斯洛文尼亚 Slovenia（MiCA）加密资产服务提供商（CASP）牌照

申请注册指南

Slovenia (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**唐上永（唐生，Tang Shangyong）**业务经理提供专业讲解。

服务商：**仁港永胜（香港）有限公司**｜**Rengangyongsheng (Hong Kong) Limited**

牌照名称：斯洛文尼亚 Slovenia（MiCA）加密资产服务提供商（CASP）牌照｜Crypto-Asset Service Provider（CASP）｜MiCA 体系下 Crypto-Asset Service Provider（CASP）授权

主管机构：Banka Slovenije（斯洛文尼亚央行）|ATVP（Agencija za trg vrednostnih papirjev，证券市场监管机构）

✅ 点击这里可以下载 PDF 文件：关于仁港永胜

注：本文模板、清单、Word/PDF 可编辑电子档，可向仁港永胜唐生有偿索取（用于监管递交与内部落地）。

适用对象

拟以**斯洛文尼亚 Slovenia**为 MiCA 申请国（**Home Member State**），申请并运营 **CASP（Crypto-Asset Service Provider）**，并在获批后通过 **MiCA 护照机制（passporting）**向欧盟其他成员国跨境展业的机构（交易所/经纪/OTC/托管/转账/投顾/做市相关等）。

法律底座（以欧盟主法 + 斯洛文尼亚落地为准）

- **MiCA：Regulation (EU) 2023/1114**（统一授权与持续监管框架）
- **Travel Rule / TFR：Regulation (EU) 2023/1113**（加密资产转账随行信息规则）
- **DORA：Regulation (EU) 2022/2554**（ICT 风险与数字韧性，外包/事件/测试/供应链）
- **斯洛文尼亚 MiCA 落地法：ZIUTK**（执行/程序/处罚框架等）
- **斯洛文尼亚 TFR 落地与配套：ZIUIPSK**（与加密转账信息/AML 衔接相关）

交付提示（PDF/附件索取）

本指南按"**可递交、可审计、可补件（RFI-ready）**"标准编制。可配套提供（可向仁港永胜唐生有偿索取）：

- Master Checklist（A–I：治理/资本/业务/AML/IT/外包/客户文件/报告/退出）
- BP 模板（监管可读版 + 财务模型）
- AML/CFT 手册 + Travel Rule 端到端 SOP + 监控规则库
- ICT/DORA 外包治理制度（外包审计权/退出条款包）
- 面谈题库（100–300 题）+ 现场演示脚本（证据链）
- MiCA 护照通报包（跨境展业通知材料包）

一、牌照名称、监管机构与"斯洛文尼亚路径"一句话结论

1）牌照名称

MiCA 体系下 Crypto-Asset Service Provider（CASP）授权（以斯洛文尼亚为 Home Member State，获批后可按 MiCA 护照机制向欧盟跨境提供已获批服务）。

2）监管机构（谁管什么：申请材料必须按"监管分工"拆册）

ESMA 公示的主管机关分工显示：

- **Banka Slovenije（斯洛文尼亚央行）**：负责 MiCA **Title III/IV/V**（其中 **Title IV 为 CASP** 授权核心）
- **ATVP（Agencija za trg vrednostnih papirjev，证券市场监管机构）**：负责 **Title II/VI**（通常更偏向白皮书/市场行为/滥用防控等模块）

  实操含义：**CASP 申请主线以 Banka Slovenije 的审慎/组织/风险/资本/外包/退出为轴**，同时把 **ATVP 关切的市场行为/披露/市场滥用防控**做成"可并行审阅"的子册（减少来回补件）。

3）一句话结论（给老板/投资人）

斯洛文尼亚 CASP 的关键不在"写一套材料"，而在于：把 MiCA 的要求做成**可运行的合规操作系统**（AML/Travel Rule/交易监控/权限与日志/外包审计权/对账/风控限额/投诉闭环），并能在监管面前**现场演示证据链**。

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。

按**欧盟 MiCA + TFR（Travel Rule）+ DORA**及**斯洛文尼亚主管机关分工**（ATVP / Banka Slovenije）最新公开框架进行"交付版"深度展开。斯洛文尼亚在 MiCA 下的主管机关分工（含 ATVP、Banka Slovenije）可参考 ESMA 已发布的成员国主管机关清单（2025-07 更新）。

二、MiCA 统一框架价值 + 斯洛文尼亚作为 Home Member State 的策略优势

2.1 MiCA 统一框架的核心价值

- **单一授权 + 护照机制**：一国获批，全欧盟跨境通报展业（设分支或自由提供服务）。
- **统一客户保护/治理/外包/记录保存与报告**：合规中台可复制到多个国家。
- **与 Travel Rule 并行**：涉及转账/托管/平台对接的，必须实现**字段 + 流程 + 留痕**端到端合规。

2.2 选择斯洛文尼亚的常见策略理由（实操视角）

- **监管分工清晰**（央行/证券监管各管一块），材料更易模块化、项目管理更可控。
- **过渡期已明确结束节点**：斯洛文尼亚采用较短过渡安排——已公开信息显示存量 VASP 可持续到 **2025-07-01**或直至申请被批/被拒（以规则适用为准）。
- **适合打造"欧盟合规运营中心"**：把合规、风控、技术与数据治理放在本地主体，再通过护照扩张（注意：营销与消费者保护仍需按落地国补丁）。

三、适用法律全景（EU 主法 + 斯洛文尼亚落地法 + 合规外延）

你在 BP/制度包中建议至少建立"**法规映射矩阵**"（条款 → 制度/SOP → 系统证据 → 附件编号）。

- MiCA（授权/持续义务/资本与审慎/治理/外包/投诉等）
- TFR/Travel Rule（转账信息随行、缺失处理、留存、互操作）
- DORA（ICT 风险、重大事件、外包第三方、韧性测试）
- **斯洛文尼亚：ZIUTK（MiCA 执行）**
- **斯洛文尼亚：ZIUIPSK（TFR/配套）**
- AML/CFT：FIU/主管机关沟通、STR/制裁/记录保存（见第十三章；斯洛文尼亚 AML 主管机关清单含"防止洗钱办公室"联系方式）

四、监管机构与分工（Banka Slovenije vs ATVP：双口径材料打法）

4.1 Banka Slovenije（央行侧：CASP 授权主线）

典型审查重点（你要用"证据链"回答）：

- 资本与持续经营、财务稳健性
- 公司治理、关键岗位、三道防线
- 风险管理（市场/流动性/操作/对手方/技术/合规）
- 重大外包与第三方风险、退出与迁移
- 业务连续性与有序退出（wind-down）

4.2 ATVP（证券监管侧：市场行为/滥用/披露等）

ATVP 公开提供 MiCA 相关指引入口/资讯汇集，可用于引用监管口径与 ESMA 指引。

> **项目管理建议**：
>
> - **主册（央行口径）**：申请表 + A–I 附件
> - **副册（ATVP 口径）**：市场行为/披露/市场滥用防控/平台规则（如申请平台类）

五、CASP 服务范围（MiCA 服务清单）与"申请组合策略"

5.1 先把"你到底提供什么服务"定清楚：这是整个申请的总开关

MiCA 不是"给你一个牌照随便做"，而是**按加密资产服务（crypto-asset services）逐项核准**：
你选的服务类别，会直接决定：

- **最低初始资本/持续自有资金（own funds）门槛**（第七章的资本模型会随之改变）
- **制度包厚度**（平台/托管/兑换类比"传递订单/执行订单"更重）
- **系统证据链要求**（尤其撮合、市场监测、钱包与密钥、对账、日志）
- **外包与第三方控制强度**（云、托管、KYC、链上分析、Travel Rule 通道）
- **监管面谈"必问模块"**（业务边界越重，面谈越技术化/可演示化）

在斯洛文尼亚，MiCA 相关本地信息入口由 ATVP 汇总并链接 EU 法与 ZIUTK（本地实施法）。

5.2 MiCA 下 CASP 典型服务模块（建议用"服务→流程→制度→系统证据"四联表写入 BP）

建议你在 BP / Operating Model 里，用下面这种"监管可读"的颗粒度写法：**每一项服务都要有端到端流程 + 控制点 + 留痕**。

A. 传递订单 / 接收与传递（RTO）

- 典型业务：经纪导流、报价聚合、路由到交易对手/平台
- 监管关注：客户分类与适当性（若触达零售）、费用与利益冲突披露、记录保存、广告合规
- 系统证据：订单链路日志（接收—路由—确认）、客户确认留存、渠道佣金与冲突披露台账

B. 代表客户执行订单（Execution）

- 典型业务：代客下单、代客成交、OTC 执行
- 监管关注：执行政策（best execution/公平执行）、滑点与价格偏离披露、冲突管理
- 证据链：执行政策文件 + 客户同意机制 + 成交回放（timestamp / quote source / routing）

C. 兑换：加密资产↔法币（Crypto-Fiat）/ 加密资产↔加密资产（Crypto-Crypto）

- 典型业务：现货兑换、报价、价差收入
- 监管关注：报价机制（来源、过滤、异常行情）、费用透明、市场操纵防控、客户资产隔离（如你持有客户资产）
- 证据链：报价源清单、异常报价过滤规则、价格快照存证、对账报表

D. 托管与管理（Custody & Administration）

- 典型业务：钱包托管、密钥管理、转出审批、白名单
- 监管关注：资产隔离、密钥控制、对账、保险/保障、权限分层、事件响应
- 证据链：MPC/多签流程图、HSM/密钥生命周期、对账与差异处理、可导出日志

E. 运营交易平台（Trading Platform）

- 典型业务：撮合引擎、盘口、订单簿、上币下币
- 监管关注：平台规则、市场监测、滥用识别、异常处置、上币治理、交易数据审计轨迹
- 证据链：Rulebook、监测规则库、异常处置工单、上币评估委员会纪要、不可篡改日志策略
  （ATVP 也在其 MiCA 指引栏目汇总 ESMA 指引（含市场滥用监测类）。）

F. 代表客户转移加密资产（Transfer）

- 典型业务：提币、链上转账、内部转账、跨 VASP 转账
- 监管关注：Travel Rule（EU 2023/1113）字段与流程、无法获取信息的处置、制裁与高风险地址拦截
- 证据链：Travel Rule SOP、字段映射、消息失败重试/人工复核、留存与审计导出机制

以上服务定义与框架来自 MiCA 主法及其授权逻辑（EU 2023/1114）。

5.3 “申请组合策略”——按监管难度、资本压力、系统压力分层（实操打法）

你可以把申请组合当成“三档路线图”，用**阶段化授权 + 后续扩项**降低一次性风险：

（1）合规入门组合（更易打穿、资本压力低）

- RTO / Execution / Transfer
  适合：经纪、OTC 执行、支付型转账场景
  核心交付：**AML + Travel Rule + 记录保存 + 冲突管理 + 投诉机制**（系统证据链要能演示“开户—交易—监控—报告—留痕”）

（2）中阶营收组合（兑换类为主）

- Exchange（Crypto-Fiat / Crypto-Crypto）+ Execution
  适合：现货兑换、撮合前置的报价执行
  核心交付：**报价与公平执行、异常行情处置、冲突隔离、对账与客户报表**

（3）重资产全栈组合（最吃资本与安全）

- Trading Platform + Custody + Exchange
  适合：交易所/托管平台
  核心交付：**平台规则 + 市场监控 + 上币治理 + 钱包安全 + 对账 + 外包治理 + 灾备演练 + 保险/保障方案**

六、申请主体与“实质运营（Substance）”要求（斯洛文尼亚落地核心门槛）

监管对“Substance”的判断，核心不是“你在斯洛文尼亚租了办公室”，而是：**决策、控制、关键职能、证据留存、可检查性**是否真实落在本地实体上；外包是否仍“可控、可审计、可退出”。
斯洛文尼亚 MiCA 本地框架由 ZIUTK 承接，并由 ATVP 汇总披露。

下面给你一套“可递交口径”的 Substance 交付结构（建议直接写进 BP，并配套附件）：

6.1 “有效管理（effective management）”四件套：监管要看你能被问责

（1）决策链（Decision Chain）可追溯

- 董事会/管理层职责矩阵（RACI）
- 授权矩阵（DoA：哪些事项必须董事会批、哪些可由 CEO/COO/CO 级别批）
- 会议机制：频率、议题清单、纪要模板、决议编号与附件索引（Index）

（2）关键控制职能（Key Control Functions）能独立履职
最少要把以下功能写成“岗位说明书 + 权限 + 升级路径 + 留痕”：

- 合规（Compliance）
- AML/MLRO
- 风险管理（Risk）
- 信息安全/ICT 风险（CISO/IT Security）
- 内审（可外包，但要独立性与审计权）

（3）监管检查可即时取证（Inspection Readiness）
必须承诺并证明：

- 客户 KYC/KYB 文件可即时导出
- 交易、撮合、转账、风控、告警、处置工单可回放
- 安全日志、权限变更、密钥签名审批链可导出
- 外包合同可出示（含审计权/监管访问权/数据权/退出条款）

（4）关键活动不等于“外包甩锅”
外包可以，但必须满足：你仍拥有**控制权、可解释性、复核能力**。
（外包治理的细化条款建议你在第十九章形成模板包；这里先把 Substance 的核心边界定清。）

6.2 组织与人员“最低可解释模型”（建议口径）

小型/中型 CASP（非平台/非托管重业务）建议：

- 董事会（含 1 名具金融合规/风险背景成员更优）
- CEO/COO（负责日常管理与业务连续性）
- Compliance Officer（2LOD）
- MLRO（可与合规分工或兼任，但要避免与销售 KPI 绑定）
- IT Security / ICT Risk Owner（可外包执行，但要内部负责人）
- 内审（外包可行，但要年度计划、底稿与整改闭环）

平台/托管类 CASP必须把“技术与安全”抬到更高优先级：

- 交易平台：Market Surveillance Owner（市场监测负责人）
- 托管：Wallet Security Owner（钱包/密钥负责人）+ 对账负责人（Reconciliation Owner）
- 事件响应：IR 负责人 + 24/7 值守机制（或委外 SOC 但保留控制权）

6.3 “三份图” + “两本账”是 Substance 的必交付件

三份图（建议强制做成附件 A3 可打印）

1. 集团穿透图（到自然人 UBO，含控制权说明）
2. 组织架构图（含三道防线与关键岗位汇报线）
3. 系统架构三流图：业务流 / 数据流 / 权限流（含第三方与跨境数据路径）

两本账

- 权限台账：RBAC 角色、特权账号、审批链、变更留痕
- 外包台账：供应商清单、重要性分级、年度评估、退出预案、审计记录

七、资本金与审慎保障（MiCA 取高规则）+ 现金流可持续证明

7.1 资本规则的“监管语言”：不是“我有钱”，而是“我持续稳健”

MiCA 对 CASP 的审慎逻辑，通常体现为三层：

1. **初始资本（initial capital）门槛**：按服务类别分档
2. **持续自有资金/审慎保障（own funds / prudential safeguards）**：需要持续维持，且通常与固定开支、风险暴露相关
3. **现金流可持续（going concern）证明**：监管会用压力情景看你能否覆盖合规成本与运营成本

MiCA 主法适用全欧盟，且自 2024-12-30 起全面适用（相关解读也常见于权威律所）。

7.2 初始资本分档（实操写法：把服务组合映射到资本档）

市场通行的 MiCA 分档口径（亦被多份合规解读引用）为：

- **€50,000**：偏“轻服务”（如投顾/组合管理、传递/执行等非托管非平台重业务）
- **€125,000**：涉及**托管**与/或**兑换**等更高风险服务
- **€150,000**：涉及**运营交易平台**（Trading Platform）等最高档位
  （分档逻辑在多家合规解读中一致呈现；你在申请材料里应以 MiCA 条文表述为准，并在“资本测算表”中逐项映射服务清单。）

  交付建议（监管最喜欢）：做一张“服务→资本档→附加制度包→系统证据包”的映射表，并写清“取高规则”：
  若你同时申请多项服务，按要求取更高档位，并叠加相应的风控/系统/外包治理证据。

7.3 “MiCA 取高规则 + 固定开支口径”怎么写得像真的（而不是 PPT）

监管最怕两件事：

- **资本刚达标，但现金流撑不起合规成本**
- **预算表漏掉关键合规支出（尤其平台/托管/Travel Rule/安全）**

所以你至少要交付“三张表 + 两个机制”：

（1）资本测算表（Capital Calculation Sheet）

包含：

- 申请服务清单（逐项）
- 对应资本档位（解释为何归档）
- 资本形式（实缴股本、留存收益等；并说明不可接受的“软资本”）
- 资本到位证明（银行入资、验资/会计证明、股东决议）

（2）固定开支口径说明（Fixed Overheads Memo）

把所有“监管必花钱”的东西写进去（尤其常被漏掉的）：

- 人员：合规、AML、风控、内审、信息安全、客服工单
- 工具：KYC/制裁、链上分析、交易监控、Travel Rule 通道
- 安全：渗透测试、漏洞扫描、代码审计、SIEM/SOC（自建或委外）
- 审计与法律：财务审计、合规外部评估、法律意见
- 外包治理：年度供应商审计/评估费用、退出迁移预案成本
- 灾备：DR 环境、演练成本、备份与密钥保管设施

（3）3 年财务预测 + 12 个月滚动现金流（Financial Model）

至少交付：

- P&L、资产负债表、现金流量表
- 单位经济模型（每客户获客成本、每笔交易毛利、留存率）
- 月度 burn rate（最坏月度现金消耗）
- **压力测试**：
  - 市场波动导致交易量下滑
  - 黑天鹅安全事件（停机、赔付、额外安全投入）
  - 监管要求升级（新增报告、提高监测强度、额外人手）

（4）资本补充机制（Capital Top-up Mechanism）

写清：

- 触发条件（亏损、快速扩张、重大事件、监管要求）
- 补充路径（股东增资承诺、可行融资渠道、预算削减预案）

- 治理审批（董事会决议流程、时限、对监管通报原则）

（5）客户资产保护/审慎保障机制（Client Asset & Safeguards）

尤其涉及托管/平台/兑换时，必须写清并提供证据链：

- 客户资产隔离（链上地址隔离、账务隔离、法币隔离账户）
- 对账机制（频率、差异处理、追溯与纠正）
- 保险/保障安排（如采用）与覆盖范围说明
- 重大事件下的客户资产处置路径（与第 23 章 Wind-down 衔接）

7.4 斯洛文尼亚落地时的“口径提醒”（避免补件）

- **以 ATVP/本地 ZIUTK 入口对齐**：目录与引用要能直接链接到本地实施法与 EU 主法，减少“法源不清”补件。
- **平台/托管越重，越要把资本与安全预算写实**：否则监管会追问“你拿什么持续履行客户保护与安全义务”。
- **把资本与现金流写成“可检查的证据链”**：银行证明、董事会决议、预算批复、供应商合同报价、审计/安全报告计划表——这些都能显著提高通过率与降低补件轮次。

八、股东/UBO 与适当人选（Fit & Proper）+ SoF/SoW（资金/财富来源）

8.1 监管核心判断：你“是谁、钱从哪来、会不会干预合规”

在 MiCA 授权语境下，“股东/UBO 审查”通常不止是形式上的 KYC，而是**控制权风险**与**金融犯罪风险**的前置筛查，监管会围绕三条线做结论：

1. **控制权透明**：是否能穿透至最终自然人（UBO），并解释控制权如何实现（股权、表决权、协议控制、董事委派权、否决权等）。
2. **适当性与诚信**：是否存在重大违法犯罪/监管处罚/破产清算/重大诉讼/失信记录/制裁命中等。
3. **资金路径可审计**：SoF/SoW 能否形成“可回放证据链”，且与税务与资产形成逻辑一致（不自相矛盾）。

   实务提醒：很多申请被“卡住”并非股东不合规，而是**资金路径解释与文件证据不闭环**（尤其跨境注资、多层控股、加密资产收益、OTC/场外资金往来、家办结构等）。

8.2 适用对象范围（谁必须做尽调、做多深）

建议在项目启动即按“强制+高风险扩展”两层锁定人员/实体清单（后续 RFI 会围绕它补件）：

A. 强制尽调对象（建议默认全做）

- 直接或间接 **⩾10% 持股**股东（自然人/法人）
- 控股股东、实际控制人（含协议控制/一致行动）
- **最终 UBO（穿透至自然人）**
- 董事、CEO/GM 等管理层（与第十章岗位胜任力联动）
- 关键关联方：集团母公司/同控实体/共享服务中心（若影响运营与数据）

B. 高风险扩展对象（触发则纳入）

- 资金提供方（如股东借款、可转债、夹层融资、融资担保人）
- 关键业务伙伴：做市商、流动性提供者、托管方、清算/支付通道方
- 重大外包商的控制方（若被认为“关键功能外包”导致实控外移）

8.3 Fit & Proper（适当人选）——交付口径与证据清单

把适当性做成“可审核包”（不是一句话声明）。建议以“四维度+证据索引”交付：

8.3.1 声誉与合规记录（Reputation）

要点：刑事/行政违法、金融监管处罚、AML 处罚、市场操纵/欺诈、重大诉讼仲裁、被监管取消资格、制裁命中等。
证据（建议）

- 无犯罪记录证明 / 良民证（适用时）
- 监管处罚与诉讼披露声明（Declaration）+ 解释备忘录（如有历史事项）
- 制裁/PEP/负面新闻筛查报告（含复核记录与结论）
- 董事/高管过往雇主证明或推荐信（可选但加分）

8.3.2 能力与经验（Competence）

要点：股东/控制人是否具备“理解受监管业务”的能力（尤其平台/托管等高风险业务），以及是否会引入不当干预。
证据（建议）

- 股东/UBO 简历（CV）+ 业务履历证明
- 关联企业业务说明与监管资质（如曾控股金融机构/加密机构）

8.3.3 财务稳健性（Financial Soundness）

要点：是否存在过度杠杆收购、资不抵债、重大违约、无法解释的资金暴露。
证据（建议）

- 财务状况声明 + 资产负债概览（高持股股东建议提供）
- 银行资信证明/资产证明（分级提供）

8.3.4 独立性与诚信（Integrity & Independence）

要点：是否存在利益冲突未披露、关联交易控制平台规则、项目方控制上币决策、做市商控制风控参数等。
证据（建议）

- 关联方清单（Related Parties Register）
- 利益冲突披露表 + 回避机制
- 股东协议关键条款摘要（否决权/控制权/业绩对赌是否影响合规独立）

8.4 SoW/SoF（财富/资金来源）——“监管可回放”的证据链设计

这是最关键模块之一，建议按“**SoW 解释财富形成** + **SoF 解释本次入资资金**”双层搭建。

8.4.1 SoW（Source of Wealth）财富来源——解释“你整体财富怎么来的”

常见可接受类型（需匹配证明文件）：

- 长期薪酬/分红（雇佣合同、完税证明、分红决议）
- 企业经营利润（审计报表、股权证明、分红/退出协议）
- 投资收益（券商对账单、基金报告、资产出售协议）
- 资产处置（房产/股权/企业出售：买卖协议、收款证明、税务文件）
- 加密资产收益（**需特别谨慎**：必须证明来源合规、交易路径与对手方清洁度、税务处理一致）

8.4.2 SoF（Source of Funds）资金来源——解释“这笔钱怎么到公司资本金账户”

你要给监管的是**资金路径图**（Money Trail Map）：

> Source（来源账户） → 银行 A →（换汇/支付）→ 银行 B → 公司资本金账户
> 并且每一跳都有文件支持与解释：

- 银行流水（覆盖关键日期与金额）
- 换汇/支付凭证（SWIFT、FX contract、支付指令）
- 入资证明（验资/银行入账证明）
- 如为借款/融资：贷款合同、放款凭证、还款计划与财务可持续性说明

8.4.3 证据链“最容易被质疑”的 6 类情形（提前规避）

1. 资金来自高风险司法辖区或无法解释的中间账户
2. 资金多次拆分汇入（structuring）或短期频繁大额进出
3. 大量来自 OTC/场外换汇/第三方代付
4. 加密资产变现未提供交易所/链上证据与税务解释
5. 家办/信托结构未解释受益人、控制权与资金分配规则
6. 资金来源文件与商业计划/资本金规模不匹配（例如“只有一页声明”）

8.5 “重大持股/10% 规则”+ 持续通知义务（把合规写进公司治理）

建议把股东与控制权管理制度化（否则获批后也会成为检查重点）：
建议纳入公司制度/章程/股东协议的触发器

- 直接或间接持股达到/跨越/低于 **10%** 的变动
- 控制权变化（投票权协议、一致行动、质押导致控制权转移）
- UBO 变化或受益安排变化
- 股东被调查、制裁命中、出现重大负面事件
- 资金结构重大变化（新增重大债务、再融资、对赌条款触发等）

  交付建议：做一份《股东与控制权变更 SOP》（RACI+时限+模板），把“何时通知、通知什么、谁批准、证据留存”写清楚。

九、公司治理（Governance）与“三道防线”落地（监管可问责模型）

9.1 治理目标：让监管看到“能管住风险、追责到人、留痕可审计”

MiCA 下 CASP 的治理不是“写一个董事会章程”，而是要证明：

- **决策机制**：谁提出、谁审批、谁复核、谁能否决
- **风险与合规独立性**：业务不能自己给自己开绿灯
- **证据链**：会议纪要、审批记录、告警处置记录、审计底稿、整改闭环
- **外包可控性**：关键外包不等于“把合规外包掉”

同时，ESMA 也在持续强化对 CASP 的监管一致性与行为标准，尤其关注**误导营销与受规管/不受规管产品混同**等风险点。

9.2 “三道防线”在 CASP 的可落地版本（小团队也能跑）

第一线（1LOD｜业务线自控）

覆盖：开户、交易、托管、客服、上币、风控运营
交付要求：

- 每个关键流程都有 SOP：开户审批、风险评分、限额调整、异常交易处置
- 业务人员必须留痕：工单、审批链、对客沟通记录
- KPI 不能鼓励违规（例如把成交量与合规豁免绑定）

第二线（2LOD｜合规/风险/AML/信息安全）

覆盖：合规监督、风险框架、AML/制裁、Travel Rule 质检、信息安全控制
交付要求：

- 合规意见必须“可追溯”（谁签、依据条款、附件编号）
- 规则库与阈值调整要有审批与复核
- AML 与交易监控必须可解释、可抽样复核、可导出报告
- 信息安全要有资产清单、权限模型、日志与事件响应（与第十八章联动）

第三线（3LOD｜内审/独立审查）

小公司可以外包内审，但必须做到：

- 内审计划（年度）+ 抽样测试方法
- 审计底稿与整改闭环（缺陷评级、整改责任人、完成日期、复核记录）
- 外包内审合同具备审计权、数据访问权与保密条款

9.3 治理结构建议（可直接用于递交附件）

建议按“最少但够用”原则配置委员会与文件：

治理文件包（建议清单）

- Governance Charter（治理总章程）
- Board Terms of Reference（董事会职权）
- 委员会章程（按规模选择）：风险委员会/审计委员会/合规委员会
- Delegation of Authority（DoA 授权矩阵：金额阈值、事项类型、审批层级）
- RACI Matrix（流程责任矩阵）
- Conflicts of Interest Policy（利益冲突政策：披露、回避、记录、对外披露）
- Related Party Transactions Policy（关联交易政策）
- Remuneration Policy（薪酬与激励：避免诱导违规）
- Whistleblowing Policy（举报与保护机制）
- Record Retention & Auditability Standard（记录保存与可审计性标准）

9.4 董事会“可问责”的证据链：监管最爱看的 8 个东西

1. 董事会年度日历（议题规划：风险、合规、审计、外包复核）
2. 会议纪要模板（含决议编号、附件索引、表决结果、回避记录）
3. 风险偏好声明（Risk Appetite Statement）+ KRI/KPI 面板
4. 风险登记册（Risk Register）+ 控制措施与剩余风险评估
5. 合规年度计划（含培训、抽样检查、制度更新节奏）
6. AML 年度有效性评估（含 Travel Rule 质检结果）
7. 外包年度复核报告（供应商评分、事故统计、退出演练）
8. 重大事件复盘（安全事件/市场异常/重大投诉：根因+整改+复核）

9.5 利益冲突：CASP 最容易踩雷的“治理红区”

建议把利益冲突做成“登记—审批—披露—抽查”闭环，重点覆盖：

- 项目方/做市商/股东对上币治理的影响
- 自营交易与客户交易冲突（如有）
- 员工个人交易、礼品招待、介绍费/返佣
- KOL/代理渠道营销的误导性风险（与客户披露联动）
- 同一集团内共享系统/共享人员导致的数据与权限串联风险

十、关键人员与岗位胜任力（面谈“必问模块”）

10.1 监管面谈的底层逻辑：不是问“你懂不懂”，而是问“你能不能负责”

MiCA 面谈与 RFI（补件）经常围绕“关键岗位”做穿透式提问。
此外，ESMA 已发布多份与 CASP 相关的指南（例如：**知识与能力**、**适当性与定期报表**等），会实质影响监管对人员胜任力的口径与检查方式。

10.2 “关键岗位清单”与最低交付要求（建议直接做成附件）

下面按“岗位—必须提交—面谈常问”给你交付版口径。

A. 董事/高级管理层（Management Body：CEO/COO/CFO/GM）

必须提交

- 监管版 CV（突出受监管行业、治理、风险与技术理解）
- 岗位职责说明书（JD）+ 汇报线（必须能追到董事会）
- 有效管理（effective management）证明：出勤安排、签批权限、值勤机制
- 重大外包审批机制、预算与资源安排证明

面谈常问

- 你申请的服务组合里，最大风险是什么？如何量化与控制？
- 出现重大安全事件/挤兑/市场异常，谁拍板？依据什么阈值？
- 外包到集团/第三方后，你如何确保仍由你控制？退出怎么做？

B. 合规负责人（Compliance Officer）

必须提交

- MiCA 行为义务映射表（条款→制度→流程→证据）
- 合规年度计划、培训计划、抽样检查计划
- 客户披露与营销审查机制（避免“受规管/不受规管混同”）

面谈常问

- 你如何确保对外宣传不误导？哪些内容必须披露？
- 投诉与争议处理的 SLA 是什么？如何复盘与整改？
- 如何处理利益冲突与关联交易？

C. MLRO / AML 负责人（含制裁与 Travel Rule）

必须提交

- 企业级 AML 风险评估（方法论、评分、年度复核）
- STR 决策流程与证据链（告警→调查→结论→上报→留存）
- Travel Rule 端到端 SOP（字段、对接、异常处理、留存）
- 名单筛查（制裁/PEP/负面新闻）命中处置与复核记录机制

面谈常问

- 你们的高风险客户 EDD 触发器是什么？谁批准？
- Travel Rule 信息缺失怎么办？拒绝/延迟/人工复核的规则是什么？
- 你如何证明监控有效（不是“装了系统”）？

D. 风险负责人（Risk Officer，若公司规模允许；或由第二线承担）

必须提交

- 风险偏好声明、限额体系、压力测试
- 操作风险与第三方风险管理框架
- KRI 报告样式与升级路径

面谈常问

- 市场剧烈波动下，你们怎么控制滑点、穿仓、流动性枯竭？
- 第三方事故如何纳入风险报告？如何触发退出？

E. 信息安全负责人（CISO/IT Security Officer）

必须提交

- 系统架构三张图：业务流/数据流/权限流
- RBAC 最小权限与特权账号审计
- 日志与监控（SIEM/SOC）策略、渗透测试与整改闭环

- 事件响应预案 + 演练记录 + BCP/DR（RTO/RPO）

面谈常问

- 你怎么证明密钥安全/钱包安全？多签/MPC 的审批链是什么？
- 发生泄露/被盗，第一小时怎么做？谁授权冻结？怎么取证？
- 数据在外包商/云上，监管可访问性如何保障？

10.3 知识与能力（K&C）体系：把“胜任力”制度化

建议直接建立《知识与能力管理制度》并形成可审计记录：

- 岗位能力矩阵（岗位→必备知识领域→最低年限/证书/培训时长）
- 入职/年度培训计划与考试题库
- 关键岗位持续胜任力评估（每年/半年度）
  ESMA 已就 MiCA 场景下的知识与能力评估发布指南/报告，可作为你制度设计的重要欧盟口径依据。

10.4 仁港永胜“面谈必胜打法”（可复制执行）

1. **把每个岗位 JD 映射 MiCA 条款**：条款→SOP→证据（附件编号）
2. **准备“标准答案卡”**：每岗 30–50 题（可背诵、可追溯）
3. **做一场“系统演示彩排”**：开户、监控告警、Travel Rule、日志导出、权限审批、投诉工单
4. **预制 RFI（补件）应答结构**：监管问题→依据→改进→证据→责任人→完成日（形成闭环）

仁港永胜建议（针对斯洛文尼亚 CASP 的可执行清单）

- **先定服务组合**：MiCA 服务类别选定后，资本、系统、治理、披露才能一一对齐。
- **股东/资金链前置**：SoF/SoW 做成“可回放证据链”，避免后期补件拖延。
- **治理先做证据链**：会议纪要模板、DoA、RACI、冲突登记册、外包年度复核报告先跑起来。
- **关键岗位先到位再递交**：胜任力不是简历，而是“制度+流程+演示+留痕”。
- **营销合规要单独加固**：杜绝“拿 MiCA 牌照做噱头、把不受规管产品混卖”的红线风险。

选择仁港永胜的好处（核心优势）

- **监管导向的材料工程化能力**：把条款写成“可递交、可审计、可补件”的证据链与索引体系。
- **模板库可直接落地**：股东尽调包、SoF/SoW 证据链包、治理三道防线包、K&C 胜任力体系、RFI 应答包、面谈题库等。
- **跨境护照与集团结构经验**：多层控股穿透、共享服务/外包治理、数据与权限分层、跨境营销合规补丁一体化交付。

十一、所需材料清单（Master Checklist）A–I（交付版｜对齐 Banka Slovenije/ATVP 并行审阅）

> 交付方法论：**用“ITS 表格字段 → 附件编号 → 证据链位置”**做交叉引用。监管真正看的不是“写得漂亮”，而是你能否：1）清晰声明申请服务边界；2）证明可持续经营；3）证明 AML/TFR 可运行；4）证明 ICT/外包可控；5）证明客户保护与披露可上线。

A｜申请人身份与公司法文件（Applicant & Corporate）

A1 主体身份与注册文件

- 公司注册证书、章程（Articles）、商业登记摘录、税号、LEI（如已办理/计划办理）
- 董事会/股东会决议：授权申请 CASP、任命关键岗位、批准外包、批准资本注入与资金来源说明
- 申请主体在集团内定位说明：是否为控股主体/运营主体/技术中台/持牌主体

A2 集团与控制权披露（强制“可穿透”）

- 集团股权结构穿透图（到自然人 UBO）
- 控制权说明：投票权、否决权、委派权、协议控制（SHA/投票协议/可转换债等）
- 关联方清单：母公司、兄弟公司、共享服务公司、做市/流动性提供、项目方、外包方（含潜在冲突说明）

A3 在斯洛文尼亚的设立与“实质运营”证据（Substance Pack）

- 实际办公场地证明：租赁/产权、照片、工位/门禁、IT 资产清单、会议室/档案区
- 关键人员在欧盟/当地的履职安排：雇佣合同、值勤表、远程与在场机制、签批权限链
- 关键管理与控制在当地的证明：董事会会议安排、会议纪要模板、授权矩阵（DoA）

B｜业务模式与商业计划（Business Plan & Operating Model）

B1 3年 BP（监管可读版）

- 产品与客户：零售/专业客户分层、地域分布、渠道（直营/代理/KOL/白标）
- 业务流程“端到端”：开户→风评→下单/撮合/执行→清算交收→对账→争议→退出
- 收费与收入拆解：交易费、点差、托管费、上币费、提币费、质押收益等（逐项披露是否对客户透明）

B2 财务模型与可持续经营（Going Concern Evidence）

- 3年 P&L / BS / CF（含月度现金消耗、关键假设、压力情景）
- 合规成本写实：AML 工具、TFR 通道、链上分析、SOC/SIEM、渗透测试、外包审计权成本等
- 资本补充机制：触发条件 + 股东承诺函 + 融资路径

B3 市场进入与营销合规模块

- 营销政策：禁止误导、禁止收益承诺、KOL/代理管理、佣金披露与冲突管理
- 客户入门材料：风险披露、费用披露、关键条款摘要（Plain Language）

C｜公司治理与内控框架（Governance & Internal Control）

- 治理章程（Board Charter）与委员会职责（风险/合规/审计）
- 三道防线（1LOD/2LOD/3LOD）RACI + 报告路线图
- 利益冲突政策（含员工交易、礼品招待、关联方交易、信息隔离墙）
- 记录保存与可审计性：日志、工单、录音录像、审批留痕、数据导出机制

D｜资本金与审慎保障（Prudential Safeguards）

- 最低资本测算表（按所申请服务类型映射）+ “取高规则”说明
- 资本注入证明：银行入资、验资/审计口径说明
- 客户资产隔离：链上地址隔离、法币客户资金隔离账户、对账频率与差异处置
- 会计制度与外部审计安排：月度管理报表模板、年审计划、关键会计政策

E｜AML/CFT + Travel Rule（Financial Crime Compliance）

- 企业级 ML/TF 风险评估（方法论、评分卡、年度复核）
- CDD/EDD/KYB：UBO 穿透、PEP/制裁/负面新闻、来源资金/财富证据链
- 交易监控：规则库、阈值、告警分级、调查底稿、STR 决策与提交 SOP
- TFR（EU 2023/1113）落地：字段、消息标准、VASP 对接、缺失信息处置与留存机制

F｜ICT / DORA 数字韧性（ICT Risk & DORA Alignment）

- ICT 风险管理框架：资产清单、补丁/漏洞管理、威胁建模
- 权限体系：RBAC、特权账号审计、变更管理
- 日志与证据：不可篡改日志、时间同步、SIEM/SOC 流程
- 事件响应：分级、通报、根因分析、复盘整改闭环（含演练记录）

G｜外包治理与第三方风险（Outsourcing & Third-Party）

- 外包清单与重大外包识别（云、托管、KYC、链上分析、撮合引擎、客服等）
- 第三方尽调：安全、合规资质、财务稳定性、分包链
- 合同关键条款包：审计权/监管可访问、数据权属与驻留、分包限制、退出与迁移

H｜客户保护与市场行为（Conduct, Disclosures & Client Protection）

- 客户协议（T&Cs）与披露包：费用、风险、执行政策、冲突披露、投诉渠道
- 适当性/合适性（如涉及投顾/组合管理）：问卷、知识测评、产品分层、强提醒
- 市场滥用防控：异常交易监测、刷量/操纵识别、内部信息墙、上币/下币治理

I｜监管沟通、递交流程与护照通报（Regulatory Process & Passporting）

- ITS 表格 + 附件 Index（字段→附件编号→页码/段落）
- RFI（补件）应答包模板：**条款依据→回应→整改→证据→责任人→日期**
- MiCA 护照通报包：目标成员国清单、服务范围、当地营销/消费者保护补丁清单

  注：斯洛文尼亚监管实践中，CASP 口径主要由 ATVP 侧进行监管沟通与指南发布/承接；你在材料包结构上建议拆成“审慎/组织与风控包”与“行为/客户保护包”两册，并提供统一 Index，提高并行审阅效率。

十二、董事/股东/合规人员/管理人员要求：什么情况下符合申请人条件（交付版）

核心原则：MiCA 对 CASP 的授权要求，落地到审查动作本质上就是三句话：
（1）谁在控制公司；（2）公司由谁在真实运营；（3）关键风险是否被独立且可问责地管理。

12.1 董事与高管（Management Body）——“有效管理”与问责链

最低合格画像（建议交付口径）

- 覆盖与你申请服务相匹配的经验：交易平台/托管安全/AML/ICT/风控/运营中的至少两项以上
- 能用“条款→制度→SOP→证据链”回答：客户保护、冲突管理、资产隔离、外包治理、记录保存、异常处置
- “有效管理”证明：
  - DoA（授权矩阵）、签批权限
  - 例会机制（周/月/季）、董事会纪要模板与决议编号
  - 重大事件升级链（安全事件/资金风险/重大投诉/重大外包）

常见不通过点（你要在材料里主动规避）

- 全部管理层在欧盟外 + 当地仅“挂名办公室”
- 没有人能解释撮合/钱包安全/监控规则库（监管会认为不可控）
- 决策外包给集团母公司但无监督、无审计权、无退出预案

12.2 股东/UBO/重大持股（≥10%）——Fit & Proper + 穿透 + SoF/SoW

强制尽调对象范围（建议你在尽调矩阵里写清）

- ≥10% 股东、控股股东、实际控制人、最终 UBO（穿透至自然人）
- 董事/高管（含关键控制职能负责人）
- 关键外包方的控制人/关联方（如形成重大利益冲突）

Fit & Proper 四维度（交付版写法）

1. **声誉**：刑事/行政处罚、监管处分、重大诉讼、制裁/观察名单
2. **能力**：角色匹配度、过往管理与合规履历、关键岗位胜任力
3. **财务稳健性**：破产/重大债务/杠杆收购风险、可疑资金通道

4. **诚信与独立性**：利益冲突披露、关联交易透明、控制权安排清晰

SoF / SoW（资金/财富来源）证据链（建议按风险分层）

- SoW：财富形成路径（经营利润/薪酬分红/投资收益/资产处置）+ 税务/审计证明
- SoF：本次入资/收购资金路径（Source→银行A→支付/换汇→银行B→资本金账户）
- 每一跳解释：金额、时间、对手方、凭证（流水/合同/完税/审计报告）

持续通知与变更触发器（建议写进公司制度 + 股东协议）

- 股权达到/跨越 10% 的变化、控制权变化、UBO 变化
- 董事/高管变更、关键外包变更、资金结构重大变化
- 重大负面事件：被调查、被制裁、重大诉讼/破产风险

12.3 关键控制职能（Compliance / MLRO / Risk / Internal Audit）——独立性与资源

监管最关注你能否“独立制衡业务”

- 合规负责人：制度、合规意见、营销审查、投诉与纠纷、年度合规计划
- MLRO：AML 风险评估、监控规则库、STR 决策、培训与独立复核
- 风险负责人：风险偏好、限额/KRI、压力测试、风险报告
- 内审：年度计划、抽样测试、整改闭环（小机构可外包但要独立性与审计权）

“合格”的证据链（建议你逐项准备）

- 任命决议 + JD（岗位说明书）+ 直接向董事会汇报的路线
- 预算/资源证明：系统权限、数据调取权、外包审计权
- 年度计划：合规计划、AML 年审、内审计划、ICT 演练计划

12.4 一张“可递交判定表”（你内部用来过线）

满足以下 8 项，基本可进入“可递交阶段”（监管沟通/预审更顺畅）：

1. 服务边界已做 MiCA 映射（每项服务都有制度与系统支撑）
2. 当地实质运营成立（场地+关键岗位+决策链）
3. 资本满足 + 12 个月持续经营证明（含压力情景）
4. 三道防线落地（RACI/DoA/会议纪要）
5. AML/TFR 可运行可演示（开户→监控→STR→留存）
6. ICT/DORA 可解释（架构/权限/日志/渗透测试/演练）
7. 外包可控（审计权/退出权/监管可访问）
8. 客户保护与披露可上线（协议+披露+投诉机制）

十三、AML/CFT + Travel Rule（TFR）端到端运营设计（交付版要点）

> 结论先行：CASP 的 AML/TFR 不是“写一本手册”，而是**可运行的“制度 + 系统 + 留痕 + 复核 + 报告”闭环**。其中 TFR（EU 2023/1113）要求你对转账随行信息做到字段、流程、异常处置与留存。

13.1 AML 总体框架（Policy Stack）

你应形成“六件套”并能演示：

1. AML 总政策（董事会批准、年度复核）
2. 企业级 ML/TF 风险评估（方法论、评分卡、复核机制）
3. CDD/EDD/KYB 操作规程（含 UBO 穿透与 SoF/SoW）
4. 制裁/PEP/负面新闻筛查制度（命中处置与误报复核）
5. 交易监控与可疑申报（规则库、调查底稿、STR 决策 SOP）
6. 培训与独立审查（年度计划、测试题库、抽样复核、整改闭环）

13.2 客户生命周期（Onboarding → Ongoing → Exit）“可审计证据链”

开户（KYC/KYB）

- 身份核验、地址证明、税务居民声明
- UBO 穿透至自然人（多层结构要解释控制权）
- 风险分级：客户/产品/地域/渠道
- SoF/SoW：按风险分层收集（证据链要可回放）

持续尽调（Ongoing Due Diligence）

- 触发器：交易量突增、频繁小额分拆、风险地址交互、制裁命中、资料过期
- 动态调档：补充文件、重新评级、限制/冻结/终止

退出（Offboarding）

- 触发条件：拒绝提供信息、持续异常、制裁/高风险不可接受
- 清退流程：资产提取、对账、留存、必要时 STR/监管沟通

13.3 交易监控（On-chain + Off-chain）与 STR 决策

规则库建议分三层（交付可直接用）

- L1 阈值规则：金额/频次/分拆/异常时段
- L2 行为模式：混币/跳转、短进短出、跨链桥高频、与高风险 VASP 对敲
- L3 网络与关联：多账户同设备/同IP、关联地址簇、与已知风险实体关系

告警处理流程（必须留痕）

- 告警分级（低/中/高）→ 指派调查员 → 调档 → 结论 → 处置（放行/延迟/拒绝/冻结/终止）
- STR 决策记录：为什么报/为什么不报、复核人、时间戳、证据附件编号

13.4 Travel Rule（TFR）端到端落地（字段 + 流程 + 异常处置 + 留存）

（1）字段与数据标准（你要写进系统需求与 SOP）

- 发起方/受益方信息字段、账户标识、地址信息、交易标识、时间戳
- 与链上 TX hash、内部订单号、KYC 档案号进行关联（形成一条“证据链”）

（2）消息交换与对接模式

- 对接 Travel Rule 通道供应商或点对点协议（要纳入外包治理）
- “对方不是合规 VASP / 无法传递字段”的处置策略：
  - 延迟/拒绝/人工复核
  - 限额/白名单
  - 客户补充声明与风险提示（并留存）

（3）留存与可取证

- 规定留存年限、可检索、可导出
- 保存：字段原文、交换回执、失败原因、人工复核结论、升级记录

13.5 制裁合规（Sanctions）与“命中处置四步法”

1. 命中即暂停（Hold）
2. 二次核验（误报/同名/相似）
3. 升级审批（合规/MLRO/管理层）
4. 处置与记录（放行/拒绝/冻结/终止 + 通知与报告）

13.6 培训、独立审查与年度改进闭环

- 培训分层：董事/高管、前台、合规/AML、客服、技术
- 年度独立审查：抽样开户、抽样告警、抽样 STR 决策、抽样 TFR 失败处置
- 缺陷评级（高/中/低）→ 整改计划 → 复测 → 结案

十四、客户保护与信息披露（"写给客户看的合规"】

监管审阅逻辑：**把 MiCA 行为规则"翻译"为客户可读语言**，并做到"可证明客户已理解/已确认/已留痕"。在斯洛文尼亚实际项目中，客户保护相关材料通常需要同时满足**证券市场行为口径（ATVP）与审慎/金融稳定口径（Banka Slovenije）**对消费者风险提示的关注（至少要做到：客户能核验你是否持牌、能区分受规产品/不受规产品、能找到投诉渠道）。

四件套必须"可上线、可留痕、可回放"：

1. **披露包**：费用/风险/执行方式/利益冲突/资产保管方式/投诉渠道
2. **客户条款 T&C**：权责边界、暂停/终止、强平/冻结、硬分叉/空投处理、争议解决
3. **风险提示**：清晰可理解（零售客户尤其），并留存客户确认记录
4. **营销合规**：禁止误导性陈述、收益承诺；KOL/代理管理与佣金披露

14.1 必交付"四件套"：对外披露包（Disclosure Pack）

建议做成**"网页披露 + PDF披露 + App内弹窗确认 + 版本留存"**四位一体，确保可审计。

A）机构与牌照状态披露（License & Scope Disclosure）

- 公司全称、注册信息、LEI（如适用）、实际经营地址、监管联系渠道
- **MiCA 授权状态**：牌照编号（获批后）、Home Member State、主管机关、授权日期
- **授权服务范围**：清晰列出你获批的 CASP 服务（例如：兑换/平台/托管/传递订单/执行/转移等），并声明**未获批服务不提供**
- **"受规/不受规"隔离声明**：如同一界面存在非 MiCA 受规产品（或第三方链接），必须以醒目方式标识，避免"拿持牌身份误导营销"的监管风险（ESMA 近期也公开提示过此类风险）。

B）费用与成本披露（Fees & Charges Disclosure）

- 费用清单：交易费、价差/点差、充值/提现费、托管费、链上矿工费/网络费、做市费/上币费（如有）、法币通道成本
- **"全成本展示"**：以案例方式列出某笔交易从下单到到账的总成本（含滑点、网络费、汇差）
- 费用变更机制：提前通知周期、客户选择权（同意/拒绝/退出）、历史版本可下载

C）风险披露（Risk Warnings & Product Risk Statements）

- 通用风险：价格波动、流动性枯竭、系统故障、链上不可逆、欺诈与社会工程学
- 服务特定风险：
  - 平台：撮合失败/极端行情暂停、熔断、价格异常、市场操纵风险
  - 托管：私钥风险、第三方托管风险、冻结/扣划条件、硬分叉/空投处理
  - 兑换：报价来源、滑点、执行延迟、最佳执行并非总能实现
- "不保证收益/不承诺保本"与"过往表现不代表未来"必须显著展示
- **消费者教育链接**：建议引用主管机关关于加密资产风险与"缺乏保护"的提醒材料入口，作为合规加分项。

D）利益冲突披露（Conflicts of Interest Disclosure）

- 披露你的角色：代理/自营/做市/与第三方关系
- 典型冲突清单：自营对冲 vs 客户交易；上币收费/做市合作；员工交易；关联方项目方；返佣渠道/KOL
- 冲突缓释：信息隔离墙、账户隔离、回避表决、事后抽样复核
- 披露必须"详细、具体、清晰"（ESMA 技术标准已对披露内容颗粒度提出要求）。

14.2 客户协议体系（Client Contract Suite）——"可签署、可执行、可审计"

建议至少形成 8 份对外文件（并以"主协议 + 附件政策包"结构管理版本）：

1. 《客户主协议/条款》（T&Cs）
2. 《风险披露声明》+ 客户确认回执（点击/电子签）

3. 《费用披露与费率表》
4. 《订单执行与公平执行政策》（Execution / Fair Execution Policy）
5. 《资产保管与客户资产隔离条款》（Custody/Safeguarding）
6. 《隐私政策与数据授权》（含 Travel Rule 数据共享告知）
7. 《投诉处理与争议解决条款》（含 ADR/仲裁/法院管辖）
8. 《账户冻结/限制/终止政策》（制裁、AML、欺诈、法院命令等触发）

关键写法：每条高风险条款都要“触发条件—流程—时限—通知方式—客户救济”。监管最反感“笼统保留解释权”。

14.3 客户分层与适当性（Suitability/Appropriateness）——“写进系统”

- 客户分层：零售/专业（Professional）/合格交易对手（如适用）
- 触发情形：若提供投顾/组合管理/带杠杆或复杂产品，应建立知识测评、风险承受评估、产品分层准入
- **留痕要求**：问卷版本、评分逻辑、阈值、豁免审批、复核记录、客户确认
- **反误导营销**：对零售客户不得使用“安全、稳定、保本”等表述；KOL/代理推广必须受控并可追责（合同+监控+抽检）。

14.4 投诉处理（Complaints Handling）——“可闭环、可统计、可升级”

- 建立独立投诉渠道（网页表单/邮箱/电话/工单）
- 分级：一般/重大/潜在系统性事件
- SLA：受理确认、调查、答复、结案时限
- 统计与复盘：按原因分类、整改闭环、向管理层/董事会定期报告
- 监管标准趋势：ESMA/技术标准对投诉处理制度的治理责任与流程要求越来越细（建议直接对齐 RTS 口径落地）。

十五、平台类业务（Trading Platform）专项制度（规则 + 监测 + 证据链）

平台业务是“最吃系统、最吃证据链”的 CASP 服务类型之一：监管会围绕三件事问到你崩溃——
①平台规则是否公平透明；②市场滥用/操纵是否可监测可处置；③交易日志是否可取证可复盘。
你需要把制度写成“平台可运行的规则书 + 监测模型 + 取证机制”。（MiCA 对市场完整性与监管预期可参考 ESMA 对 MiCA 的公开说明与 ATVP 汇总的 MiCA 指引入口。）

15.1 平台规则手册（Rulebook）——必须覆盖的目录

1. 市场结构：交易对、报价币种、最小变动价位、交易单位
2. 订单类型：限价/市价/止损/只做 Maker 等（如提供）
3. 撮合规则：价格优先/时间优先、部分成交、撤单规则
4. 异常行情与保护机制：价格带、熔断、暂停、撮合回滚（原则上谨慎）
5. 手续费与返佣：透明披露、做市商费率、VIP 分层
6. 上币/下币：评估维度、委员会机制、信息披露、紧急下架
7. 做市与流动性安排：做市协议、禁止操纵条款、监控指标
8. 争议处理：错单/穿仓（如有）/系统故障赔付原则
9. 市场公告机制：重大事件公告模板与时限

交付建议：Rulebook 做成“客户可读版”+“监管审阅版（含风控参数与触发阈值原则）”两册。

15.2 市场监测与滥用识别（Market Surveillance）

至少建立“行为场景库 + 告警分级 + 调查工作台 + 处置措施表”。

A）核心监测场景（示例）

- Wash trading / 自成交
- Spoofing / Layering（挂撤单诱导）
- Pump & dump（拉盘砸盘）
- 关联账户对敲、团伙操纵
- 异常价格偏离、异常成交量、盘口异常堆单

- 上币前后异常交易与信息泄露疑点

B）告警到处置的标准链路

- Alert → Triage（初筛）→ Case（立案）→ Investigation（取证）→ Decision（处置）→ Reporting（必要时报告）→ Closure（结案复盘）
- 处置措施：限制交易/提高保证金（如有）/限制提币/冻结账户/下架币对/移交执法/STR（如涉及洗钱）

C）证据链

- 原始订单流（order events）
- 撮合事件（match events）
- 账户关系图谱（device/IP/钱包地址/资金流）
- 沟通记录（客服工单/邮件/聊天记录）
- 处置决策记录（谁批、依据、时间戳）

> ESMA/各国主管机关对“市场滥用防治”正在形成更一致的监督实践；ATVP 已公开列示 MiCA 相关指引入口，建议你在制度映射中引用并声明“采用该指引的方法论”。

15.3 上币/下币治理（Listing/Delisting Governance）

上币评估至少 8 维（可做评分表并留存底稿）：

- 法律属性与白皮书要素（是否触及 ART/EMT 或其他受规品）
- 项目方治理与UBO
- 技术安全（合约审计/多签/升级权限）
- 市场风险（流动性、波动性、集中度）
- 合规风险（制裁、隐私币、Mixer 风险）
- 操纵风险（代币分配、解锁计划）
- 信息披露与持续披露能力
- 退出机制（紧急下架触发器、客户善后）

下币触发器：重大欺诈/漏洞/制裁/信息披露失真/持续无流动性/监管要求等。

15.4 “平台可演示证据链”清单（监管面谈必杀）

- 现场演示：从某个订单→撮合→成交→对账→客户对账单→日志导出
- 演示：某个监测告警→立案→调查→处置→结案报告
- 演示：上币决策底稿→投票纪要→公告→上线后监测与复盘

十六、托管（Custody）专项制度（资产隔离、密钥、对账、责任边界）

> 托管业务的监管核心就一句话：**客户资产必须可隔离、可证明、可追溯、可在危机中安全返还**。MiCA 对 CASP 的组织、治理、客户保护与审慎要求构成托管制度的“上位法底座”。

16.1 资产隔离（Segregation）——链上、账务、权限“三重隔离”

A）链上隔离（On-chain Segregation）

- 客户独立地址（理想）或客户分组地址（可接受但要可核验）
- 热/冷钱包分层：热钱包限额+自动补充策略+人工复核
- 白名单与提币延迟（延时生效 + 二次确认）

B）账务隔离（Books & Records）

- 客户分户账（sub-ledger）与总账一致性
- 每日（至少）对账：链上余额 vs 内部账 vs 客户可见余额
- 差异处理：差异分类、冻结措施、补偿原则、审计留痕

C）权限隔离（Access Segregation）

- RBAC 最小权限
- 特权账号双人审批（4-eyes）
- 权限变更工单化、定期复核、离职即刻回收

16.2 密钥管理（Key Management）——监管最关心的“硬核点”

建议交付 **Key Management Policy + Key Ceremony SOP + Key Risk Register**：

- MPC / 多签 / HSM 的选型说明（为什么安全、边界在哪里）
- 密钥生成仪式（Key Ceremony）：参与人、地点、设备、录像、封存
- 备份与恢复：分片存储、异地保管、启用条件
- 轮换与撤销：周期、触发器（人员变更/疑似泄露/供应商风险）
- 紧急流程：疑似被盗→冻结→风险评估→客户通知→执法协作→事后复盘
- 供应链安全：第三方库、签名模块、构建流水线、代码审计

16.3 提币与转账控制（Withdrawals & Transfers Controls）

- 风险评分：设备/IP/地址风险/新地址冷却期/大额阈值
- 分级审批：小额自动化、中额人工复核、大额管理层审批
- Travel Rule 对接：信息不全的处置（拒绝/延迟/人工补全）
- “冻结/扣划”边界：仅在法律要求、制裁、AML 风险、法院命令等情形触发，并在客户协议中写清

16.4 托管责任边界（Liability Boundary）与客户沟通

你需要在协议里把以下边界写清（否则投诉/诉讼必爆）：

- 你是“托管人”还是“技术保管/外包协调人”（角色决定责任）
- 因客户自身过错（钓鱼/泄密/错误地址）导致损失的责任划分
- 因链上协议漏洞、硬分叉、网络拥堵导致延迟的处理方式
- 保险/保障（如有）：覆盖范围、免赔额、理赔流程
- 资产处置：硬分叉/空投/质押收益（如有）归属与处理规则

16.5 托管对账与审计（Reconciliation & Audit）

- 对账频率：热钱包实时/日终、冷钱包日终/周对账
- 审计轨迹：不可篡改日志、时间同步、导出格式（供监管/审计师）
- 定期独立审查：抽样验证地址控制权、签名流程合规性、权限复核记录

十七、兑换与执行（Exchange / Execution）专项制度

- 报价机制：来源、聚合、异常报价过滤、滑点披露
- 公平执行/最佳执行（尤其零售）：执行政策、冲突披露
- 自营与客户交易冲突：信息隔离、顺序公平、禁止抢跑
- 费用透明：对账单可追溯、可解释

  适用范围：

  - **兑换**（Crypto-Crypto / Crypto-Fiat）：报价/点差/滑点/撮合与成交确认
  - **执行**（Execution of orders on behalf of clients）：接受客户指令并代表客户执行（含路由、撮合、成交分配）
  - **传递订单/接收传递**（Reception & Transmission）：如申请包含该服务，则需补齐“传递—执行”的责任切分

17.1 监管目标与“监管会问什么”

MiCA 下，ATVP（行为监管口径）通常会抓三件事：

1. **客户是否被公平对待**：价格形成是否透明、是否存在“暗箱加价/隐性费用”。
2. **利益冲突是否被识别与隔离**：自营/做市/关联方是否影响报价与执行。
3. **证据链是否可回放**：每笔交易“报价来源—风控校验—执行路径—成交确认—对账单”能否复现。

交付标准：不是“写政策”，而是提供**可演示**的执行与风控证据链（日志、报表、抽样回放、工单）。

17.2 报价与价格形成机制（Pricing Policy｜可审计口径）

必须交付《报价与点差政策（Pricing & Spread Policy）》并在 BP/制度里清晰写明：

A. 报价来源与优先级

- 外部市场数据源（交易所/聚合器/经纪商）清单
- 数据质量规则：延迟阈值、断流处理、异常值剔除、价格跳变识别
- **多源聚合**：加权规则、主备切换规则、手工干预权限与留痕

B. 点差/加价（Markup）与费用透明

- 点差形成：固定点差 / 动态点差（随波动率、流动性、库存风险调整）
- 费用拆分：交易费、点差费、网络费、法币通道费、外汇点差
- **客户披露**：在报价页面/确认页/对账单中分别展示（避免“把点差藏进价格”）

C. 滑点（Slippage）与再报价（Re-quote）

- 滑点容忍区间（按产品/客户等级）
- 再报价触发：波动过快、报价过期、风控拦截
- 失败订单处理：取消/部分成交/排队/延迟执行的规则与客户告知

D. 异常行情与保护机制

- 价格保护带（Price Collar）/熔断（如适用）
- 极端行情：暂停交易、只许平仓、提高保证（若涉及杠杆则另套制度）

17.3 执行政策（Order Execution Policy｜类“最佳执行/公平执行”框架）

MiCA 对 CASP 并非完全照搬证券法“最佳执行”，但监管实务会要求你证明“公平、透明、可解释”。建议交付《订单执行政策》至少包含：

A. 订单生命周期（必须画流程图）

下单 → KYC/制裁校验 → 余额/限额校验 → 风险引擎 → 路由/撮合 → 成交分配 → 确认 → 记账/对账 → 报表与留存

B. 订单类型与优先级

- 市价单/限价单/止损单（如提供）
- 撮合优先级：价格优先、时间优先、数量优先
- 部分成交与剩余撤销规则

C. 执行质量指标（Execution Quality Metrics）

- 报价延迟、成交率、滑点分布、拒单率、故障率
- 每日/每周监控报表 + 阈值告警 + 根因分析（RCA）

D. 公平对待与“反滥用”

- 禁止抢跑/插队（含员工与做市）
- 禁止“选择性延迟”“对散户更差报价”等歧视
- 同一客户多账户/关联账户识别（与 AML/欺诈联动）

17.4 利益冲突与做市/自营的隔离（CoI Controls）

若你存在以下任一情况，必须加厚交付：

- 平台同时做市；或关联方做市；或存在自营交易
- 上币项目方/做市商与股东/管理层有关联
- 通过同一界面销售“非 MiCA 受规产品”

建议按 ESMA 对 MiCA 冲突管理 RTS 的结构输出制度包：

- 冲突识别清单（场景库）
- 预防措施（信息墙、权限隔离、账户隔离）
- 管理措施（回避、审批、披露、限制交易）
- 披露模板（网站披露/客户协议披露）

17.5 对账、结算与客户对账单（Statement & Reconciliation）

交付要点（监管很爱抽查）：

- **账本三层一致性**：撮合成交记录 / 内部客户账 / 链上或托管账（如涉及）
- 差异处理流程：发现—冻结—调查—冲正—客户通知—复盘
- 对账频率：T+0/T+1（按业务复杂度）
- 客户对账单字段：成交时间、价格、费用拆分、点差披露、汇率、网络费

17.6 可递交的“证据链附件包”（建议编号）

- EX-01《报价与点差政策》
- EX-02《订单执行政策 + 执行质量KPI》
- EX-03《做市/自营隔离与利益冲突制度》
- EX-04《异常行情与交易中断处置预案》
- EX-05《对账与冲正SOP + 样例报表》
- EX-06《客户披露页面截图/对账单样例/费用披露样例》

十八、信息安全、系统合规与“可演示证据链”（决定审批效率）

> MiCA 申请的“系统关”与 DORA 的“韧性关”正在合流：你不仅要安全，还要**证明你能持续安全运营**。DORA 自 2025-01-17 起适用，对多数金融实体提出统一 ICT 风险管理要求。

18.1 交付思路：把 IT 写成“审计可回放”

监管要的不是“我们很安全”，而是：

- **谁**有权做什么（RBAC）
- **何时**做了什么（不可篡改日志）
- **为什么**允许（审批链/工单）
- **出了事**怎么发现/怎么止损/怎么复盘（IR + RCA + CAPA）

18.2 必交“系统四图”（一图顶十页文字）

1. **系统架构图**（组件、边界、信任域、云/本地）
2. **数据流图**（KYC→交易→风控→报表→监管导出；含 Travel Rule 字段流）
3. **权限流图**（管理员、开发、运维、合规、财务、客服的权限分层）
4. **关键资产清单**（钱包/密钥系统、撮合引擎、KYC库、日志库、风控库）

18.3 身份与权限（IAM / RBAC / PAM）

交付要求（建议可直接变成附件）：

- RBAC 最小权限矩阵（岗位→系统→权限→审批人）
- 特权账号（PAM）管理：双人授权、临时提权、全程录屏/日志

- MFA 强制、密钥轮换、离职/调岗权限回收SOP
- 开发/测试/生产隔离与变更审批（Change Management）

18.4 日志与可追溯（Logging & Monitoring）

- 日志范围：登录、提权、订单、撮合、资金划转、地址白名单、风控规则变更、KYC变更、导出报表
- 日志特性：时间同步、不可篡改、留存期限、检索与导出（监管抽查一键导出）
- SIEM/SOC：告警分级、7x24（可外包但必须有内部负责人）

18.5 安全开发与漏洞管理（SSDLC）

- 代码审计、依赖组件管理（SBOM 可加分）
- 漏洞管理：分级、修复SLA、复测与闭环证据
- 渗透测试：范围、频率、整改报告（监管常要看整改闭环）

18.6 事件管理与监管通报（Incident Management）

按 DORA 逻辑建立：

- 事件分级（重大/一般/可疑）
- 响应流程：检测→隔离→止损→取证→恢复→通报→复盘
- 复盘（RCA）+ 改进（CAPA）+ 再演练记录
  并准备：事件通报模板、客户公告模板、媒体口径模板。

18.7 BCP/DR（业务连续性与灾备）

交付要点：

- RTO/RPO（按关键系统分层）
- 灾备策略：同城/异地、冷备/热备、密钥备份策略
- 演练：桌面演练 + 技术演练 + 恢复证明（截图/日志/工单）

18.8 “可演示证据链”清单（监管面谈可直接出示）

- SEC-01《ICT风险管理框架》
- SEC-02《资产清单 + 数据分类分级》
- SEC-03《RBAC/PAM 权限矩阵 + 审批样例》
- SEC-04《日志留存与导出机制说明 + 样例导出》
- SEC-05《渗透测试报告 + 整改闭环》
- SEC-06《事件响应预案 + 演练记录 + RCA/CAPA》
- SEC-07《BCP/DR 文档 + 恢复演练证明》

十九、外包与第三方治理（Outsourcing）+ 供应链风险

> 监管现实：CASP 极度依赖第三方（云、KYC、链上分析、Travel Rule 通道、钱包基础设施）。监管最怕你“外包=失控”。DORA 也把第三方 ICT 风险提升为硬要求。

19.1 外包治理总框架（Outsourcing Framework）

建议交付一套《外包治理制度》，核心模块：

- 外包定义与范围（含集团内共享服务）
- 重要性分级：一般/重要/关键（critical/important）
- 全生命周期：准入尽调→签约→上线→持续监控→退出迁移

同时关注 EBA 对第三方风险管理框架的最新监管趋势（非 ICT 外包也会被“纳入同等严谨的第三方风险治理”）。

19.2 外包清单与“关键外包识别”（监管必看表）

必须提交《Outsourcing Register》（外包登记表），建议字段：

- 供应商名称、服务描述、数据类型、数据位置
- 是否涉及客户资金/密钥/交易撮合/核心KYC
- SLA/KPI、分包链、审计频率
- 退出方案（Exit Plan）与替代供应商
- 责任人（业务Owner + 合规Owner + IT Owner）

典型“关键外包”：

- 云基础设施（IaaS/PaaS）、托管HSM/MPC
- KYC/制裁筛查、链上分析/风控模型
- Travel Rule 通道与消息传递网络

19.3 第三方尽调（Vendor Due Diligence｜三维度）

A. 合规与法务

- 许可资质、分包政策、数据处理条款（GDPR/跨境）
- 监管可访问性：监管/审计可进入、可取证、可复制数据
- 争议与责任：违约责任、赔偿、服务中断责任

B. 信息安全与韧性

- 安全认证/审计报告（ISO27001/SOC2等）
- 漏洞与事件通报义务、演练配合
- 数据隔离、密钥管理、访问控制

C. 财务与持续经营

- 财务稳定性、关键人员依赖、并购/倒闭风险
- 供应商集中度风险（单点依赖）

19.4 外包合同“八大硬条款”（缺一项就容易补件）

1. 审计权（含现场/远程/第三方审计）
2. 监管访问权（监管可直接或经你协调访问）
3. 数据所有权与可携带（导出格式、频率、费用）
4. 分包限制与透明披露（分包链可控）
5. 事件通报时效与协作（含取证支持）
6. SLA/KPI 与违约救济（服务中断赔偿/降费）
7. 退出与迁移（Exit assistance、过渡期支持）
8. 业务连续性（灾备、恢复目标、演练配合）

19.5 持续监控与年度评估（Ongoing Monitoring）

- 月度/季度服务评估（SLA、事故、缺陷、整改）
- 年度风险重评（重要性是否上升、是否需替代方案）
- “供应链风险”专题：关键供应商的关键分包商也需纳入评估

19.6 退出策略（Exit Plan｜必须写“怎么换掉它”）

监管喜欢看到你能回答：**“供应商断供当天你怎么办？”**
Exit Plan 至少包含：

- 触发条件（违约、事故、监管要求、并购变化）
- 迁移路径（数据导出→环境重建→验证→切换→回退）
- 时间表与资源（人、预算、替代供应商）
- 客户沟通模板（若影响服务）

19.7 可递交的“外包证据链附件包”

- OUT-01《外包治理制度 + 重要性分级方法》
- OUT-02《外包登记表（Register）+ 关键外包清单》
- OUT-03《供应商尽调报告样例 + 评分表》
- OUT-04《外包合同条款包（审计权/退出权/监管访问）》
- OUT-05《持续监控报表样例 + 年度评估模板》
- OUT-06《退出计划（Exit Plan）+ 演练记录（如已演练）》

二十、数据治理（含税务/报告导向）与记录保存

（MiCA + DAC8 + TFR 叠加下的“可报告、可追溯、可审计”体系）
监管一句话逻辑：**你不是“存数据”，而是要证明——任何时间点，监管问你一个问题，你都能“拉得出、对得上、说得清”。**

20.1 监管框架叠加关系（为什么这章很重）

在斯洛文尼亚 CASP 项目中，**数据治理**同时服务于四个监管目标：

监管来源	核心要求
MiCA	交易、订单、客户、资产、风控、投诉等“经营记录”
TFR / Travel Rule	转账随行信息、发送方/接收方、失败/拒绝处理
DAC8	加密资产税务信息自动交换（客户、交易、价值）
AML/CFT	KYC/EDD、监控、STR、调查证据链

唐生结论：必须搭建**统一数据治理层**，而不是“AML 一套、税务一套、运营一套”。

20.2 数据治理总体架构（三层模型｜监管推荐）

第一层：字段与口径标准层（Data Standardisation）

统一定义“同一字段在不同制度下的口径一致性”。
必须统一的关键字段示例：

- 客户身份字段（姓名 / ID / 税务居民 / UBO）
- 钱包地址（自托管 / 托管 / 白名单）
- 交易字段（时间戳、价格、数量、费用、点差）
- Travel Rule 字段（Originator / Beneficiary）
- 税务字段（资产类型、估值方法、年度汇总）

  交付件：《数据字典（Data Dictionary）》+ 字段映射表（MiCA / TFR / DAC8）

第二层：留存、追溯与证据封存层（Record & Evidence）

解决“**多久存？存什么？怎么防篡改？**”
最低监管期望（实操建议）：

- 交易/订单/对账：≥ 5–7 年
- AML/STR/EDD：≥ 7 年
- 客户协议与披露确认：≥ 7 年

- 日志（关键系统）：≥ 12–24 个月（可冷存）

关键要求：

- **不可篡改**（WORM / 哈希校验 / 审计轨迹）
- **时间同步**（UTC + 本地）
- **可快速导出**（监管抽查）

第三层：报告与抽取层（Reporting & Extraction）

必须证明你能：

- 按 **MiCA 定期报告** 抽数
- 按 **DAC8** 做年度税务申报
- 按 **AML** 即时导出调查包

> **监管最怕**：“系统能跑，但报表要人工拼 Excel。”

20.3 DAC8（加密税务信息交换）下的实操准备

20.3.1 DAC8 的实质影响

- 覆盖 **交易平台、托管、经纪、转账服务**
- 要求向税局报告：
  - 客户身份
  - 年度交易次数
  - 年度交易总值（EUR）
  - 持仓与估值方法

20.3.2 CASP 必须准备的三件事

1. **客户税务居民识别机制**（入职 + 年度复核）
2. **交易价值计算方法**（法币/稳定币/换算口径）
3. **年度汇总与审计轨迹**

20.4 数据访问控制与合规读取

监管会问：

- 谁能看客户数据?
- 谁能导出?
- 是否留痕?

最低交付要求：

- RBAC 权限矩阵（角色 × 数据集）
- 导出审批工单
- 合规/监管专用只读账户
- 数据最小化原则（GDPR 对齐）

20.5 数据治理交付附件清单（示例）

- DG-01《数据治理政策（MiCA / DAC8 / TFR 一体化）》
- DG-02《数据字典 + 字段映射表》
- DG-03《记录保存与不可篡改策略》
- DG-04《监管/税务报表抽取流程图》

- DG-05《数据访问与导出审批日志样例》

二十一、投诉处理、ADR 与争议解决

（ATVP 高敏感模块｜“写给监管看的客户保护机制”）
在斯洛文尼亚，**客户投诉**不仅是运营问题，而是：**ATVP 判断你是否“适合服务零售客户”的核心证据。**

21.1 监管目标（ATVP 视角）

ATVP 通常关注四点：

1. 客户是否**容易投诉**
2. 投诉是否**被及时、独立、公平处理**
3. 是否有**系统性问题复盘**
4. 是否提供 **ADR（替代争议解决）渠道**

21.2 投诉处理制度的“必备结构”

21.2.1 投诉定义与分类

- 一般投诉（信息/操作）
- 服务质量投诉
- 交易争议
- 资金/托管争议
- 合规/误导营销投诉

21.2.2 投诉处理时序（必须量化）

阶段	建议时限
受理确认	T+2 工作日
调查完成	T+15–30
正式回复	不超过 30
升级/ADR	如客户不接受

21.2.3 升级与独立性

- 客服 ≠ 最终裁决
- 合规部门必须参与
- 重大投诉上报管理层

21.3 ADR（替代争议解决）机制

斯洛文尼亚要求：

- 明确 ADR 机构
- 在客户协议中披露
- 在网站显著位置公示

CASP 需准备：

- ADR 信息页
- 争议升级流程图
- ADR 接口责任人

21.4 投诉数据的“监管用途”

投诉并不是“处理完就算了”，而是：

- 输入到 **风险管理**
- 输入到 **产品改进**
- 输入到 **监管年度报告**

必须保留：

- 投诉类型统计
- 根因分析（RCA）
- 整改措施（CAPA）

21.5 投诉模块交付附件

- CP-01《投诉处理政策（Complaint Handling Policy）》
- CP-02《投诉流程图 + 时限表》
- CP-03《ADR 信息披露模板》
- CP-04《投诉台账样例 + RCA 表》
- CP-05《客户协议中投诉条款摘录》

二十二、财务模型、定价与“可持续经营”证明

（Banka Slovenije 审慎判断的“生死线”）
监管核心问题：**你能不能“长期合规地活下去”，而不是“拿到牌照就没钱”。**

22.1 MiCA 下的财务审慎逻辑

MiCA 要求 CASP：

- 持续满足 **最低资本**
- 持续覆盖 **固定开支**
- 证明 **12 个月持续经营能力**

在斯洛文尼亚，**财务模型的可信度**直接影响审批节奏。

22.2 三年财务模型（最低交付）

22.2.1 必须包含的报表

- P&L（损益表）
- Cash Flow（现金流）
- Capital Adequacy（资本充足测算）

22.2.2 关键假设必须“可解释”

- 客户增长逻辑
- 交易量与费率
- 客户结构（零售 vs 专业）
- 留存率 / 活跃率

监管常问：“为什么你第 2 年收入翻倍？”

22.3 定价模型与费用透明

22.3.1 定价结构

- 交易费
- 点差
- 托管费
- 网络费
- 外汇转换费

22.3.2 必须做到

- 与客户披露一致
- 与系统计算一致
- 与对账单一致

22.4 合规成本必须“写实”

监管最讨厌的模型特征：

- AML 成本写 0
- 审计成本写 0
- IT 安全写 0

建议明确列示：

- KYC / 链上分析
- Travel Rule 通道
- SOC / SIEM
- 审计 / 内审
- 法律与合规外包

22.5 压力测试（必交）

至少三种场景：

1. 交易量下降 50%
2. 重大安全事件
3. 监管成本上升

每种要说明：

- 现金还能撑多久
- 是否触发资本补充
- 股东承诺机制

22.6 财务模块交付附件

- FIN-01《三年财务模型（含压力测试）》
- FIN-02《资本测算与持续经营说明》
- FIN-03《定价与费用披露对照表》
- FIN-04《合规成本明细表》
- FIN-05《股东资本支持承诺函》

唐生结论（监管视角一句话）

- **数据治理**：你是否“随时能报、报得准、追得回”

- **投诉机制**：你是否“真正保护客户，而不是应付流程”
- **财务模型**：你是否“能在合规成本下长期经营”

二十三、有序退出（Wind-down Plan）与业务连续性（BCP/DR）

（监管要看到：你“出问题也能善后”）

监管一句话逻辑：**CASP 不仅要会经营，更要“能安全地停止经营”。**

23.1 监管依据与核心期望

MiCA 明确要求 CASP 具备：

- **有序退出能力（Orderly Wind-down）**
- **业务连续性与灾难恢复（BCP/DR）**
- **客户资产与客户权益优先保护**

在斯洛文尼亚实践中：

- **Banka Slovenije** 更关注：资本、流动性、运营中断下的持续履约能力
- **ATVP** 更关注：客户资产、客户信息、投诉与沟通安排

23.2 Wind-down Plan 的监管定位（不是破产清算）

⚠ 监管明确区分：

- **Wind-down**：主动/被动、有计划、有秩序的退出
- **Insolvency**：破产程序（监管不希望走到这一步）

Wind-down 是 **合规工具**，不是财务失败。

23.3 触发条件（Triggers｜必须写清楚）

至少应覆盖以下六类触发器，并明确“谁判断、谁批准、谁执行”：

1. **资本触发**
   - 资本低于 MiCA 最低要求
   - 连续亏损触及内部阈值
2. **监管触发**
   - 监管要求暂停/限制业务
   - 重大违规调查
3. **运营触发**
   - 核心系统长期不可用
   - 关键外包服务中断且无法替代
4. **安全触发**
   - 私钥/托管安全重大事件
   - 大规模数据泄露
5. **商业触发**
   - 失去关键银行/支付通道
   - 主要股东撤资
6. **战略触发**
   - 集团战略退出欧盟/该业务线

23.4 Wind-down 执行路径（四阶段模型）

第一阶段：决策与冻结（Decision & Freeze）

- 董事会紧急会议决议
- 停止新增客户 / 新交易
- 冻结高风险操作（转账、上币等）

第二阶段：客户资产与客户关系处理（Client Protection）

- 客户资产清点与对账
- 托管迁移 / 清退安排
- 明确客户取回资产路径与时限

第三阶段：运营与合规收尾（Operational Close-out）

- 结清未完成交易
- 完成投诉与争议处理
- 向监管提交阶段性报告

第四阶段：数据与档案封存（Data & Records）

- 数据封存、不可篡改存储
- 保留监管/审计访问权限
- 指定责任人

23.5 客户资产与资金处理（监管最敏感点）

必须单独成章说明：

- **客户资产隔离是否持续有效**
- **客户优先级**（优先于公司债权）
- **链上资产与账务一致性**
- **客户通知模板**（多语言）

23.6 BCP / DR（业务连续性与灾难恢复）

23.6.1 关键业务识别

至少覆盖：

- 客户访问与资产查询
- 提现/转账
- 客户支持与投诉渠道
- 合规与监管沟通

23.6.2 RTO / RPO（必须量化）

- 不同系统设定不同 RTO / RPO
- 核心托管/交易系统要求更严格

23.6.3 演练与证据

监管期待看到：

- 桌面演练（Table-top）
- 技术演练（Failover）
- 恢复成功证明（截图/日志）

23.7 Wind-down / BCP 交付附件清单

- WD-01《有序退出总体方案（Wind-down Plan）》
- WD-02《触发器与决策权限矩阵》
- WD-03《客户资产清退与迁移流程》
- WD-04《客户通知与公告模板》
- WD-05《BCP/DR 文档 + 演练记录》

二十四、授权申请流程（ITS 表格化递交）与补件打法（RFI-ready）

（斯洛文尼亚：Banka Slovenije 受理 + ATVP 并行审阅）
监管现实：**MiCA 申请不是“交一次材料”，而是“持续问答工程”。**

24.1 申请路径总览（MiCA 标准流程）

1. **Pre-Application 准备**
   - 服务映射
   - 差距评估（Gap Analysis）
   - 材料目录与编号体系
2. **正式递交（ITS 表格）**
   - 通过欧盟统一 ITS 表格
   - 附件 A–I 全量提交
3. **形式审查（Completeness Check）**
   - 是否齐全
   - 是否按表格字段映射
4. **实质审查（Substantive Review）**
   - Banka Slovenije（审慎）
   - ATVP（行为/客户保护）
5. **补件（RFI）**
6. **批准 / 附条件批准**

24.2 ITS 表格化递交的“实操要点”

24.2.1 ITS 的核心特征

- 每一字段 ≠ 描述
- 每一字段 = **指向附件编号**

推荐做法：

> **ITS 字段 → 附件编号 → 页码/段落**

24.2.2 常见 ITS 填写“雷区”

- 服务范围写模糊
- 引用附件但附件中找不到对应内容
- 同一信息在不同章节不一致

24.3 RFI（补件）高频主题（斯洛文尼亚经验）

1. Substance 不充分
2. 外包合同缺少审计权/退出权

3. AML/Travel Rule “写了但不能演示”
4. 财务模型不覆盖合规成本
5. 系统安全缺乏证据链
6. 客户披露不清晰

24.4 仁港永胜 RFI-ready 补件打法

每一条 RFI 按以下结构回应：

项目	内容
法规依据	MiCA / RTS / 本地法条
监管问题	原文复述
现状说明	我们现在如何
改进措施	新增/修订
证据编号	附件编号
责任人	姓名/岗位
完成日期	明确

这是监管最认可的应答结构。

24.5 申请流程交付附件

- APP-01《MiCA ITS 填写指引（斯洛文尼亚）》
- APP-02《附件编号与字段映射索引表》
- APP-03《常见 RFI 问题库 + 标准答复框架》
- APP-04《监管沟通与会议纪要模板》

二十五、处罚与合规风险地图（MiCA 红线清单）

（监管底线：哪些事“不能碰”）

> 监管不会每天罚你，
> 但**一旦触红线，后果非常重**。

25.1 MiCA 下的处罚框架概览

可能的制裁包括：

- 高额罚款（固定金额或营业额比例）
- 业务限制/暂停
- 撤销授权
- 公示处罚（Reputational Risk）

25.2 CASP 典型“红线行为”清单

25.2.1 授权与范围

- ❌ 未获授权即展业
- ❌ 超范围提供服务

25.2.2 客户资产

- ❌ 客户资产未隔离
- ❌ 客户资产被挪用/混用

25.2.3 信息披露

- ❌ 误导性营销

- ❌ 隐藏费用/点差
- ❌ 风险披露不足

25.2.4 AML / TFR

- ❌ 未执行 Travel Rule
- ❌ 未提交 STR / 延迟提交
- ❌ KYC/EDD 形同虚设

25.2.5 系统与外包

- ❌ 关键外包失控
- ❌ 无审计权/无退出方案
- ❌ 数据泄露未通报

25.3 风险地图（Risk Heat Map｜实操建议）

建议把风险分为：

- **高风险（必须实时监控）**
- **中风险（定期审查）**
- **低风险（年度复核）**

并明确：

- 责任岗位
- 监控指标
- 升级路径

25.4 合规风险交付附件

- RISK-01《MiCA 合规红线清单》
- RISK-02《风险地图与责任分配表》
- RISK-03《违规事件应急处置流程》
- RISK-04《监管通报与媒体应对模板》

唐生结论（监管视角）

- **Wind-down / BCP**：你是否“出问题也能保护客户”
- **申请流程**：你是否“材料可读、补件可控”
- **红线管理**：你是否“知道什么绝对不能做”

二十六、仁港永胜交付方案（建议 + 优势 + 联系方式 + 免责声明）

26.1 仁港永胜建议（可执行清单）

1. **先做服务映射**：把业务拆到 MiCA 服务类别，明确申请范围与制度边界
2. **材料按监管分工拆册**：央行审慎主册 + ATVP 行为/滥用副册（减少补件返工）
3. **系统证据链优先**：权限、日志、监控、Travel Rule、对账、外包审计权做到可演示
4. **资本与现金流前置**：把合规成本写实并纳入压力测试
5. **护照通报作为第二阶段工程**：先定目标国清单，再做多语言披露/投诉/营销补丁
6. **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。

26.2 选择仁港永胜的好处（核心优势）

- **监管导向写作 + RFI 能力强**：把技术/风控落成"监管可读证据链 + 附件编号体系"
- **模板库可直接落地**：Checklist（A–I）、BP、AML/Travel Rule SOP、平台规则、上币评估、外包/退出条款包、面谈题库
- **跨境护照与集团结构经验**：UBO 穿透、资金路径、数据治理、外包治理一体化交付

26.3 关于仁港永胜

仁港永胜（香港）有限公司长期为金融机构、支付机构、加密资产平台、基金与家办提供：

- 牌照申请与持续合规（MiCA CASP、EMI/PI、SFC、MSO、VARA 等）
- AML/CFT 体系搭建、制度与系统合规、监管面谈与检查应对
- 跨境展业合规结构设计（护照机制、集团治理、数据治理、外包治理）

26.4 联系方式

唐上永（唐生，Tang Shangyong）｜业务经理

- 手机 / 微信（深圳）：**15920002080**
- 香港 / WhatsApp：**+852 9298 4213**
- 邮箱：**Drew@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。

26.5 免责声明

本文由仁港永胜（香港）有限公司拟定，并由唐生提供专业讲解。本文依据欧盟与斯洛文尼亚公开法规与监管信息整理（含 MiCA、TFR 及斯洛文尼亚执行法与主管机关分工等）。
本文仅供一般性合规筹备参考，不构成法律意见、监管承诺或获批保证。具体申请策略、材料清单、审查要点与时间/费用，应以斯洛文尼亚主管机关及欧盟最新 RTS/ITS、ESMA/EBA 指引与个案事实为准。仁港永胜保留更新与修订本文内容的权利。

如需进一步协助，包括斯洛文尼亚 Slovenia（MiCA）CASP 申请／收购、合规指导及后续维护服务，请联系仁港永胜（www.jrp-hk.com，手机：15920002080 / 852-92984213）获取专业支持，以确保业务在 MiCA 框架下合法合规、稳健运营。
