



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)

卢森堡 Luxembourg (MiCA) 加密资产服务提供商 (CASP) 牌照 申请注册指南

Luxembourg (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) 提供专业讲解

Rengangyongsheng (Hong Kong) Limited

文档说明: 本指南为仁港永胜唐生拟定的“交付版结构化正文”, 可直接用于内部立项、与律师/审计/技术供应商对齐、以及向 CSSF 进行 Pre-Application 沟通的底稿。

如需我司提供 **PDF 版 (带封面/目录/页眉页脚/版本控制)**、以及 **全套模板包 (Word/Excel/Visio)**, 可在文末“我司配套文件清单/联系信息”处有偿向唐生索取。

卢森堡 CASP 的主管机关为 **CSSF**, 其官网已发布 CASP 专区、申请表格 DOCX、MiCA 适用日期、以及适用的 EU RTS/ITS 清单。

✅ 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 (欧盟统一): Crypto-Asset Service Provider (CASP) Authorisation / Authorisation as a CASP (MiCAR Title V)

卢森堡主管机关: Commission de Surveillance du Secteur Financier (CSSF)

适用起算: MiCAR 对 CASP 自 **2024 年 12 月 30 日** 起适用 (full applicability to CASPs)。

本交付物定位:

- 面向: 股东会/董事会立项、合规与技术落地、对接 CSSF (Pre-Application)、以及申请材料编制。
- 输出: 按“奥地利 CASP 模板”24 栏目, 一次性补齐 (含 Checklist、预算、甘特图、矩阵)。
- 附件可选: CSSF 申请表/声明表、Q&A Pack、制度模板包 (详见第 20 栏)。CSSF 已提供 CASP 申请表 DOCX 及相关表格下载入口。

2) 牌照介绍与申请优势 (MiCA 统一框架 + 卢森堡优势)

2.1 MiCA 下 CASP 的“统一牌照 + 护照通行”

MiCA (Regulation (EU) 2023/1114) 在欧盟范围内统一了:

- CASP 的授权与持续监管框架 (组织治理、资本/审慎、客户保护、冲突管理、投诉、记录保存、信息披露等)。
- 一旦在卢森堡获 CSSF 授权, 可按 MiCA 的“跨境护照机制”向其他成员国开展业务 (需通知/登记流程与接收国监管联动, 实务上需做好语言/营销合规与本地消费者保护差异适配)。

2.2 卢森堡的“申请优势”(实务视角)

- 监管路径清晰: CSSF 已建立 CASP 专区, 列明服务类型、适用日期、申请类型 (Article 60 通知 vs Article 62/63 授权) 以及官方表格 (DOCX)。
- 与传统金融生态的兼容性强: 若集团已持有银行/投行/基金管理/EMI 等牌照, MiCA 允许特定金融实体以“**通知制**”开展“等同服务” (Article 60), 对集团协同有利。
- 过渡期安排明确: 已在 2024/12/30 前注册为 VASP 的主体, 可在 **至 2026/07/01** 或取得/被拒 CASP 授权前维持既有 VASP 注册 (孰早)。这对存量主体的迁移窗口、系统改造排期与资金安排非常关键。

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 主管机关（NCA）

- **CSSF**：卢森堡金融业监管机构，已被卢森堡法律明确指定为 MiCA 的主管机关。

3.2 欧盟主法与二级规则（强相关）

- **MiCA: Regulation (EU) 2023/1114**（主法，Title V/VI 涉及 CASP）。
- **申请材料 RTS/ITS**：例如 **Commission Delegated Regulation (EU) 2025/305**（明确授权申请应包含的信息），以及相应 ITS 模板（EU 2025/306 等，CSSF 页面亦汇总）。
- **记录保存 RTS**：如 **Commission Delegated Regulation (EU) 2025/1140**（规定 CASP 需保存的记录范围与细则）。
- **冲突管理、投诉处理、业务连续性等 RTS**：CSSF 页面列示多个 RTS（冲突、投诉、连续性/服务稳定性等）。

3.3 卢森堡本国实施法（关键）

- **Law of 6 February 2025**：在卢森堡官方公报发布，并正式指定 CSSF 为 MiCA 主管机关，同时对本国框架作相应衔接安排（含过渡措施等）。

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、跨境护照、第三国招揽边界）

这一栏给“董事会一页纸”——先看能否做、差距有多大、需投入什么资源。

4.1 公司实体与实质经营（Substance）

- 申请主体须为 **法律实体/企业**（MiCA 对 CASP 的定义为提供加密资产服务的法律实体或其他企业）。
- 卢森堡实务重点：
 - 卢森堡公司设立（Sàrl / SA 常见）+ **实际管理与关键职能在卢森堡可被监管触达**（董事会运作、关键岗位在岗、外包可控）。
 - 运营地点、关键系统/数据治理、审计可达性、第三方外包合同（含分包链）要可穿透。

4.2 资本/审慎与“保障”思路

- MiCA 对 CASP 设定 **最低自有资金/资本金**要求（按服务类型分档），同时要求持续满足“自有资金/保险或等效保障”等审慎安排（具体以 MiCA 条款+业务范围映射为准）。
- 卢森堡审查口径通常会将：资本金、运营费用覆盖（固定开支）、客户资产隔离、保险覆盖（职业责任/网络安全/托管风险）作为一体化风险缓释组合来评估。

4.3 治理与三道防线

- 董事会/管理层适任性（Fit & Proper）、关键职能独立性、合规/MLRO 资源配置、内审（可外包但需独立性）是“是否可批”的底层门槛。
- 股东/UBO（重大持股）透明、资金来源可解释、持续变更通知机制要前置搭好。

4.4 业务模型与客户保护

- 产品/服务映射 MiCA 服务清单（托管、交易平台、法币兑换、币币兑换、执行、传递、承销/配售、投顾、组合管理、转移服务等）。CSSF 已在 CASP 页面列明服务类型。
- 客户分类、适当性/适配性、费用披露、投诉机制、冲突管理、营销合规（尤其跨境/第三国招揽）需成体系。

4.5 技术安全与外包（含 DORA 关联）

- 钱包/密钥管理（冷热分离、多签、权限控制）、渗透测试与漏洞管理、BCP/DR、监报告警、供应商管理与可审计性。
- 卢森堡同时推进 DORA 适用（2025/01/17 起适用的背景下，金融实体 ICT 风险治理与外包管理会被更严格地“同向要求”审视）。

4.6 跨境护照与第三国招揽边界

- **护照**：获批后可按 MiCA 的跨境机制扩展至其他成员国（实操：需要营销材料合规、语言/投诉/消费者保护本地化、以及接收国监管沟通节奏）。
- **第三国**：对第三国客户的获客、反向招揽（reverse solicitation）边界必须在制度与话术层面固化，否则会被视为无照跨境。

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)

CSSF 强烈建议“先对话、后递交”。市场实践中, Pre-Application 能显著降低补件轮次与节奏失控风险。CSSF 亦公开邀请有项目的实体进行初步沟通 (preliminary dialogue)。

Step 0 | 项目立项与差距评估 (2–4 周)

- 服务范围确认: MiCA 服务清单映射 (做哪些、不做哪些、边界怎么控)。
- 差距评估: 资本、人员、制度、IT/钱包、外包、数据治理、风控与财务模型。
- 输出: 差距清单 + 里程碑计划 + 预算框架 (见第 22 栏甘特图)。

Step 1 | Pre-Application 沟通 (4–8 周)

- 与 CSSF (ipig@cssf.lu 或既有监管联系人) 进行预沟通: 业务模型、组织与外包、资金与客户保护、系统架构与上线计划。
- 输出: Pre-app deck + Q&A pack (我司可提供, 见第 20 栏)。

Step 2 | 递交申请 (Article 62/63 授权申请)

- 使用 CSSF 提供的 CASP 授权申请表 DOCX 及配套声明表 (Declaration of honour) 等。
- 同步准备股东/UBO 重大持股评估材料 (见第 7 栏)。

Step 3 | 完整性审查 (Completeness Check)

- 监管先看“是否齐套”: 缺关键制度/关键岗位/关键外包合同/关键风险评估, 通常会直接进入补件。
- 经验: 材料结构化、引用清晰 (MiCA 条款对照) 可显著提高通过率。

Step 4 | RFI (补件问询) / 监管面谈 (Interview)

- 重点问:
 - 客户资金/资产隔离与托管安排;
 - 冲突管理与收费披露;
 - AML/KYC、链上监测、Travel Rule、制裁筛查;
 - 钱包密钥治理与外包可控性;
 - 治理与关键岗位独立性;
 - 跨境获客与第三国边界。

Step 5 | 批准 (Authorisation) → 注册/公告 → 上线准备

- 获批后进入: 业务通知/护照、客户条款更新、上线演练、外包 SLA 执行、首期报告准备。

6) 所需材料清单 (Master Checklist) (A–I 分类)

下面为“可交付级”结构; 仁港永胜可按此输出 整套 Word/Excel Checklist (带责任人/状态/证据链接/版本号)。

A 类 | 公司与治理 (Corporate & Governance)

- 公司注册文件: 章程、股东名册、董事/管理层任命文件、集团结构图 (含穿透至最终自然人)。
- 董事会议事规则、授权矩阵 (Delegation of Authority)、三道防线框架。
- 关键政策: 冲突管理政策 (含利益冲突识别/缓释/披露)、关联方交易政策。
- 组织结构与岗位说明书 (含独立性与汇报线)。

B 类 | 业务范围与商业计划 (Business Model)

- 服务清单映射 (MiCA 服务类型逐项勾选)、目标客群、目标市场与获客渠道。
- 收费模型与披露样例 (费率表、点差、托管费、上市费、做市/返佣等)。
- 客户协议、风险披露、产品条款、隐私与数据说明。

C 类 | 股东/UBO/重大持股与资金来源 (Shareholders/UBO)

- 10%/重大持股（qualifying holding）相关：股东/UBO 身份、声誉声明、无犯罪/监管处分说明、资金来源（SOF）与财富来源（SOW）证据链。
- 控制权安排：股东协议要点、表决权、最终受益人控制说明。
- 持续通知机制：股权变更触发阈值、预先沟通与申报流程（见第 7 栏）。

D 类 | 合规与 AML/CFT (Compliance & AML)

- AML/KYC 手册（客户尽调、增强尽调、链上监测、可疑交易报告、制裁、PEP、名单管理）。
- 交易监控规则库与案例、STR/SAR 流程图。
- Travel Rule 方案（适用范围、消息标准、对手方合规、失败处理）。
- 培训计划、年度合规计划、合规监控测试计划。

E 类 | 风险管理与客户保护 (Risk & Client Protection)

- 风险偏好声明、风险评估（含市场/流动性/操作/技术/外包/合规/声誉）。
- 客户资产隔离方案：托管结构、银行账户/链上地址隔离、对账与审计轨迹。
- 投诉处理机制（按 EU RTS 要求结构化：受理、时限、升级、记录与复盘）。
- 适当性/适配性：投顾/组合管理/高风险产品分层与评估问卷（如适用）。

F 类 | ICT/钱包/安全 (ICT & Security)

- 系统架构图（生产/灾备/监控）、数据流图、权限分层与审计日志。
- 钱包治理：冷热钱包策略、多签策略、密钥生成/备份/轮换/销毁、HSM（如用）。
- 安全管理：渗透测试、漏洞管理、SOC/告警、事件响应、BCP/DR 演练。
- 供应链安全：第三方依赖清单（含云、托管、KYT、KMS、支付通道）。

G 类 | 外包与第三方 (Outsourcing)

- 外包政策（尽调、审批、持续监控、退出计划、分包链管理）。
- 合同包：SLA、审计权、数据归属、事故通报、监管访问权、跨境数据条款。
- 关键外包清单与“关键性评估”(materiality assessment)。

H 类 | 财务、资本、保险与审计 (Financial/Prudential)

- 三年财务预测（含压力情景）、固定开支测算、资本金到位证明。
- 保险/等效保障：职业责任险、网络险、托管/盗损相关保障（按业务风险定制）。
- 审计安排：审计师选聘、审计范围、对账与控制测试计划。

I 类 | 跨境护照与营销合规 (Passporting & Marketing)

- 护照扩张计划：目标国家清单、语言与本地合规适配、投诉/客服安排。
- 营销合规手册：广告审批、KOL/代理管理、第三国反向招揽边界话术。
- 监管沟通日志模板与重大事件报告机制。

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

7.1 重大持股 (Qualifying Holding) 与阈值管理

- 实务上以**10%及以上**（或能施加重大影响/控制）作为重大持股管理起点：
 - 需要提交穿透结构、控制权解释、SOF/SOW 证据链；
 - 需要建立“变更触发清单”：增持/稀释/表决权安排变更/一致行动等。
- CSSF 已在其 MiCA 材料清单中纳入“重大持股评估相关的 EU 规则/模板”，并汇总相关 Delegated Regulation（qualifying holding assessment）链接。

7.2 声誉与适当人选 (Reputation & Integrity)

- 股东/UBO、董事、高管：

- 监管记录、刑事/行政处罚、破产/失信、重大诉讼；
- 过往金融机构任职与离任原因；
- 是否与高风险司法辖区、制裁主体存在关联。

7.3 资金来源（SOF）与财富来源（SOW）——“可核验、可追溯、可解释”

- 监管期待的是“证据链闭环”：
 - 资金从哪里来（工资/股息/企业盈利/融资/资产出售）；
 - 怎么到位（银行流水、审计报告、交易合同、纳税证明）；
 - 为什么合理（与个人/集团规模匹配、与业务计划匹配）。

7.4 持续通知与变更管理（Post-licence）

- 需要制度化：
 - 股权变更预沟通机制（重大变更先沟通再实施）；
 - 董事/高管变更、关键岗位离任、关键外包更换等的报备流程（见第 12 栏）。

8) 合规/MLRO/关键岗位要求（详细）（资历、独立性、资源、汇报线、外包可否）

8.1 必备关键岗位（建议最低配置）

- 合规负责人（Head of Compliance）：负责 MiCA 合规框架落地与持续监控。
- MLRO（反洗钱负责人）：负责 AML/CFT 制度、STR/SAR、培训与风险评估。
- 风险负责人（Head of Risk）：负责风险偏好、模型、监控与压力测试（规模较小时可与合规区分但须避免自我复核）。
- 信息安全/ICT 负责人（CISO/Head of ICT Security）：钱包与系统安全治理。
- 内审（Internal Audit）：可外包，但需保持独立性与审计计划的覆盖。

8.2 资历与独立性（监管关注点）

- 资历：相关行业经验（支付/证券/交易所/托管/信息安全/AML）、管理经验、监管沟通能力。
- 独立性：
 - 合规/MLRO 不应被业务 KPI 绑架；
 - 汇报线建议“直达董事会/审计或风险委员会”；
 - 三道防线的职责边界要写进制度与组织章程。

8.3 资源充足性（Resourcing）

- CSSF/欧盟层面越来越强调“纸面合规不够”，要看到：
 - 人员编制、外包辅助、系统工具（制裁筛查/KYT/Travel Rule）、预算。
- CSSF 对 VASP（AML 注册）层面亦明确其监督与执法主要聚焦 AML/CFT，并可收取费用；CASP 授权后则进入更全面监管。

8.4 外包可否（结论）

- 可外包：部分合规支持、KYT 工具、内审、部分 IT 运维等。
- 不建议外包：核心治理职责“完全外包”（如 MLRO 仅挂名、关键控制不在本体掌握）——通常会在面谈中被打回。

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

这是 CASP 申请里“最容易被 RFI 拉长周期”的部分，务必用 图 + 制度 + 证据 三件套呈现。

9.1 钱包与密钥治理（Wallet & Key Management）

- 冷热分离：热钱包限额、自动补充策略、异常触发冻结。
- 多签：多签门限、签名人角色分离、紧急替换机制。
- 密钥生命周期：生成/备份/分片/托管/轮换/销毁；HSM 使用策略。

- 地址治理：客户地址隔离、归集策略、链上标签与可追踪性。

9.2 权限分层与操作控制（IAM / SoD）

- 最小权限、双人复核、特权账号管理（PAM）、操作审计日志不可篡改。
- 上市/下币、风控参数、名单策略、费用参数等关键配置须有变更审批与回滚。

9.3 安全测试与持续防护

- 渗透测试（至少年度+重大变更后）、漏洞扫描、代码审计（核心钱包/交易系统）。
- 事件响应：分级响应、取证、对外通报、客户沟通模板。
- BCP/DR：RTO/RPO、灾备演练、关键供应商故障演练。

9.4 外包与 DORA 关联（实务提示）

- 卢森堡 DORA 相关立法与适用节奏，会让监管更看重 ICT 风险与外包可控性（尤其关键外包的审计权与退出）。

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（Segregation）

- 法律与操作双隔离：
 - 客户法币：独立客户资金账户、与自有资金隔离、日对账与差异处理。
 - 客户链上资产：地址隔离/子账户、可追溯对账、托管人（如有）三方核对。

10.2 费用披露与“误导性定价”风险

- 点差、撮合费、上市费、提现费、托管费、做市返佣、清算费用：
 - 必须在客户协议与费率表中清晰披露；
 - 若存在“自营对手方/关联方流动性提供”，需额外披露冲突与定价机制。

10.3 投诉处理（Complaints）

- CSSF 页面列出关于投诉处理的 EU RTS（适用于 CASP 投诉处理要求），建议将：渠道、时限、升级、复盘、统计报表制度化。

10.4 利益冲突（Conflicts of Interest）

- CSSF 页面亦列出冲突管理 RTS（政策与程序细化）。
- 实务重点：
 - 自营/做市与客户撮合的冲突；
 - 上市评估与商业利益冲突；
 - 关联方供应商/渠道的利益输送；
 - 员工交易与信息隔离墙。

10.5 适当性/适配性（如提供投顾/组合管理）

- 若服务范围包含投顾/组合管理，需要适当性评估、定期对账/报告格式等；CSSF 已发布适用 ESMA 指引的通函（portfolio management 的适当性与定期报表格式）。

11 官方收费与预算（政府费/监管年费/审计/法律/技术/保险/人员成本）

费用必须分“监管收费（官方）”与“落地成本（市场）”两层；前者以最终法规为准，后者以业务复杂度为准。

11.1 监管/官方费用（以最新公布/草案口径管理）

- CSSF 侧：已存在对 VASP（AML 注册）收费的法定基础描述。
- 关于 CASP 授权/年费：卢森堡在 2025 年末出现一份关于收费“固定包干（forfait）”的文件（含：新 CASP 申请审查费、扩展服务审查费、通知类审查费、以及年度固定年费等具体金额）。该文件显示例如：新 CASP 申请审查费 30,000 欧元、年度固定 40,000 欧元等

(并对“已有其他 CSSF 牌照实体”给出较低档)。请注意：该材料需核对其是否已最终生效并发布为正式法规，我司实务会以 CSSF/Legilux 最终文本为准进行预算锁定。

11.2 落地预算（建议按“最小可批配置”估算）

- 法律顾问：申请材料定稿、合同包、外包条款、跨境营销合规。
- 审计/会计：财务预测模型、控制测试、年审与对账框架。
- 技术：KYT/制裁筛查/Travel Rule、钱包托管/多签、SOC、安全测试、DR。
- 保险：职业责任险/网络险/托管相关保障（取决于托管规模与风险）。
- 人员：合规、MLRO、风控、信息安全、运营、客服、财务。

我司可提供“预算表（Excel）”按模块拆分：一次性（setup）+ 运行性（run-rate）+ 缓冲金（contingency）。

以上报价未含服务费用，具体金额以仁港永胜业务顾问报价为准。

12) 后续维护与续牌/持续合规（报告、审计、变更报备、培训、演练）

1 持续合规（核心清单）

- 定期报告：监管报表/运营数据/客户投诉统计/重大事件通报（按 MiCA + CSSF 要求）。
- 审计与内控：年审、控制测试、外包审计与渗透测试报告归档。
- 变更报备：股权/董事/高管/关键岗位/关键外包/系统重大变更/新业务上线前沟通与报备。
- 培训：年度 AML/合规/信息安全培训与考核；演练：BCP/DR、事件响应、制裁冻结演练。

2 记录保存（Record-keeping）

- CSSF 已在 CASP 页面列示记录保存 RTS（EU 2025/1140），意味着必须建立“可导出、可审计、可追溯”的订单/交易/指令/服务记录体系。

卢森堡版 | 后续维护与续牌/持续合规

MiCA 对 CASP 采取“授权 + 持续监管”框架；在卢森堡由 CSSF 执行监管与跨境护照通报管理。

12.1 持续合规总框架（你可以直接写进《合规年度计划》）

持续合规建议拆成 6 条“主线”，每条主线都要形成 制度 + 系统 + 证据链：

1. 授权范围合规（Scope Control）

- 上线后的实际业务、产品、客户旅程、营销口径必须与授权服务完全一致（Programme of Operations 版本控制）。
- 任一“新增服务/新增重大功能/新增目标国家”→ 必须先走“合规评估 + 监管沟通/通报/报备”闭环（见 12.4）。

2. 治理与适任性（Governance & Fit&Proper）

- 董事会/高级管理层：持续满足适任性、时间投入、利益冲突管理与问责制。
- 关键岗位（合规、MLRO、风险、ICT 安全、内审等）：不得“空心化”，要留存履职证据（报告、会议纪要、抽查记录、KRI/KPI）。

3. AML/CFT 持续运行（Run-the-AML）

- 客户风险评级、CDD/EDD、制裁/PEP、交易监控、STR 决策链必须真实运行并可审计。
- 卢森堡如仍处于 VASP 注册阶段或并行安排：CSSF 的 VASP 监管侧重 AML/CFT（注册、监督、执法）。

4. ICT / 安全 / 外包（DORA 对齐）

- 自 2025-01-17 起，DORA 对在范围内金融实体的 ICT 风险管理、事件通报、第三方外包治理、韧性测试提出统一要求。
- 强制动作：外包登记册（Register of Information）、重大 ICT 事件通报流程、DR 演练、渗透测试整改闭环等（详见 12.3）。

5. 客户保护与市场行为（Conduct & Client Protection）

- 费用透明披露、利益冲突、投诉处理、适当性/适配性（如涉及投顾/组合管理）、客户资产隔离与对账机制持续有效。

6. 报告与审计 (Reporting & Assurance)

- 年度审计/独立评估 (财务审计 + 合规独立审查 + ICT 安全评估/渗透测试 + AML 独立审查)。
- 形成“年度合规包”: 年度合规报告、年度风险报告、年度 ICT/DORA 报告、年度 AML 报告 (含 STR 统计与改进计划)。

12.2 必做报告 (建议做成“持续合规日历”)

MiCA 报告的具体模板与频率, 会随着 ESMA Level 2/3 的 RTS/ITS/Guidelines 持续标准化; 项目上应预留“报送能力建设”。

A. 常规经营类 (Management Reporting) (建议: 月/季)

- 经营指标: 客户数、活跃度、交易量、收入结构 (手续费/点差/托管费等)
- 风险指标: KRI (欺诈、制裁命中、异常交易、系统告警、冷钱包出入金异常)
- 合规指标: KYC 完整率、EDD 占比、STR 流转时效、培训覆盖率
- 外包指标: SLA 达成、重大故障、审计发现与整改

B. 监管类 (Regulatory Reporting) (按监管要求触发/定期)

- 重大变更报备/通报 (股权、董事、关键岗位、外包、系统架构、服务范围、客户条款等)
- 重大事件报告 (合规/AML/安全/客户资产相关事件)
- 护照通报: 向其他成员国提供服务前的通知程序 (见 16.3)

12.3 DORA (2025-01-17 生效) 下的持续义务 (卢森堡 CSSF 可执行清单)

DORA 关键点 (你要落地成制度 + 工具 + 证据):

1. ICT 风险管理框架: 资产清单、风险评估、控制库、监控告警、事件响应
2. 重大 ICT 事件通报: 分级、时限、模板、责任人、演练
3. 第三方风险管理: 供应商尽调、合同条款、审计权、退出与迁移
4. 数字韧性测试: 渗透测试、场景演练、DR 演练 (RTO/RPO)
5. 外包登记册报送: CSSF 对“register of information”提交窗口/参考日期有明确安排 (例如首年参考日期与提交窗口)。

12.4 变更报备 (Change Management) —建议按“触发阈值”建规则

建议把变更分为三类, 并在内部制度写明 “先评估→再沟通/报备→后实施→留档”:

(1) 重大变更 (通常需预沟通/正式报备)

- 股权: UBO/重大持股变动 (含新增 10%+、控制权变化、投票权协议/可转债触发等)
- 董事/高管/关键岗位: CEO/COO/CTO、合规负责人、MLRO、ICT 安全负责人、内审负责人
- 服务范围: 新增/变更 CAS 服务类型; 新增撮合规则/做市机制; 新增托管方式
- 外包: 新增关键外包、变更关键供应商、数据迁移到新云区域
- ICT: 核心架构调整、钱包体系重构、密钥管理机制变更 (HSM/多签门限/签名仪式)
- 客户保护: 条款、披露、费用结构、投诉机制的重大调整

(2) 一般变更 (留档+定期汇报)

- 非关键人员调整、内部流程优化、非关键系统升级等

(3) 紧急变更 (先处置后报告)

- 安全事件紧急修复、零日漏洞紧急补丁等: 必须保留事件记录与复盘报告

12.5 培训与演练 (Training & Drills) —监管最爱抽查“证据链”

建议形成“四张表”:

1. 年度培训计划 (入职/年度/岗位专项: 合规、AML、制裁、数据保护、ICT、客服)
2. 培训证据包 (课件、签到、测验、通过率、补训记录)
3. 年度演练计划 (DR 演练、事件响应演练、密钥灾备演练、外包退出演练)

12.6 “续牌”怎么理解？

MiCA 下 CASP 是持续授权逻辑，通常不按“到期续牌”运作；但你必须持续满足监管条件，否则可能被整改、限制业务或撤销授权。CSSF 对 MiCA/CASP 授权与持续监管的总体口径以其 MiCA 专页与后续公告为准。

13) 办理时间预估（公司设立、文件编制、审查窗口、缓冲）

这里给你“项目可控”的时间表：把不可控因素（股东资金来源、关键岗位、外包/系统复杂度、补件轮次）放入缓冲。

13.1 公司设立与实质搭建（2–6 周）

- 卢森堡公司设立、银行账户（或临时资金安排）、办公地址、核心岗位到岗/合同签署
- 治理体系落地：董事会章程、授权矩阵、三道防线、会议纪要模板

13.2 申请文件编制（8–14 周 | 取决于服务范围）

- Programme of Operations + Business Plan：2–4 周
- 股东/UBO 资金来源闭环包（SoW/SoF+资金路径图）：2–6 周（最容易拖延）
- AML 制度+系统说明+STR 机制：2–4 周
- ICT/钱包/外包（DORA 对齐）文件：3–6 周
- 客户协议/披露/投诉机制：2–3 周

并行推进是关键：否则周期翻倍。

13.3 预沟通（Pre-application dialogue）（建议 2–4 周）

CSSF 明确鼓励拟申请 CASP 的实体尽早联系、启动预沟通，用于提前识别潜在问题点（结构、外包、治理、材料缺口）。

13.4 监管审查窗口 + 补件缓冲（核心不确定性）

你要预留：

- 完整性审查（材料齐全性检查）
- 实质审查（RFI/面谈/反复补件）
- 获批条件落实（注资/保险/系统验收/演练证据/人员正式任命）

实务上最影响周期的前三名：**SoF/SoW 证据链、关键岗位资历与独立性、ICT/外包可审计性（DORA 化）**。

13.5 过渡期主体（Grandfathering）时间轴提醒（卢森堡 18 个月）

ESMA 公布的成员国过渡期清单显示：**Luxembourg 为 18 个月**（MiCA Article 143(3) 选项）。

对既有主体：必须倒排“可持续营业窗口 + 递交点 + 补件缓冲”，避免错过关键节点导致业务被迫停摆或宣传合规风险。

唐生简单预估，以“交付级材料”标准估算（不同复杂度差异很大）：

- 公司设立与开户准备：2–6 周（视股东结构与银行尽调）。
- 文件编制（制度+合同+系统证据）：8–16 周（交易平台/托管类更长）。
- Pre-Application + 首轮反馈：4–10 周（取决于 CSSF 排期与项目成熟度）。
- 正式递交后 Completeness + RFI：常见 2–6 轮补件（材料成熟可显著减少轮次）。
- 总体：**6–12 个月**常见；“平台型/托管型/多国护照扩张”可能更长。

关键不是“天数”，而是：是否提前把 **治理、关键岗位、钱包安全、外包合同包、客户资产隔离**做成可审计证据。

14) 常见问题（FAQ）（Q1–Q50，可扩展 Q1–Q200）

（卢森堡 Luxembourg crypto license FAQ | 本文由仁港永胜唐生拟定讲解）

A. 牌照定义与适用范围（Q1–Q20）

Q1 什么是 MiCA 下的 CASP？

A：在欧盟 MiCA 框架下向客户提供加密资产服务并需取得授权的机构。

Q2 卢森堡 CASP 的主管机关是谁？

A：卢森堡金融监管机构 **CSSF** 负责受理授权与持续监管。

Q3 MiCA 的 CASP 授权何时适用？

A：MiCA 对 CASP 的统一授权要求自 2024-12-30 起适用（欧盟统一节点）。

Q4 CASP 可以覆盖哪些服务？

A：可涵盖托管、交易平台、兑换（法币/加密、加密/加密）、执行/传递订单、转移、投顾、组合管理等（以 MiCA 服务清单为准）。

Q5 我只做 OTC 撮合算不算 CASP？

A：通常要看你是否为客户执行/传递订单、是否提供兑换、是否控制客户资产；建议做业务定性备忘录。

Q6 我只做托管能否只申请托管类？

A：可以按单项服务申请，但托管对钱包/密钥/隔离/对账要求更严。

Q7 交易平台与执行订单有何区别？

A：平台一般涉及撮合机制与市场监控；执行订单偏向为客户在外部场所执行，合规重点不同。

Q8 兑换服务为什么审查更严？

A：涉及资金流与洗钱风险更高，AML/制裁筛查与监控规则需要更强。

Q9 投顾/组合管理要额外做什么？

A：加强适当性/适配性、利益冲突、记录留存，并证明人员资历与方法论。

Q10 转移服务的监管关注点？

A：地址风险、制裁筛查、错误转账处理、链上/链下对账、事件响应。

Q11 只做 B2B API 服务还要牌照吗？

A：若实质上向客户提供受规管加密资产服务，仍可能需要授权；需看服务边界与客户旅程。

Q12 拿到卢森堡 CASP 能否护照到全欧盟？

A：可通过 MiCA 通报机制向其他成员国提供服务（自由提供或设分支）。

Q13 护照通报由谁办理？

A：由 CSSF 作为本国主管机关协助执行通报流程。

Q14 我能否先在别国拿 CASP 再来卢森堡展业？

A：可走护照通报，但仍要遵守当地消费者保护与营销合规要求。

Q15 申请材料能否用英文？

A：通常可用英文更利于跨境团队准备，但关键法定文件可能需符合 CSSF 要求（以沟通口径为准）。

Q16 申请一定要在卢森堡设公司吗？

A：以卢森堡作为授权国，通常需在欧盟设立实体并满足有效管理与可触达监管要求。

Q17 “有效管理地”怎么证明？

A：董事会决策留痕、关键岗位履职、外包与系统可审计、监管可触达。

Q18 可以远程运营吗？

A：可以，但要证明合规、AML、ICT 治理不因远程而失控，并保留证据链。

Q19 申请前是否建议联系 CSSF？

A：建议，CSSF 明确鼓励尽早启动预沟通以识别问题点。

Q20 卢森堡 VASP 注册与 MiCA CASP 授权有何区别？

A：VASP 注册主要用于 AML/CFT 目的，**不等同 MiCA 授权，也不带 EU 护照**。

B. 过渡期与合规宣传（Q21–Q35）

Q21 卢森堡是否有 MiCA 过渡期？

A：ESMA 清单显示卢森堡为 **18 个月**。

Q22 过渡期适用于谁？

A：通常针对在 MiCA 节点前已在本国合法开展相关业务的既有主体（需逐案匹配本国条件）。

Q23 过渡期内可以继续运营吗？

A：取决于你是否满足过渡安排条件及是否按要求提交/推进授权申请；需按 CSSF 口径执行。

Q24 过渡期内能否对外宣传“已受监管/等同持牌”？

A：必须谨慎，避免误导性营销；建议统一话术“申请中/过渡安排中”的合规表述与审批机制。

Q25 错过关键节点会怎样？

A：可能面临被迫停止受规管服务、监管执法或声誉风险。

Q26 过渡期项目的最关键动作？

A：倒排时间轴 + 提前补齐 SoF/SoW、关键岗位、ICT/DORA、AML 证据链。

Q27 申请期间能否先做市场推广？

A：可做品牌建设，但应避免“招揽、受理、执行、托管”等受规管行为与表述。

Q28 若同时服务欧盟与第三国客户要注意什么？

A：跨境招揽边界、制裁风险、数据跨境、AML 风险分层与限制策略。

Q29 申请过程中客户协议能先上线吗？

A：可先准备，但对外生效前需完成合规审查与版本控制，避免承诺超授权范围。

Q30 过渡期内是否仍要满足 AML/CFT？

A：是，且 AML 是最常见执法抓手之一，必须真实运行并可审计。

Q31 若原先仅 VASP 注册，是否可直接转 CASP？

A：可作为基础但不等同“自动升级”，仍需完成 MiCA 授权包与持续义务建设。

Q32 监管更关注什么来判断你是“真实经营”？

A：人员、系统、外包治理、客户保护、董事会治理与可审计证据链。

Q33 过渡期内可以护照到其他国家吗？

A：护照机制一般基于 MiCA 授权后通报；过渡期不当然等同护照资格。

Q34 过渡期主体最容易踩的雷？

A：宣传误导、实际业务超范围、AML 运行不足、ICT/外包不可审计。

Q35 仁港永胜建议的过渡期打法？

A：双轨合规（旧框架 + MiCA/DORA），并建立“补件战情室”机制确保应答效率。

C. 股东/UBO/资金来源（Q36–Q60）

Q36 10% 股东就要做尽调吗？

A：建议按“10%/重大影响”门槛准备全套：穿透、声誉、SoF/SoW、持续通知机制。

Q37 UBO 穿透到什么层级？

A：穿透到最终自然人控制人，并解释控制权路径（投票权、协议控制、可转工具）。

Q38 资金来源（SoF）与财富来源（SoW）有什么区别？

A：SoW 解释财富如何形成；SoF 解释本次出资资金从哪里来及路径证明。

Q39 资金路径图（Money Trail Map）要多细？

A：要能把“钱从哪里来→经过哪些账户→如何进入公司”闭环，并与银行流水对应。

Q40 可以用加密资产证明资金来源吗？

A：需更谨慎：估值、流动性、合规来源、链上证据与法币出入金路径都要可核验。

Q41 股东有媒体不利信息怎么办？

A：做不利信息解释备忘录：事实、时间线、处置、改进措施、是否影响诚信与声誉。

Q42 股东背景调查需要哪些维度？

A：诉讼/破产、监管处罚、刑事记录、制裁与 PEP、媒体与商业纠纷。

Q43 股东是公司/基金时要额外提供什么？

A：公司注册文件、董事/控制人信息、受益人结构、审计报告、资金链与治理授权。

Q44 股东变更是否必须报备？

A：重大持股与控制权变更通常需提前评估并报备/沟通。

Q45 股东贷款注资可行吗？

A：可行但需解释条款、偿付能力、是否影响审慎保障与持续经营。

Q46 如何证明“资金足以覆盖 12–36 个月运营”？

A：三年预测 + 成本结构 + 压力测试 + 资金到位证明（含应急资金安排）。

Q47 关联方交易会被重点看吗？

A：会；需关联交易政策、定价依据、转让定价/商业实质证明与审批留痕。

Q48 能否用 SPV/多层控股结构？

A：可用，但要把穿透与控制权解释清楚，避免“看不见的控制人”。

Q49 需要持续更新股东资料吗？

A：需要；建立文件有效期管理与触发更新机制（住址、身份、控制权变化等）。

Q50 股东是否必须在欧盟？

A：不必然，但跨境股东更强调可核验资料、制裁风险与资金链清晰度。

Q51 UBO 是 PEP 是否一定拒绝？

A：不一定，但必须 EDD、管理层审批、加强监控与资金来源核验。

Q52 如何处理“隐名股东/代持”？

A：高风险；建议透明化并完整披露，否则很容易被否决或要求整改。

Q53 是否要提交股东承诺书？

A：建议提交（遵守 AML/制裁/治理要求、配合监管、重大变更及时通知）。

Q54 股东的时间投入也要证明吗？

A：对董事/高管更关键；股东则强调影响力与是否干预经营的治理边界。

Q55 资金来源解释不清会发生什么？

A：最常见的补件点，直接拉长周期甚至导致否决。

Q56 如何让资金来源材料“更容易过”？

A：用“来源—路径—证明—一致性校验”四段式，并建立证据索引。

Q57 新融资计划要披露吗？

A：建议披露未来融资/可转工具/期权安排，避免未来触发控制权变化争议。

Q58 重大持股门槛只看股权比例吗？

A：不只；投票权、协议控制、董事席位安排也可能构成重大影响。

Q59 股东在第三国有监管处罚记录怎么办？

A：如实披露并解释整改与当前状态，配合律师意见与补充证据。

Q60 仁港永胜在股东包能提供什么？

A：穿透结构图、SoF/SoW 模板、资金路径图、负面信息澄清备忘录、全套签署包与版本控制。

D. 董事/高管/关键岗位（Q61–Q90）

Q61 Fit & Proper 评估看哪四项？

A：胜任能力、诚信声誉、时间投入、利益冲突。

Q62 董事必须是卢森堡本地人吗？

A：通常不强制，但需证明治理有效、监管可触达、会议与决策留痕清晰。

Q63 关键岗位可以外包吗？

A：可外包部分工作，但责任不外包；合规/MLRO/ICT 风险等通常需要内部责任人。

Q64 合规负责人应向谁汇报？

A：建议直达董事会或合规委员会，确保独立性与资源保障。

Q65 MLRO 与合规负责人能否同一人？

A：小型机构可能可行，但需证明资源足够、无冲突、能履职并留痕。

Q66 内审必须内部设立吗？

A：可外包，但要独立、可审计、合同有审计权与整改跟踪机制。

Q67 CTO/安全负责人最关键的证明材料？

A：相关经验可核验、系统治理能力、事件响应与安全管理经验、DORA 体系理解。

Q68 时间投入怎么证明？

A：时间投入声明 + 兼职清单 + 董事会会议计划 + 关键职责分工与替补机制。

Q69 利益冲突怎么管？

A：利益冲突政策 + 申报表 + 回避机制 + 审批留痕。

Q70 关键岗位离职怎么办？

A：要继任计划、过渡安排、监管沟通与临时控制措施，避免控制失效。

Q71 如何准备监管面谈？

A：建立 Q&A pack：业务、AML、ICT、外包、客户保护、股东资金来源六大模块逐题演练。

Q72 董事会要开多频繁？

A：建议至少季度 + 重大事项临时会议，并保留纪要与决议。

Q73 三道防线怎么落地？

A：一线运营自控，二线合规/风险监督，三线内审独立评价；每条线要有记录产出。

Q74 小团队如何做到“资源充足”？

A：用“人员 + 工具 + 外包（可审计）”组合，并证明内部能管理外包。

Q75 监管最怕什么“空心化”？

A：关键岗位挂名、制度不运行、外包无审计权、事件无法解释与追溯。

Q76 客服算关键岗位吗？

A：在客户保护与投诉机制上是关键触点，应有 SLA、升级机制与投诉闭环留痕。

Q77 做市/流动性团队要单独披露吗？

A：如涉及平台/撮合/做市安排，应披露利益冲突、市场监控与客户披露。

Q78 反贿赂与员工纪律要做吗？

A：建议做，监管会看企业文化与合规氛围的制度化证据。

Q79 数据保护官 DPO 必须吗？

A：取决于业务与 GDPR 触发条件；但 GDPR 文件与治理必须完善。

Q80 仁港永胜能提供岗位 JD 与汇报线模板吗？

A：可以（合规/MLRO/风险/ICT/内审全套 JD + RACI + 委任函模板）。

Q81 关键岗位是否需要本地常驻？

A：不一定，但要保证可触达、可履职、可出席监管沟通与审计检查。

Q82 高管的项目经验要怎么写才“监管可验证”？

A：写清项目规模、职责、团队、系统、合规成果、监管对接经历，并提供证明材料。

Q83 是否需要董事会技能矩阵？

A：强烈建议，用于证明治理能力覆盖业务风险。

Q84 关键岗位能否用集团共享？

A：可用集团支持，但本地实体需具备足够控制力与监督能力。

Q85 监管抽查时最常要的证据？

A：会议纪要、合规监控记录、STR 决策记录、外包评估、事件响应记录、培训记录。

Q86 KPI 是否要与合规挂钩？

A：建议挂钩，体现“管理层问责”与合规优先。

Q87 新产品上线需要审批吗？

A：需要，新产品审批流程（NPC）是监管常见关注点。

Q88 关键岗位外包合同必须包含什么？

A：审计权、SLA、数据保护、安全要求、分包限制、退出与迁移、事件通报。

Q89 如果关键岗位短期空缺？

A：需临时代理与控制措施并留档，必要时与 CSSF 沟通。

Q90 仁港永胜对关键岗位配置的建议？

A：按“业务复杂度”分层配置，并以 DORA/AML 要求倒推最小可行团队+工具组合。

E. AML/KYC/制裁/STR（Q91–Q125）

Q91 卢森堡 VASP 注册与 AML 关系？

A：在卢森堡提供虚拟资产服务通常需在 CSSF 注册并接受 AML/CFT 监督（VASP 体系）。

Q92 仅有 VASP 注册能否护照到欧盟？

A：不能，VASP 注册不带 EU 护照；MiCA CASP 授权后才走护照。

Q93 AML 手册最小目录？

A：风险评估、CDD/EDD、制裁/PEP、交易监控、STR、记录保存、培训、独立审查。

Q94 必须做链上分析吗？

A：做转移/托管/平台/兑换基本都需要；监管会问你如何识别高风险地址与混币暴露。

Q95 STR 决策由谁做？

A：通常由 MLRO 负责最终判断与报送，并需独立汇报线。

Q96 如何降低误报率？

A：规则库分层+白名单治理+模型调参与版本管理+复核工单闭环。

Q97 如何管理 unhosted wallet 风险？

A：地址风险评分、限额分层、额外核验、链上追踪与异常报警。

Q98 高风险国家客户一定拒绝吗？

A：不一定，但要加强 EDD、限制产品/额度、提高监控，并保留决策记录。

Q99 第三方付款怎么处理？

A：高风险；建议限制或增强核验，并设异常模式识别与升级审批。

Q100 记录保存要多久？

A：按当地 AML 规定执行，并确保可检索归档与审计追溯。

Q101 AML 培训怎么才合格？

A：年度计划+入职培训+岗位专项+测验，通过率与补训记录齐全。

Q102 AML 独立审查必须吗？

A：强烈建议每年至少一次，形成整改闭环。

Q103 制裁筛查频率怎么设？

A：开户时+持续监控（名单更新触发）+交易触发（高风险场景）。

Q104 PEP 怎么管理？

A: EDD、管理层审批、资金来源核验、加强持续监控与定期复核。

Q105 KYC 能外包吗？

A: 可外包部分流程，但必须可审计、可监督、责任仍在持牌主体。

Q106 交易监控必须系统化吗？

A: 是，监管倾向“制度+系统+证据链”，仅文件合规风险极高。

Q107 OTC 现金场景如何控？

A: 限额、来源核验、增强尽调、可疑模式库、录像/签署留痕（视业务而定）。

Q108 如何处理无法核验 SoF 的客户？

A: 拒绝或限制服务，并留存证据；必要时按程序评估 STR。

Q109 AML 风险评级模型怎么做？

A: 客户/地域/产品/渠道/交易行为/链上风险六维评分，映射 CDD 深度与监控频率。

Q110 如何应对监管抽样检查？

A: 准备“抽查包”：样本档案、风险评分、监控处置、STR 记录、培训与审计报告。

Q111 返佣/代理渠道怎么管？

A: 渠道尽调、合同约定、合规培训、持续监控与抽查。

Q112 如何识别链上黑产资金？

A: 链上标签库+聚类分析+交易路径追踪+高风险暴露阈值。

Q113 是否要做反诈骗（Fraud）体系？

A: 建议，欺诈与 AML 常交叉；建立异常登录、社工防护、账户接管识别机制。

Q114 AML 与客户体验冲突怎么办？

A: 用分层策略：低风险简化、高风险强化，并把解释写入条款与披露。

Q115 需要建立黑名单吗？

A: 建议建立（客户/地址/设备/银行卡/对手方），并记录命中与处置。

Q116 STR 不报送也要留痕吗？

A: 要，必须记录“不报送原因”与依据，防止事后问责。

Q117 AML 工具选型要注意什么？

A: 覆盖制裁/PEP、链上分析、规则可配置、审计导出、数据留存与 API 集成。

Q118 如何证明 AML “有效运行”？

A: 以 KPI/KRI 证明：命中率、处置时效、复核闭环、培训覆盖、审计整改完成率。

Q119 账户冻结流程要写吗？

A: 要，包含触发条件、审批、通知、申诉、解冻与记录保存。

Q120 交易限额要怎么设？

A: 按客户风险分层，结合产品风险与链上风险，形成动态调整机制。

Q121 AML 与隐私（GDPR）冲突怎么办？

A: 按法定留存义务优先，建立数据最小化、访问控制与用途限制，并保留法律依据说明。

Q122 AML 报告要向董事会汇报吗？

A: 建议季度/半年汇报，体现治理层对 AML 的监督与问责。

Q123 仁港永胜能提供 STR 决策树吗？

A: 可以（规则触发→复核→MLRO 决策→报送/不报送留痕→复盘整改）。

Q124 申请阶段 AML 哪块最容易补件？

A: 风险评估方法论、交易监控规则与链上策略、STR 留痕机制、外包可审计性。

Q125 获牌后 AML 的第一优先级是什么？

A: 把 AML 变成“可运行的系统工程”：规则、工单、证据、复盘与持续改进。

F. ICT/钱包安全/外包（含 DORA）（Q126–Q165）

Q126 DORA 何时适用？

A: 自 **2025-01-17** 起直接适用；CSSF 亦发布了相关实施与报送指引/说明。

Q127 DORA 最重要的三件事？

A: ICT 风险管理、重大事件通报、第三方风险管理与韧性测试。

Q128 钱包体系监管最关注什么？

A: 密钥控制、冷热钱包分层、多签门限、权限分离、对账与审计轨迹、灾备与赔付机制。

Q129 多签怎么做才“监管友好”？

A: 最小权限+关键人分离+签名仪式留痕+定期轮换+可审计日志。

Q130 HSM 必须吗？

A：不绝对，但通常是最佳实践；关键是密钥管理的安全性、可审计性与灾备策略。

Q131 热钱包风险怎么控？

A：限额、白名单、实时监控、异常报警、自动冻结、分层审批。

Q132 冷钱包需要灾备吗？

A：需要：密钥分片/异地保管/恢复流程演练，并留存演练记录。

Q133 渗透测试必须做吗？

A：强烈建议，且要形成整改闭环与复测证据。

Q134 DR 演练要多细？

A：要能落地：RTO/RPO、演练脚本、恢复步骤、责任人、复盘与整改。

Q135 SOC 必须自建吗？

A：不一定，但必须具备等效 7×24 监控与告警处置能力，并留存记录。

Q136 外包清单必须披露吗？

A：必须，尤其关键外包；并要证明尽调、SLA、审计权与退出预案。

Q137 供应商合同必须包含什么？

A：审计权、数据与安全条款、分包限制、事件通报、业务连续性、退出与迁移。

Q138 云服务可以用非欧盟区吗？

A：需评估数据跨境、监管可触达与供应商风险；一般建议优先欧盟区域降低不确定性。

Q139 如何证明系统“可审计”？

A：不可篡改日志、权限变更留痕、关键操作双人复核、审计导出、对账可回溯。

Q140 内部人员作恶怎么防？

A：四眼原则、最小权限、强制休假/轮岗、行为监控、关键操作录屏/留痕、审计抽查。

Q141 订单撮合引擎用开源可以吗？

A：可以，但要代码审计、供应链风险管理、版本控制与漏洞响应机制。

Q142 市场操纵/刷量怎么管？

A：异常交易监控规则、处置流程、黑名单机制、披露与复盘。

Q143 重大 ICT 事件发生后要做什么？

A：分级→隔离→取证→通报→恢复→复盘整改（并保留完整证据链）。

Q144 外包 KYC/链上分析合法么？

A：可以，但必须可审计、可监督、数据合规、替代方案明确。

Q145 外包是否能“转移责任”？

A：不能，责任仍在持牌主体。

Q146 系统上线前需要什么“验收包”？

A：权限矩阵、对账机制、压力测试、渗透测试报告、DR 演练记录、日志审计演练。

Q147 DORA 的外包登记册是什么？

A：对 ICT 第三方服务依赖的登记与报送要求；CSSF 对报送有窗口安排。

Q148 供应商尽调要查哪些？

A：安全能力、合规资质、财务稳定性、分包链、数据处理、事故记录、BCP 能力。

Q149 如何管理配置变更？

A：变更管理流程、审批、回滚计划、记录留存与审计。

Q150 如何做数据分类？

A：按敏感级别分类、加密与访问控制、最小化与用途限制。

Q151 需要做数据字典吗？

A：强烈建议（MiCA/DAC8 报送趋势下会越来越刚性）。

Q152 钱包对账机制怎么设计？

A：链上余额、内部账、客户账三账一致；差异处理工单化。

Q153 客户资产证明（Proof of Reserves）必须吗？

A：不一定强制，但作为客户保护与透明度措施非常加分。

Q154 发生私钥泄露怎么办？

A：立即冻结/迁移、事件通报、客户通知、取证、赔付/保险路径、复盘整改。

Q155 需要网络分区吗？

A：建议做（生产/测试隔离、关键系统隔离、最小访问路径）。

Q156 开发流程要合规吗？

A：要（代码审计、发布管理、漏洞管理、补丁策略）。

Q157 供应链攻击怎么防？

A: SBOM、依赖库管理、签名校验、代码审计、供应商安全评估。

Q158 第三方访问怎么管？

A: 最小权限、临时授权、强 MFA、访问记录、定期复核。

Q159 设备安全怎么管？

A: 终端加密、EDR、补丁管理、远程办公安全策略。

Q160 仁港永胜能提供 DORA 外包条款库吗？

A: 可以（审计权、SLA、退出、事件通报、分包限制等条款库）。

Q161 申请阶段 ICT 哪块最易补件？

A: 密钥控制与审计轨迹、外包可审计性、DR/BCP 的可执行性。

Q162 获牌后 ICT 合规的第一件事？

A: 把“事件通报 + 演练 + 外包登记册”制度化并形成年度证据链。

Q163 冷钱包签名仪式要记录吗？

A: 要，签名日志/审批日志/人员到场记录是关键审计证据。

Q164 钱包权限矩阵要多细？

A: 细到角色-动作-环境-审批人-日志字段，且可导出。

Q165 ICT 治理最核心的底层逻辑？

A: “可审计、可追溯、可解释、可恢复”。

G. 客户保护/条款披露/投诉（Q166–Q200）

Q166 客户资产必须隔离吗？

A: 必须有清晰隔离与对账安排，尤其托管/平台/兑换场景。

Q167 客户协议至少包含什么？

A: 服务描述、费用、风险披露、资产处理规则、投诉、终止、隐私、责任限制与赔付框架。

Q168 费用披露要多细？

A: 交易费、点差、提现费、托管费、第三方费用、返佣/利益冲突都应透明。

Q169 投诉机制要做什么？

A: 渠道、时限、分级、复核、记录保存、定期复盘改进。

Q170 客户分类（零售/专业）怎么做？

A: 设认定标准、证明文件清单、适用保护差异与条款说明。

Q171 适当性/适配性何时需要？

A: 涉及投顾/组合管理/复杂产品分销时应建立问卷、评分、限制与记录留存。

Q172 误导性营销怎么防？

A: 营销合规审批流程 + Marketing Log + 禁用话术清单 + 留档。

Q173 能否提供杠杆/衍生品？

A: 需另行评估是否落入其他金融监管框架；不能默认纳入 MiCA CASP 范围。

Q174 客户资金（法币）由谁承接？

A: 若无 EMI/PI，通常通过银行/支付机构合作；责任边界需在合同与流程中写清。

Q175 退款/赎回机制要写吗？

A: 要：触发条件、时限、费用、AML 复核、异常冻结与申诉路径。

Q176 错误转账如何处理？

A: 工单化、链上追踪、对手方联系流程、风险披露、争议解决与赔付边界。

Q177 账户被盗怎么办？

A: 异常登录监控、冻结、取证、通知、重置、赔付规则与复盘整改。

Q178 客户死亡/继承怎么办？

A: 法律文件要求、身份核验、资产冻结与转移流程、合规审批留痕。

Q179 客户数据删除请求怎么处理？

A: AML 留存义务优先；在法定留存期内不得删除，期满后按流程安全销毁。

Q180 GDPR 文件必须有哪些？

A: 隐私政策、DPA、数据主体权利流程、跨境传输评估（如适用）。

Q181 利益冲突典型场景有哪些？

A: 做市、返佣、关联方服务费、内部自营账户交易、上市利益安排等。

Q182 如何披露利益冲突？

A: 在条款与披露文件中说明来源、影响、缓释措施与客户选择权。

Q183 客户资产被盗是否必须赔付？

A：取决于条款与保险/保障安排，但监管会看你是否明确赔付政策与处置机制。

Q184 是否建议购买保险？

A：建议纳入审慎保障方案（尤其托管/平台/兑换场景），并解释承保范围与索赔机制。

Q185 客户支持 SLA 要写吗？

A：要，投诉与客服是监管抽查重点，需可量化时限与升级路径。

Q186 客户教育要做吗？

A：建议做（风险提示、常见骗局、资产安全提示），对降低投诉与欺诈有直接帮助。

Q187 账户冻结是否要通知客户？

A：一般要，但在 AML/执法情形可能受限制；制度中需明确例外规则与留痕。

Q188 是否要设置交易限额？

A：建议按风险分层设置（新客、未完成增强尽调、高风险地址等）。

Q189 如何处理跨境客户的消费者保护差异？

A：采用“最低共同保护标准 + 目标国特定补充条款”的策略，并建立国家矩阵。

Q190 可以用仲裁条款吗？

A：可用，但需符合消费者保护与适用法律要求；建议律师审阅。

Q191 客户资产对账多久一次？

A：建议至少日对账（核心业务），并保留差异处理记录。

Q192 客户资产隔离如何证明？

A：账户结构说明、钱包分层、内部账务设计、对账报表与审计轨迹。

Q193 上市/上新资产要审批吗？

A：要：Listing 评估机制、风险评估、冲突披露与记录留存。

Q194 广告能写“受监管/持牌”吗？

A：仅在事实成立且表述准确时可写；建议合规审核并保留审批记录。

Q195 最常见投诉来源是什么？

A：费用不透明、提现延迟、账户冻结解释不足、误转纠纷、诈骗与账户接管。

Q196 如何降低投诉？

A：透明披露+客服 SLA+工单闭环+定期复盘改进+客户教育。

Q197 客户条款版本更新怎么管？

A：版本控制、变更摘要、客户通知、必要时重新同意、留档。

Q198 客户资产与公司资产混同会怎样？

A：重大合规红线，极易触发监管整改与声誉风险。

Q199 申请失败最常见原因？

A：SoF/SoW 不闭环、关键岗位不匹配、AML 与系统脱节、ICT/外包不可审计、客户保护不足。

Q200 仁港永胜对“通过率”的核心建议？

A：用“可审计、可证据化、可解释”的结构做全套材料与系统闭环，并建立补件战情室快速应答。

15) 我司服务建议与配套说明（交付包/流程/沟通节奏）

仁港永胜建议采用“三条线并行”：合规制度线 + 技术证据线 + 监管沟通线。

- **制度线**：把 MiCA 条款拆成可审计制度（AML/冲突/投诉/适当性/外包/记录保存等）。
- **技术线**：把钱包/权限/日志/BCP/DR/安全测试做成证据包（图+报告+演练记录）。
- **沟通线**：Pre-app 的 deck、Q&A pack、RFI 应答机制与版本控制。

15.1 我们的交付理念：一次性把 MiCA + AML + DORA 做成“可运行系统”

你要拿牌，不是“写材料比赛”，而是把 **制度、系统、外包、人员、证据链** 一次性打通，减少后期整改成本（尤其 DORA 生效后）。

15.2 交付包（Deliverables）—你可直接复制到报价书

A. 申请主文件包（可提交版）

- Programme of Operations（服务范围、客户旅程、跨境模式、外包与控制）
- Business Plan（含 3 年预测、成本结构、压力测试、审慎保障逻辑）
- 组织治理包：Board Charter、DoA 授权矩阵、三道防线、委员会机制、会议纪要模板
- 股东/UBO/资金来源包：SoW/SoF、资金路径图、负面信息解释备忘录、持续通知机制

- Fit & Proper 包：董事/高管/关键人员 CV（监管版）、声明、时间投入、冲突管理、Skill Matrix

B. AML/CFT 运行体系包

- AML 手册（CDD/EDD/制裁/PEP/监控/STR/留存/培训/独立审查）
- 风险评估方法论 + Risk Register + 规则库框架
- STR 决策树 + 工单模板 + “不报送原因”留痕模板

C. ICT/DORA 对齐包

- ICT 风险管理框架（DORA 化）
- 钱包安全说明（冷热钱包、多签、HSM、签名仪式、对账、灾备）
- 外包治理制度 + 供应商尽调清单 + SLA/审计权/退出条款库
- DR 演练脚本 + 事件响应手册 + 渗透测试整改闭环模板

D. 客户保护与对外文本包

- 客户协议（T&C）、风险披露、费用披露、投诉机制与 SLA
- 营销合规审批流程 + 禁用话术清单 + Marketing Log

E. 监管沟通与补件应答包

- Pre-app 沟通材料（Gap Assessment + 里程碑计划）
- RFI/Q&A Log（问题追踪表）+ 补件 Cover Letter 模板
- 面谈题库与答题稿（业务/AML/ICT/外包/客户保护/股东六大模块）

15.3 项目流程与沟通节奏（你团队好落地）

- **每周例会**：项目经理 + 合规 + 技术 + 运营（60–90 分钟）
- **战情室机制**（RFI/补件期）：48 小时内出应答草案，72 小时内出可提交版
- **版本控制**：所有文件采用编号与变更记录（监管最吃这一套）

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

- MiCA 本身对 CASP 的组织、治理、客户保护与运营提出系统性要求。
- 卢森堡 AML/CFT：VASP 时代 CSSF 监督主要聚焦 AML/CFT；CASP 授权后 AML/CFT 仍是底层核心（并叠加 MiCA 的更广监管要求）。
- CSSF 通函/指引：CSSF 已发布与 MiCA 相关的通函（例如采用 EBA/ESMA 指引等），实务应纳入合规框架并在申请材料中引用。

16.1 卢森堡监管结构（你可写进“监管章节”）

- **MiCA/CASP**：CSSF 负责授权、持续监管、跨境护照通报安排与相关指引。
- **VASP（AML 注册）体系**：CSSF 侧重 AML/CFT 监督与执法。

16.2 AML 合规模块（卢森堡重点：VASP 体系与 AML/CFT 监督）

- 在卢森堡提供虚拟资产服务通常触发 CSSF 的 VASP 注册与 AML/CFT 监督安排（具体服务类型见 CSSF VASP 注册页面）。
- 你在 MiCA 时代的策略通常是：**MiCA 授权（CASP）主线 + AML/CFT 真实运行主线** 同时构建，避免“只拿牌不运行”的监管风险。

16.3 护照机制与通报（你可直接作为“跨境扩张章”）

CSSF 明确：在卢森堡获授权的 CASP，可在完成通报程序后向其他成员国/EEA 提供服务（设分支或自由提供服务）。

16.4 DORA 报送与外包登记册（卢森堡非常实操）

CSSF 对 DORA 生效后的报送与程序（如外包登记册提交窗口与参考日期）有明确说明与时间安排，你在落地时必须把“登记册字段、数据来源、维护责任”做成可运行机制。

17) 税务与法律配套（CIT/VAT/预提税/雇佣/架构建议）

以下为“项目筹划层面”的关键税务参数（以最终适用与个案为准，需税务师落地）。

17.1 企业所得税（CIT）

- 2025 年起，卢森堡公司所得税标准税率出现从 17% 下调至 16% 的更新，并影响卢森堡市等地综合税负（叠加 municipal business tax 等）。

17.2 增值税（VAT）

- 卢森堡标准 VAT 税率为 17%（2023 年曾临时降至 16%，2024 起恢复 17% 的口径在多方资料中一致）。

17.3 雇佣与用工（简要）

- 关键岗位在卢森堡配置通常涉及：劳动合同、薪酬税务、社保、可能的外派安排与工时/保密/竞业条款。
- 建议：对合规/MLRO/CISO 等关键岗设置“监管面谈可解释”的职责、权限与独立性条款。

17.4 架构建议（CASP 常见）

- 常见：Lux OpCo（持牌）+ 集团控股（EU/非 EU）+ 技术服务公司（可在集团内但需外包合规化）
- 重点：把“关键控制”留在持牌主体（或至少可被持牌主体有效控制与审计）。

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

- **ESMA/EBA Level 2/3**：MiCA 的 RTS/ITS 在 2024–2025 持续落地（CSSF 页面持续更新清单），意味着申请材料与持续合规要“动态对齐”。
- **AMLA（欧盟反洗钱管理局）**：未来 AML 监管趋向更集中、更一致，CASP 的 AML 体系会被持续加压（尤其链上风控与制裁执行）。
- **DAC8（加密资产税务信息交换）**：对加密资产服务提供商的数据、客户识别与报送能力提出更高要求（建议提前把数据模型与报送口径纳入 IT 方案）。

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

阶段一：Preparation（把“可批”做出来）

- 先完成：治理架构、关键岗位到位、钱包与权限、客户资产隔离与对账、外包合同包、AML 与监控工具选型。

阶段二：Application（把“证据”交上去）

- 用 RTS/ITS 的结构来组织材料（对照表 + 证据索引）。
- RFI 用“答复模板”统一口径：结论 → 依据 → 证据 → 附件编号 → 变更记录。

阶段三：Post-Licence（把“持续合规”跑起来）

- 报告日历、审计计划、演练计划、供应商 KPI、投诉与冲突台账、重大事件通报机制。

20) 我司可提供的配套文件清单（BP、AML、Risk Register、Q&A pack、图表等）

A | 申请文件包（可直接递交级）

- 业务说明书（MiCA 服务映射）+ 三年 BP 财务模型（Excel）
- 治理与三道防线文件包（Charter/DoA/委员会章程）
- 股东/UBO 尽调包（SOF/SOW 模板 + 穿透图 + 声誉问卷）

B | 合规制度包（Word）

- AML/KYC 手册（含链上监测、Travel Rule、制裁、STR）
- 投诉处理、冲突管理、客户资产隔离、适当性/适配性（如适用）
- 外包管理制度（含关键外包评估与退出计划）

C | ICT/安全证据包（Visio/Word）

- 冷热钱包与多签示意图、权限分层图、数据流图

- 渗透测试/漏洞管理/事件响应/BCP-DR 演练模板
- 供应商尽调与 SLA 模板（审计权/监管访问权/分包链条款）

D | 监管沟通包（可背诵/可面谈）

- Pre-app deck（英文）+ Q&A pack（50/100/200 题可选）
- RFI 应答模板（版本控制、附件索引、证据矩阵）

21) 唐生结论：卢森堡在 MiCA 版图中的定位

卢森堡的定位非常明确：以 **CSSF** 为核心的“**制度化监管 + 金融生态兼容**”路径，适合：

- 想要在欧盟长期经营、对银行/审计/机构合作有要求的交易/托管/经纪平台；
 - 以及集团已有传统牌照、希望通过 Article 60 通知或集团协同降低合规摩擦的项目。
- 同时，存量 VASP 过渡窗口至 2026/07/01，为“迁移上岸”提供了确定性的排期基础。

一句话定位：

卢森堡不是“最低门槛套利地”，而是更适合走 **机构化、可审计、可对接银行与基金生态** 的 MiCA 合规路线（尤其适配：托管、机构经纪/执行、B2B 服务、与基金/家办/机构客户协同的业务模型）。

21.1 卢森堡的“结构性优势”

1. **金融中心底盘**：对接机构客户（基金、家办、跨境集团）时，“治理与审计化”路径更容易被接受。
2. **监管沟通方式偏“文件化+证据化”**：CSSF 明确鼓励尽早预沟通，项目管理空间更大。
3. **过渡期长度（18 个月）**：对既有主体提供相对更充足的迁移窗口（但不代表可以拖，补件与系统仍是硬仗）。
4. **DORA 时代的“先建强再扩张”**：2025-01-17 起 DORA 直接适用，卢森堡路线更适合一次性把 ICT/外包做强，后续护照扩张成本更低。

21.2 卢森堡路线的“成功关键因子”（也是监管审查主轴）

- **股东/UBO 资金来源闭环**（SoW/SoF + Money Trail Map）
- **关键岗位真实可履职**（合规/MLRO/ICT 风险 owner）
- **ICT/外包 DORA 化可审计**（登记册、审计权、退出预案、演练证据）
- **客户保护与披露透明**（费用、条款、投诉、资产隔离、对账）
- **补件战情室能力**（速度与质量决定周期与通过率）

21.3 唐生建议（最落地的三句话）

1. **先定服务范围，再定系统与制度深度**：Programme of Operations 是一切文件的“母文档”。
2. **DORA 直接按最高标准建**：越早标准化，后续越少整改。
3. **把 AML 做成“可运行的证据链”**：STR 决策、监控工单、培训与独立审查必须跑得起来。

22) 项目执行计划与甘特图（里程碑）

下面给“文字版甘特图”；如需 **Excel/Visio 甘特图** 我司可交付。

- W1-W2：服务范围映射 + 立项 + 差距评估
- W3-W6：治理/人员到位（合规/MLRO/ICT）+ 外包方案定稿
- W5-W10：制度编制（AML/冲突/投诉/隔离/外包/记录保存）
- W6-W12：系统与安全证据包（钱包/权限/日志/BCP/DR/测试）
- W9-W14：Pre-Application deck + Q&A pack + CSSF 预沟通
- W15：递交申请（含表格与声明）
- W16+：Completeness / RFI / 面谈 / 修订迭代
- 获批后 4-8 周：上线演练 + 护照扩张通知 + 首期报告准备

23) 监管审查重点矩阵（资本/适任性/AML/ICT/客户保护/护照）

模块	监管会看什么	常见被追问题	我司建议的“证据形态”
资本/审慎	资本金、费用覆盖、保险/保障	资金到位来源、压力情景	资本证明+模型+压力测试
适任性	董事/高管/关键岗位资历与独立性	MLRO 是否名义、三道防线是否可运作	CV+职责说明+汇报线图
AML/CFT	KYC/EDD、链上监测、制裁、STR	Travel Rule、可疑交易阈值与案例	AML 手册+规则库+案例
ICT/安全	钱包与密钥、权限、日志、测试、DR	多签治理、外包可审计性	架构图+测试报告+演练记录
客户保护	隔离、披露、投诉、冲突	自营/做市冲突、费用透明度	协议条款+披露样例+台账
护照/跨境	获客、广告、第三国边界	反向招揽滥用、KOL 管理	营销手册+审批留痕

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

24.1 结论与行动建议（最关键三句话）

- 卢森堡 CASP 申请应以 CSSF 的 CASP 专区与 EU RTS/ITS 为“材料结构主轴”，先做 Pre-Application 再递交，可显著减少 RFI 轮次。
- 通过的核心不是“写制度”，而是“制度+系统证据+治理独立性”三位一体：钱包/权限/隔离/外包合同包必须可审计。
- 若贵司为存量 VASP（2024/12/30 前已注册），务必利用过渡期窗口（至 2026/07/01）完成迁移排期与资金、人员、系统改造。

24.2 申请建议（仁港永胜方法论）

- 先做“可批最小集（MVA：Minimum Viable Authorisation）”：把关键岗位、关键控制、关键证据先固化；
- 用“RFI 应答工厂”管理补件：统一模板、证据索引、版本控制；
- 护照扩张不要一口吃成胖子：先 1-3 个目标国试点，把营销合规与客服/投诉闭环跑通，再规模化。

24.3 为何选择仁港永胜（优势）

- 模板体系成熟：MiCA/CASP 全套制度与证据包可直接落地（BP、AML、风险登记、外包合同包、Q&A Pack、图表）。
- 监管沟通能力：我们以“条款对照 + 证据索引 + 可背诵题库”方式准备 Pre-app 与面谈，降低反复补件。
- 跨境结构经验：擅长集团多牌照协同（EMI/PI/基金管理/投行等）与 MiCA 服务边界设计，避免“越界经营”风险。

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）、以及持续合规维护**等领域。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）

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。

免责声明

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。本文所载内容仅供一般信息与项目沟通之用，不构成法律、税务、审计或投资建议。具体监管要求、申请材料口径、费用及审查尺度以欧盟 MiCA 正式文本、ESMA/EBA 技术标准及卢森堡主管机关Commission de Surveillance du Secteur Financier（CSSF）最新公布为准。仁港永胜保留对本文内容进行更新与修订的权利。如需针对贵司业务模式提供可落地的合规方案、文件编制与申请支持，请联系仁港永胜获取专业协助。

© 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。