



仁港永胜

协助金融牌照申请及银行开户一站式服务



正直诚信
恪守信用

网址: www.CNJR.com 手机: 15920002080 地址: 香港环球贸易广场86楼 852 92984213 (WhatsApp)

波兰 Poland (MiCA) 加密资产服务提供商 (CASP) 牌照 申请注册指南

Poland (MiCA) Crypto Asset Service Provider (CASP) License Registration Guide

本文由 仁港永胜 (香港) 有限公司 拟定, 并由 唐生 (Tang Shangyong) 提供专业讲解。

适用对象: 拟以波兰为 MiCA 申请国 (Home Member State), 申请并运营 **CASP (Crypto-Asset Service Provider)**, 并通过 **MiCA 护照机制**向全欧盟跨境展业的机构。

法律底座: MiCA (EU 2023/1114) 统一授权与持续监管框架。

交付提示 (PDF/附件索取): 本指南由仁港永胜唐生拟定讲解, 可提供可编辑的 **Master Checklist (A-I)**、BP 模板、AML 手册、ICT/DORA 外包治理制度、RFI (补件) 应答包、面谈题库与“护照通报包”等 (可向仁港永胜唐生有偿索取)。

✅ 点击这里可以下载 PDF 文件: [波兰 Poland \(MiCA\) 加密资产服务提供商 \(CASP\) 牌照申请注册指南](#)

✅ 点击这里可以下载 PDF 文件: [MiCA 的实践: 缺乏国家法规阻碍在波兰获得 CASP 授权](#)

✅ 点击这里可以下载 PDF 文件: [关于仁港永胜](#)

1) 牌照名称

- 牌照名称: MiCA 体系下 **Crypto-Asset Service Provider (CASP)** 授权 (以波兰为申请地/主管机关)。
- 主管机关 (拟): 波兰拟制定的《加密资产市场法》草案中明确由 **Komisja Nadzoru Finansowego (KNF, 波兰金融监管局)** 承担加密资产市场监管与监督框架。
- 文档定位: 以“可递交、可审计、可补件”为写作标准, 直接对齐 MiCA、ESMA 技术标准 (RTS/ITS)、DORA 与波兰本地 AML 义务。
- 服务商: 仁港永胜 (香港) 有限公司 | Rengangyongsheng (Hong Kong) Limited

2) 牌照介绍与申请优势 (MiCA 统一框架 + 波兰优势)

2.1 MiCA 统一框架的核心价值

- 单一授权 + 欧盟护照 (passporting): 在一个成员国获批后, 可通过跨境通报向其他成员国提供服务 (自由提供服务/设分支)。
- 统一行为规范: 客户保护、利益冲突、信息披露、治理与关键岗位、审慎保障、外包治理、记录保存与报告制度等以欧盟规则统一。
- 与 Travel Rule 并行: 加密资产转账信息规则由 (EU 2023/1113) 确立, 尤其涉及转账业务/托管/平台对接时应同步落地数据字段与流程。

2.2 选择波兰作为申请地的常见“策略理由”(实操视角)

- 监管框架正在成型: 波兰政府持续推进 MiCA 本地实施立法 (《加密资产市场法》草案体系), 明确监管架构与职责方向。
- 成本与团队配置友好: 中东欧人才与运营成本相对更可控 (适合做“欧盟合规中台/技术与合规运营中心”)。
- 面向欧盟全域扩张: 以波兰获批后, 护照通报可覆盖主要欧盟市场 (但“营销与消费者保护”仍需按落地国补充合规)。

3) 监管机构与适用法律 (NCA + 本国实施法/监管公告 + MiCA 主法)

3.1 欧盟层面 (主法 + 关键配套)

- **MiCA: Regulation (EU) 2023/1114** (CASP 授权、持续义务、客户保护与治理核心来源)。
- **DORA: Regulation (EU) 2022/2554** (ICT 风险管理、外包第三方风险、韧性测试、事件管理; 自 2025-01-17 起适用)。
- **Transfer of Funds / Crypto Travel Rule: (EU) 2023/1113** (加密资产转账信息随行规则)。

- **AMLA: Regulation (EU) 2024/1620**（欧盟反洗钱管理局设立，推动 AML 监管趋同与更高执行标准）。
- **DAC8: Directive (EU) 2023/2226**（加密资产税务信息交换/报告框架，倒逼客户税务信息与交易数据治理）。

3.2 波兰层面（本地实施与 AML）

- 波兰《加密资产市场法》草案体系（用于承接 MiCA 的本地监管安排、处罚与程序等；监管架构指向 KNF）。
- 波兰 AML 主管/FIU: **GIIF (General Inspector of Financial Information)**，属于财政部体系下的金融情报单位/主管机关之一（涉及 STR、信息报送、检查等）。

4) 申请条件概览（公司实体、实质经营、资本/保障、治理、业务模型、技术安全、客户保护、护照、第三国边界）

监管的底层逻辑：“你是谁（股东/人）—你做什么（服务范围）—你怎么做（流程/系统/外包）—你是否能持续做（资本/保障/资源）—客户是否被保护”。

4.1 公司实体与实质经营（Substance）

- 在欧盟内设立法人实体并实现**有效管理地**（董事会决策、关键岗位履职、关键系统与外包治理可被监管触达与审计）。
- 建议配置：波兰本地办公地址 + 本地/欧盟常驻的合规与管理职责（可远程团队，但必须“可审计、可到场、可解释”）。

4.2 资本/审慎保障（Prudential safeguards）

- 按 MiCA 对应服务类型，提交资本与/或保险等效保障安排、三年财务预测、压力测试、运营风险覆盖逻辑。

4.3 治理与关键岗位

- 董事/高管适任性（Fit & Proper）、冲突管理、三道防线、合规与 AML 职能独立汇报线、内审机制（可外包但需独立与审计权）。

4.4 技术安全与外包（DORA 强关联）

- ICT 风险管理、外包第三方治理、事件响应、韧性测试/演练、BCP/DR、日志可追溯等应直接对齐 DORA。

4.5 客户保护与跨境护照

- 资产隔离、披露透明、投诉处理、利益冲突、适当性/适配性（视服务类型）必须制度化并可证明运行。
- 护照：获批后通报目标国；落地国消费者保护/营销规则仍需补充。

4.6 第三国客户招揽边界

- 需管控第三国营销、制裁、数据跨境、旅行规则对接、当地“反向招揽/主动提供服务”边界（建议出具《第三国招揽合规备忘录》）。

5) 申请流程与时序安排（Pre-app → 提交 → 完整性审查 → RFI/面谈 → 批准 → 上线）

强烈建议走 **Pre-Application**：先把监管最关心的“四件套”做成闭环：运营方案（PoO）+ 审慎保障 + 治理适任性 + ICT/AML。

Step 0 | 立项与差距评估（Week 1–2）

- 服务范围定稿（MiCA 服务清单映射）
- 结构/人/制度/系统/外包差距评估
- 输出：差距清单 + 里程碑计划 + 预算表

Step 1 | Pre-Application 沟通（Week 2–4）

- 与监管沟通材料结构、关键外包披露口径、拟定补件机制

Step 2 | 正式递交（Week 8–12）

- 以 A-I 索引递交申请包（可审计编号体系）

Step 3 | 完整性审查（Completeness check）

- 常见卡点：股东 SoF/SoW 不闭环、关键岗位不匹配、ICT/外包不可审计、AML 规则与系统脱节

Step 4 | 实质审查 + RFI/面谈 (RFI War-Room)

- 建议建立“补件战情室”：合规+法务+技术+运营四线联动

Step 5 | 批准与上线 (Go-Live)

- 注资/保险到位、系统验收、关键岗位任命、培训与演练证据、客户条款上线
- 启动护照通报

6) 所需材料清单 (Master Checklist) A–I 分类 (交付版)

目标：做成“可递交、可审计、可补件”的索引体系（每份文件：编号、版本、责任人、证据来源、更新频率）。

A. 公司设立与法定文件

- 注册证书/章程/注册地址/股东与董事名册
- 董事会章程、授权矩阵 (DoA)、三道防线框架
- 实质经营证据：办公租约、组织架构、会议纪要模板、关键决策留痕机制

B. 股东/UBO/重大持股包

- 股权穿透结构图（至自然人 UBO）
- SoF/SoW 说明与证据链（银行流水、审计报告、资产处置、分红、薪酬等）
- 不利信息检索与解释备忘录、制裁/PEP 自查、关联方披露
- 控制权说明信（投票权/协议控制/可转债期权等）

C. 董事/高管 Fit & Proper

- 监管版 CV、学历/资格、任职证明、推荐信
- 无犯罪/诚信声明、时间投入声明、利益冲突声明
- 技能矩阵 (Skill Matrix)、董事会 KPI、继任与替补计划

D. 控制职能 (合规/MLRO/风险/内审/ICT)

- 任命函 + JD + 汇报线独立性说明
- 年度合规计划、AML 年度计划、内审计划、风险偏好与 KRI/KPI
- STR 决策记录模板、监控处置工单、整改跟踪机制

E. Programme of Operations + Business Plan

- 服务范围逐项对齐 MiCA；客户旅程流程图（开户→交易→提币→投诉→关户）
- 三年财务预测 (P/L、BS、CF) + 压力测试
- 审慎保障方案（资本/保险/风险覆盖逻辑）
- 费用表、营销审批机制、外包清单与依赖评估
- 退出/关停计划 (Wind-down Plan)

F. AML/CFT/CPF 制度包 (波兰 AML + 欧盟趋势)

- 企业级 AML 政策、风险评估方法论、CDD/EDD、制裁/PEP
- 交易监控规则库 + 链上分析策略 + STR 决策树与提交流程
- 记录保存、培训、独立审查、外包 AML 监督机制
- Travel Rule 字段与流程对接（如提供转账/托管/平台对接）

G. ICT/钱包/安全 (DORA)

- 架构图/数据流/敏感数据分类、RBAC、MFA、密钥管理 (HSM/分片)、多签与签名仪式
- 冷热钱包策略、对账与审计轨迹、日志不可篡改

- 渗透测试/漏洞管理、BCP/DR (RTO/RPO)、事件响应与取证
- 外包/云：尽调、SLA、审计权、退出迁移 (DORA 第三方风险)

H. 客户条款/披露/投诉

- 客户协议 (T&C)、风险披露、费用披露、资产隔离说明
- 投诉机制 (时限/升级/复盘)、利益冲突政策、适当性/适配性 (如适用)
- GDPR 隐私政策、DPA、数据主体权利流程

I. 申报声明/费用/项目管理

- 申请表、附件目录、董事会决议、授权书 (PoA)
- RFI 应答模板、监管 Q&A Log、里程碑甘特图、RACI、Issue Log
- 年审/报告日历、持续合规证据归档规则

7) 董事/股东/UBO 要求 (10%/重大持股、声誉、资金来源、穿透、持续通知)

7.1 关键定义与触发门槛 (必须先统一口径)

(1) “重大持股/合格持股 (Qualifying holding)” = 10% 起算

MiCA 明确定义：在 CASP 的直接或间接持股达到至少10%资本或表决权即构成 qualifying holding (并引用欧盟关于表决权计算的规则)。

(2) “重大持股变更”的监管触发线 (拟收购/增持 & 拟减持/处置)

任何拟收购/增持 qualifying holding，若将达到或超过20%/30%/50%或形成子公司关系，须向主管机关书面通知；拟处置/减持亦需通知，尤其当持股将降至低于10%/20%/30%/50%等阈值时。

交付提示：在波兰项目里，建议把股权结构设计、章程条款、股东协议里的“通知义务/先决条件/过户限制”直接对齐这些触发线，避免后期“交易完成了但没报备”导致重大合规瑕疵。

7.2 监管的“适当人选 (Fit & Proper)” 框架 (适用于：股东/董事/关键岗位)

MiCA 对 CASP 的治理要求明确：

- 管理层/董事 (management body) 应具备良好声誉、知识技能经验、能够投入足够时间履职；
- 持有 qualifying holding 的股东/成员须具备“足够良好声誉”，尤其不得有洗钱/恐怖融资等相关犯罪定罪记录；
- 主管机关如认为大股东影响可能损害机构“稳健审慎经营”，可采取措施 (包括限制表决权等)。

同时，MiCA 要求 ESMA/EBA 发布“适当人选评估指引”，并已形成联合指引，覆盖管理层与关键岗位的能力与诚信维度。

7.3 股东/UBO 合规包 (SoF/SoW/穿透闭环) —— 最高频补件点

监管的真实关注点通常不是“你是谁”，而是：**你怎么赚到钱、钱从哪里来、是否可核验、是否与业务风险匹配**。建议按以下“可审计闭环”交付：

A | UBO 穿透与控制证明 (必须做到自然人终点)

- 全套集团结构图 (含持股比例、投票权、控制链条、最终自然人UBO)；
- 注册证书/章程/股东名册/董事名册 (每层实体)；
- 受托持股/代持/投票委托/一致行动协议 (如有必须披露并解释)。

B | 资金来源 SoF (Source of Funds) 与财富来源 SoW (Source of Wealth)

- SoW：收入路径 (经营利润/股权退出/分红/薪酬/房产处置/投资收益等) + 证明材料；
- SoF：本次出资/增资/收购款的**银行流水链** (账户→账户→入资账户) + 换汇路径 (如涉及) + 交易对手尽调；
- 资金“洁净证明”：税单/审计报表/对账单/股权交易文件/公证 (视风险等级)。

C | 声誉与合规记录 (Reputation pack)

- 无犯罪记录/诉讼与破产记录声明；
- 监管处罚/行政处分披露 (如有需解释整改)；
- 媒体负面筛查报告 (含制裁、PEP、Adverse Media)。

唐生实务建议：把 SoF/SoW 做成“证据索引表（Evidence Index）”，每条结论都能回指到具体文件页码/流水日期/交易编号，提升一次过审概率。

7.4 董事/管理层（Management Body）要求——“能力 + 时间 + 治理独立性”

MiCA 对管理层的核心要求（监管面谈也会围绕它问）：

1. **专业能力（Knowledge/Skills/Experience）**：加密资产业务、金融风控、ICT安全、AML/CFT、客户保护等；
2. **良好声誉（Good repute）**：无影响声誉的定罪/重大违规；
3. **时间投入（Time commitment）**：兼职过多/跨境多任职需解释如何保证履职；
4. **治理结构有效**：职责分工、决策机制、冲突管理、委员会设置（风险/审计/合规）等应可落地。

建议交付的董事/高管 Fit & Proper 套件（可直接递交）

- 履历（突出相关经验与监管理解）；
- 资格证明（证书/培训/以往项目）；
- 利益冲突声明、关联交易声明；
- 面谈问答包（业务模式/收费/客户资产隔离/钱包治理/外包/STR决策）。

7.5 持续通知与变更报备（股东/董事/UBO 的“持续义务”）

触发场景（建议在内部制度写死）

- 股权结构变化触及 10%/20%/30%/50% 阈值或控制权变化；
- 新增/更换董事、关键岗位、UBO；
- 重大负面事件：刑事调查、制裁命中、破产、重大诉讼、重大税务争议；
- 一致行动关系/代持安排变化。

内部控制做法（交付版）

- “股权与控制变更SOP” + 法务门禁（未完成报备/评估不得过户）；
- 季度股权核对（cap table + voting rights recon）与 UBO 重新确认；
- 负面新闻与制裁名单持续监控（含股东/董事/关键员工）。

8）合规/MLRO/关键岗位要求（资历、独立性、资源、汇报线、外包可否）

8.1 关键岗位清单（监管通常按“控制职能 Key Functions”审视）

建议按“最小可行 + 可扩展”组织架构准备，至少覆盖：

- 合规负责人（Compliance Officer / Head of Compliance）
 - MLRO（反洗钱报告负责人）/AML负责人
 - 风险管理负责人（Risk Management）
 - 内审负责人（Internal Audit）（可外包，但需独立与审计计划）
 - ICT/信息安全负责人（CISO/ICT Security Officer）
 - 数据保护（DPO，如触发GDPR强制情形）
- 上述岗位的能力要求与评估口径，会被纳入 ESMA/EBA 适当人选联合指引的框架内审视（知识、经验、诚信、独立性、时间投入）。

8.2 “适当人选”具体到合规/MLRO：什么条件下算合格？

下面给出可直接写入申请材料与岗位说明书（JD）的“合格判定标准”。

A | 合规负责人（Head of Compliance）——合格判定标准

硬条件（建议）

- ≥5年（或同等强度）金融合规/监管事务经验；有虚拟资产、支付、证券或银行合规更佳；
- 熟悉 MiCA 下 CASP 义务链：客户披露、利益冲突、治理、外包、客户资产保护、投诉处理等；

- 具备制度落地经验：合规监测计划、抽样检查、RFI回复、整改闭环；
- 能与董事会/管理层有效沟通，能解释风险取舍。

独立性与资源

- 汇报线：**可直接向董事会或董事会委员会升级**；
- 不应由“营收/销售负责人”兼任；如小团队兼任必须写明防火墙（审批权、否决权、升级路径）。

证据化交付（监管喜欢看）

- 年度合规计划（含主题、频率、抽样方法、输出物）；
- 合规培训计划 + 记录模板；
- 重大事件通报机制（Incident escalation）；
- 合规KPI与问责机制（Management accountability）。

B | MLRO（AML负责人）——合格判定标准

硬条件（建议）

- 反洗钱/制裁/交易监测/STR（可疑交易报告）实务经验；
- 熟悉虚拟资产 AML 风险：链上/链下资金流、混币/隐私币、跨境制裁规避、OTC与高风险通道；
- 能主导 AML 制度体系：客户风险评级、EDD、PEP/制裁筛查、交易监测规则、STR 决策与留痕。

独立性

- MLRO 需具备**独立提交 STR/内部升级**的权力；
- 交易监测团队可在运营线，但 MLRO 对规则与阈值拥有最终治理权。

证据化交付

- STR 决策树（Decision Tree）+ 会议纪要/审批日志模板；
- 模型/规则变更管理（Model governance）；
- 名单筛查（Sanctions/PEP）命中处置SOP；
- 交易监测有效性评估报告（Alert-to-STR 转化、误报率、回溯测试）。

注意：MiCA 对股东和管理层“不得有洗钱/恐怖融资相关定罪”的要求非常明确，AML岗位的“能否有效运作”往往会反向影响管理层适当人选评估与整体通过率。

8.3 汇报线、授权边界与“三道防线”（写给监管看的版本）

建议在 PoO/治理章节写清楚：

- **第一道防线（业务/运营）**：客户准入、交易执行、客户沟通；
- **第二道防线（合规/风险/MLRO）**：规则制定、监控抽查、否决与升级、STR决策；
- **第三道防线（内审）**：独立评估、审计计划、整改追踪。

并明确：

- 合规与 MLRO 的**否决权**（对高风险客户、产品、外包、营销）；
- 重大风险事项可**直达董事会**的升级路径；
- 资源配置（人数、系统、预算）与外包边界。

8.4 外包可否（尤其合规/内审/ICT）——可外包，但必须“可控、可审计、可退出”

MiCA 允许合理外包，但监管核心问题永远是：

1. 你是否保留**最终责任**；
2. 你是否能做到**审计权/监督权/数据与安全控制/分包控制**；
3. 你是否有**退出与迁移计划（Exit plan）**。

交付建议：把“外包尽调清单 + 合同条款库 + 退出迁移方案”作为申请附件，能显著降低补件。

8.5 “关键岗位适当人选” 联合指引的实务对齐（建议写入自评报告）

ESMA/EBA 联合指引对“管理层与关键岗位”的适当性评估，通常会落到四类证据：

- **诚信/声誉**（犯罪/处罚/失信/利益冲突）；
- **能力与经验**（含金融、加密、AML、ICT安全等知识结构）；
- **独立性**（是否受业务线不当影响）；
- **时间投入与有效履职**（是否有足够时间与资源）。

仁港永胜建议

1. 先把股东/UBO SoF/SoW 做成“闭环证据链”：这是欧洲CASP申请里最高频补件项。
2. 把合规/MLRO做成“可审计的运营系统”而不是“纸面制度”：从第一天就留存培训、抽查、演练、STR决策记录。
3. 治理与外包一次性对齐（含ICT安全与退出机制）：避免拿到牌后再“二次大改”成本爆炸。

选择仁港永胜的好处与服务优势

- **一体化交付**：股东UBO证据仓库（SoF/SoW）+ Fit&Proper 套件 + 合规/MLRO制度与证据化运行包，一次性成体系。
- **强模板库**：重大持股申报包、董事/关键岗位面谈题库、外包尽调清单、利益冲突与治理文件包、RFI应答包。
- **实操导向**：以“可递交、可审计、可补件”的索引化方式组织材料，提高审查效率与通过率。
- **合规服务**：选择一间专业专注的合规服务商协助牌照申请及后续维护及合规指导尤为重要，在此推荐选择仁港永胜。

9) ICT/钱包/安全与外包要求（冷热钱包、多签、权限、渗透测试、BCP/DR、DORA 关联）

9.1 钱包与密钥（监管最敏感）

- 冷/热钱包分层：热钱包限额 + 自动风控 + 异常冻结
- 多签门限（M-of-N）与“签名仪式”留痕（双人复核、关键人分离、强制休假/轮岗）
- HSM/分片/密钥轮换、应急密钥恢复流程（含审批与取证）

9.2 权限与日志可审计

- RBAC 最小权限、关键操作四眼原则
- 日志不可篡改、可检索、留存期与导出机制（满足审计与监管抽查）

9.3 安全测试与韧性

- 渗透测试 + 漏洞管理闭环（发现—分级—修复—复测—归档）
- BCP/DR：RTO/RPO、演练记录、灾备地点、恢复步骤、通讯机制

9.4 外包/云（DORA 强化）

- 外包登记册、关键外包识别、供应商尽调
- SLA/KPI、审计权、数据所在地、分包控制、退出迁移计划（Exit Plan）
- ICT 事件管理、分级、通报与复盘（DORA 框架）。

10) 客户保护机制（资产隔离、费用披露、投诉、利益冲突、适当性/适配性）

10.1 客户资产隔离与对账

- 客户资产与自有资产隔离（账务/钱包地址/权限）
- 日/周/月对账机制 + 异常差异处置工单
- 托管类业务：资产证明（Proof of Reserves）与审计协作机制（建议）

10.2 信息披露与费用透明

- 费用清单：交易费、点差、提币费、托管费、第三方费用、潜在返佣/做市安排
- 风险披露：价格波动、链上不可逆、第三方风险、系统中断、制裁冻结等

10.3 投诉与争议解决

- 投诉渠道、时限、升级机制、复盘与整改闭环
- 争议解决条款：司法管辖、适用法律、证据留存

10.4 利益冲突与市场秩序（平台/撮合/做市）

- 利益冲突政策、关联交易审批、员工交易/内幕信息控制
- 市场滥用监控（刷量/操纵）规则与处置流程

10.5 适当性/适配性（视服务类型）

- 若涉及投顾/组合管理/复杂产品分销：建立问卷、评分、分级限制、记录留存。

11）官方收费与预算（政府费/监管年费/审计/法律/技术/保险/人员）

官方费用在波兰最终实施细则/收费表出台前，应以 KNF 与波兰《加密资产市场法》最终文本为准。（本节给出“预算科目与建模方法”，用于你们做对外报价与内部预算控制。）

11.1 政府/监管相关

- 申请费/年费/变更报备费：以最终法规与 KNF 公告为准（建议在预算中预留“监管费用缓冲金”）。

11.2 强制/高概率发生的专业成本

- 法律顾问（公司法、金融监管、合同/GDPR、外包条款）
- 审计与会计（年度审计、独立 AML 审查/内审、PoR 协作）
- AML 工具：制裁/PEP、交易监控、链上分析、案例管理系统
- ICT：渗透测试、SOC/监控、HSM/密钥管理、灾备、日志与 SIEM
- 保险或等效保障（与审慎保障方案相关）
- 人员：合规/MLRO/风险/ICT 安全/内审/客服/运营
- 办公与本地化：办公室、雇佣、薪税与社保、董事会运作成本

12）后续维护与续牌/持续合规（报告、审计、变更报备、培训、演练）

MiCA 是“持续监管”体系：拿牌只是开始，关键在“持续满足 + 可证明运行”。

12.1 持续合规四件套（建议固定为年度循环）

1. 年度合规计划（合规监控、抽查、整改）
2. 年度 AML 计划（风险评估更新、规则校准、STR 复盘、培训）
3. 年度 ICT 韧性计划（DORA）（演练、渗透测试、第三方评估、事件复盘）
4. 年度内审/独立审查（可外包但必须独立）

12.2 报告与记录（建议建立“证据仓库 Evidence Vault”）

- 董事会/合规/风险/IT 会议纪要与决议
- 客户投诉台账、KYC 抽查记录、监控报警处置记录、STR 决策记录
- 外包登记册、供应商评估报告、SLA 达标报告、退出演练记录
- 事件响应记录、取证材料、整改验证报告

12.3 重大变更报备（Change Management）

- 股权/UBO、董事与关键岗位、服务范围、关键外包、核心系统、费用结构、客户条款重大变动
- 标准流程：变更评估→风险与合规意见→必要时预沟通→实施→验收→归档

13) 办理时间预估（公司设立、文件编制、审查窗口、缓冲）

以下为“项目管理口径”时间模型；实际取决于：监管窗口、补件轮次、股东资金来源闭环质量、系统与外包复杂度。

- 公司设立与实质搭建：**2–6 周**
- 文件编制（BP/PoO/AML/ICT/合同披露/股东与适任性包）：**6–12 周**
- 递交后完整性审查 + RFI：**取决于补件轮次（建议预留 8–16 周缓冲）**
- 获批前条件落实与上线验收：**4–8 周**
- 护照通报与跨境上线：**2–6 周/国家**（视目标国要求与营销合规准备）

14) 常见问题（FAQ）（Q1–Q200）—波兰版

波兰 Poland（MiCA）加密资产服务提供商（CASP）牌照常见问题（FAQ 大全）

模块结构：

A 牌照与范围 | B 实体与实质 | C 股东/UBO | D 董事适任性 | E 资本/保障 | F AML/制裁/STR | G ICT/DORA/外包 | H 客户保护 | I 护照与跨境 | J 运营与持续合规

本文由 **仁港永胜（香港）有限公司** 拟定，并由 **唐生（Tang Shangyong）** 提供专业讲解。

A | 牌照与范围（Q1–Q20）

Q1: MiCA 下 CASP 牌照是什么？在波兰获批后意味着什么？

A: CASP 是欧盟统一框架下的“加密资产服务提供商”授权。获批后，你在波兰成为受监管实体，可在获授权服务范围内向客户提供 MiCA 列举的加密资产服务，并在满足护照程序后扩展到其他欧盟/欧洲经济区市场。重点是：**服务范围“以授权为准”**，不能用“我们是加密公司”泛化替代具体服务类别。

Q2: CASP 能覆盖哪些服务？是否“一个牌照通吃交易所+托管+经纪+撮合”？

A: MiCA 将服务拆分为多个类别（例如：托管与管理、交易平台运营、兑换法币/加密、兑换加密/加密、执行订单、接收与传递订单、提供建议、投资组合管理、转移服务等）。可以多项同时申请，但监管会看：

- 你是否具备对应的**系统能力、风控能力、人员能力**；
- 业务是否存在**利益冲突与隔离机制**；
- 同时申请会提高审查深度与材料体量。并非“一次申请越多越好”。

Q3: 我们做 OTC（场外）算哪类服务？

A: 通常落在“加密资产兑换服务”（法币↔加密、加密↔加密）和/或“执行订单/接收传递订单”。如果你以自营对手盘报价、赚取点差，监管会重点问：

- 定价机制与披露；
 - 对手盘风险与库存风险；
 - 客户是否理解你是“做市/自营对手方”。
- 若你只是撮合第三方，可能涉及“订单接收与传递/执行”或“平台运营”性质（视交易组织方式而定）。

Q4: 我们只做“钱包”算 CASP 吗？

A: 若提供托管钱包（你掌握私钥或可影响客户资产转移），通常属于“托管与管理”。若是纯非托管软件（客户自持私钥、你不接触资产），可能不构成该项服务，但仍可能触发其他监管（营销、数据安全、消费者保护等）。监管会以**实际控制权**判断，而不是你自称“非托管”。

Q5: 做“交易平台”与做“经纪/兑换”在监管上差别在哪里？

A: 平台运营的关键在于：

- 交易规则与市场秩序（撮合、挂单、撤单、异常处理）；
 - 市场滥用防控（操纵、刷量、抢跑等）；
 - 透明度与披露（撮合优先级、费用、冲突）；
 - 系统韧性、容量、灾备。
- 经纪/兑换更强调：报价透明、客户适当性、执行质量、库存与对手风险、投诉与纠纷处理。

Q6: CASP 能否经营“稳定币”？

A: 能否经营取决于你提供的服务类别以及稳定币本身是否合规（例如符合 MiCA 下 ART/EMT 的发行与流通要求）。监管会要求你对：

- 稳定币合规属性与风险；
- 赎回、流动性、脱锚风险披露；
- 交易与托管的操作控制
建立清晰制度。很多项目卡在“把不合规稳定币当作普通币”处理。

Q7: CASP 是否等同于 VASP (FATF 口径) ?

A: 概念有交集但不等同。VASP 是国际反洗钱框架用语；CASP 是 MiCA 的监管授权主体。你作为 CASP，仍必须满足 AML 法项下义务（通常会被视为 AML 义务主体），并在 Travel Rule、制裁、STR 等方面满足要求。

Q8: 我们可否先申请最小范围（例如仅兑换），后续再扩项？

A: 可以，且是常见策略。优点：缩小审查面、降低首次材料与系统复杂度；缺点：未来扩项仍需“重大变更/再授权”流程，需再做系统与制度升级、可能触发再审。建议用“三阶段路线图”写进 PoO：**首期可监管落地、二期扩项、三期跨境护照。**

Q9: 广告宣传能否写“欧盟牌照/全欧通行”？

A: 宣传必须准确、可核验。通常需要：

- 清晰写明授权国家、授权主体名称；
- 列明授权服务范围（不夸大）；
- 披露关键风险。
“全欧通行”应表述为“可依法定程序申请跨境护照提供服务”，并且在护照未完成前不得暗示已在他国被允许展业。

Q10: CASP 是否能帮我们开银行账户更容易？

A: 一般会改善银行尽调的可解释性，但不是保证。银行还会看：

- 业务模式风险（高风险客户/OTC/跨境）；
- AML 与制裁成熟度；
- 技术安全与审计；
- UBO 背景与资金来源。
建议准备“银行尽调包”：牌照进度、制度摘要、风险评估、交易监测说明、审计计划、治理架构。

Q11: MiCA 对“加密资产”定义是什么？我们做的是不是“加密资产”？

A: 监管会看是否属于可转让、可存储、使用 DLT 或类似技术的数字表示价值/权利。若是证券型代币/金融工具，则可能落入 MiFID/MiFIR 体系而非 MiCA。你需要做“分类备忘录”：Token 分类、权利属性、是否金融工具、是否 EMT/ART、是否 utility。

Q12: NFT 业务需要 CASP 吗？

A: 需看 NFT 是否“唯一且不可替代”并且是否具备金融化特征（分割、集合、可替代化、类证券化）。很多“看似 NFT 实为可替代系列”可能被纳入监管关注。建议对 NFT 产品做：结构说明、流通机制、可替代性分析、营销与风险披露。

Q13: 我们提供“质押/借贷/收益产品”是否在 CASP 范围？

A: MiCA 的 CASP 服务清单并不直接等同于所有收益型业务。收益、借贷、质押可能触发其他金融监管框架或消费者保护规则。监管会重点问：收益来源、对手风险、资产再质押、是否形成存款类或集合投资性质。务必先做“监管映射 (Regulatory Mapping)”。

Q14: 我们能否向零售客户提供服务？

A: 通常可以，但零售面向意味着更强的客户保护义务：风险披露、费用透明、投诉机制、适当性/适配性、营销合规、冷静期/撤销权（如适用）、以及更高强度的运营控制。

Q15: 专业客户与零售客户的差别有哪些？

A: 差别通常体现在：

- 披露深度（零售更详细）；
- 适当性评估要求（零售更严格）；
- 风险承受能力与杠杆/复杂产品限制（若涉及）；
- 投诉处理与争议解决路径。
建议建立分层客户政策：零售/专业/机构/合格对手方（如适用），并在开户流程固化。

Q16: 我们是否必须在波兰本地雇人？可否全部远程？

A: 可以有跨境团队，但监管关注“实质经营”。关键职能（合规、MLRO、风控、ICT 安全、管理层）需要能有效履职、可被监管联系、能在波兰形成可解释的治理中枢。完全“空壳+海外遥控”是高风险。

Q17: 申请前可以先试运营/内测吗？

A: 内部测试可以，但对公众提供服务、收取费用、对外营销可能被视为未授权经营。建议：

- 沙盒/试点（如主管机关提供）；
- 封闭测试：不对外、无真实客户资产；
- 预营销材料必须谨慎：不得暗示已获批。

Q18：是否需要保险？

A：多国主管机关在客户资产风险、网络安全风险方面会期待适度保险配置（职业责任险、网络险、犯罪险等），尤其当你托管客户资产、处理法币资金或大规模零售客户时。保险不是万能，但能体现风险管理成熟度。

Q19：CASP 与 DORA 有什么关系？

A：DORA 是欧盟数字运营韧性框架，适用于金融实体及其 ICT 第三方风险管理。CASP 在欧盟体系下与 DORA 的技术治理要求高度耦合：外包治理、渗透测试、事件报告、BCP/DR、访问控制、日志留存等都需要对齐。

Q20：波兰主管机关会最关注什么？

A：通常是“可控性”四件事：

1. 股东/UBO 资金来源闭环；
2. 管理层与关键岗位适当人选；
3. AML/制裁/交易监测与 STR 决策留痕；
4. ICT 安全与外包可控（含退出迁移）。

B | 实体与实质（Q21–Q40）

Q21：在波兰设立什么实体形态更常见？

A：常见为 Sp. z o.o.（有限责任公司）或其他符合本国公司法的形式。监管更关心：公司治理结构是否清晰、章程是否支持合规要求（例如董事权限、合规否决权、股权变更门禁、审计权、外包审批机制）。

Q22：MiCA 申请前公司必须先设立吗？

A：多数情况下需要：申请主体必须是可承担监管义务的法人实体。可以先设立，再启动申请；若你用欧盟其他国实体在波兰申请，涉及跨境结构解释、实质安排与监管协调，材料更复杂。

Q23：什么叫“实质经营（Substance）”？

A：不是办公室摆设，而是：

- 关键决策与治理在波兰有落点；
- 关键岗位能履职、可被监管接触；
- 运营活动（开户、监测、客服、投诉、事件响应）有明确责任人；
- 记录留存、审计、报表能在本地调取或可控。

Q24：需要实体办公室吗？

A：通常建议有。即便你采用混合办公，也应具备：注册地址、合规档案存放安排、受监管沟通机制、数据与记录访问控制。监管会问：如果突击检查，你在哪里展示记录？

Q25：董事是否必须常驻波兰？

A：未必，但需要可解释的时间投入、沟通机制、会议安排、签署权限。若董事都在境外，需证明：治理仍有效、关键决策记录完整、监管联络顺畅。

Q26：可以用集团共享服务中心吗？

A：可以，但必须：

- 明确服务边界（哪些职能共享）；
 - 具备外包/内部服务协议；
 - 保证监管可穿透、可审计；
 - 数据安全与访问控制符合要求；
 - 退出迁移计划明确。
- 共享服务中心本质上也会被监管按“外包风险”审视。

Q27：能否用“名义董事/挂名合规”降低成本？

A：高风险。监管会做真实性判断：履历、面谈问答、时间投入、实际工作产出（合规抽查、STR记录、培训记录等）。一旦被判断为“名义任职”，容易被拒或后续被处罚。

Q28：管理层需要设置哪些委员会？

A：视规模。常见做法：风险与合规委员会、审计委员会、ICT/安全委员会。小公司可合并，但必须明确职责、会议频率、议题模板、决议留痕、跟踪整改闭环。

Q29：公司章程/股东协议建议加入哪些监管友好条款？

A：建议加入：

- 股权变更触发监管通知的门禁（未完成报备不得过户）；
- 董事/关键岗位任免需合规审查；

- 合规否决权与升级路径；
- 外包需董事会批准并保留审计权；
- 数据与记录可访问条款；
- 重大事件（制裁命中、数据泄露、重大投诉）报告机制。

Q30：申请期间能不能对外签客户？

A：可签意向或框架协议，但不得开展受监管服务、不得收取客户资产/资金进行交易或托管。所有对外材料必须加清晰声明：尚未获批，不提供受监管服务。

Q31：实质要求会影响护照吗？

A：会。护照扩张本质上建立在“你被本国有效监管”。如果本国监管认为你实质薄弱，会在护照阶段更谨慎，或在后续检查中要求整改，甚至影响跨境扩张节奏。

Q32：是否需要本地审计师/会计师？

A：通常建议配置本地审计资源，特别是涉及法币账务、客户资金隔离、财务报表审计、监管报表支持。即便可用国际所，也要保证波兰本地可执行与沟通效率。

Q33：是否必须有本地法律顾问？

A：强烈建议。因为除了 MiCA，还涉及波兰本地 AML 法、雇佣法、数据法、消费者保护、广告法等。没有本地法律支持，制度落地与合同条款容易与本地强制性规定冲突。

Q34：集团控股结构复杂会增加审查吗？

A：会。尤其多层控股、离岸结构、代持、信托安排、跨境资金链，会显著提升 SoF/SoW 与穿透披露要求。建议尽量简化层级，或提前准备“穿透备忘录+证据链索引”。

Q35：是否允许同一集团多个 CASP？

A：允许但需解释：分工、冲突隔离、共享服务、客户迁移、数据流、品牌与营销边界。监管会问：是否存在监管套利、是否会混同客户资产与责任。

Q36：如何证明“关键管理在波兰”？

A：用证据说话：董事会会议安排与纪要、关键决策清单、审批流程、签署权限矩阵、系统后台权限日志、合规抽查报告的签署与跟进、事件响应演练记录等。

Q37：申请材料语言用什么？

A：通常需满足主管机关要求（可能是波兰语/英语）。实务上建议：核心制度与 PoO 可提供英文主版本，并准备关键章节的波兰语摘要或官方要求格式，避免翻译差错引发补件。

Q38：我们能否把运营放在其他欧盟国，波兰只做牌照？

A：风险极高。监管会认为你在波兰缺乏实质，可能拒批或要求重大整改。更合规的做法是：波兰作为真正的治理与控制中心，其他国家作为分支/营销据点在护照后逐步落地。

Q39：如何设计“最小合规团队”？

A：建议至少：合规负责人、MLRO、ICT 安全/运维负责人、运营负责人、客户支持/投诉负责人。内审可外包但要有审计计划与整改跟踪责任人。团队最小化可以，但不能牺牲关键控制职能。

Q40：实质要求最常见补件是什么？

A：通常是：岗位是否真实、汇报线是否独立、资源是否足够、外包是否可控、记录留存是否可调取、决策留痕是否可审计。

C | 股东/UBO（Q41-Q60）

Q41：10% 持股为什么敏感？

A：10% 是 qualifying holding 起算线。达到或超过该比例的直接/间接股东通常需要做更深入的适当人选与资金来源审查，并触发后续变更通知义务。

Q42：UBO 的认定按什么原则？

A：以最终自然人控制为核心：直接/间接持股、投票权、控制安排（协议控制、一致行动、委托投票、信托受益）。必须披露至自然人终点，不能“停在公司”。

Q43：资金来源（SoF）与财富来源（SoW）有什么区别？

A：SoW 解释“你整体财富怎么来的”（长期路径）；SoF 解释“本次出资/收购/增资的钱具体从哪里来、怎么到位”。监管通常两者都要，并要求可核验的证据链。

Q44：哪些 SoW/SoF 证据最有说服力？

A：审计报告、纳税证明、股权出售协议与对价流水、分红决议与入账、工资与雇佣证明、房产处置合同与收款、银行对账单、交易所或经纪账户报表（视情况）等。关键是“结论能回指证据”。

Q45：如果资金来自加密资产收益怎么办？

A：必须更细：

- 资产形成路径（何时买入/挖矿/项目分配）；
- 交易平台/钱包地址证明；

- 链上可追溯性与对手风险；
 - 兑换成法币的路径与合规性；
 - 税务处理说明。
- 监管会对“加密收益直接作为资本金”格外敏感。

Q46：股东有 PEP 或高风险背景能过吗？

A：不必然否定，但会显著提高 EDD 深度：资金来源、关联交易、制裁风险、声誉风险、治理隔离机制、额外监控与披露。若涉及制裁命中或重大负面事件，风险极高。

Q47：股东在其他国家曾被监管处罚会怎样？

A：必须披露并解释：处罚原因、整改措施、现状（是否已解除/是否持续影响）。隐瞒通常比处罚本身更致命。监管更看重透明度与整改能力。

Q48：多层离岸架构是否一定不行？

A：不是一定不行，但一定更难：穿透、文件公证/认证、税务与资金链解释、代持/信托安排披露、真实控制权证明。建议能简化就简化；不能简化就提前做“穿透说明书”。

Q49：是否需要提供股东的银行推荐信？

A：有时可作为辅助，但不是核心。核心仍是可验证的 SoF/SoW、合规与声誉证明、以及资金到位路径。

Q50：股东出资是否必须实缴？

A：取决于公司法与监管要求。监管更在意：你是否具备满足资本与稳健经营的资金实力、资本是否可用、是否存在抽逃或短期过桥资金。

Q51：股东借款给公司算资本吗？

A：通常不同资本金。可作为营运资金来源，但监管会问：期限、利率、从属安排、是否影响偿付能力、是否可随时抽走导致风险。若用借款“伪装资本”，风险很大。

Q52：关联方注资/往来需要披露吗？

A：需要。关联交易是监管重点：定价、公允性、利益冲突、资金回流、是否输送利益。建议建立关联交易政策与董事会审批流程。

Q53：股权变更后多久必须通知？

A：一般要求在法定触发下“事前/事后及时通知”。实务上建议：**交易前先做监管沟通**，在 SPA 里设定“监管不反对/批准”为先决条件，避免交易完成后被认定违规。

Q54：股东是否必须提供个人无犯罪记录？

A：通常需要对关键股东/UBO 提供相应的声明与证明（视国家要求）。即便不强制出具纸质证明，也应至少提供宣誓声明、背景调查报告与可核验信息。

Q55：如果股东是法人，董事也要审查吗？

A：会审查法人股东的控制人、董事、实际管理层以及最终自然人 UBO，尤其当法人股东本身是受监管实体或跨境集团时，审查会更深入。

Q56：股东的“声誉”怎么评估？

A：综合：刑事/行政记录、监管处分、破产与失信、重大诉讼、制裁名单、负面媒体、业务道德争议等。关键是：是否影响稳健经营、是否引入 AML/制裁风险。

Q57：股东是否要承诺不干预合规？

A：建议。监管不喜欢“股东直接指挥合规/风控”。可通过治理文件：明确管理层独立履职、合规否决权、董事会监督机制、股东不当干预的举报与升级机制。

Q58：UBO 信息需要持续更新吗？

A：需要。建议制度化：季度 cap table 核对、年度 UBO 确认、重大事件触发更新（新增代持、投票委托、一致行动等）。

Q59：监管最常问的 SoF/SoW 细节有哪些？

- A：
- 钱从哪来、哪一年赚到、凭什么赚到；
 - 资金链是否完整、是否有第三方代付；
 - 是否涉及高风险司法区、现金密集行业；
 - 是否有税务合规证明；
 - 是否存在循环交易或“短期过桥”。

Q60：我们怎样把 SoF/SoW 做成“可审计交付版”？

A：建议三件套：

1. 结构图（穿透到自然人）；
2. 叙事备忘录（SoW/SoF 逻辑）；
3. 证据索引表（每条结论对应文件编号、日期、页码、流水号）。

D | 董事适任性（Q61–Q80）

Q61：董事/管理层“适当人选”核心看什么？

A：四个维度：诚信与声誉、能力与经验、时间投入、治理有效性（独立性、冲突管理、决策留痕）。

Q62：董事必须有金融牌照经验吗？

A：不一定，但必须具备与业务匹配的综合能力。若没有直接监管经验，应通过：顾问支持、培训体系、合规与风险控制机制、面谈准备来补足，并证明“能理解并执行监管要求”。

Q63：技术型创始人可以当董事吗？

A：可以。但监管会问：谁负责合规、谁负责风险、谁负责财务稳健、谁负责客户保护。技术型董事需能解释：钱包治理、权限分层、事故响应、外包管理与安全控制。

Q64：董事是否要通过考试？

A：MiCA 不以“统一考试”为核心，但波兰本地可能要求声明、履历、无犯罪、以及面谈。关键是**面谈表现与证据化履历**：你做过什么、如何做、如何管理风险。

Q65：董事兼职太多会怎样？

A：可能被质疑时间投入。需要：时间承诺说明、会议安排、授权机制、替代安排、关键决策参与证据。监管担心“挂名董事”。

Q66：董事的利益冲突如何管理？

A：必须有制度：关联交易审批、持仓与交易限制、内幕信息管理、礼品与招待政策、外部任职披露、与供应商/代币项目方关系披露。

Q67：董事能否兼任 CEO 与合规负责人？

A：小公司可能出现兼任，但必须解释独立性与防火墙：

- 合规否决权如何实现；
- STR 决策如何独立；
- 内审如何独立（通常建议外包）；
- 董事会如何监督。
兼任越多，监管越谨慎。

Q68：管理层需要哪些关键政策必须“亲自批准”？

A：通常包括：风险偏好声明、AML政策、制裁政策、外包政策、客户资产保护政策、事件响应与BCP/DR、投诉与纠纷处理政策、利益冲突政策。

Q69：董事会会议与纪要要写到什么程度？

A：要能证明“真正治理”。建议纪要包含：议题、风险讨论、决策依据、反对意见、整改事项、责任人与截止日期。监管抽查会看“是否走形式”。

Q70：董事是否要对客户投诉负责？

A：董事会需监督投诉机制有效性，重大投诉与系统性问题应上升到董事会层面，并形成整改闭环。投诉不是客服问题，是合规与声誉风险。

Q71：董事对 AML 的责任边界是什么？

A：董事会负责设定风险偏好、批准 AML 框架、确保资源充分、监督 MLRO 的独立性与有效性。MLRO负责具体执行与 STR 决策，但董事会对体系有效性负最终责任。

Q72：董事对 ICT 安全的责任边界是什么？

A：董事会需监督 ICT 风险管理：外包、渗透测试、事件报告、BCP/DR、权限治理、关键系统变更。不能把“安全”完全甩给技术团队。

Q73：董事是否必须懂区块链？

A：不必人人都懂，但必须确保治理层具备足够知识覆盖关键风险。建议至少一名董事或高管具备加密/ICT安全实战背景，并通过定期培训提升整体治理能力。

Q74：董事背景调查通常包括什么？

A：身份与地址、无犯罪记录、破产与失信、监管处分、重大诉讼、制裁与PEP筛查、负面媒体、学历与工作经历核验、利益冲突与关联方披露。

Q75：董事曾经创业失败或破产是否必然被拒？

A：不必然，但需解释原因、是否存在诚信问题、是否对稳健经营产生重大疑虑，并展示改进与治理能力。关键在透明披露与可解释性。

Q76：董事需提交哪些声明类文件？

A：常见包括：适当人选声明、无利益冲突声明、时间投入声明、无刑事定罪声明、遵守监管义务承诺、信息真实完整承诺等。

Q77：董事能否由集团母公司委派？

A：可以，但需防止母公司利益凌驾于客户保护与合规之上。需明确：本地实体董事对本地实体负信义责任，关键决策不得被母公司不当干预。

Q78：董事更换后需要报备吗？

A：通常属于重大变更事项，需要及时通知主管机关，并提供新任董事的完整适当人选材料包与过渡安排。

Q79：如何准备监管面谈？

A：建议准备“面谈题库+证据包”：业务模式、收入来源、客户类型、AML风险、制裁处置、钱包治理、外包与退出、投诉机制、资产隔离、事件响应演练。

Q80：最常见的董事适任性补件是什么？

A：履历与业务不匹配、时间投入不足、利益冲突未披露、对 AML/ICT/客户保护理解不清、治理证据不足（纪要、审批、整改闭环缺失）。

E | 资本/保障（Q81–Q100）

Q81：MiCA 对资本金怎么要求？

A：按服务类型与风险，存在最低资本要求与持续稳健经营要求。你需要把：服务范围、客户资产规模、运营成本、风险暴露映射到资本规划，并写入资本充足性评估（ICAAP类思路）。

Q82：资本是否需要一次性到位？

A：通常申请阶段需要证明可满足最低资本并支撑启动期运营（含技术、合规、人员、审计、保险）。若计划分期注资，必须有可执行的资金承诺与时间表，并解释启动期如何满足稳健经营。

Q83：资本来源可以是股东贷款吗？

A：贷款不等同资本。可作为营运资金，但监管会担心随时抽走。若你用贷款支撑关键控制职能，监管可能要求更稳健的资本结构或从属安排。

Q84：是否需要准备“资本与财务预测模型”？

A：强烈建议。至少3年预测：收入、成本、人员、技术、审计、保险、外包费用、合规成本、市场扩张成本。并做压力测试：币价波动、交易量下滑、制裁事件、系统事故。

Q85：客户资产是否必须隔离？

A：客户保护是 MiCA 核心之一。若你托管或可控制客户资产，必须有隔离机制：账务隔离、钱包隔离、权限隔离、以及破产隔离的法律安排说明。

Q86：需要设立保证金或储备吗？

A：具体取决于服务类型与主管机关要求。即便无明确保证金要求，监管也会期待：运营储备、事故应对资金、赔付能力安排（含保险）。

Q87：是否要做外部审计？

A：通常需要年度财务审计，且关键控制领域（客户资产隔离、AML有效性、ICT安全）也可能被要求独立评估或专项审计。建议提前选定审计师与审计计划。

Q88：资金与资产如何估值？

A：资本认定通常以法币计量；加密资产作为资本或储备需要谨慎，监管会关注波动性与可用性。建议核心资本以稳定法币资产为主。

Q89：如果我们只做“非托管软件”，资本要求会更低吗？

A：风险可能更低，但仍需支撑合规、客户保护、ICT安全与运营韧性。监管不会因为你“轻资产”就接受“零治理”。

Q90：如何证明公司不会挪用客户资产？

A：制度+技术+审计三位一体：

- 权限分层、多签、冷存储策略；
- 资产变动审批与日志；
- 定期对账与审计；
- 关联方交易限制；
- 员工行为与访问控制。

Q91：资本不足会怎样？

A：可能导致拒批或附条件批准并要求补足资本、限制业务规模、限制扩张。持牌后资本不足可能触发监管介入、整改命令甚至暂停业务。

Q92：是否需要建立“资金管理政策（Treasury Policy）”？

A：建议建立：资金头寸管理、银行账户权限、支付审批、法币与加密头寸限额、对手方管理、收益与成本核算、异常交易监测等。

Q93：我们做做市/自营库存，资本怎么考虑？

A：做市会带来市场风险与流动性风险。资本规划需考虑：库存限额、对冲策略、极端行情压力测试、交易对手风险、资金占用与保证金安排。

Q94：是否要设立客户赔付机制？

A：建议在客户条款与投诉机制中明确赔付原则、责任边界、争议解决与仲裁/法院管辖，并结合保险与事故响应计划形成闭环。

Q95：能否以集团担保代替资本？

A：担保可作为补充，但不应替代最低资本要求。监管更偏好实体具备可持续的自有资本与稳健经营能力。

Q96：我们需要准备“破产处置计划（wind-down plan）”吗？

A：非常建议。说明：若停止经营，如何安全退出、如何返还客户资产、如何通知客户与监管、如何迁移系统与数据、如何处理未完成交易与投诉。

Q97：审查时监管会问哪些财务细节？

A：收入来源是否真实、费用结构是否合理、合规与安全预算是否足够、外包费用是否低估、是否存在不合理关联交易、是否有资金挪用风险。

Q98：税务会影响资本吗？

A：会。税负会影响利润与净资产。财务预测应纳入 CIT/VAT/预提税、雇佣成本与社保、公允价值会计处理等。

Q99：客户法币资金如何处理最合规？

A：通常建议：客户资金专户、受信安排或等效隔离机制；支付流程审批；对账与异常识别；清晰披露资金性质与可用性；避免混同公司营运资金。

Q100：资本/保障模块最常见补件是什么？

A：财务预测过于乐观、没有压力测试、未解释做市/库存风险、客户资产隔离描述过于概念化、缺少退出计划与对账审计安排。

F | AML/制裁/STR (Q101–Q120)

Q101：CASP 在波兰一定属于 AML 义务主体吗？

A：实务上大概率是。你必须满足本国 AML 法要求（客户尽调、持续监控、STR、记录保存、培训、独立审查等），并与 MiCA 的客户保护与治理要求一起形成统一合规体系。

Q102：我们需要 MLRO 吗？

A：强烈建议必须设置（或等效职责负责人），并且具备独立性、资源与直接升级路径。没有 MLRO 的体系很难通过审查。

Q103：KYC 的最低要做到什么程度？

A：至少包括：身份核验、受益人识别（法人）、风险评级、PEP/制裁筛查、资金来源信息收集（视风险）、持续监控与定期复核。

Q104：EDD 什么时候触发？

A：高风险客户/国家、PEP、制裁相关、异常交易、复杂结构、加密资产来源不明、频繁跨境、与混币/暗网风险相关等，均触发增强尽调：更多文件、更多验证、管理层批准、降低限额或拒绝。

Q105：制裁筛查要筛哪些？

A：至少：EU 制裁名单 + UN + 本地要求；很多项目还会加 UK/US OFAC 等（取决于业务风险与银行通道要求）。筛查对象包括：客户、UBO、收款/付款对手、受益人、地址、设备指纹（可选）。

Q106：链上监控必须做吗？

A：如果你处理链上转账、托管或兑换，强烈建议使用链上分析工具与规则体系：高风险地址识别、混币器/暗网关联、制裁地址、跳转路径、风险评分与处置SOP。

Q107：Travel Rule 怎么做？

A：建立信息收集、传递、验证机制：发送方/接收方信息字段、阈值规则、与对手机构的互通方式、失败处理（缺字段/对手不支持）、留痕与审计。对 OTC/自托管钱包交互要特别设计。

Q108：什么是 STR？谁决定报不报？

A：STR 是可疑交易报告。通常由一线触发警报→合规/AML团队调查→MLRO 决策→必要时报送→留痕保存。必须有**决策树与记录模板**，证明“为什么报/为什么不报”。

Q109：STR 不报会怎样？

A：风险极高：监管处罚、刑事风险、银行通道终止、牌照风险。最常见问题不是“漏报一次”，而是“没有可解释的决策与留痕”。

Q110：我们可以因为“商业原因”不报 STR 吗？

A：不可以。STR 决策必须以风险与法律义务为准，不得被营收压力或客户关系左右。MLRO 的独立性就是为防这种情况。

Q111：交易监测规则如何设计？

A：建议分三层：

- 基础规则（频次、金额、地域、设备、账户行为）；
- 场景规则（分散/聚合、快速进出、跨链跳转、混币、异常对手）；
- 风险自适应（高风险客户更严阈值）。
并做回溯测试、误报率评估、规则变更管理。

Q112：如何处理“自托管钱包”出入金？

A：关键是证明你对风险有控制：地址归属证明（签名验证/小额验证）、链上风险评分、限额、冷却期、异常触发人工复核、必要时拒绝或冻结并升级 MLRO。

Q113：可以把 AML 外包吗？

A：部分可外包（例如工具、部分调查支持），但 MLRO 决策与体系责任不能外包掉。必须保留审计权、监督权、数据控制、退出迁移计划。

Q114：培训要怎么做才算“可审计”？

A：要有：年度培训计划、课件、签到、测验、通过率、补训记录、培训覆盖矩阵（岗位→课程），并与真实案例/STR复盘结合。

Q115：记录保存要多久？保存什么？

A：按本国 AML 法要求（通常多年）。保存内容包括：KYC文件、风险评级、筛查结果、交易监测警报与处置、STR 决策记录、客户沟通、投诉、培训、审计与整改等。关键是：可检索、可调取、不可篡改。

Q116：如何管理“黑名单/拒绝客户”？

A：建立拒绝与退出政策：触发条件（制裁、欺诈、虚假信息、拒绝提供资料、链上高风险等）、审批流程、通知策略、资金处理、STR评估与留痕。

Q117：我们发现制裁命中怎么办？

A：立即冻结/停止服务（按法律与银行通道要求）、升级 MLRO 与管理层、评估是否必须报告、记录所有动作、与监管/执法沟通（如适用）。

Q118：如何避免员工内鬼/合规绕过？

A：权限最小化、四眼原则、多签、关键操作录像/日志、异常行为监控、强制休假、轮岗、背景调查、举报机制、内审抽查。

Q119：AML 体系最常见被问穿的点是什么？

A：

- STR 决策没有留痕；
- 规则过于模板化、不贴合业务；
- 高风险客户照样放行但没管理层批准；
- 没有链上监控或不会用；
- Travel Rule 无落地流程。

Q120：如果我们只服务机构客户，AML 可以简化吗？

A：可相对简化，但不能缺失。机构客户也可能高风险（OTC商、做市商、跨境支付商）。你仍要做 UBO 穿透、交易监测、制裁筛查、持续复核与STR机制。

G | ICT / DORA / 外包（Q121–Q140）

Q121：监管眼里“合规的系统”要具备哪些最小能力？

A：至少：身份与权限管理、交易与资金流记录、日志不可篡改、报警与工单、对账、冷/热钱包治理、密钥管理、多签审批、BCP/DR、事件响应与报告流程。

Q122：冷热钱包怎么设计更容易过审？

A：常见“监管友好”结构：

- 绝大部分资产冷存储；
- 热钱包限额与自动补给机制；
- 冷钱包多签（不同角色分持、地理隔离）；
- 提币风控（白名单、延迟、人工复核）；
- 全流程日志与定期对账审计。

Q123：多签签名人如何配置？

A：建议分散在不同职能：运营、合规/风控、技术安全，并设置替代人机制与紧急流程。避免单点或同一部门掌控所有签名。签名权限与变更必须有董事会级审批与记录。

Q124：权限管理（RBAC）要做到多细？

A：越细越好，至少到：

- 查看/操作/审批分离；
- 关键操作双人复核；
- 管理员权限审计；
- 临时权限（Just-in-time）与到期回收；
- 定期权限复核（Access Review）。

Q125：渗透测试必须做吗？

A：强烈建议做，并形成报告与整改闭环。监管更看重“发现问题后怎么修、多久修、谁负责、是否复测”。

Q126：BCP/DR 要写到什么程度？

A：要能执行：

- RTO/RPO 指标；
- 关键系统与数据备份策略；
- 备援演练计划与记录；
- 第三方依赖与替代方案；
- 客户沟通与公告机制。

Q127：安全事件发生时的流程？

A：必须有：检测→分级→隔离→调查→修复→通报→复盘。并明确：谁是事件指挥官、谁对接监管、谁对接客户、谁保全证据。事件日志要可审计。

Q128：我们用云服务可以吗？

A：可以，但监管会看：数据位置、访问控制、加密、密钥管理、供应商尽调、审计权、分包控制、退出迁移、SLA、事故通报与协作机制。

Q129：外包哪些属于“关键或重要职能”？

A：通常包括：托管与密钥管理、核心交易系统、客户身份核验、交易监测、制裁筛查、云基础设施、数据存储等。关键外包的治理要求更严：审批、尽调、合同条款、持续监控、退出计划。

Q130：外包合同必须写哪些条款才算合规？

A：至少包括：

- 审计权与访问权（含第三方审计）；
- 数据安全与保密、加密、访问控制；
- 分包限制与审批；
- 事件通报时限与协作；
- SLA/可用性/灾备；
- 退出与迁移（Exit plan）与数据返还/销毁；
- 监管可接触条款（监管要求时可提供信息）。

Q131：如何做供应商尽调？

A：从五类证据：公司资质与财务稳健、信息安全认证与报告（ISO/SOC等）、人员与流程、过往事件与整改、服务连续性与退出能力。并建立供应商评分与年度复评。

Q132：可以把合规系统外包给 SaaS 吗？

A：可以，但要证明：

- 数据可控；
- 规则可配置、可解释；
- 记录可导出、可审计；
- 供应商不会成为单点；
- 退出迁移可执行。

Q133：日志保存怎么做才“不可抵赖”？

A：建议：集中日志、时间同步、访问控制、不可篡改存储（WORM/等效）、日志审计与定期抽查、日志保留期限与检索能力。尤其是密钥操作、提币审批、权限变更、风控豁免。

Q134：代码变更与上线需要合规参与吗？

A：需要。建立变更管理：需求→评审→测试→安全扫描→上线审批→回滚方案→上线后监控。合规/风控需对影响客户保护与 AML 的变更有审阅权。

Q135：如何证明系统容量能扛高峰？

A：提供容量规划、压力测试报告、扩容策略、限流熔断、关键指标监控。监管担心高峰宕机导致客户损失与市场秩序风险。

Q136：私钥如何生成、存储、备份？

A：建议采用 HSM/硬件隔离、密钥分片或多签、离线备份、访问控制、密钥轮换、应急恢复流程，并做演练与记录。监管会问“如果签名人失联怎么办”。

Q137：第三方托管是否更容易过审？

A：不一定。第三方托管降低自建难度，但引入外包风险。你仍需证明：选择理由、尽调充分、合同可审计、退出可迁移、客户条款披露清晰。

Q138：DORA 会要求我们做什么额外工作？

A：核心是 ICT 风险治理体系化：外包治理、韧性测试、事件管理、第三方风险、持续改进。即使你还未完全纳入某些细项，监管也会期待你“对齐方向与落地计划”。

Q139：系统最常见补件是什么？

A：外包合同缺审计权/退出条款、钱包治理描述泛泛、权限分层不清、BCP/DR没有演练证据、事件报告流程不完整、日志与对账机制不清晰。

Q140：如何把 ICT 模块做成“交付版”材料？

A：建议交付包：系统架构图、数据流图、权限矩阵、钱包与签名流程图、变更管理SOP、BCP/DR手册、渗透测试报告与整改、外包尽调与合同条款库、事件响应演练记录模板。

H | 客户保护（Q141–Q160）

Q141：MiCA 客户保护最核心三件事？

A：透明披露（费用/风险/执行/冲突）、客户资产保护（隔离/控制/返还）、投诉与纠纷机制（可用、可追踪、可整改）。

Q142：费用披露要披露到什么程度？

A：不仅是“手续费多少”，还应包括：点差、滑点、提币费、托管费、换汇费、网络费、第三方费用、返佣、隐藏成本。并说明费用触发条件、计费方式与示例。

Q143：定价与执行质量如何披露？

A：如果你是对手盘（OTC/做市），必须披露你如何报价、是否可能与客户利益冲突、如何确保执行公平。若是撮合平台，要披露撮合规则、优先级、异常处理、停牌机制。

Q144：客户风险披露要覆盖哪些？

A：至少：价格波动、流动性、技术风险、托管风险、链上风险（地址错误不可逆）、制裁与冻结风险、稳定币脱锚风险、第三方依赖风险、监管变化风险。

Q145：适当性/适配性怎么做？

A：建议对零售客户做：知识与经验问卷、风险承受能力评估、产品分级（高风险/复杂）、风险提示与确认、必要时限制某些产品或提高门槛。

Q146：客户资产隔离怎么向客户解释？

A：条款里要写清：资产是否托管、谁控制私钥、是否使用第三方托管、是否会再质押/借出、破产情况下的处理原则、对账频率与客户查询权。

Q147：我们能否在条款里写“任何损失不负责”？

A：不建议。过度免责可能被认定不公平条款。更合规做法是：明确责任边界、合理免责（例如客户自身错误地址）、同时提供事故处理与赔付原则。

Q148：投诉机制要怎么设计？

A：必须可用：线上入口、工单编号、处理时限、升级路径、证据收集、赔付/纠正、复盘与整改。并明确：监管投诉渠道与争议解决方式。

Q149：客户资金进出金要注意什么？

A：要防洗钱与欺诈：同名校验、第三方代付限制、异常频次与金额监控、提现白名单、冷却期、可疑情况冻结与升级 MLRO。

Q150：账户冻结条件如何设定才不引发纠纷？

A：条款中明确冻结触发（制裁命中、欺诈、虚假信息、监管要求、司法协助）、冻结期间客户通知策略、资金处理、申诉机制与时间预期。

Q151：如何防止市场操纵与不公平交易？

A：建立市场监控：异常挂单撤单、刷量、对敲、抢跑、内幕信息滥用等检测规则。平台应具备暂停交易、限制账户、调查与报告机制。

Q152：利益冲突政策应包含哪些？

A：公司自营交易、做市与客户交易冲突、员工持仓与交易限制、返佣与佣金安排、关联方项目上线、供应商关系、信息隔离与“优先执行”承诺等。

Q153：客户数据与隐私怎么保护？

A：GDPR 合规：合法性基础、最小化、保留期限、数据主体权利、跨境传输、数据泄露通报、第三方处理协议、访问控制与审计。

Q154：客户教育是否必要？

A：强烈建议，尤其零售。提供风险教育、常见骗局提示、地址安全、2FA、钓鱼防范、冷钱包基础。教育材料也可作为监管证据：你在降低客户风险。

Q155：如何处理“误转账/误提币”？

A：流程要写清：能否追回取决于链上特性与对手合作；你能提供的协助范围；收费；证据收集；冻结窗口（如有）；以及客户需承担的不可逆风险提示。

Q156：客户条款需要本地语言吗？

A：通常建议提供客户能理解的语言版本（波兰语/英语视市场）。语言不清晰会直接影响客户保护评估与投诉风险。

Q157：如果我们提供杠杆或衍生品相关服务呢？

A：这可能触发 MiFID 等其他监管体系。MiCA 不是万能牌照。若涉及杠杆、期货、差价合约等，必须做监管映射并可能需要额外授权。

Q158：如何处理“代币上线/下架”对客户影响？

A：要有透明政策：上线评估标准、风险披露、下架触发、客户通知、资产处置窗口、异常情况应急。尤其下架时要避免客户被动损失扩大。

Q159：客户保护模块最常见补件是什么？

A：费用披露不够细、对手盘冲突未披露、投诉机制无时限与升级、资产隔离描述缺技术与法律支撑、冻结条款过于宽泛或过度免责。

Q160：如何把客户保护做成“交付版”材料？

A：建议交付包：客户条款（T&C）、风险披露书、费用表与示例、投诉SOP与工单模板、利益冲突政策、资产隔离说明书、冻结/退出政策、客户教育材料清单。

I | 护照与跨境（Q161–Q180）

Q161：什么是 MiCA 护照？

A：在一国获授权后，通过通知程序向其他成员国提供跨境服务或设立分支。关键是：必须先在本国被有效监管，且跨境营销与客户保护要逐国合规落地。

Q162：护照是否“自动生效”？

A：不是“你想去就去”。需要按程序通知、等待窗口期，并满足目标国的消费者保护、营销与语言等本地要求（即使 MiCA 统一，也仍有本地规则差异）。

Q163：护照前必须准备哪些材料？

A：建议准备：目标国清单、服务范围、营销计划、客户支持与投诉安排、语言与披露适配、税务与VAT影响评估、数据跨境与本地存储要求评估、当地合作伙伴/外包安排说明。

Q164：跨境提供服务时 AML 怎么做？

A：通常由本国 AML 体系承担主体责任，但你必须识别目标国风险差异（高风险国家、当地制裁与执法合作），并确保客户尽调与交易监测能覆盖跨境行为。

Q165：我们能否在目标国找代理做营销？

A：可以，但营销外包也要治理：合规审批、话术与材料审查、禁止误导宣传、客户引流数据保护、投诉转交机制、佣金与利益冲突披露。

Q166：护照是否允许我们“先在目标国做业务再补手续”？

A：不建议。被认定为未授权跨境展业会带来严重后果：监管处罚、护照受阻、银行通道中断、声誉受损。

Q167：如果目标国对某类代币更敏感怎么办？

A：要做逐国“产品可售清单”与限制策略。例如某些国家对高波动或特定结构代币的营销更严格，你需要有地理围栏、风险提示增强、产品限制等。

Q168：跨境客户支持要如何配置？

A：至少：多语言支持、时区覆盖、投诉与纠纷处理机制、重大事件通知机制。监管会问：目标国客户遇到问题找谁、多久回应、谁负责。

Q169：护照会影响税务吗？

A：可能影响 VAT、常设机构风险、预提税、雇佣与社保、以及转移定价。建议在护照路线图中加入税务评估与合规安排。

Q170：我们能否在目标国设分支机构？

A：可以，通常需要更充分的计划：人员、办公室、治理、合规联络、记录可访问。分支比纯跨境服务的实质要求更高。

Q171：跨境数据流（客户数据、交易数据）需要披露吗？

A：需要。尤其涉及云与第三方处理。要说明数据存储地点、访问控制、跨境传输机制、DPA、以及客户告知与同意（如适用）。

Q172：跨境扩张时最常踩雷是什么？

A：营销误导（“已在当地获批”）、语言与披露不足、投诉机制无法覆盖、税务未评估、代理乱承诺、目标国高风险客户与资金路径未被 AML 体系覆盖。

Q173：护照扩张要不要做“国家级时间轴”？

A：建议必须做。每个国家：通知→材料适配→营销合规→客服配置→税务评估→上线。把里程碑写清可控，避免同时铺开导致失控。

Q174：护照后，目标国监管会来查我们吗？

A：可能。尽管主要监管在本国，但目标国可以就消费者保护、营销、投诉等问题提出要求或协助检查。你需要准备跨境监管协作机制。

Q175：我们做机构业务跨境是不是更容易？

A：相对容易，但仍需合规。机构客户也要 KYC/UBO、制裁筛查、交易监测。营销与披露可相对简化，但不能缺失。

Q176：跨境业务是否要求本地银行账户？

A：不必然，但业务上可能需要。若涉及本地法币通道，银行尽调会看你是否在当地有合规落点、是否能处理当地投诉与争议。

Q177：跨境合作伙伴如何选择？

A：做尽调：合规记录、资金路径、客户质量、技术安全、合同条款（审计权、分包控制、退出）。并把合作伙伴纳入持续监控。

Q178：护照扩张是否影响我们申请更多服务类别？

A：会增加复杂度。建议策略：先把核心服务在波兰稳健运营并形成证据，再扩张护照，再在稳定基础上扩项服务类别。

Q179：护照扩张对“品牌宣传”有什么限制？

A：不能夸大授权范围、不能暗示在目标国被许可超出事实、必须披露风险与服务提供主体。所有广告素材需有合规审批与版本管理。

Q180：护照模块最常见补件是什么？

A：目标国服务范围不清、营销材料不合规、客户支持不足、税务与数据跨境未评估、代理外包缺治理与审计权。

J | 运营与持续合规（Q181–Q200）

Q181：持牌后有哪些“必须持续做”的合规动作？

A：至少包括：持续 AML 监控与 STR 决策留痕、客户投诉处理与复盘、定期培训、风险评估更新、外包与供应商复评、系统安全测试与演练、财务审计与监管报表、重大变更报备。

Q182：需要提交哪些监管报表？

A：取决于主管机关要求与服务类型。通常会涉及：业务规模、客户数量、交易量、客户资产规模、事件与投诉、财务与资本状况、外包与 ICT 风险、AML 活动指标（警报数量、STR 数量等）。

Q183：重大变更需要报备什么？

A：典型包括：股权/控制权变化、董事与关键岗位更换、服务范围扩项、重大外包、核心系统迁移、客户资产托管方式变化、重大安全事件、重大合规事件、业务模式重大调整。

Q184：培训多久一次？培训对象有哪些？

A：建议年度计划+按事件触发补训。对象覆盖：董事会、全员、关键岗位、前线客服与运营、技术运维。要有签到、测验、通过率、补训与记录留存。

Q185：内部审计怎么安排？

A：可外包，但必须独立。要有年度审计计划、审计范围（AML、客户资产、ICT、外包、投诉等）、发现问题整改闭环（责任人+期限+复检）。

Q186：如何做“合规监测计划”？

A：按主题设定频率与抽样：开户KYC抽查、制裁筛查复核、交易监测警报质量、费用披露一致性、营销材料合规、投诉处理时效、权限与日志抽查等。输出“月报/季报”。

Q187：如何证明我们的 AML 有效？

A：用指标与证据：警报命中质量、误报率、调查时效、STR 决策记录、回溯测试、模型变更管理、培训覆盖、独立审计结论与整改。

Q188：如何做“事件响应演练”？

A：至少年度演练：数据泄露、钱包被盗、供应商宕机、制裁命中、异常挤兑、关键签名人失联等。每次演练要有：剧本、参与人、时间线、改进清单。

Q189：外包供应商复评多久一次？

A：建议至少年度复评，关键外包可更频繁。复评内容：SLA、事件记录、审计报告、分包变化、财务稳健、合规事件、退出可行性。

Q190：客户资产对账频率怎么设？

A：建议至少每日对账（系统对账+链上对账+银行对账），并对异常设定工单与升级机制。对账是托管业务的生命线。

Q191：如何处理监管问询（RFI）？

A：建立“RFI应答战情室”：合规牵头、法务/技术/运营联动；建立证据仓库；每一问都以“结论+证据引用+附件编号”回复；全程版本管理与留痕。

Q192：如何做记录管理（Recordkeeping）才符合审查？

A：建立记录清单与保留期限矩阵；集中存储；访问控制；不可篡改；可检索。并明确：谁负责、如何备份、如何应对监管抽查。

Q193：持牌后如果业务增长很快，监管会担心什么？

A：担心你控制失效：KYC质量下降、监测规则跟不上、客服与投诉积压、系统容量不足、外包失控。要准备“增长控制计划”：扩员、扩容、提高抽查与监测强度。

Q194：如果发生客户资金损失或被盗怎么办？

A：启动事件响应：冻结、隔离、调查、通知客户与监管（如需）、保全证据、评估赔付、复盘整改。并依据条款与保险安排处理赔付边界。

Q195：如何管理“新币上线/新产品上线”的持续合规？

A：建立产品治理委员会：评估风险、合规与客户保护；上线前审查披露材料与营销话术；上线后监控投诉与异常交易；必要时下架并通知客户。

Q196：如何确保员工持续合规？

A：员工行为准则、交易限制、冲突披露、强制休假与轮岗、权限最小化、日志审计、举报机制、绩效不以“合规违规”为代价。

Q197：持牌后是否还需要法律顾问长期支持？

A：建议保留。监管变化（ESMA Level 2/3、AMLA、DAC8 等）、新产品、跨境扩张、重大合同外包、争议处理，都需要持续法律与合规协同。

Q198：持续合规最常见被罚点有哪些？

A：未及时报备重大变更、AML体系形式化、STR 决策无留痕、外包合同缺审计权与退出、客户投诉处理不当、营销误导、数据泄露处置不合规。

Q199：我们如何把“持续合规”做成可交付的运营体系？

A：用“证据仓库（Evidence Vault）”思想：每项合规活动都产出证据（培训、抽查、演练、会议纪要、对账报告、供应商复评、STR记录、投诉闭环），并可随时导出给监管/银行/审计。

Q200：这份FAQ如何直接用于申请与面谈？

A：建议把 FAQ 映射到你的 PoO 与制度目录：

- 每个问题对应制度章节/流程图/证据模板；
- 面谈按模块演练（AML/ICT/客户保护为重中之重）；
- 对高风险点（SoF/SoW、外包、钱包治理、STR）准备“附件包”随问随给。

仁港永胜唐生 | 交付提示（针对波兰 CASP FAQ 的落地用法）

1. 把 Q1–Q200 变成“问答索引+附件索引”：每个答案后挂“制度章节/证据模板/附件编号”，立刻变成可审计材料。
2. 优先打穿四个高频补件区：SoF/SoW（股东/UBO） | MLRO/STR留痕 | 外包合同三件套（审计权/分包/退出） | 钱包权限与对账。
3. 把“持续合规证据化”从 Day 1 做起：培训、抽查、演练、日志、对账、会议纪要都留档——这是后期检查的护城河。
4. 合规服务：选择一间专业专注的合规服务商协助牌照申请及后续维护及合规指导尤为重要，在此推荐选择仁港永胜。

15) 我司服务建议与配套说明（交付包/流程/沟通节奏）

15.1 交付方法论：三条主线一体化

- **合规主线**：MiCA 授权材料 + 持续监管制度
- **AML 主线**：KYC/监控/STR 机制（对齐 GIIF 实务要求与欧盟趋同）
- **ICT 主线**：按 DORA 建设 ICT 风险与外包治理（避免获牌后大整改）

15.2 项目流程（建议节奏）

- Week 1–2：范围定稿 + 差距评估 + 计划/预算
 - Week 3–6：股东/适任性包闭环 + AML/ICT 框架搭建
 - Week 7–10：PoO+BP 定稿 + 客户条款披露 + 外包合同框架
 - Week 11：递交申请
 - 递交后：RFI 战情室（48–72 小时内完成首轮应答草案）
-

16) 波兰 CASP 合规与报告制度（MiCA + 本国 AML 法/监管报表）

16.1 MiCA 维度（持续义务）

- 客户资产保护、披露与投诉、利益冲突、记录保存、外包治理、重大变更管理等（以 MiCA 主法为纲）。

16.2 AML 维度（GIIF 相关）

- 风险评估、CDD/EDD、制裁/PEP、持续监控、STR 报告与证据留存
- 关键点：监管趋势从“有没有制度”转向“是否有效运行”（AMLA 趋同驱动）。

16.3 报表与数据治理（DAC8/Travel Rule 驱动）

- 交易与客户数据字段治理、可追溯性、报表可生成能力（DAC8/税务信息交换；Travel Rule 转账信息随行）。
-

17) 税务与法律配套（CIT/VAT/预提税/雇佣/架构建议）

17.1 企业所得税 CIT（波兰）

- 波兰常见 CIT 税率口径：**19% 标准税率**；对**小规模纳税人/新设企业可适用 9%**（需满足条件）。

17.2 预提税 WHT（结构规划要点）

- 向境外支付股息/利息/特许权使用费/部分服务费可能触发 WHT；税协与受益所有人（beneficial owner）实质要求需要税务顾问逐项评估（集团架构尤其关键）。

17.3 VAT 与交易/服务费属性

- 平台手续费、托管费、订阅/API 费、推广返佣等 VAT 定性与跨境申报路径（B2B/B2C、OSS/IOSS 适用性）需出具税务备忘录（按你们实际收费模式逐项判定）。

17.4 雇佣与薪税社保

- 本地雇佣成本直接影响三年预测；跨境远程团队需评估常设机构（PE）风险与薪税合规。

17.5 架构建议（合规边界清晰）

- **CASP 主体**（MiCA 授权）
 - **法币通道**：银行/EMI/PI 合作（合同划分责任边界 + 对账）
 - **技术/研发**：集团内服务协议（转让定价与实质）
 - **客户资产托管**：自建/第三方托管（责任边界与审计权）
-

18) 后续监管趋势与政策走向 (ESMA Level 2/3、AMLA、DAC8)

- **ESMA Level 2/3 趋势**：模板化、数据格式化、报送口径趋同（制度要“可执行、可生成报表、可审计”）。
- **AMLA 推动 AML 执行更强、更一致**：对 KYC 质量、链上风险识别、STR 决策留痕、外包责任边界会更严格。
- **DAC8 促成税务穿透数据治理**：客户税收居民信息、自证、交易分类计量、地址映射、数据留存与对账能力成为“强制能力”。

19) 项目实操建议（三阶段法：Preparation / Application / Post-Licence）

Phase 1 | Preparation (4–8 周)

- 服务范围定稿 (MiCA 映射) → 系统蓝图 (含钱包与外包) → 关键岗位到位
- SoF/SoW 闭环、风控与 AML 框架落地、条款披露初稿
- 建立证据仓库与文档编号体系 (为 RFI 做准备)

Phase 2 | Application (6–12 周)

- 按 A-I 索引递交
- 建立补件战情室：Q&A Log、责任到人、72 小时应答机制

Phase 3 | Post-Licence (持续)

- 年度合规/AML/ICT 计划与证据链
- 重大变更报备闭环
- 护照通报与跨境营销合规审核机制常态化

20) 我司可提供的配套文件清单 (交付包)

- 《MiCA-CASP Programme of Operations (可递交版模板)》
- 《Business Plan (含三年预测+压力测试+审慎保障)》
- 《AML/CFT 手册 + Risk Assessment 方法论 + STR 决策树与记录模板》
- 《Travel Rule 数据字段与流程对接说明》
- 《ICT/DORA 合规包：外包治理制度 + 供应商尽调清单 + SLA 条款库 + 退出计划》
- 《客户协议/风险披露/费用披露/投诉机制 (整套)》
- 《Fit & Proper：董事/高管 CV 改写 + 技能矩阵 + 面谈题库》
- 《RFI 应答包 (Cover letter + 证据索引 + 版本控制)》
- 《护照通报包 (目标国清单 + 通报材料模板 + 营销合规审查表)》
- 《监管审查重点矩阵 + 甘特图 + RACI》

21) 唐生结论：波兰在 MiCA 版图中的定位

波兰更适合以下类型项目作为 MiCA 申请地与欧盟合规中枢：

1. 以“合规中台 + 技术与运营中心”驱动护照扩张 (中东欧成本与人才结构友好)；
 2. 愿意按 DORA 标准一次性把 ICT/外包治理建成体系 (避免获牌后大整改)；
 3. 股东结构清晰、SoF/SoW 能闭环、关键岗位可真实履职 (决定审批效率与成功率)。
- 同时需要客观提示：波兰本地实施法与收费细则仍在落地过程中，项目必须以“法规最终文本 + 监管沟通口径”为准并预留时间与预算缓冲。

22) 项目执行计划与甘特图 (里程碑示例)

- Week 1–2：范围定稿/差距评估/计划预算
- Week 3–6：股东与适任性包闭环/AML+ICT 框架
- Week 7–10：PoO+BP 定稿/条款披露/外包合同框架

- Week 11：递交
- Week 12–20：完整性审查 + RFI/面谈（多轮）
- Week 21–28：条件落实（注资/保险/系统验收/培训演练）→ 上线
- Week 29+：护照通报与跨境上线（分国家批次）

23) 监管审查重点矩阵（资本/适任性/AML/ICT/客户保护/护照）

审查项	监管关注	你必须提供的“证据形态”
运营方案（PoO）	服务类型/地点/方式清晰可审计	PoO 正文 + 客户旅程流程图 + 外包清单
审慎保障	风险覆盖与持续经营能力	资本/保险方案 + 三年预测 + 压力测试
股东/UBO	穿透 + SoF/SoW 闭环 + 声誉	结构图 + Money-Trail Map + 不利信息备忘录
董事适任性	胜任/诚信/时间投入/冲突	监管版 CV + 声明包 + Skill Matrix
AML/KYC	风险评估/监控/STR 留痕	AML 手册 + 规则库 + STR 决策记录
ICT/DORA/外包	可控、可审计、可退出	安全方案 + 外包制度 + SLA/审计权 + DR 演练
客户保护	披露透明/投诉/资产隔离	条款披露 + 费用表 + 投诉台账模板
护照	跨境通报与营销合规	通报包 + 目标国营销审查表

24) 结论与行动建议 + 申请建议 + 为何选择仁港永胜 + 关于仁港永胜

栏目定位说明：本栏目用于在“整套申请注册指南”最后一章，向董事会/投资人/项目组给出可执行的结论、最优实施路径、关键风险与缓释措施、项目管理打法，并以“交付包”形式阐明仁港永胜可提供的具体支持与边界，同时附上对外正式免责声明。

24.1 结论与行动建议（最关键三句话 + 深度解释与落地要点）

结论 1：先定服务范围，再定系统与制度深度——PoO（Programme of Operations）是申请的“总纲”。

- **为什么：**MiCA 体系下，监管对 CASP 的审查不是“你想做什么”，而是“你能否证明你已经准备好按某一明确业务模型持续运营”。PoO 贯穿：服务清单、客户旅程、风控/AML、资金与资产隔离、外包、ICT、投诉、数据、财务预测等，监管所有问题最终都会回到 PoO 的一致性。
- **落地动作：**
 1. 先做**服务清单映射表**（你到底要做：撮合/交易、托管、换币、执行订单、接收与传递订单、投顾/组合管理、转移服务等）
 2. 再画**客户旅程流程图**（开户→KYC→入金/链上入账→交易→提币→异常处置→投诉→关户）
 3. 最后把**制度、系统、外包、人员全部“挂”在流程图上**，确保每一环都有责任人与证据产出
- **你会获得什么：**PoO 一旦“闭环”，补件概率会显著下降；反之，所有材料会互相打架（这是最高频被质疑点）。

结论 2：股东/UBO 的 SoF/SoW 必须闭环可核验——这是 MiCA 申请最常见、最耗时的补件点。

- **为什么：**监管对虚拟资产业务高度敏感，股东/UBO 的资金来源与财富来源是“反洗钱入口”，一旦证据链不闭环，会触发持续补件，甚至导致整体项目停滞。
- **落地动作：**
 1. 做“**Money-Trail Map**”：资金从哪里来 → 经谁账户 → 何时入境/入账 → 何时注资/增资 → 对应银行流水/审计报告/完税证明
 2. 建“**解释 + 证据**”双层结构：解释信（叙事）+ 证据包（可核验材料）
 3. 对潜在敏感点（第三方代付、历史诉讼/负面、关联方交易、股权代持/一致行动）出具**专项说明信**与缓释措施（如回避、披露、治理安排）
- **你会获得什么：**把 SoF/SoW 做成“可审计资产包”，不仅用于获牌，更能直接用于银行开户、合作方尽调、后续扩张融资。

结论 3：ICT/外包按 DORA 一次性建好——DORA 已适用，越早对齐越省整改成本。

- **为什么：**监管不接受“先上线再补制度”。尤其托管、交易平台、钱包、多签、权限、日志、第三方云/外包等，如果不按 DORA 的外包治理、韧性与管理事件体系搭建，获牌前后都会被要求补齐，成本更高且影响上线节奏。
- **落地动作：**
 1. 先固化**安全与控制底座**：RBAC/MFA、密钥管理（HSM/分片）、冷/热钱包策略、多签门限、签名仪式、日志不可篡改
 2. 再固化**外包治理底座**：尽调→合同→SLA→审计权→分包控制→退出迁移（Exit Plan）
 3. 把**演练与证据**做成常态：BCP/DR 演练、渗透测试、漏洞管理闭环、事件响应演练与复盘
- **你会获得什么：**系统被审查时“说得清、拿得出、查得到”，大幅提高获批与后续监管检查的抗压能力。

24.2 申请建议（可直接执行 | “项目战术 + 标准动作 + 关键产物”）

以下适合直接抄进项目计划书与董事会纪要，由仁港永胜唐生拟定讲解。

A) 设立“补件战情室（RFI War-Room）”：四方联动 + 时间纪律

- **人员编制（最低）**：合规负责人、MLRO、技术负责人（CTO/安全）、运营负责人、法务/外部律师、财务/审计接口
- **机制**：
 - 统一 RFI 入口（不要多头回复）
 - 统一 Q&A 日志（每一问：责任人、截止时间、证据链接、版本号）
 - “72 小时首轮应答纪律”（先给结构与证据索引，再补充细节）
- **关键产物**：RFI Tracker、Answer Pack 模板、证据索引表（Evidence Index）

B) 建立证据仓库 Evidence Vault：从第一天开始“可证明运行”

- **归档原则**：每份制度 = “版本号 + 责任人 + 审批记录 + 培训记录 + 抽查记录 + 整改记录”
- **必须沉淀的证据类型**：
 1. 培训：签到、课件、测试、培训评估
 2. 抽查：KYC 抽查、制裁抽查、交易监控抽查、外包 SLA 抽查
 3. 演练：BCP/DR、事件响应、提款异常、密钥恢复
 4. STR：触发 → 调查 → 升级 → 决策 → 提交/不提交理由 → 复盘
 5. 治理：董事会/委员会纪要、风险接受记录、冲突审批记录
- **关键产物**：Evidence Vault 索引目录、留存周期表、监管抽查导出包

C) 外包合同必须写进“七件套条款”（监管最常问）

1. 审计权与取证权（含现场/远程）
 2. 数据安全与加密、数据所在地与跨境传输
 3. 分包控制（Subcontracting）与事前批准
 4. SLA/KPI 与违约救济（含服务中断赔付/降级机制）
 5. 事件通知与协作（通报时限、联合处置、根因分析）
 6. 业务连续性与灾备协作（RTO/RPO、演练频次）
 7. 退出迁移（Exit Plan：数据迁移、替代供应商、切换窗口）
- **关键产物**：Outsourcing Register、供应商尽调报告、合同条款库、Exit Plan

D) 护照扩张要做“国家级时间轴”（不要拿牌后才开始想）

- **做法**：按目标国拆“合规落地包”：营销审批规则、语言与披露、投诉渠道、消费者保护、当地广告合规、税务/VAT 影响、数据本地化要求（如有）
- **关键产物**：Passporting Roadmap、Country Pack 模板、Marketing Approval SOP

E) 把“资本/保险/预算”做成可承受的 24-36 个月运营模型

- **做法**：在三年预测里明确：人员成本、审计与法律、AML 工具、链上分析、SOC/安全、渗透测试、保险、云成本、外包成本
- **关键产物**：Budget Model（可调参）、压力测试（3 场景）、Wind-down Plan

24.3 为何选择仁港永胜（服务优势 | “我们交付什么、怎么交付、交付到什么颗粒度”）

24.3.1 一体化交付：把“监管语言”翻译成“可落地运行的制度 + 系统证据”

- **我们不是只写文件，而是把申请材料与落地运营绑在一起**：
 - MiCA 授权材料（PoO/治理/审慎保障/客户保护）
 - AML 制度与运行机制（风险评估、监控规则、STR 流程与证据）
 - ICT/DORA 外包治理与韧性体系（供应商尽调、合同条款、演练证据）
 - 客户条款与披露（可直接上线的 T&C/风险披露/费用披露/投诉机制）

- **价值：**避免“材料漂亮但无法运行”的监管否定。

24.3.2 强模板库 (Template Library)：可直接递交 + 可审计 + 可补件

- 你将获得（按需选配）：
 - BP/PoO 成套模板（含流程图、控制点、证据点）
 - Risk Register + RCSA（风险与控制自评）
 - STR 决策树 + 记录模板 + 提交流程图
 - 外包尽调清单 + Outsourcing Register + SLA 条款库 + Exit Plan
 - 面谈题库与标准答案结构（含“证据引用”）
 - RFI 应答包（Cover letter + Evidence Index + Version control）
 - 护照通报包（国家级落地清单 + 通报材料索引）
- **价值：**让项目从“写作型”变成“工程型”，提升通过率与速度。

24.3.3 实操导向 (Audit-ready)：以“可证明运行”作为最终验收标准

- **我们交付的每一份制度都配套：**审批链、培训包、抽查表、整改闭环表、证据留存规则。
- **我们做项目管理：**里程碑、RACI、Issue Log、Q&A Log、版本控制，确保你们内部团队能接续运维。
- **价值：**拿牌后不慌、不乱、不靠人治。

24.3.4 沟通与节奏：监管沟通、补件应答与董事会汇报“三线并行”

- 对监管：统一口径 + 证据索引 + 快速应答
- 对董事会：月度进展包 + 风险与决策点清单
- 对技术与运营：控制点落地清单 + 演练计划 + 上线验收表

24.4 关于仁港永胜

仁港永胜为专业的合规与金融咨询服务机构，专注于全球金融牌照申请、虚拟资产合规（MiCA/CASP、VASP）、支付与电子货币（EMI/PI）及持牌后持续合规维护。我们在香港、深圳及多个司法辖区协同配置合规团队，可为客户提供从战略评估 → 申请文件编制 → 面谈辅导 → 监管沟通 → 持牌后持续合规的一站式服务支持。

仁港永胜（香港）有限公司 | Rengangyongsheng (Hong Kong) Limited

- 官网：jrp-hk.com
- 香港：852-92984213（WhatsApp）
- 深圳：15920002080（微信同号）
- 电邮：tsy@cnjrp.com

办公地址：

- 香港湾仔轩尼诗道253-261号依时商业大厦18楼
- 深圳福田卓越世纪中心1号楼11楼
- 香港环球贸易广场86楼

注：本文涉及的模板/清单/电子档（如 Master Checklist、制度模板包、面谈题库等）可向仁港永胜唐生有偿索取。

24.5 免责声明

免责声明：本文由仁港永胜（香港）有限公司拟定并由唐生讲解，仅供一般信息与项目沟通之用，不构成亦不应被视为法律、税务、审计、会计、监管合规或投资建议。任何具体项目应结合申请主体实际业务模式、股权结构、客户群体、产品服务范围、系统架构、外包安排及目标市场要求，在取得合格的当地律师、税务师、审计师及其他专业人士意见后实施。波兰本地 MiCA 实施法、监管程序、官方费用、监管解释口径及审批时限等均可能随主管机关公告、二级/三级技术标准与监管实践更新而变化，应以最终颁布文本及 KNF/相关主管机关最新公告为准。仁港永胜对因使用本文信息而导致的任何直接或间接损失不承担责任（除非适用法律另有强制规定或双方另有书面约定）。

© 2025 仁港永胜（香港）有限公司 | Rengangyongsheng Compliance & Financial Licensing Solutions – 由仁港永胜唐生提供专业讲解。