# Internal Controls

# Internkontrollrutiner — Drop (ALAI Holding AS)

**Dokument:** Rammeverk for internkontroll **Hjemmel:** Finansforetaksloven §13-5, hvitvaskingsloven §§7-8 og §37, internkontrollforskriften **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

Internkontrollrutinene skal sikre at ALAI Holding AS gjennom produktet Drop:

- Overholder gjeldende lovverk, herunder finansforetaksloven, hvitvaskingsloven og personopplysningsloven
- Har effektiv risikostyring og kontroll med virksomheten
- Har klare ansvarslinjer og rapporteringsveier
- Identifiserer, vurderer og håndterer operasjonelle risikoer
- Har en kultur for etterlevelse (compliance)

---

# 2. Tre forsvarslinjer

Selskapet organiserer sin internkontroll etter prinsippet om tre forsvarslinjer, jf. Finanstilsynets veiledning og internasjonale standarder (COSO/IIA):

## 2.1 Første forsvarslinje — Operativ drift

**Hvem:** Alle ansatte i operative roller (utvikling, drift, kundeservice)

**Ansvar:**

- Daglig etterlevelse av rutiner og policyer

- Identifisere og rapportere avvik til nærmeste leder
- Gjennomføre kontroller integrert i arbeidsprosesser
- Dokumentere egne kontrollhandlinger

**Kontrollaktiviteter:**

| Kontroll | Frekvens | Ansvarlig |
|---|---|---|
| KYC-kvalitetskontroll ved onboarding | Hver kunde | Operativ medarbeider |
| Verifikasjon av transaksjonsdata | Fortløpende | System (automatisk) |
| Rapportering av hendelser og avvik | Ved forekomst | Alle ansatte |
| Oppfølging av automatiske varsler | Fortløpende | Operativ medarbeider |

# 2.2 Andre forsvarslinje — Risikostyring og Compliance

**Hvem:** Hvitvaskingsansvarlig / Compliance-funksjon

**Ansvar:**

- Overvåke og teste etterlevelse av lover, forskrifter og interne rutiner
- Utarbeide og vedlikeholde policyer og rutiner
- Gjennomføre risikiovurderinger
- Rådgi første forsvarslinje
- Rapportere til daglig leder og styret
- Håndtere forholdet til tilsynsmyndigheter

**Kontrollaktiviteter:**

| Kontroll | Frekvens | Ansvarlig |
|---|---|---|
| Stikkprøvekontroll av KYC-dokumentasjon | Månedlig (min. 10% av nye kunder) | Hvitvaskingsansvarlig |
| Gjennomgang av flaggede transaksjoner | Ukentlig | Hvitvaskingsansvarlig |
| Testing av transaksjonsovervåkingsregler | Kvartalsvis | Compliance |
| Oppdatering av risikovurdering | Årlig + ved vesentlige endringer | Hvitvaskingsansvarlig |
| Regelverksovervåking | Løpende | Compliance |
| Compliance-rapport til styret | Kvartalsvis | Hvitvaskingsansvarlig |

# 2.3 Tredje forsvarslinje — Uavhengig kontroll

**Hvem:** Ekstern revisor / Uavhengig internrevisor

**Ansvar:**

- Uavhengig vurdering av internkontrollens effektivitet
- Vurdering av risikostyringsrammeverket
- Rapportering til styret

**Kontrollaktiviteter:**

| Kontroll | Frekvens | Ansvarlig |
|---|---|---|
| Ekstern revisjon av AML-program | Årlig | Ekstern revisor |
| Revisjon av IT-sikkerhet | Årlig | Ekstern IT-revisor |
| Uavhengig gjennomgang av internkontroll | Årlig | Ekstern revisor |
| Rapportering av funn og anbefalinger | Etter hver revisjon | Ekstern revisor |

---

# 3. Governance og organisering

## 3.1 Styret

**Ansvar:**

- Fastsette overordnet strategi for risikostyring og internkontroll
- Godkjenne policyer, rutiner og risikoappetitt
- Motta og behandle kvartalsrapporter fra compliance og revisor
- Sikre tilstrekkelige ressurser til internkontroll
- Overordnet ansvar for etterlevelse

**Styreaktiviteter:**

| Aktivitet | Frekvens |
|---|---|
| Behandle compliance-rapport | Kvartalsvis |
| Godkjenne oppdatert risikovurdering | Årlig |
| Godkjenne oppdaterte hvitvaskingsrutiner | Årlig |
| Behandle revisjonsrapporter | Etter mottakelse |
| Evaluere internkontrollens effektivitet | Årlig |

# 3.2 Daglig leder

**Ansvar:**

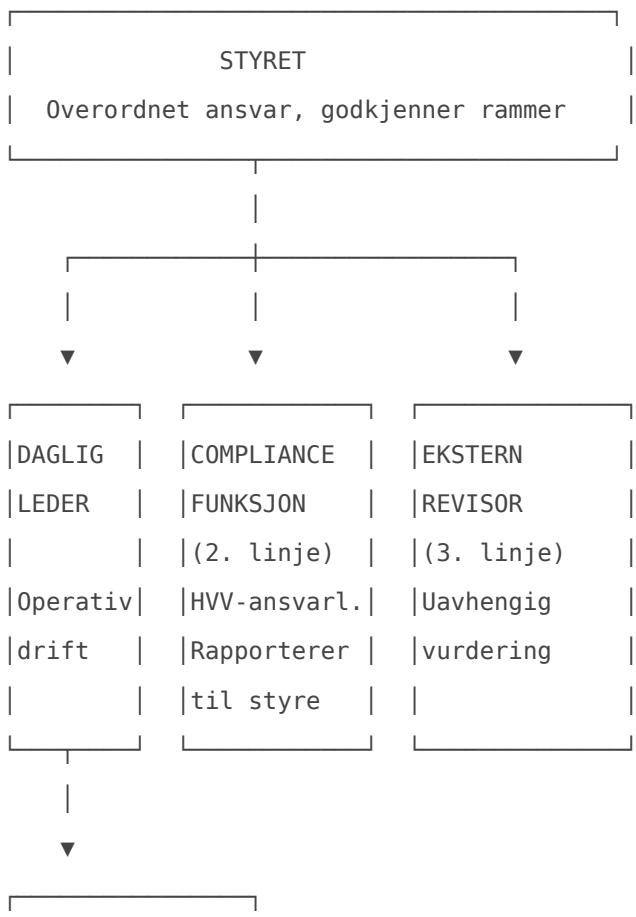
- Operativt ansvar for implementering av styrets vedtak
- Sikre at organisasjonen har nødvendig kompetanse og ressurser
- Godkjenne høyrisiko-kundeforhold (etter anbefaling fra compliance)
- Rapportere til styret om vesentlige risikoforhold

# 3.3 Hvitvaskingsansvarlig / Chief Compliance Officer

**Ansvar:**

- Daglig leder for compliance-funksjonen
- Hvitvaskingsansvarlig etter hvitvaskingsloven §8 fjerde ledd
- Rapporterer direkte til daglig leder og styret (uavhengig av operative linjer)
- Har myndighet til å stoppe transaksjoner og avvise kundeforhold

# 3.4 Organisasjonskart — internkontroll



```
│OPERATIVE       │
│MEDARBEIDERE    │
│(1. linje)      │
│Tech, support,  │
│kundeservice    │
└────────────────┘
```

---

# 4. Risikostyring

## 4.1 Risikorammeverk

Selskapet identifiserer og vurderer følgende risikokategorier:

| Risikokategori | Beskrivelse | Eier |
|---|---|---|
| HV/TF-risiko | Risiko for misbruk til hvitvasking/terrorfinansiering | Hvitvaskingsansvarlig |
| Operasjonell risiko | Systemfeil, menneskelige feil, prosesssvikt | Daglig leder |
| IT- og cyberrisiko | Datainnbrudd, tjenestenekt, systemsårbarhet | Tech Lead |
| Compliance-risiko | Brudd på regelverk, tilsynssanksjoner | Compliance |
| Omdømmerisiko | Hendelser som skader selskapets omdømme | Daglig leder |
| Strategisk risiko | Feil forretningsbeslutninger | Styret |

## 4.2 Risikovurderingsprosess

1. **Identifisering:** Kartlegge relevante risikoer per kategori
2. **Vurdering:** Sannsynlighet x konsekvens (skala 1-4)
3. **Tiltak:** Definere risikoreduserende tiltak
4. **Overvåking:** Løpende overvåking av risikoindikatorer
5. **Rapportering:** Kvartalsvise risikorapporter til styret
6. **Revisjon:** Årlig oppdatering av risikovurderingen

## 4.3 Risikoindikatorer (KRI)

| Indikator | Terskel (gul) | Terskel (rød) | Frekvens |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Antall flaggede transaksjoner | >50/mnd | >100/mnd | Månedlig |
| Gjennomsnittlig behandlingstid flagg | >48 timer | >72 timer | Ukentlig |
| Andel EDD-kunder | >10% av kundebasen | >20% | Kvartalsvis |
| Antall EFE-rapporter | >2/kvartal | >5/kvartal | Kvartalsvis |
| KYC-mangler ved stikkprøve | >5% | >10% | Månedlig |
| Systemnedetid | >99.5% oppetid | <99% oppetid | Daglig |
| Antall sikkerhetshendelsar | >1/mnd | >3/mnd | Månedlig |

---

# 5. Compliance-overvåking

## 5.1 Overvåkingsplan

| Område | Kontrollhandling | Frekvens | Ansvarlig | Rapporteres til |
|---|---|---|---|---|
| KYC/CDD | Stikkprøve av onboarding-kvalitet | Månedlig | Compliance | Daglig leder |
| Transaksjonovervåking | Review av regler og terskler | Kvartalsvis | Compliance | Styret |
| PEP/sanksjoner | Test av screeningeffektivitet | Halvårlig | Compliance | Styret |
| Opplæring | Kontroll av gjennomføring | Årlig | Compliance | Daglig leder |
| Rutiner | Gjennomgang og oppdatering | Årlig | Compliance | Styret |
| Regelverksendringer | Overvåking av nye krav | Løpende | Compliance | Daglig leder |
| Hendelseslog | Gjennomgang av logger | Ukentlig | Compliance | Daglig leder |
| IT-sikkerhet | Penetrasjonstesting | Årlig | Ekstern | Styret |
| Personvern | DPIA-oppdatering | Årlig | Compliance | Daglig leder |

## 5.2 Rapporteringskalender

| Rapport | Mottaker | Frekvens | Innhold |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Compliance-statusrapport | Styret | Kvartalsvis | HV/TF-statistikk, avvik, tiltak, regelverksendringer |
| Risikorapport | Styret | Kvartalsvis | KRI-status, risikoendringer, handlingsplan |
| AML-årsrapport | Styret | Årlig | Full gjennomgang av AML-programmet |
| Hendelsesrapport | Daglig leder | Ved hendelse | Beskrivelse, tiltak, læringspunkter |
| Revisjonsrapport | Styret | Årlig | Ekstern revisors funn og anbefalinger |

---

# 6. Avviksbehandling

## 6.1 Definisjon

Et avvik er ethvert brudd på, eller manglende etterlevelse av:

- Lover og forskrifter
- Interne rutiner og policyer
- Styrets vedtak og retningslinjer
- Tilsynsmyndighetenes pålegg

## 6.2 Avviksprosess

```
1. IDENTIFISERING          2. REGISTRERING          3. VURDERING
   Alle ansatte →             Avvikslogg →             Compliance →
   rapporterer                dokumenteres             alvorlighetsgrad

4. TILTAK                  5. OPPFØLGING            6. RAPPORTERING
   Korrigerende →             Verifisere →             Til styre/
   tiltak defineres           effekt                   tilsynsmyndighet
```

## 6.3 Alvorlighetsgrader

| Grad | Beskrivelse | Responstid | Rapporteres til |
|---|---|---|---|
| Kritisk | Lovbrudd, tilsynssanksjon, stor kundeeksponering | Umiddelbart | Styre, Finanstilsynet |

| Grad | Beskrivelse | Responstid | Rapporteres til |
|---|---|---|---|
| Høy | Vesentlig rutinebrudd, gjentatte avvik | 24 timer | Daglig leder, styre |
| Middels | Enkeltavvik fra rutiner, forbedringspotensial | 1 uke | Daglig leder |
| Lav | Mindre prosessavvik, ingen kundekonsekvens | 30 dager | Compliance-logg |

## 6.4 Avvikslogg

Alle avvik registreres i avviksloggen med:

- Dato og tidspunkt
- Beskrivelse av avviket
- Hvem som oppdaget det
- Alvorlighetsgrad
- Korrigerende tiltak
- Ansvarlig for oppfølging
- Frist for lukking
- Status (åpent/lukket)
- Læringspunkter

---

# 7. Eskalering

## 7.1 Eskaleringsprosedyre

| Situasjon | Eskaleres til | Tidsfrist |
|---|---|---|
| Mistenkelig transaksjon (flagget av system) | Hvitvaskingsansvarlig | 24 timer |
| Bekreftet mistanke om HV/TF | EFE/Økokrim + daglig leder | Uten ugrunnet opphold |
| Sanksjonstreff (bekreftet) | Daglig leder + UD | Umiddelbart |
| Kritisk avvik | Styre + eventuelt Finanstilsynet | Umiddelbart |
| Sikkerhetshendeelse (datainnbrudd) | Daglig leder + Datatilsynet (72t) | Umiddelbart |
| Tilsynsforespørsel | Daglig leder + compliance | Innen tilsynets frist |
| Kundeklage (compliance-relatert) | Compliance | 5 virkedager |

## 7.2 Varsling (Whistleblowing)

Jf. arbeidsmiljøloven kapittel 2A:

- Alle ansatte har rett til å varsle om kritikkverdige forhold
- Varslingskanal er etablert (direkte til styreleder)
- Varsler beskyttes mot gjengjeldelse
- Alle varsler behandles konfidensielt og dokumenteres

---

# 8. IT-kontroller

## 8.1 Tilgangsstyring

| Prinsipp | Implementering |
|---|---|
| Minste privilegium | Brukere får kun tilgang til det de trenger |
| Rollebasert tilgang (RBAC) | Tilgang basert på rolle, ikke person |
| Separation of duties | Kritiske funksjoner krever to personers godkjenning |
| Periodisk tilgangsgjennomgang | Kvartalsvis gjennomgang av alle tilganger |
| Logging | Alle tilgangsendringer og datautrekk logges |

## 8.2 Systemovervåking

| Kontroll | Beskrivelse | Frekvens |
|---|---|---|
| Oppetidsovervåking | Automatisk varsling ved nedetid | Kontinuerlig |
| Ytelsesovervåking | Responstider og feilrater | Kontinuerlig |
| Sikkerhetslogg-gjennomgang | Analyse av innloggingsforsøk og anomalier | Daglig |
| Sårbarhetsskanning | Automatisk skanning av kjente sårbarheter | Ukentlig |
| Penetrasjonstesting | Ekstern testing av sikkerhet | Årlig |
| Backup-verifisering | Test av gjenoppretting fra backup | Månedlig |

## 8.3 Endringsstyring

Alle endringer i produksjonssystemer skal:

1. Dokumenteres med beskrivelse og begrunnelse
2. Testes i staging-miljø

3. Godkjennes av tech lead og compliance (ved regelverksrelevante endringer)
4. Rulles ut med rollback-plan
5. Overvåkes etter utrulling

---

# 9. Opplæring og kompetanse

## 9.1 Opplæringsprogram

| Kurs | Målgruppe | Frekvens | Innhold |
|---|---|---|---|
| Grunnkurs HV/TF | Alle ansatte | Ved ansettelse + årlig | Lovverk, rutiner, gjenkjennelse |
| Avansert AML | Compliance, operativ | Årlig | Typologier, caseøvelser, EDD |
| PEP og sanksjoner | Compliance, operativ | Årlig | PEP-definisjoner, screeningprosess |
| IT-sikkerhet | Alle ansatte | Årlig | Phishing, passord, hendelsesrapportering |
| GDPR | Alle ansatte | Ved ansettelse + årlig | Personvern, behandlingsgrunnlag |
| Etikk og varsling | Alle ansatte | Årlig | Etiske retningslinjer, varslingskanal |

## 9.2 Kompetansekrav

| Rolle | Minimumskompetanse |
|---|---|
| Hvitvaskingsansvarlig | Sertifisering (f.eks. CAMS), min. 3 års erfaring |
| Compliance-medarbeider | Relevant utdanning, opplæring i HV/TF |
| Daglig leder | Egnethetsvurdering, grunnleggende HV/TF-forståelse |
| Styremedlemmer | Egnethetsvurdering, forstå regulatorisk rammeverk |
| Tech Lead | IT-sikkerhetskompetanse, forståelse av compliance-krav |

---

# 10. Beredskapsplan

## 10.1 Scenarioer

| Scenario | Alvorlighet | Umiddelbare tiltak |
|---|---|---|
| Datainnbrudd / personopplysninger kompromittert | Kritisk | Isolere system, varsle Datatilsynet (72t), varsle berørte kunder |
| Sanksjonert transaksjon gjennomført ved feil | Kritisk | Fryse midler, varsle UD, rapportere til EFE |
| Systemnedetid > 4 timer | Høy | Aktivere failover, informere kunder, loggføre |
| Tjenestenektangrep (DDoS) | Høy | Aktivere DDoS-beskyttelse, eskalere til hosting-partner |
| Mistanke om intern svindel | Kritisk | Fryse tilganger, undersøke, varsle styre og evt. politi |

## 10.2 Kommunikasjonsplan ved hendelse

| Interessent | Tidsfrist | Kanal | Ansvarlig |
|---|---|---|---|
| Finanstilsynet | Uten ugrunnet opphold | Altinn / epost | Daglig leder |
| Datatilsynet | 72 timer (datainnbrudd) | Altinn | Daglig leder |
| Berørte kunder | Uten ugrunnet opphold | App + epost | Kundeservice |
| Styret | Umiddelbart | Epost + telefon | Daglig leder |
| Ansatte | Umiddelbart | Intern kanal | Daglig leder |

---

# 11. Endringslogg

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

---

*Dokumentet er utarbeidet i henhold til finansforetaksloven §13-5, hvitvaskingsloven §§7-8 og §37, og Finanstilsynets veiledninger om internkontroll i betalingsforetak.*

---

Revision #5
Created 2026-02-18 08:44:40 UTC by John
Updated 2026-05-25 07:24:33 UTC by John