



# 仁港永胜

协助申请金融牌照及银行开户一站式服务



正直诚信  
恪守信用

地址：深圳市福田区福华三路卓越世纪中心1号楼1106  
网址：[www.CNJRP.com](http://www.CNJRP.com) 手机：15920002080

## 挪威电子货币机构（EMI）牌照申请注册常见问题（FAQ 大全）

Frequently Asked Questions (FAQ) about Registering an Electronic Money Institution in Norway

本文内容由仁港永胜（香港）有限公司拟定，并由唐生提供专业讲解，旨在为拟在挪威申请 EMI 牌照的跨境支付 / 钱包 / 金融科技机构，提供一份可直接用于内部立项与对接监管的实操级指南。

说明：本 FAQ 更偏“给股东 / 管理层 / 合规负责人看的实战问答”，也兼顾监管书面回复和面谈场景，可直接抽取片段用于回复 Finanstilsynet 的 RFI (Request for Information)。

### 第一部分 | 基础认知篇（概念 & 定位）

#### Q1：挪威 EMI 与欧盟国家 EMI 在法律效力上有什么区别？

A:

从监管框架和护照功能角度看，**挪威 EMI 与欧盟 EMI 基本等效**——

- 挪威是 EEA 成员国，已把 **EMD2 / PSD2 / AMLD 系列** 等效纳入本国法；
- 挪威 EMI 获批后，可通过护照机制在 EU+EEA 内开展电子货币及支付服务；
- 对银行、卡组织、合作机构而言，**挪威 EMI ≈ 欧盟成员国 EMI**，在合规层级上是被等同对待的。

差异在于：

- 监管机构是 **挪威 Finanstilsynet (FI)**，而非欧盟成员国的中央银行或金融监管局；
- 某些本地化要求（比如语言、本地董事、本地办公室）会体现挪威的监管特色。

#### Q2：挪威 EMI 与挪威支付机构（Payment Institution, PI）有什么区别？

A:

比较维度	EMI (Electronic Money Institution)	PI (Payment Institution)
核心功能	发行电子货币 (e-money)，存储价值	提供支付服务，但不发行电子货币
客户资金处理	必须遵守 e-money 发行与赎回规则	仅处理支付流水，不形成“存款式余额”
商业模式	可做钱包、预付卡、账户余额、虚拟 IBAN 等	更偏汇款/支付通道/收单等
监管要求	资本要求更高，审查更严	相对较低一些
护照使用	同样可以护照，但 EMI 对 B2B 合作更有吸引力	适合轻量化支付业务

如果你的业务需要：

- 提供“账户余额”，
- 做类似“钱包+卡+多币种账户”模式，  
那么应该考虑 **EMI 而非 PI**。

#### Q3：挪威 EMI 是否只能做本地业务？可以面向全球客户吗？

A:

- 在许可范围内，挪威 EMI 可以服务 **全球客户**，但必须遵守：
  - 挪威 AML/CFT 法规；
  - 欧盟 / EEA 的制裁与 KYC 要求；
  - 客户所在国的金融/外汇、制裁规则（尤其高风险国家）。
- 对于高制裁或高风险国家，监管会特别关注：
  - 是否禁止或限制开户；
  - 是否有详细的高风险客户增强尽调 (EDD) 制度。

#### **Q4：挪威是否适合作为亚洲项目进入欧洲的第一块牌照？**

A:

适合，但前提是：

- 你接受北欧监管的高标准；
- 你愿意投入足够的合规与管理资源，而不是“拿牌不运营”。

对于中大型跨境支付、B2B 结算、金融科技项目，挪威 EMI 是非常好的“**北欧门面 + 欧洲桥头堡**”。

---

## **第二部分 | 申请条件篇（股东 / 董事 / 管理层）**

#### **Q5：股东需要满足什么条件？是否可以是中国或香港公司 / 个人？**

A:

可以，但须满足：

1. **清晰、可验证的资金来源** (Source of Funds / Source of Wealth)；
2. 无严重负面记录：
  - 无金融犯罪、洗钱、恐怖融资相关记录；
  - 无重大税务欺诈、监管重罚历史；
3. 能提供**合理的财富累积路径说明**，包括：
  - 经营企业所得；
  - 投资、股权退出；
  - 明确的纳税记录等。

挪威 FI 不禁止来自中国/香港/其他地区的股东，但对高风险司法辖区资金的透明度要求更高。

---

#### **Q6：董事必须是挪威居民吗？可以用“挂名董事”吗？**

A:

- 至少要有**本地董事**或对挪威法规非常熟悉、能参与实际管理的董事。
- FI 非常不喜欢“挂名董事”。在面谈与问答中，若发现董事对业务一无所知，审批会被拖延甚至拒绝。

建议结构：

- 1-2 名具有支付/金融背景的非本地董事（可来自香港/欧盟其他国家）；
- 1 名挪威或北欧本地董事，负责对接当地监管文化与法律。

#### **Q7：MLRO（反洗钱负责人）可以外包吗？**

A:

- 职责**不能完全外包**，可以委托外部顾问支持，但公司内部必须有被正式任命的 **MLRO**。
- 该 MLRO 必须：
  - 直接向董事会汇报；
  - 有足够资历与独立性，可对业务进行制衡；
  - 有权阻止或拒绝高风险交易与客户。

#### **Q8：如果股东和董事以前没有做过 EMI/PI 项目，会不会影响获批？**

A:

会增加难度，但**不是绝对障碍**。

思路是：

- 提升“管理层与中层”配置质量：
  - 聘请拥有支付/银行背景的 CEO/COO/Head of Compliance；
  - 借助外部专业顾问（如仁港永胜）设计严谨的业务与合规框架；
- 在商业计划书中充分展示：
  - 风险意识、合规文化、长线投入。

监管更看重的是：

“公司整体是否有能力识别与管理风险”，而不仅仅是股东过去是不是 EMI 老兵。

---

### 第三部分 | 资本 / 结构 / 成本篇

#### Q9：挪威 EMI 最低资本要求是多少？必须一次性到位吗？

A:

- 最低资本通常为 **350,000 欧元**（欧盟 EMI 一般标准）；
- 实务上，FI 还会看：
  - 未来 3-5 年业务计划是否需要更高资本；
  - 资本是否能覆盖应急亏损。

监管期望：

资本金需在正式获批前实缴到位，并存放于挪威银行/指定机构作为初始自有资金。

---

#### Q10：资本金可以从中国或香港直接汇出吗？是否涉及外汇管制？

A:

挪威方面原则上接受合法、可追溯的境外资金汇入；

但投资方所在国需考虑：

- 中国内地公司 / 个人：
  - 需完成 ODI / 对外投资备案、外汇审批；
  - 建议在中国聘请本地律所/会计师就资金出境合规做规划。
- 香港实体较为灵活，但也需提供完整资金来源证明。

仁港永胜可以协助你：

- 一并规划 **ODI + 挪威 EMI 投资结构**，避免后期监管问询时出现资金路径不清的问题。
- 

#### Q11：除了资本金外，额外预算大概需要多少？

A:

视项目规模而定，不同项目区间可能是：

- 合规顾问 + 法律 + 审计 + 本地团队前两年成本：
  - 保守估算：**€200,000 – €400,000**；
  - 若计划做卡组织接入/多币种清算，技术 & 合规成本会更高。

重点在于：

挪威 EMI 不是“低成本拿牌”，而是“长期运营 + 品牌 + 北欧背书”的战略选择。

---

### 第四部分 | 合规 / 反洗钱 / 风险管理篇

#### Q12：挪威对 AML/KYC 的要求重点在哪里？

A:

主要包括：

1. **风险为本 (Risk-based Approach, RBA)** —— 所有客户分类、交易监控都必须体现“风险权重”；
  2. **高风险客户增强尽调 (EDD)** —— 涉及：
    - 高风险国家
    - PEP (政治公众人物)
    - 复杂结构公司
    - 大额频繁跨境交易
  3. **制裁名单与不良媒体筛查 (Sanctions & Adverse Media)**；
  4. **STR (可疑交易报告) 机制** —— 需有内部流程 + 向 FI 通报机制；
  5. **培训与记录** —— 员工 AML 培训、考核记录、内部审计。
-

#### **Q13：挪威是否接受使用第三方 KYC 服务商？**

A:

可以，但须满足：

- 第三方必须是规范、合规的供应商；
- 必须与 EMI 签署正式的 Outsourcing / Service Agreement；
- EMI 仍对 KYC 结果负责，不得以“是第三方做的”为理由免责；
- 必须对第三方进行持续尽调，包括：
  - 技术可靠性
  - 数据保护（GDPR）
  - 合规能力

---

#### **Q14：如何向 Finanstilsynet 展示我们有足够的风险管理能力？**

A:

一般通过以下文档与答复体现：

- 完整的 **Risk Management Policy** 与 **Risk Register**；
- 将各类风险分为：
  - 信用风险
  - 流动性风险
  - 操作风险
  - IT/网络安全风险
  - 合规风险
- 为每类风险指定：
  - 风险指标（KRI）
  - 控制措施
  - 责任人
- 展示董事会 **定期审阅风险报告** 的机制。

---

### **第五部分 | IT / 系统 / DORA 合规篇**

#### **Q15：挪威 EMI 的系统是否必须在本地部署？可以使用云吗？**

A:

- 挪威原则上允许使用云服务（包括公有云），但必须符合：
  - 数据保护法规（GDPR 及本地隐私法）；
  - Outsourcing / ICT Risk 管理要求；
- 若使用境外云（例如欧盟以外地区），需要特别说明：
  - 数据存放国家
  - 访问控制
  - 应急恢复（Disaster Recovery）
  - 监管访问权（FI 是否可获取数据、检查日志）。

---

#### **Q16：对于 DORA（数字运营韧性法规）类要求，挪威是否也遵循？**

A:

挪威作为 EEA 成员国，监管在 ICT/Operational Resilience 上的要求和 DORA 非常接近。实务上需做到：

- 定期进行渗透测试、漏洞扫描；
- 制定并测试 BCP/DRP（业务连续性 & 灾备计划）；
- 有专门的 ICT Risk Policy；
- 清晰划分内部 IT 与外包 IT 的职责界面。

---

### **第六部分 | 护照 / 跨境运营篇**

## **Q17：挪威 EMI 获批后，如何将业务护照到欧盟其他国家？**

A:

流程一般为：

1. 向 Finanstilsynet 提交护照通知（Passporting Notification），列明：
  - 目标国家
  - 提供何种服务（支付、发行 e-money、收单等）
  - 是否设立分支或仅以跨境方式提供服务
2. FI 审核后，会将信息转交给目标国家监管；
3. 一般在 2–3 个月内 完成，具体依各国效率。

---

## **Q18：是否可以在护照后的国家做本地营销和员工部署？**

A:

可以，但要注意：

- 若只通过跨境方式提供服务，一般不构成本地“分支机构”；
- 若设立固定营业场所、员工团队，可能触发该国对“分支机构”的单独要求；
- 应提前由律师对结构进行评估。

---

## **第七部分 | 监管沟通 & 面谈篇（书面说明 + Q&A 示例）**

这一部分可以直接给 CEO/MLRO 练习使用。

---

### **示例一：FI 问 ——**

“为什么选择挪威作为贵公司的设立地，而非其他欧盟成员国？”

答复思路要点（可用于英文书面说明）：

1. 挪威拥有成熟、稳定的金融体系，监管标准与欧盟高度一致；
2. 公司希望以高合规标准国家作为欧洲业务中心，以获得长期品牌与合作优势；
3. 董事会重视风险管理与 AML 控制，认为挪威 Finanstilsynet 的监管文化与公司理念高度契合；
4. 北欧地区在数字化、IT 安全方面领先，非常适合作为金融科技业务的核心枢纽；
5. 公司计划在中长期将挪威作为欧洲总部与风险管理中心，而非单纯的“拿牌地”。

---

### **示例二：FI 面谈问 ——**

“请 CEO 解释贵司的商业模式中，客户资金如何被保护？”

标准答复结构建议：

1. **客户资金账户与公司自有资金账户完全隔离：**
  - 客户资金存放在指定 safeguarding account；
  - 公司运营成本从自有账户支出。
2. **严格的每日/每周对账机制：**
  - 系统余额与银行余额对账；
  - 异常情况自动触发内部警报。
3. **在极端情况下的资金保障安排：**
  - 若公司破产，客户资金不进入破产财产池；
  - 有合同与制度支撑（可提供相关条款）。
4. **董事会与风险委员会的监督机制：**
  - 定期审阅 Safeguarding 报告；
  - 内部审计随机抽查。

---

### **示例三：FI 问 ——**

**“作为 MLRO，你如何看待来自高风险国家的客户申请？”**

建议答复逻辑：

1. 公司实施**风险为本方法（RBA）**，对高风险国家客户采用严格标准；
2. 对高风险国家客户的处理方式包括：
  - 通常不主动开展业务；
  - 如确需接入，必须进行增强尽调（EDD）；
  - 涉及多重信息核实、资金来源文件、公司结构穿透。
3. 系统会自动标记高风险国家，所有相关账户必须由 MLRO 审批；
4. 对持续性交易进行实时+事后监控，异常交易立即评估是否提交 STR。

---

## 第八部分 | 项目执行 / 时间 & 成本篇（客户经常问的现实问题）

**Q19：从启动到拿到挪威 EMI 牌照，大概需要多久？**

A:

在材料准备充分、问答顺畅的前提下：

- 材料准备：3–6 个月
- FI 审核：6–10 个月
- 总体：**9–15 个月** 较为常见

如果：

- 结构复杂、股东较多、跨多司法辖区；
- 监管问答回合较多；  
可能需要更久。

---

**Q20：哪些因素会导致时间拉长甚至被拒？**

A:

1. 股东 / 资金来源解释不清；
2. 董事与管理层实质能力不足（面谈表现很薄弱）；
3. 业务模型存在较高 AML / 制裁风险但控制不足；
4. 外包结构过度依赖第三方，缺少内部能力；
5. 回答 FI 问题拖延、敷衍或风格不专业。

---

## 第九部分 | 风险与策略建议篇

**Q21：挪威 EMI 项目最常见的“坑”有哪些？**

A:

1. 把挪威当成“快速拿牌”国家——实际上监管相当认真；
2. 低估本地实体投入——办公室、团队、本地服务供应商都是长期成本；
3. 业务模式过度依赖高风险国家 / 行业——极易被监管视为高风险项目；
4. 不重视监管沟通的专业度——书面回复随意、口头表述不统一，容易引起信任问题。

---

**Q22：如何设计项目路径，降低整体失败率？**

A:

1. 项目启动前，先进行**合规可行性评估（Feasibility Study）**；
2. 通过专业团队（如仁港永胜）进行：
  - 结构设计
  - 董事 & 管理层配置方案
  - AML / IT / Risk 政策框架搭建
3. 在正式向 FI 提交前，先完成：
  - 模拟问答（Mock Interview）

- 文档一致性检查

## 第十部分 | 业务模式与产品合规模块

### Q23：挪威 EMI 是否允许提供“虚拟 IBAN (vIBAN)”？监管态度如何？

A:

允许，但必须满足严格条件：

1. **vIBAN 必须绑定到真正的托管银行账户；**
2. EMI 不得误导客户认为该账户是“存款账户”或“银行账户”；
3. 所有资金流入流出，必须由 EMI 实施 KYC/KYB + 交易监控；
4. 若 vIBAN 由合作银行/第三方生成，必须有 **IT 外包协议 + Safeguarding 机制**；
5. 对 Corporate 客户必须进行 **结构穿透 (UBO Identification)**，并维持持续尽调。

监管特别关注：

vIBAN 是否会被用于规避银行 KYC、跨境隐匿资金等风险。

如果商业模式涉及 vIBAN，建议提前撰写独立说明文件《vIBAN Risk Analysis & Safeguarding Approach》。

### Q24：挪威 EMI 是否允许发行实体卡 / 虚拟卡？

A:

可以，前提是：

- 使用 受监管的 **BIN Sponsor / Card Issuer**；
- 卡发行属于 e-money 范畴，而非信用业务；
- 卡片体系须遵守：
  - PSD2
  - EMD2
  - 卡网络规则 (Visa/Mastercard 规则)
  - GDPR

监管常提出的问题包括：

- 卡是否可透支？（不可）
- 卡是否支持匿名充值？（不可）
- 谁负责卡的 AML/KYC？（必须是 EMI 自身，而不是发卡第三方）

如涉及卡业务，应准备：《Card Programme Compliance Manual》。

### Q25：挪威 EMI 是否能做加密货币 (Crypto) 相关服务？

A:

不能做 **Crypto 托管**、不能做虚拟资产交易。

但可以做：

- Crypto 买卖的 法币出入金通道 (**fiat on/off ramp**)；
- 合规 Crypto 平台的 收单 / 结算服务；
- 提供针对 Crypto 用户的支付桥 (Payment Rails)。

前提：

1. Crypto 部分的 AML 风险控制必须更严；
2. 必须与 Crypto 平台建立 **KYB + 风险分级协议**；
3. 必须证明 EMI 并不“接触或持有 Crypto 资产”。

FI 通常会要求提交：《Crypto-Related Risk Assessment》。

## **Q26：挪威 EMI 能否提供金融衍生品、贷款、证券服务？**

A:

不能。

- 贷款/信贷业务属于银行牌照领域；
- 衍生品属于投资服务，需投资公司牌照；
- 证券业务需资本市场牌照。

EMI 的“业务边界”必须明确且禁止越界。

---

## **Q27：电子钱包中的客户余额是否可以计息？**

A:

不能。

任何利息、收益、投资行为都可能被视为“吸收存款”，违反银行业务限制。

---

## **Q28：商户收单 / 收款业务（Acquiring）在挪威 EMI 里是否被允许？**

A:

允许，但需满足：

- EMI 必须有明确的 **Merchant Onboarding Policy**；
- 对高风险行业（FX、博彩、Crypto 等）需有特别说明；
- 必须确保商户不利用 EMI 结构进行洗钱或套现。

监管问答中经常出现：

- “如何对商户的业务模型进行验证？”
- “是否会处理高 chargeback/退款风险的行业？”

如涉及收单业务，应准备：《Merchant Due Diligence Procedures》。

---

# **第十一部分 | 资金处理 & Safeguarding 机制**

## **Q29：客户资金必须存放在哪里？是否允许使用外国银行？**

A:

客户资金必须存放于：

- 挪威监管批准的信托银行（Trust Account）
- 或欧盟/EEA 的监管银行
- 或 FI 批准的 safeguarding institution

使用欧盟/EEA 以外银行，难度极高。

---

## **Q30：Safeguarding（客户资金隔离）有哪些常见错误？**

A:

监管最常拒绝的几点：

1. 客户资金与公司自有资金混存；
2. 未每日对账（FI 要求至少每日）
3. 未准备 safeguarding audit report；
4. 使用不合规的 safeguarding 账户结构；
5. 第三方托管银行不受欧盟/EEA 监管。

建议准备独立文件：《Safeguarding Strategy & Daily Reconciliation SOP》。

---

### **Q31：电子货币发行时是否需要 1:1 备兑？**

A:

必须 1:1 备兑。

监管非常强调：

“所有电子货币都是100%即时备兑，不得超发。”

---

### **Q32：客户资金是否必须实时赎回？**

A:

必须允许客户随时赎回，并禁止：

- 延迟赎回
  - 扣除不合理手续费
  - 条款隐藏限制
- 

### **Q33：客户资金每日对账的最低要求是什么？**

A:

1. 系统余额 vs 银行账户余额
  2. 客户分类账 vs 总账
  3. 异常差异须在当日修复
  4. 异常超过限额须由 MLRO 及 CFO 审批
- 

## **第十二部分 | 外包（Outsourcing）与供应商管理**

### **Q34：IT 运营是否可以完全外包？**

A:

不可以完全外包。

公司必须保留内部 ICT 控制能力。

---

### **Q35：外包清单（Outsourcing Register）是否强制要求？**

A:

强制要求。必须包含：

- 供应商资料
- 合同期限
- 服务范围
- 风险等级
- 备援机制
- 监管访问权条款

FI 若发现 Register 缺失，通常会要求重新提交 IT 全套文件。

---

### **Q36：是否允许使用非欧盟的第三方供应商？**

A:

可以，但风险等级高。

不同国家需要提交：

- 数据访问说明
- 数据加密与存储位置
- GDPR 合规

- 监管可访问性

敏感系统最好选择：

**AWS EU Zone、Azure EU、Google Cloud EU、欧盟本地云。**

---

## 第十三部分 | GDPR & 数据保护篇

---

### Q37：挪威 EMI 需要 appoint DPO（数据保护官）吗？

A:

若满足以下任一条件，则必须 appoint DPO：

- 处理大量客户敏感数据
- 跨境数据传输
- 使用自动化决策系统（如 AI 风控）
- 处理交易行为数据

绝大多数 EMI 项目都满足上述条件，因此通常 必须设 DPO。

---

### Q38：GDPR 下的合法处理（Lawful Basis）如何确定？

通常采用：

1. **Contract** – 基于合约履行
2. **Legal Obligation** – 监管要求（AML）
3. **Consent** – 非必要但用于营销时必须
4. **Legitimate Interests** – 风控、欺诈检测

常见错误：

所有事情都写“Consent”，这是不合规的。

---

### Q39：数据是否可以回传到中国？

A:

非常敏感，不建议。

若确需：

- 必须使用 Standard Contractual Clauses (SCC)；
- 必须做 Transfer Impact Assessment (TIA)；
- 必须提供加密与访问控制证明。

建议：

将所有客户数据存放在 EEA 内，由中国团队仅访问匿名化数据。

---

## 第十四部分 | 监管沟通 & 申请流程细节 FAQ

---

### Q40：FI 在申请期间最常问的问题有哪些？

包括但不限于：

1. 商业模式具体如何盈利？
2. 客户资金在每个阶段的流动路径是什么？
3. 内外包职责边界是否清晰？
4. 董事会如何参与日常监督？
5. MLRO 如何审核高风险交易？

6. ICT 系统如何保证数据完整性？
7. 是否会处理来自高风险国家的客户？

我们可为你准备：《Finanstilsynet 常见问答（RFI）模板集》。

---

#### **Q41：FI 是否会要求召开面谈？什么情况下会面谈？**

A:

常见触发条件：

- 股东来自高风险国家；
- 商业模式复杂（Crypto、vIBAN、多国结构）；
- 董事缺乏支付行业经验；
- IT 外包比例高。

面谈对象：

- CEO
- MLRO
- CTO
- 董事（至少 1–2 人）

仁港永胜可提供：

《仿真面试（Mock Interview）》服务。

---

#### **Q42：被问到不确定的问题怎么办？能否回答“我们还在评估”？**

A:

不要直接回答“我们还在评估”。

可以这样表达：

“我们已制定初步方案，目前正在根据风险级别进一步细化，正式版将随附于最终 IT/AML 政策中提交。”

要显示：

你已在推进，而不是没有计划。

---

## **第十五部分 | 公司治理（Corporate Governance）FAQ**

#### **Q43：挪威 EMI 董事会必须多久开一次会？**

建议：

- 每季度至少一次（Quarterly Board Meeting）
- 重大事件或风险事件须即时召开临时会议

监管重视会议记录（Minutes）。

---

#### **Q44：董事会必须设哪些委员会？**

建议（非强制，但监管喜欢看到）：

- 风险委员会（Risk Committee）
- 合规委员会（Compliance Committee）
- 审计委员会（Audit Committee）

若是初创 EMI，可由董事会本身承担委员会职能。

---

#### **Q45：董事是否需要合规培训？**

需要。

至少包括：

- AML/CFT
- ICT 风险
- GDPR
- Operational Risk
- Safeguarding

我们可提供：《董事合规培训材料（Board Compliance Training Pack）》。

---

## 第十六部分 | 审计、年检、监管报告 FAQ

---

### Q46：挪威 EMI 是否需要提交年度审计？

必须。

包括：

1. 年度财务审计
  2. AML 独立审核
  3. ICT 风险审计（部分情况下）
  4. Safeguarding 审计
- 

### Q47：年度审计是否必须由挪威本地审计事务所完成？

原则上建议使用挪威/北欧本地审计机构。

FI 更信任本地机构出具的报告。

---

### Q48：需要向监管定期提交什么报告？

一般包括：

- KRT-100（监管报表）
- 可疑交易报告（STR）
- ICT 事件报告
- 运营中断报告
- 年度 AML 风险评估

仁港永胜可为您有偿拟定一份：《挪威 EMI 年度监管日历（Regulatory Calendar）》。

---

## 第十七部分 | 银行开户 FAQ

### Q49：挪威 EMI 是否难以开立 safeguarding account？

是的，与立陶宛、爱尔兰类似，银行开户是最难的部分之一。

银行会重点审查：

- 股东背景
- 业务风险
- 高风险国家敞口
- AML 政策质量
- 客户构成（C2C vs B2B）

若业务偏 B2C，开户更难。

---

### Q50：可以在欧盟其他国家开 safeguarding account 吗？

可以。

常见选择：

- 德国
- 荷兰
- 法国
- 比利时

前提是：

银行愿意承接你的商业模式。

---

## 第十八部分 | 拒批风险与缓解措施 FAQ

---

### Q51：挪威 EMI 申请最容易被拒的原因是什么？

1. 董事/管理层能力不足
  2. AML 风险控制不充分
  3. 业务本质上高风险 (Crypto、跨境 C2C 等)
  4. 资金来源不透明
  5. 外包比例过高，内部能力不足
  6. 监管问答质量差、逻辑不清晰
- 

### Q52：如何提升成功率？

核心三点：

1. 优秀的董事与 MLRO 配置
2. 高质量的 Policy Suite (AML + Risk + ICT + Safeguarding)
3. 专业监管沟通 (RFI 回复 + 面谈)

仁港永胜可有偿完整提供。

---

## 第十九部分 | 跨境运营、护照机制 (Passporting) 与集团结构 FAQ

---

### Q53：挪威 EMI 能否在整个欧盟/EEA 使用护照机制开展业务？

A:

可以，但有重要区别：

- 挪威不是欧盟成员国
- 挪威属于 EEA (欧洲经济区)
- EMI 护照 覆盖整个 EEA，但不覆盖非 EEA 国家

护照覆盖范围包括：

- 挪威
- 冰岛
- 列支敦士登
- 欧盟 27 国全部

不覆盖：

- 瑞士
- 英国（脱欧后不再属于 EEA）
- 新加坡 / 香港 / 阿联酋等非欧盟国家

护照模式在挪威属于 **通知型机制 (Notification)**，即：  
只需向 FI (挪威监管) 提交跨境业务计划与 AML 说明，由 FI 通知目标国监管机构即可。

---

#### **Q54：如果挪威 EMI 要在其他国家设立实体办事处，需要重新申请牌照吗？**

A:

取决于设立方式：

##### **① 设立分公司 (Branch)**

- 需要向目标国家监管申请“护照化分公司 (Passporting Branch)”  
无需重新申请 EMI 牌照

##### **② 设立子公司 (Subsidiary)**

- 子公司不自动继承护照
- 如子公司本身提供 EMI 服务，则必须 **重新申请 EMI / PI 牌照**

##### **③ 设立代表处 (Representative Office)**

- 只用于市场推广
  - 不允许从事支付服务
  - 无需重新申请牌照
  - 必须报备监管
- 

#### **Q55：挪威 EMI 是否可以在英国提供服务 (Brexit 后) ?**

A:

不可以直接护照进入英国。

目前英国与欧盟/EEA 已完全分离监管体系。

如需在英国开展 EMI 或 PI 业务，必须：

1. 申请英国 FCA 电子货币牌照  
或
2. 与英国 EMI 合作 (Agent / Distributor 模式)

英国的监管强度极高 (接近瑞士)，需单独评估。

---

#### **Q56：挪威 EMI 能否为全球客户提供服务 (如亚洲、拉美、中东) ?**

A:

可以，但需注意：

1. **不能在当地“落地经营”**  
意思是：  
不得在当地招揽、落地宣传、设立办事处，否则可能触发当地许可要求。
2. **跨境 KYC 风险更高**  
需有跨境客户风险分级方案。
3. **高风险国家与制裁名单必须严格审核**  
OFAC / EU Sanctions / UNSC Sanctions / Local Sanctions
4. **部分国家禁止未持牌外资支付机构为其居民提供服务**  
如：印度、土耳其、印尼、部分非洲国家。

物流、教育行业、跨境贸易常见场景可以支持；  
但博彩、私募基金、外汇、虚拟资产等行业必须特别谨慎。

---

#### **Q57：控股结构 (Shareholding Structure) 存在什么合规要求？**

挪威 FI 对股东非常严格，要求：

1. 穿透至最终自然人 (UBO)

2. UBO 必须提供资金来源证明
3. 若股东是法人：需提供完整公司链条
4. 若涉及跨境控股：需提供 **Group Structure Chart**
5. 若控股方来自高风险地区：FI 会加强审查

建议准备：《控股集团结构说明信（Shareholder Structure Declaration）》。

## **Q58：是否允许中国主体作为 100% 控股人？**

允许，但监管会更严格。

FI 审查重点包括：

- UBO 的资金来源是否清晰
- 对中国 AML 制度是否了解
- 是否具备国际化运营能力
- 是否建立挪威本地治理机制（local governance）
- 是否有本地董事 + 本地高级管理层

所以并非不能申报，而是必须做好：

**高标准的透明度 + 高质量 AML/Risk 文件 + 高水平本地团队配置。**

## **Q59：挪威 EMI 是否可以设多层海外控股（如香港—新加坡—开曼）？**

可以，但风险更高。

监管会特别关注：

1. 是否存在控股空壳结构（Shell Company Risk）
2. 是否存在税务规避（Tax Avoidance）
3. 是否存在资金链复杂、难以穿透的情况
4. 是否存在地缘政治风险（如高风险国家）

适合结构：

- 香港控股
- 新加坡控股
- 欧盟控股

不建议结构：

- 太多层开曼 / BVI / 马绍尔 / 塞舌尔等离岸结构

建议提前准备：《跨境控股架构风险分析报告（Group Risk Assessment）》。

## **Q60：挪威 EMI 是否允许采用双实体结构（Operational Company + EMI License Holder）？**

可以。

这是监管欢迎的结构，因为可以：

- 用 EMI 实体持牌
- 用运营实体负责技术开发、外包、客户支持
- EMI 本身保持纯净的牌照结构

但必须提交：

- 《Transfer Pricing Policy》转移定价政策
- 服务协议（Intercompany Service Agreement）
- 合规边界说明

仁港永胜可提供模板。

# 第二十部分 | 技术系统（ICT）与操作风险（Operational Risk） FAQ

---

## Q61：挪威 EMI 必须准备哪些 ICT 文档？

监管至少要求以下 ICT 文件（共 14–28 份）：

1. ICT Policy
2. Information Security Policy
3. Access Control Policy
4. IT Outsourcing Agreement
5. Incident Management Policy
6. Backup & Restore Plan
7. Disaster Recovery Plan
8. Business Continuity Plan
9. Penetration Testing Reports
10. Change Management Policy
11. System Architecture Diagram
12. Data Flow Mapping (GDPR)
13. Logging & Monitoring Policy
14. Network Security Controls

许多申请机构因 ICT 文件不足而被 FI 延迟审批。

---

## Q62：IT 系统是否必须在挪威本地？

不需要。

但必须：

- 数据存放在 **EEA 区域**（欧盟/挪威/冰岛/列支敦士登）
- 若需跨境访问：必须提供
  - 加密方案
  - 访问权限限制
  - 日志记录
  - GDPR 合规说明
- 不允许在无监管支持国家存放敏感数据（如某些亚洲、中东国家）

## Q63：是否必须提供渗透测试（Pen Test）报告与漏洞评估？

需要。监管要求至少：

- 年度 Pen Test
- 季度漏洞扫描
- 第三方安全审计报告（可外包）

这是 EMI 申请的必备硬要求。

---

## Q64：如果技术系统完全使用 SaaS 平台可以吗？

可以，但要满足：

1. SaaS 平台必须在 EEA 或合规国家
2. 必须有 **Regulatory Access Clause**（监管访问条款）
3. 必须确保数据加密并可随时导出
4. EMI 自身必须保留对系统的核心控制权（关键节点不可由第三方单方面掌控）

需要说明文件：《SaaS System Risk Evaluation》。

---

# 第二十一部分 | AML / CFT & 交易监控 (Transaction Monitoring) FAQ

---

## Q65：挪威 EMI 需要设立 MLRO 和 AML Officer 吗？

必须。

并且两者不能是外包人员。

- MLRO（反洗钱负责人）必须驻挪威或欧盟
- AML Officer 可以在其他 EEA 国家

不可使用兼职、不可外包、不可用实习生。

---

## Q66：是否必须进行持续尽调 (Ongoing Due Diligence) ?

需要，监管要求：

- 高风险客户：每 6 个月
- 中风险客户：每 12 个月
- 低风险客户：每 24 个月

并必须对：

- 客户身份文件
- UBO
- 地址
- 商业活动
- 风险分级

进行重新审核。

---

## Q67：是否必须做交易监控？如何做？

必须做，并且应覆盖：

1. 行为模型 (Behaviour Monitoring)
2. 异常金额规则 (Threshold Rules)
3. 地域风险规则 (Geographical Risk)
4. 模式识别 (Pattern Recognition)
5. 潜在洗钱链检测 (Layering Detection)
6. 可疑行为自动报警 (Alert Automation)

建议采用专业反洗钱软件，如：

- Fcase
- Salv
- ComplyAdvantage
- Sumsub (部分能力)
- Seon

仁港永胜可为你设计完整《AML System Mapping》。

---

## Q68：是否必须向 FI 提交 STR (可疑交易报告) ?

必须。

STR 应提交给挪威金融情报部门 (FIU)，并遵守：

- 必须立即提交
- 不得在客户不知情的情况下延迟

- 不得透露 STR 已提交 (Tipping-off)

STR 是监管处罚最敏感的领域之一。

---

## 第二十二部分 | 费用预算、时间、项目规划 FAQ

---

### Q69：挪威 EMI 申请的审批时间一般多久？

- 监管总周期：**6–12 个月**
- FI 问答/RFI 往返：2–5 轮
- 银行开户 (Safeguarding Account)：2–6 个月
- IT 审核：1–2 个月
- AML 审核：1–3 个月

因此整体时间需 **12–18 个月** 更为稳妥。

---

### Q70：除了官方费用外，还有哪些预算？

典型预算（参考值）：

项目	金额区间（欧元）
注册资本（最低）	€350,000
Safeguarding 启动资金	€50,000–€500,000
董事、本地团队工资	€150,000–€300,000/年
AML/ICT 软件	€20,000–€150,000/年
年度审计	€10,000–€30,000
外部法律费用	€10,000–€25,000
持续合规维护成本	€50,000–€150,000

如业务复杂 (Crypto、跨境 B2B、vIBAN)，成本更高。

---

### Q71：初创团队如何降低成本？

可采用：

1. 双实体结构：EMI 持牌实体 + 运营公司
2. 业务初期采用 部分外包 + 内部核心人员组合
3. 使用性价比高的 AML/ICT 工具
4. 从低风险客户群开始（降低监管关注度）
5. 采用多国 safeguarding（提高开户成功率）

仁港永胜可协助做成本规划与结构优化。

---

## 第二十三部分 | 拒批、整改 & 再申请 (Resubmission) FAQ

---

### Q72：如果申请被退回 (Rejected)，是否可以重新提交？

可以，但需满足条件：

1. 整改报告 (Remediation Report)
2. 提供新增证据与说明
3. 更换不符合条件的董事/MLRO/ICT 负责人
4. 重新提交完整文件包

一般整改周期为：3–6 个月。

---

### Q73：监管最常要求整改哪些事项？

前十个最常见整改点：

1. AML/KYC 模型不完整
  2. 董事经验不足
  3. Safeguarding 机制不合规
  4. ICT 外包过度
  5. 商业模式风险高 (Crypto、跨境 C2C、vIBAN)
  6. 风险评估不完整
  7. 董事会治理结构不足
  8. 资金来源说明不足
  9. 银行开户失败
  10. 客户定位不清晰 (Customer Profile Ambiguous)
- 

#### **Q74：如何加快审批速度？**

关键三点：

1. 提前准备完整申请材料包（而不是申请后再补）
2. RFI 问答必须专业、逻辑严密、结构清晰
3. 合规团队 / MLRO 必须能力强且经验丰富

仁港永胜可有偿提供完整《Finanstilsynet RFI 问答模板》。

---

## **第二十四部分 | 其他高频问答（综合类）**

#### **Q75：挪威 EMI 是否必须聘请当地会计师、律师？**

监管鼓励，但不强制。

强烈建议聘请挪威本地：

- 审计机构
- 律所
- 税务顾问

不仅提升信用，也提升银行开户成功率。

---

#### **Q76：是否可以聘请中国团队远程处理大部分功能？**

可以，但必须：

1. 核心职能留在挪威/EEA (AML、风险、ICT 控制、治理)；
  2. 中国团队必须通过 GDPR 访问控制；
  3. 客户敏感数据不得直接存储在中国（可匿名化）。
- 

#### **Q77：业务初期是否可以不招募太多员工？**

可以采用“小规模起步”模式：

- CEO (驻挪威或欧盟)
- MLRO (驻挪威/欧盟)
- ICT 负责人 (可外包 + 内部监督)
- 1–2 名运营人员

但“最少配置”必须满足监管要求。

---

#### **Q78：公司是否必须有实体办公地址？是否可以使用共享办公室？**

## 答案（监管级说明）：

挪威 Finanstilsynet (FI) 要求 EMI 机构必须具备：

- 真实且适合运营的实体办公场所 (**Physical Presence**)
- 必须能够支持日常合规、风控、ICT、客户支持等职能
- “共享办公室 (Coworking Space)”可以接受，但 需要满足额外条件

共享办公室 必须同时满足以下 5 条要求：

### 1. 办公地点可被监管现场检查 (On-site inspection)

FI 必须能随时进入场地检查。

### 2. 有专属区域或锁柜保存敏感文件 (Secure Storage)

云端可存储，但必须有可控制权限的实体储存区域。

### 3. 可证明团队定期在当地办公 (Local Operation Evidence)

包括：

- 考勤记录
- 员工地址
- 挪威本地雇佣合同
- 董事会议纪要

### 4. 合规/AML/风险管理等“关键岗位”需有实地办公能力

即使部分远程，也必须有实际存在。

### 5. 共享办公室协议需列明“可供监管查验”条款 (Regulator Access Clause)

⚠ 注意：虚拟办公室 (Virtual Office Address) 不被接受。

仁港永胜在欧洲配有合作办公点，可为客户提供完全符合 EMI 审批要求的办公场所解决方案。

## Q79：EMI 的管理层是否必须在挪威名本地？是否可以完全远程？

FI 监管要求：

- 至少 2 名高管必须常驻挪威 (**Senior Management Onshore**)
- AMLRO (反洗钱负责人) 必须可在 2 小时内到场
- ICT 负责人若远程需额外提交《远程 ICT 管理制度》

远程团队可存在，但必须证明：

- 实时可用
- 时区覆盖
- 权限管控合理
- 与本地团队沟通机制完善

## Q80：关键岗位是否可以外包？例如 AML、ICT、安全测试？

可外包，但需满足：

### 关键岗位可外包的范围

职能	是否可外包	监管要求
合规 (Compliance)	部分可外包	仍需指定本地负责人
AML/CTF	✓可外包 (慎)	AMLRO 必须为内部人员
ICT 系统	✓可外包	需提供外包审查文件
内部审计	✓可外包	必须任命内部审计负责人
风控 (Risk)	部分可外包	需保留核心风控职能内部化

### 注意：

外包不代表责任转移，责任仍由董事会承担。

仁港永胜可有偿提供：

《外包风险评估报告》+《供应商尽调模板》+《外包 SLA 套件》。

## **Q81：EMI 是否允许发行虚拟 IBAN (vIBAN) ?**

允许，但必须满足：

- 由具有许可的银行或金融机构发行
  - EMI 本身不能作为 IBAN 发起方
  - 必须使用 Safeguarding Account 实现资金隔离
  - 必须提供 vIBAN 对账机制
- 

## **Q82：是否允许自建钱包与自建清算系统？FI 的要求是什么？**

可以，但监管会极其严格。

需提供：

1. 系统架构图 (Architecture Diagram)
2. 数据流图 (Data Flow Diagram)
3. 可用性与冗余设计 (Availability & redundancy)
4. API 网关安全标准
5. 入侵检测 (IDS) 与日志监控 (SIEM)
6. 源代码管理策略 (Git Policy)

仁港永胜可有偿提供完整的《ICT 系统地图·挪威监管版》。

---

## **Q83：是否允许发行预付卡 (Prepaid Card) ?**

允许，但需满足：

- 与许可银行共享 BIN
  - 卡组织 (VISA/Mastercard) 审批
  - 需提交《Prepaid Product Risk Assessment》
  - 需确保 Safeguarding 机制独立于卡组织资金流
- 

## **Q84：是否可以接入加密货币服务？(Crypto + EMI)**

监管允许 EMI：

- 提供法币钱包
- 提供加密资产购买的支付接口
- 提供法币 ↔ 加密资产的支付服务

但不允许：

- 持有客户加密资产
- 运营交易所
- 运营托管钱包
- 推广加密资产投资

若涉及到 Crypto，需要额外：

- 风险评估
  - 客户适当性评估
  - 加密资产交易监测机制 (Block Chain Analytics)
- 

## **Q85：客户资金保障频率是什么？必须每日核对吗？**

FI 明确要求：

核对类型	频率	说明
客户资金对账 (Reconciliation)	每日 / Daily	必须自动化
客户资金隔离验证	每日 / Daily	系统自动验证
每月 Safeguarding 报告	Monthly	提交董事会

## Q86：是否必须聘请挪威当地的审计师？

必须。

要求：

- 必须是挪威注册会计师 (Registered Auditor)
- 需提交《审计合作意向书 (Pre-Engagement Letter)》
- 审计师需进行年度 Safeguarding Audit

仁港永胜可提供推荐名单。

## Q87：是否可以使用集团共享服务中心 (Shared Service Center) ?

可以，但需提交：

- 服务协议
- RACI 图 (职责分工)
- 外包风险评估
- 权限管理制度

监管最关心：

- 职能是否可控
- 风险是否可隔离
- 数据是否在 EEA 合规存放

## Q88：如果公司暂时没有客户，可以先拿牌再开展业务吗？

可以，但监管要求：

- 提供“无客户运营流程”
- 提供“空账模式对账流程”
- 提交“最低运营团队”
- 按计划逐步启动市场活动并报告

## Q89：董事是否需要金融背景？能否完全技术背景？

不可以完全技术背景。

Finanstilsynet 要求：

- 至少 1 名董事具备 支付 / 金融 / 银行 / 监管 背景
- 至少 1 名董事具备 技术与系统合规背景
- 两者必须互补

## Q90：EMI 可否在多个国家设分支机构？

可以，但：

- 分支机构必须纳入集团风险管理
- 必须通知监管
- 需要提交“跨境运营结构图”

仁港永胜擅长搭建：  
中国 → 香港 → 挪威 → 欧盟的跨境支付结构。

---

## Q91：申请 EMI 牌照时是否必须提交 3 年财务预测？格式有什么要求？

是的。

Finanstilsynet (FI) 明确规定：

必须提交至少 36 个月（3 年）滚动财务预测（Financial Projection）。

必须包含：

1. 损益表（P&L）
2. 现金流量表（Cash Flow）
3. 资产负债表（Balance Sheet）
4. 资本充足率（Capital Adequacy）计算
5. 风险加权因素（Risk Weight）说明
6. 流动性压力测试（Liquidity Stress Test）
7. **Safeguarding** 资金流模型（Ring-Fencing Model）

监管特别关注：

- 模型是否过度乐观
- 成本是否低估
- 是否长期亏损
- 是否有充足资本应付压力情景（Stress Scenarios）

仁港永胜可提供完整《挪威 EMI 财务预测模型（Excel）》。

---

## Q92：EMI 是否可以提供跨境支付服务？对非欧洲的客户是否有限制？

可以，但需遵守以下原则：

**允许：**

- 全球跨境支付
- 全球 B2B/B2C 钱包服务
- 全球收单与结算
- 数字钱包充值/提现
- 给非 EEA 地区的客户服务

**限制：**

对 **高风险国家（FATF 高风险名单）**：

- 需提交额外风险评估
- 加强 KYC
- 加强交易监控
- 必须提供可持续的风险缓解机制

**监管重点：**

- 高风险地区客户的 Source of Funds (SOF)
- Source of Wealth (SOW)
- 可疑活动监测

---

## Q93：董事会能否全部由外籍成员组成？是否必须有挪威籍？

外籍董事可以，但必须至少有 1 名董事 / 高管常驻挪威。

要求包括：

- 居住在挪威
  - 可随时与监管对接
  - 对挪威法律与金融监管有理解
  - 在挪威具有“实际管理权”(Mind & Management)
- 

## Q94：公司是否必须在挪威缴税？是否可以在其他国家报税？

EMI 作为金融机构，必须在挪威：

- 注册纳税实体
- 报告企业所得税
- 提交年度财务审计报告

不允许将主要收入转移至避税地区（例如塞舌尔、BVI）。

---

## Q95：客户资金必须存放在挪威境内吗？可以存在欧盟其他国家吗？

允许两种方式：

### 方式 A（推荐）

存放在挪威本地银行（例如：DNB、Nordea）。

### 方式 B

存放在 EEA 银行（例如德国、法国、荷兰等）。

限制：

- 不能存放在非 EEA 银行
  - 必须使用“Safeguarding Account”
  - 不能与公司资金混同
- 

## Q96：是否必须提交 IT 系统源代码？监管是否会检查？

不要求提交源代码。

但必须提交：

- 系统架构图（Architecture Diagram）
- 数据流图（DFD）
- 安全策略（Security Policy）
- API 文档（API Specs）
- 访问控制结构图（RBAC）
- 审计追踪（Audit Trail）机制

监管会现场检查系统部署是否真实运行。

---

## Q97：挪威 EMI 是否允许提供虚拟货币托管？

不允许。

可以：

- 处理“法币–加密资产”的支付通道

不可以：

- 托管加密资产
- 管理私钥
- 成为加密资产钱包

若需要加密货币托管服务 → 必须申请 CASP 牌照（欧盟 MiCA 框架）。

---

## **Q98：是否可以将技术团队全部放在中国、大湾区或新加坡？**

可以，但必须满足：

- 提供 ICT 外包风险评估
- 数据需存储在 EEA 区域或合规国家
- 新加坡可行，中国不可行（因数据保护不符合 GDPR）
- 系统核心管理权限必须可被挪威本地人员控制

仁港永胜可提供《ICT 外包合规套件 · 挪威版》。

---

## **Q99：EMI 是否可以没有“现场客服团队”？**

可以没有现场客服团队，但必须具有：

- 7×24 客户支持机制
- 可溯源的客户支持（记录、工单）
- 明确的客户投诉机制
- 提供“客户支持外包模型”

---

## **Q100：监管是否会对董事进行面谈？内容是什么？**

是的。

通常包含：

- 商业模式理解能力
- 对 AML/KYC 的理解
- 对风险管理的理解
- 对 ICT 架构的了解程度
- 是否具备“实质控制权”
- 是否了解本地义务（税务、报告、监管）

---

## **Q101：请说明公司如何确保“治理结构有效运行”？**

示范答案：

我们采取多层治理架构来确保决策透明、风险可控：

1. 董事会（Board）负责战略、重大政策批准与合规监督。
2. 管理层（Management）负责日常运营，包括风险、合规、财务、ICT 等。
3. 独立职能部门：
  - Compliance（合规）
  - Risk（风险）
  - AML（反洗钱）
4. 三道防线（3 Lines of Defence）机制已正式建立并文件化。

董事会每季度审阅风险报告、合规报告及财务报表，并对重大变更实施独立审查。

---

## **Q102：你们如何确保董事会具备实际控制权？（Mind & Management）**

**示范答案：**

- 所有关键决策（预算、战略、风险容忍度）均由董事会批准。
  - 董事会会议在 **挪威境内** 举行。
  - 有一名挪威本地常驻执行董事。
  - 监管沟通与批准事项由董事会直接发起，并非由外包方执行。
  - 会议记录与决议文件均由内部团队维护，并可随时接受审核。
- 

## **Q103：请解释你们的“风险偏好框架”(Risk Appetite Framework)。**

**示范答案：**

我们已经制定了 Risk Appetite Statement (RAS)，明确以下限额与阈值：

- 运营风险 (Operational Risk) 容忍度低；
- 洗钱/恐怖融资风险零容忍 (Zero Tolerance)；
- 信用风险限额极低 (仅限受监管金融机构)；
- ICT 风险通过“高可用”与“数据隔离”严格控制；
- 交易监控每日运行并设有自动报警机制。

董事会每年至少审视一次 RAS。

---

## **Q104：你们如何对第三方外包进行风险评估？**

**示范答案：**

我们遵循 EBA Guidelines on Outsourcing：

1. 对每一个外包方进行 **尽职调查 (Due Diligence)**
  2. 对每项外包实施 **风险评分** (包括 ICT、数据隐私、BCP、监管可访问性)
  3. 签署 SLA 与 Outsourcing Agreement
  4. 定期审查外包方表现
  5. 对关键外包 (Critical Outsourcing) 进行年度审计报告 (SOC1/SOC2)
- 

## **Q105：你们如何进行反洗钱风险分类 (Risk Scoring) ？**

**示范答案：**

我们采用三层风险模型：

- 国家风险 (Country Risk)
- 客户风险 (Customer Risk)
- 交易风险 (Transaction Risk)

系统自动评分，高风险客户必须通过加强尽职调查 (EDD)。

---

## **Q106：对于高风险客户，你们如何执行 EDD？**

**示范答案：**

EDD 包括：

- 核实 SOF、SOW
  - 额外身份认证 (Enhanced Verification)
  - 通过第三方数据库检查 (Dow Jones、WorldCheck 等)
  - 高级别管理层批准
  - 更严格的交易监控阈值
- 

## **Q107：请解释交易监控 (Transaction Monitoring) 模型。**

示范答案：

交易监控系统包括：

- 规则引擎 (Rule-based)
- 行为分析模型 (Behavioural Model)
- 黑名单匹配
- 场景监测 (Scenario Simulation)
- 机器学习辅助 (如适用)

所有警示必须在 24 小时内处理并记录。

---

## **Q108：你们如何识别是否存在“分拆交易”行为？**

示范答案：

- 系统会检测短时间内多笔金额接近限额的交易
- 分析客户行为模式
- 若怀疑分拆，自动发起内部调查
- 如仍可疑 → 立即 STR 上报 FIU

## **Q109：你们如何确保数据保护符合 GDPR？**

示范答案：

- 所有数据存储于 EEA 区域
- 数据加密 (AES-256)
- RBAC 权限控制
- 日志审计 (Audit Trail)
- 保留政策 (Retention Policy: 5–7 年)
- DPO 负责监督所有数据处理活动

## **Q110：你们的系统是否支持双因素认证 (2FA)？**

是。所有管理端访问必须使用 2FA，包括 MFA / OTP / 硬件令牌。

---

## **Q111：如果出现系统停机，你们的 BCP (Business Continuity Plan) 如何运行？**

示范答案：

- 24/7 监控
- 自动故障转移 (Failover)
- 灾备数据中心 (DR Site) 位于 EEA 区域
- RTO: 30 分钟
- RPO: 15 分钟
- 每年进行灾备演练并向董事会报告

## **Q112：客户资金如何隔离？如何防止与公司资金混同？**

示范答案：

- 客户资金存放于 “Safeguarding Account”
- 公司运营资金存放于公司账户
- 系统限制跨账户转账
- 每日对账 (Daily Reconciliation)

- 每月由外部审计复核

符合 EMD2、PSD2 的 safeguarding 要求。

---

## **Q113：你们如何监控外包 ICT 服务商的表现？**

- 定期 KPI 审查
  - 日志报告
  - 每季度 SLA 审查
  - 外包方必须提供 SOC 报告
  - 监管可随时现场检查（Right of Audit）
- 

## **Q114：如果 MLRO 不在岗，你们如何确保 AML 职能不中断？**

- 已任命 Deputy MLRO
  - 有清晰的职责交接（Delegation Procedure）
  - 备用人选具备同等资质
  - 所有流程已系统化，不依赖个人
- 

## **Q115：公司是否允许使用现金交易？**

禁止现金。

仅接受电子支付、银行转账、合法的第三方支付渠道。

---

## **Q116：你们如何应对“虚假商户”(Fake Merchant) 的风险？**

- 对商户进行 KYB
  - 核查公司注册、网站合法性、电话验证
  - 技术团队对系统接口进行验证
  - 设置商户“冷启动限额”(Initial Cap)
- 

## **Q117：你们如何监控跨境资金进出？**

- 对每笔交易进行实时分析
  - SWIFT / IBAN 验证
  - 监控目的国 (High-Risk Jurisdictions)
  - 自动风险打分
  - 可疑则阻断交易 + AML 调查
- 

## **Q118：贵司如何确保不会被滥用于逃税或地下钱庄？**

- 税务风险纳入 AML Risk Model
  - 所有大额交易需注明 purpose code
  - 强制 SOF/SOW
  - 对可疑模式立即 STR 报告
  - 不允许匿名交易
- 

## **Q119：你们是否使用第三方进行审计？**

是。

年度审计由挪威注册审计师执行。

内部审计外包给专业审计机构。

---

## Q120：若监管要求，你们是否可以立即提供系统访问权限？

可以。

监管拥有“Right to Access”，我们承诺：

- 开放 API 日志
  - 系统后台视图
  - 交易记录
  - 访问控制清单
  - 所有文件在 24 小时内提供
- 

## Q121：请解释你们如何确保关键岗位“不可兼任”原则？

示范答案：

我们已根据 EBA Guidelines 与 Finanstilsynet 指引进行岗位隔离（Segregation of Duties, SoD）：

- MLRO 不可同时担任 CFO、CTO、CEO
- CTO 不参与 AML 或风险审批
- 风险经理不参与业务拓展
- 产品团队无法修改交易记录或 KYC 数据

此外，我们建立系统权限矩阵（RBAC Matrix）及每季度审计。

---

## Q122：当董事会与管理层意见不一致时，如何处理？

示范答案：

我们制定了 **Conflict Resolution Policy**，流程包括：

1. 管理层提供详细风险评估
2. 由董事会审视是否影响监管义务
3. 必要时由独立董事（Independent Director）投最终票
4. 若涉及重大合规事项 → 由 Compliance/MLRO 直接向董事会汇报优先

监管优先原则（Regulatory First Principle）高于商业利益。

---

## Q123：你们是否会接受来自高风险国家的客户？

示范答案：

原则上不接受 FATF 高风险国家（High-Risk Jurisdictions）客户。

如需例外（例如跨国集团子公司），我们具有以下 EDD：

- 高级 Management Approval
  - 完整 SOF/SOW
  - 加强监控
  - 更低的交易限额
  - 实时行为监测
- 

## Q124：贵司是否接受来自未受监管支付机构的资金？

示范答案：

不接受。

所有合作清算伙伴必须为：

- 银行（Bank）

- 受监管支付机构 (PI)
- EMI
- 或 EEA 金融机构

我们使用 KYB + 监管牌照数据库确认其合法性。

---

## **Q125：你们如何防止“无经济目的交易”？(No Commercial Rationale)**

示范答案：

- 自研系统会识别非线性交易、重复金额、反向操作等模式
  - 若交易不能说明商业目的 → Block + Internal Review
  - 对企业商户审核商业模式是否真实
  - 可疑案例强制 STR 上报
- 

## **Q126：你们如何验证客户的资金来源 (SOF) 真实性？**

示范答案：

- 通过银行流水、税务证明、工资单、投资收益报告、合同等文件
  - 若文件不充分 → Video KYC 二次沟通
  - 采用第三方数据库及 OSINT 做验证
  - MLRO 审批后方可放行
- 

## **Q127：公司如何监控内部员工违规？**

示范答案：

- 建立内部 Whistleblowing 机制
  - 所有后台操作记录在案
  - 系统强制审计日志（不可修改）
  - 每年进行员工 AML 培训
  - 访问权限基于岗位动态调整
  - 合规部门直接向董事会报告员工违规
- 

## **Q128：如何判断一个企业客户是否为“空壳公司”(Shell Company) ？**

示范答案：

- 注册地是否存在高风险地区
- 无实体办公地址（仅 PO Box）
- 无实际员工
- 无真实业务
- UBO 多层穿透后指向高风险对象
- 无正常网站或业务流量

满足两项以上即进入高风险 KYB。

---

## **Q129：你们如何保证 Safeguarding 完全独立？**

示范答案：

- Safeguarding Accounts 与运营账户物理隔离
- 由挪威/EEA 持牌银行托管
- 不用于运营支出

- 自动每日对账
  - 全部由 CFO + External Auditor 定期审计
  - 若客户余额大 → 立即触发自动警示邮件给董事会
- 

## Q130：请说明产品上线前如何进行合规审查？

示范答案：

我们采用 **Product Approval Policy**：

1. 产品团队提出产品框架
  2. 合规部门评估法律风险（包括 AML、ICT、数据）
  3. 风险部门完成 ORSA (Operational Risk Self-Assessment)
  4. 法务审查条款
  5. CTO 完成渗透测试 (PenTest)
  6. 董事会审批
  7. 限量客户试运行 (Pilot Program)
- 

## Q131：你们如何监控“可疑商户跳码（MCC Fraud）”行为？

示范答案：

- MCC 分类由内部系统自动识别
  - 若发现 MCC 与交易模式不符 → 立即冻结商户
  - 要求提供发票、对账单、合同等
  - 若不符 → 终止合作 + STR
- 

## Q132：如何确保跨境客户的 AML 合规性？

示范答案：

- 加强地理风险国别控制
  - 所有跨境客户需完整 KYC、KYB
  - 实时 SWIFT 验证
  - 加强交易监控 (Country-Based Rules)
  - FATF 风险国家自动阻断
- 

## Q133：如果监管要求一个月内提交内部审查报告，你们如何应对？

示范答案：

- 我们内部使用统一文档管理系统，可立即调集资料
- 合规部可在 10 个工作日内完成初步报告
- 由 MLRO、风险、ICT 联合审阅
- 提交前由董事会签字确认

我们遵循 “Regulatory First” 原则。

---

## Q134：你们如何评估第三方供应商的“监管审计权”(Audit Right) 可执行？

示范答案：

- 合同中明确监管可直接要求访问
- 外包方必须签署 “Regulatory Access Clause”
- 若外包不接受 → 自动排除

- 年度外包审计会评估其执行度
- 

## **Q135：你们是否提供匿名预付卡或匿名钱包？**

示范答案：

绝对不提供。

所有产品必须通过完整 KYC 后才能使用。

---

## **Q136：请解释技术团队如何确保交易不可篡改（Immutability）？**

示范答案：

- 所有交易写入日志（Write-once Log Storage）
  - Hash 校验
  - 系统权限严格控制
  - 每 24 小时生成交易快照
  - 数据库采用多节点冗余（Multi-node Redundancy）
- 

## **Q137：如何防止“账户被盗用（Account Takeover）”风险？**

示范答案：

- 2FA / MFA 强制
  - IP 地理位置异常 → 触发报警
  - 登录行为评分模型
  - 限制可疑设备登录
  - 夜间大额交易二次验证
  - 若怀疑被盗 → 冻结账户 + STR
- 

## **Q138：你们是否提供虚拟 IBAN？如何防风险？**

示范答案：

我们提供虚拟 IBAN，但：

- 仅用于入账，不支持匿名
  - 所有 IBAN 必须绑定 KYC/KYB 账户
  - 大额 IBAN 入账会自动触发 AML 检查
  - 受监管银行提供底层托管
- 

## **Q139：如何确保营销团队不会触发“误导性广告”？**

示范答案：

- 所有外宣材料由合规部审查
  - 禁止承诺回报/收益
  - 禁止夸大“安全性”
  - 要求对“风险”明确披露
  - 所有广告内容保留 5 年备查
- 

## **Q140：你们如何评估是否需要提交 STR？**

示范答案：

- 通过自动警示 + MLRO 人工确认
  - 若交易无商业逻辑 / 无法解释来源 → STR
  - 若客户态度回避 → STR
  - 若涉及高风险国家 → STR
  - MLRO 最终负责 STR 决策
- 

## **Q141：你们如何进行“客户风险重新评估（Periodic Review）”？**

示范答案：

- 低风险：12 个月
  - 中风险：6 个月
  - 高风险：3 个月
  - 企业客户根据行业风险进行额外审查
  - 重新评估包括：身份、交易模式、风险国家、业务变化等
- 

## **Q142：如果客户拒绝提供 SOF/SOW，你们将如何处理？**

示范答案：

- 立即暂停其账户
  - 拒绝所有交易
  - MLRO 审查交易历史
  - 若怀疑 → 直接 STR
  - 客户拒绝提供 → 视为 AML 风险过高
- 

## **Q143：系统如何识别可疑资金路径？**

示范答案：

- 识别循环交易（Round-Tripping）
- 多跳资金（Layering Patterns）
- 交易金额接近阈值
- 识别对倒交易
- 多账号互相对冲

异常 → 自动触发调查。

---

## **Q144：贵司如何对内部系统进行渗透测试（PenTest）？**

示范答案：

- 每年外部专业团队执行一次
  - 内部团队每季度执行扫描
  - 关键组件（API、支付网关）每半年测试
  - 所有漏洞分级管理（High/Critical 必须 30 天内修复）
- 

## **Q145：你们是否允许企业账户共享登录凭证？**

示范答案：

不允许。

系统强制唯一用户 + 2FA。

多人需访问 → 使用授权委托（Delegated Access）。

---

## **Q146：你们如何确认企业 UBO 信息真实性？**

示范答案：

- 与公司注册局交叉验证
  - 要求股权结构图 + 章程
  - UBO 的护照 + 住址验证
  - OSINT 搜索（负面新闻）
  - 非自然结构 → 深度 KYB
- 

## **Q147：你们如何确保系统不会被用于批量虚假账户？**

示范答案：

- 手机号 + 邮箱 + 设备指纹
  - 身份证 OCR 验证
  - 人脸识别（Liveness Check）
  - IP 与 GPS 匹配
  - 多个账户绑定同一设备 → 触发人工审查
- 

## **Q148：如何确保董事会理解 AML 责任？**

示范答案：

- 董事会每年接受 AML 培训（强制）
  - MLRO 每季度报告 AML/KYC 数据
  - 重大风险事件必须由董事会批准
  - 董事会对 AML 框架负最终责任（Documented）
- 

## **Q149：如果出现内部欺诈行为，你们如何处理？**

示范答案：

- 立即冻结相关权限
  - 内部调查小组启动（Compliance + Risk + HR）
  - 向监管机构报告
  - 若涉及刑事 → 报警
  - 加强控制措施防止再次发生
- 

## **Q150：监管面谈结束后，你们如何确保后续整改落实？**

示范答案：

- 成立整改工作组
  - 列出整改清单
  - 每项整改指派负责人
  - 每周向董事会汇报
  - 30/60/90 天提交整改状态给监管机构
  - 所有整改文件经过 MLRO 与 Compliance 签署
- 

## **Q151：你们如何管理“第三国（Non-EEA）客户风险”？**

示范答案：

对于 Non-EEA 客户，我们制定更严格政策：

- 所在国家必须非 FATF 高风险
  - 强制 SOF/SOW
  - 交易限额降低
  - 加强行为监控
  - 若涉及高风险行业（如加密、博彩），必须进行 EDD
  - 董事会需对第三国策略进行年度审查
- 

## **Q152：你们如何确保 AML 监控规则不被业务团队修改？**

示范答案：

- 所有 AML 规则由 MLRO 控制
  - 业务团队仅能提建议，不能更改
  - 系统权限严格隔离
  - 合规部审核后由 CTO 执行变更并记录审计日志
  - 重大修改需董事会批准
- 

## **Q153：你们如何判断交易是否存在“回流（Round-Tripping）”？**

示范答案：

- 识别资金从 A → B → A 的循环路径
  - 分析异常时间间隔与金额一致性
  - 行为模型判断是否为真实商业交易
  - 如无合理商业逻辑 → STR
- 

## **Q154：如果一个客户增速过快，你们如何处理？**

示范答案：

- 风险部门执行临时风险审查
  - 重新评估 KYC 信息
  - 检查流量来源是否真实
  - 将其移入更高风险等级
  - 触发更严格的交易监控规则
- 

## **Q155：你们如何控制“系统管理员（SysAdmin）滥用权限”风险？**

示范答案：

- 双人审批（4-eyes principle）
  - 所有高权限登录必须 MFA
  - 所有操作被日志记录并监控
  - 每季度由 CTO + 合规复核权限
  - 不允许单人执行敏感操作（如生产数据库改动）
- 

## **Q156：如何控制 API 集成方（Merchants / PSP）风险？**

示范答案：

- API Key 与 IP 白名单

- 必须完成 KYB 及技术测试
  - 限制初期交易量 (Sandbox + Pilot)
  - 异常速率或异常调用自动封锁
  - 合同强制可审计条款 (Audit Clause)
- 

## **Q157：你们如何处理无法解释的大额入账？**

示范答案：

- 立即暂停交易
- 要求客户提供 SOF 文件
- MLRO 审查后决定是否放行
- 若仍可疑 → STR 上报

所有调查过程必须记录并存档。

---

## **Q158：是否允许客户将 EMI 钱包用于储蓄或投资？**

示范答案：

不允许。

EMI 钱包不是存款行为，也不产生利息。

我们所有条款明确说明“非存款产品”。

---

## **Q159：你们如何评估客户生命周期中的风险变化？**

示范答案：

- 每次重大行为变化均触发风险重新评估
  - 包括交易金额变化、地理位置变化、业务模式变化等
  - 系统自动生成风险评分重新计算
  - MLRO 或合规进行人工二次评估
- 

## **Q160：如何处理交易模式突然改变的客户？**

示范答案：

- 启动行为监控审查
  - 与客户联系确认原因
  - 若解释不足 → 暂停账户
  - 若涉及可疑 → STR
  - 新模式必要时进行 EDD
- 

## **Q161：你们如何确保商户不从事“隐藏行业”(如博彩、加密)？**

示范答案：

- KYB 阶段收集行业证明、商业模式
  - 技术团队验证 API 调用行为
  - 定期审查交易结构
  - 发现异常行业交易 → 冻结 + 终止合作
  - 隐瞒商业模式强制 STR
- 

## **Q162：当监管要求进行信息披露，你们需要多久提交？**

**示范答案：**

在 24–48 小时内提交完整、准确文件。

所有资料存储在中央文档系统，随时可调取。

---

## **Q163：你们如何检测是否存在“批量伪造交易（Synthetic Transactions）”？**

**示范答案：**

- 检查连续序列数字、规律性金额
  - 检查短时间大量交易
  - 系统识别异常使用 API
  - 商户行为分析（MACD）
  - 若无真实商业流量 → Flag + 撤销开户
- 

## **Q164：你们如何确保不会发生“无监管跨境清算”？**

**示范答案：**

- 所有跨境清算必须通过受监管的 EMI 或银行
  - 不允许使用未监管 PSP
  - 合规每季度检查合作方牌照状态
  - 必要时要求对方提供监管证明
- 

## **Q165：是否允许未成年人使用 EMI 服务？**

**示范答案：**

不允许。

最低年龄 18 岁；否则需父母共同认证与限制功能。

---

## **Q166：对于政要（PEP），你们如何进行加强控制？**

**示范答案：**

- 强制 EDD
  - 核查资金来源
  - 每 3 个月重新审查
  - 单独行为监控规则
  - 所有 PEP 需 MLRO 审批
- 

## **Q167：你们如何识别企业客户的真实业务场景？**

**示范答案：**

- 审查合同、发票、网站、供应链资料
  - 审查公司银行账户交易记录
  - 若存在不一致 → KYB Red Flag
  - 必要时要求视频访谈或现场验证
- 

## **Q168：是否允许内部员工持有客户账户？**

**示范答案：**

允许但必须遵守：

- 员工 AML/KYC 不得自批

- 必须强制审核
  - 定期检查员工异常行为
  - 员工账户标记特殊标签，否则禁止
- 

## **Q169：你们如何处理来自“共享办公地址”的企业？**

示范答案：

- 共享办公室并非自动高风险
  - 必须提供实际经营证明
  - 如果公司无员工、无电话、无网站 → 高风险
  - 必要时要求提供租赁合同或物业确认
- 

## **Q170：软件代码变更如何避免引发监管风险？**

示范答案：

- 采用 Git 版本管理
  - 所有代码变更必须 Code Review
  - 敏感改动由 CTO + Compliance 双重批准
  - 完整 UAT 测试
  - 生产环境改动记录在案
- 

## **Q171：贵司是否允许代充值、代收款服务？**

示范答案：

不提供。

禁止代收代付、资金池模式、影子账户系统。

---

## **Q172：你们是否使用机器学习做 AML？优势是什么？**

示范答案：

- 辅助检测复杂行为模式
- 识别异常行为比规则更快速
- 降低误报率
- 所有 ML 模型由 MLRO 审查并定义边界

我们不会完全依赖自动模型，人工最终审核。

---

## **Q173：你们是否支持企业批量发薪？如何控制？**

示范答案：

允许但必须：

- 完整 KYB
  - 文件验证（雇佣合同、薪资单）
  - 交易总额限制
  - 每月提供工资清单
  - 异常交易触发 AML 检查
- 

## **Q174：如何保证合规部门在公司中“独立运作”？**

示范答案：

- 合规向董事会直接报告（非 CEO）
  - 预算单独执行
  - 有权独立阻断交易
  - 合规意见对所有产品具有否决权
  - 董事会对合规有 KPI，不由业务部门决定
- 

## Q175：你们如何管理设备指纹（Device Fingerprinting）？

示范答案：

- 记录设备 ID、OS、浏览器指纹
  - 检测多账户共享设备
  - 异常设备 → 触发强制验证
  - 设备风险评分纳入 AML 模型
- 

## Q176：你们是否进行“每日平均余额（Daglig saldo）”监控？

示范答案：

是。

每日对账包括：

- 总客户余额
  - Safeguarding 账户余额
  - 差异分析（tolerance 0）
  - 异常立即报告 CFO 和 MLRO
- 

## Q177：你们如何识别“地下钱庄模式”？

示范答案：

- 高频入账 → 多次小额出账
  - 多人共享账户
  - 非家庭成员互相转账
  - 多国汇入、单国汇出
  - 若符合三项 → 立即进行 AML 调查 + STR
- 

## Q178：你们的 KYC 系统如何检测假证件？

示范答案：

- OCR 对照数据模板
  - MRZ 校验
  - 真实身份证数据库比对（国家 API）
  - 光源检测（Liveness）
  - 视频反欺诈（Blink / Head turn）
- 

## Q179：你们如何确保所有 EMoney 发行都受余额限制？

示范答案：

- 用户钱包余额上限系统自动控制
- 无法超发
- 所有余额由银行托管账户支持

- 余额=托管金
  - 每日交易清算
- 

## Q180：公司如何管理跨国服务的税务风险？

示范答案：

- 不提供逃税、匿名金融服务
  - 审查客户是否合规申报
  - 与外部税务顾问合作
  - 若客户有可疑税务行为 → 触发 AML 程序
- 

## Q181：你们对加密货币相关企业有什么额外控制？

示范答案：

- 仅支持受监管交易所
  - 客户必须提供许可证
  - 禁止匿名钱包
  - 转账需要完整交易链路（Chain-of-Custody）
  - 使用链上分析工具（Chainalysis / TRM）
- 

## Q182：你们如何审查企业客户“资金用途说明”？

示范答案：

- 需要提供合同、发票、对账单
  - 核对资金流与业务模式是否一致
  - 必要时要求 Video Call 核实
  - 若无合理商业逻辑 → 拒绝
- 

## Q183：多少笔交易会触发 AML 强制审查？

示范答案：

- 基于阈值规则
- 金额触发（大额）
- 行为触发（频繁、跳跃、不合逻辑）
- 地域触发（高风险国家）

系统自动触发，无人工干预。

---

## Q184：你们如何进行“主管部门要求”的年度内部审查？

示范答案：

- Compliance 进行年度审查
  - Risk 与 ICT 部门提交自评
  - 董事会批准后提交给 Finanstilsynet
  - 由外部审计进行抽样验证
- 

## Q185：如何确保不发生“影子账户（Shadow Accounts）”？

示范答案：

- 不允许未完成 KYC 的账户进行交易
  - 内部系统禁止创建非正式子账户
  - 所有客户 ID 必须关联唯一身份
  - 定期审计账户结构
- 

## Q186：对交易频率异常的用户如何处理？

示范答案：

- 触发风险评估
  - 降低限额
  - 要求 SOF
  - 若回答模糊或回避 → STR
- 

## Q187：你们是否允许商户使用代理服务器？

示范答案：

不允许。

检测到代理 → 强制二次验证 + 限制访问。

---

## Q188：公司如何防止“运营团队绕过合规流程”？

示范答案：

- 业务流程自动化，无法手动跳过 KYC/AML
  - 权限分离
  - 合规拥有全流程 veto 权
  - 系统行为审计
  - 合规直接向董事会报告
- 

## Q189：你们如何管理“客户自我声明”风险？

示范答案：

- 客户声明必须提供证明文件
  - 声明不能替代验证
  - 声明与行为不一致 → 高风险
  - 必要时要求 Video KYC
- 

## Q190：如何监控“异常登录行为”？

示范答案：

- IP 地理位置判断
  - 登录频率
  - 异常时间访问
  - 设备指纹不一致
  - 多地同时登录 → 强制锁定
- 

## Q191：你们如何检查 API 交易的真实性？

示范答案：

- API Keys 有效期 / 限额
  - 签名验证
  - 请求速率 (Rate Limiting)
  - 崩溃测试
  - 异常行为 → 暂停 API
- 

## Q192：你们是否对“支付失败率”设限？

示范答案：

是。

失败率 > 5% → 系统自动报警

失败率 > 10% → 限制商户

---

## Q193：如何保证董事会能实时了解合规风险？

示范答案：

- 月度 AML 报告
  - 季度合规报告
  - 重大事件立即通知制度 (within 24h)
  - 董事会可随时调阅合规系统数据
- 

## Q194：你们如何监控客户是否在暗网活动？

示范答案：

- OSINT 检索
  - 外部情报供应商 (Cyber Threat Intelligence)
  - 若发现关联 → 立即 STR + 关闭账户
- 

## Q195：对外包客服如何进行 AML 控制？

示范答案：

- 客服不能做任何审批
  - 不可修改 KYC 数据
  - 所有客服行为记录
  - 复杂问题必须由 MLRO 处理
  - 外包方必须接受 AML 培训
- 

## Q196：你们如何监控商户是否“挪用客户资金”？

示范答案：

- 监控商户钱包余额
  - 与业务量比对
  - 检查是否提前提现
  - 商户账户透明化
  - 若异常 → 立即冻结 + 调查
- 

## Q197：如何判断清算银行是否符合监管要求？

示范答案：

- 必须在 EEA 监管
  - 必须受 PSD2 / EMD2 覆盖
  - 审查其资本充足率
  - 审查外部评级 (Fitch/Moody's)
  - 必要时进行现场访问
- 

## Q198：你们如何管理“多层股权结构”风险？

示范答案：

- 完整穿透 UBO
  - 要求每层股东提供公司证明
  - 审查资金来源
  - 若结构异常复杂 → 高风险
  - 多层离岸结构可能被拒绝
- 

## Q199：如何确保内部模型不被滥用？

示范答案：

- AML 模型由 MLRO 控制
  - 所有修改记录并可追踪
  - 定期验证模型有效性
  - 数据输入不可被人为修改
- 

## Q200：你们是否允许支付给非 KYC 已完成的对象？

示范答案：

不允许。

所有收款方必须通过银行体系或受监管支付机构。

---

## Q201：公司如何处理“突发性大额出金”？

示范答案：

- 必须进行 SOF 审查
  - MLRO 审批
  - 若解释不足 → 拒绝
  - 重大异常立即 STR
- 

## Q202：你们如何评估“客户行为画像”(Behavioral Profiles) ？

示范答案：

- 基于每日交易模式
  - 基于设备使用
  - 基于地理位置
  - 基于历史数据
  - 行为偏差触发 AML 规则
- 

## Q203：企业客户交易是否会触发商业模型验证？

示范答案：

是。

例如：

- 商户收入是否与行业相符
  - 是否存在“虚假开票”
  - 对账单与交易不符 → 高风险
- 

## **Q204：如何处理加密货币 OTC 商户？**

示范答案：

- 必须有监管牌照
  - 必须有链上分析工具
  - 禁止现金交易
  - 流水必须可追溯
  - 违反 → 立即终止合作
- 

## **Q205：如何检测团伙作案（Syndicated Fraud）？**

示范答案：

- 多账号同一设备连接
- 多个账户使用同一银行卡
- 相同 IP 登录
- 快速循环交易
- 交易模式一致

符合三项以上 → 立即封禁。

---

## **Q206：如何确保系统不产生“负余额”？**

示范答案：

- 所有交易先检查可用余额
  - 禁止预授权超额
  - 技术做风控限额
  - 若因技术错误 → 自动回滚 + 审计
- 

## **Q207：你们如何管控“高额充值 → 立即提现”行为？**

示范答案：

- 行为监控自动识别
  - 若持续发生 → AML 调查
  - 必要时 SOF
  - 若无商业理由 → STR
- 

## **Q208：你们如何确保 ICT 系统与业务流程一致？**

示范答案：

- ICT 与 Compliance 每周对齐会议
- 系统更新前需“合规审核”
- 设计文档（Design Doc）需合规部门签署

- 生产环境与流程文件一致性每季度检查
- 

## **Q209：对于“支付指令撤销”，你们如何处理？**

示范答案：

- 若资金尚未清算 → 可撤销
  - 若已清算 → 需双方确认
  - 所有撤销均由系统记录并经人工审批
  - 若存在欺诈 → MLRO 介入
- 

## **Q210：你们如何监控实时外汇交易（若提供 FX）？**

示范答案：

- 价格由独立报价商提供
  - FX 交易需 AML 检查
  - 大额 FX 交易需管理层批准
  - 定期压力测试外汇风险
- 

## **Q211：你们如何确认内部员工具备 AML 能力？**

示范答案：

- 每季度强制培训
  - 内部 AML 测验必须通过
  - MLRO 定期评估
  - 若不达标 → 调离关键岗位
- 

## **Q212：客户是否可代操作他人账户？**

示范答案：

不可以。

委托授权必须通过我们审核并附合法授权书。

---

## **Q213：如何检测“空跑交易”(No-Op Transactions)？**

示范答案：

- 系统分析无资金变化的交易
  - 高频 No-Op 行为 → 高风险
  - 若无合理原因 → 阻断 + 调查
- 

## **Q214：如何控制“支付链路过长”风险？**

示范答案：

- 交易中不允许超过 2 层中转
  - 中转机构必须受监管
  - 对链路透明度进行检查
  - 复杂链路 → 立刻 EDD
- 

## **Q215：你们如何处理由第三方代缴费用？**

示范答案：

- 所有第三方付款都需验证商业逻辑
  - 必须提供合同或说明
  - 若无法解释 → 拒绝
  - 若涉及欺诈 → STR
- 

## Q216：如何确保 AML 系统阈值不过低导致漏报？

示范答案：

- 由 MLRO 每季度检查模型敏感度
  - 外部校验（Independent Validation）每年执行
  - 每次风险事件审查是否因阈值太低
  - 董事会审查 AML 模型有效性
- 

## Q217：你们如何阻断“多跳转账模式”(Layering) ？

示范答案：

- 检查连续跳转目的地
  - 识别超过三跳的交易
  - 若存在复杂路径 → 强制审查
  - 必要时冻结账户
- 

## Q218：公司如何识别“借用账户”行为？

示范答案：

- 登录设备变化
  - GPS/IP 与注册信息不一致
  - 交易模式不符合用户特征
  - 若有借用嫌疑 → 暂停账户 + 验证
- 

## Q219：你们是否允许“无 KYC 限制卡”服务？

示范答案：

不允许。

所有卡均需完成 KYC 后才能启用。

---

## Q220：监管面谈结束后，如需二次面谈，你们如何准备？

示范答案：

- 整理第一次面谈所有问题与监管关注点
- 更新内部风险报告
- 准备更多证据与文档
- 董事会、MLRO、CTO 全体参与
- 所有回答保持一致、准确、可验证

如有需要，仁港永胜团队可以有偿协助编制 二次面谈合规说明包（Second Interview Compliance Pack）。

---

## 第二十五部分 | 关于仁港永胜 – 合规服务提供商，合规咨询与全球金融服务专家

仁港永胜（香港）有限公司在香港、内地及全球多个国家和地区设有专业的合规团队，为金融机构、投资者及企业提供全方位的合规咨询解决方案，包括但不限于：

- 协助申请各类金融牌照：
  - 香港 **MSO / 放债人牌 / SFC 1/4/9 / 虚拟资产牌照**
  - 欧盟各国 **EMI / PI / CASP** (含挪威、葡萄牙、立陶宛、马耳他等)
  - 新加坡 **MPI / 资本市场服务牌照**
  - 迪拜 / 阿联酋 **DFSA / VARA** 等牌照
- 制定符合监管要求的政策与程序 (Policy Suite)；
- 提供季度 / 年度合规审查与监管报告支持；
- 设计跨境合规结构与资金流路径；
- 提供 **IT + 合规一体化解决方案** (系统 + 制度 + 流程图)。

我们致力于与客户建立长期战略合作伙伴关系，帮助客户在复杂多变的监管环境中稳健合规、可持续增长。

如需进一步协助，包括 **挪威 EMI 申请 / 收购、合规指导及后续维护服务**，欢迎随时联系：

- 官网：[www.jrp-hk.com](http://www.jrp-hk.com)
- 手机（深圳 / 微信同号）：**15920002080**
- 手机（香港 / WhatsApp）：**852-92984213**
- 点击这里可以下载PDF文件：[关于仁港永胜](#)

办公地址：

- 深圳福田：深圳福田区卓越世纪中心 1 号楼 11 楼
- 香港湾仔：香港湾仔轩尼诗道 253–261 号依时商业大厦 18 楼
- 香港九龙：香港特别行政区西九龙柯士甸道西 1 号 香港环球贸易广场 86 楼

注：本文中的模板或电子档可以向[仁港永胜](#)唐生有偿索取。[手机:15920002080 (深圳/微信同号) 852-92984213 (Hongkong/WhatsApp) 索取电子档]

## 第二十六部分 | 结语：挪威 EMI 的定位与建议

通过本指南你可以清晰看到：

- 挪威 EMI 是高声誉、高监管、高信用背书的北欧持牌路径
- 虽非快速拿牌，但非常适合长期布局金融科技和欧洲支付业务
- 最大优势是护照机制 + 北欧声誉高 + 合规友好

若你准备：

- ✓ 打通 亚洲—欧洲 支付链路
- ✓ 搭建 Wallet/清算体系
- ✓ 建立北欧区总部

挪威 EMI 是一条极具价值的路径，非常欢迎把 **挪威 EMI** 作为重点选项之一，并与仁港永胜团队沟通可执行方案。