig	
Interessekonflikter	Ingen / Håndterbare / Diskvalifiserende	
PEP/sanksjons-screening	Ingen treff / Treff (beskriv)	
Referanser	Positive / Nøytrale / Negative	

**Samlet vurdering:** Godkjent / Betinget godkjent / Ikke godkjent

**Begrunnelse:**

---

**Vurdert av:** \_\_\_\_\_ **Dato:** \_\_\_\_\_

**Styrevedtak (ref.):** \_\_\_\_\_

---

## 10. Endringslogg

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

---

*Dokumentet er utarbeidet i henhold til finansforetaksloven §§3-5 til 3-7, EBA/ESMA-retningslinjer for egnethetsvurdering, og Finanstilsynets veiledning.*